Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Προηγμένες Τεχνικές Κρυπτογράφησης για Ενίσχυση Ιδιωτικότητας

Παναγιώτης Μαχιάς

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Νοέμβριος 2022

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Προηγμένες Τεχνικές Κρυπτογράφησης για Ενίσχυση Ιδιωτικότητας

Παναγιώτης Μαχιάς

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Νοέμβριος 2022

Περίληψη

Η κρυπτογραφία διαδραματίζει στη σύγχρονη ψηφιακή εποχή ζωτικό ρόλο για την εξασφάλιση της ασφαλούς επικοινωνίας μεταξύ πολλαπλών οντοτήτων, παρέχοντας υπηρεσίες εμπιστευτικότητας των δεδομένων, ακεραιότητας και αυθεντικοποίησης. Ως εκ τούτου, καλύπτει μεταξύ άλλων και νομικές απαιτήσεις αναφορικά με την προστασία και ασφάλεια δεδομένων, αφού σε πολλά νομικά κείμενα προκρίνεται η χρήση της για την εξασφάλιση των ανωτέρω σκοπών. Οι σύγχρονες προκλήσεις έχουν ενεργοποιήσει ήδη μία συνεχή έρευνα για την ανάπτυξη μίας επόμενης γενιάς αλγορίθμων κρυπτογράφησης που επίσης αναλύονται σε αυτή την εργασία.

Ωστόσο, πέραν της ασφάλειας, πολύ σημαντικό ρόλο παίζει επίσης η κρυπτογραφία στην ενίσχυση της ιδιωτικότητας(Privacy Enhanced Cryptography). Πράγματι, υπάρχουν προηγμένες κρυπτογραφικές τεχνικές, η αξιοπιστία των οποίων έχει θεμελιωθεί από μαθηματική άποψη, οι οποίες μπορούν να δώσουν λύσεις σε ζητήματα που αποτυγχάνει η κλασική κρυπτογραφία. Τέτοιες προηγμένες τεχνικές κρυπτογράφησης είναι για παράδειγμα η Κρυπτογράφηση με Δυνατότητα Αναζήτησης (searchable encryption), η Συμμετρική Κρυπτογράφηση που διατηρεί τη διάταξη (order -preserving encryption), και η Ομομορφική Κρυπτογράφηση (homomorphic encryption).Οι εν λόγω τεχνικές επιτρέπουν την πραγματοποίηση υπολογισμών επί κρυπτογραφημένων δεδομένων, χωρίς να χρειάζονται το κλειδί αποκρυπτογράφησης (και χωρίς να έχουν πρόσβαση στα αρχικά δεδομένα).

Η παρούσα εργασία εστιάζει ιδίως στις προηγμένες τεχνικές κρυπτογράφησης για ενίσχυση της ιδιωτικότητας, οι οποίες θα μπορούσαν να αξιοποιηθούν για αντιμετώπιση προκλήσεων που απορρέουν και από συναφείς νομικές απαιτήσεις, όπως αυτές που θέτει ο Γενικός Κανονισμός Προσωπικών Δεδομένων. Πραγματοποιείται μία επισκόπηση και αποτύπωση των πιο γνωστών τέτοιων τεχνικών, προκειμένου να διαφανούν τα πλεονεκτήματά τους και οι εφαρμογές που μπορούν να έχουν. Ακολούθως, ως μελέτη περίπτωσης, εστιάζει σε ένα πρακτικό παράδειγμα μελετώντας ένα συγκεκριμένο εργαλείο λογισμικού που υλοποιεί τέτοιες προσεγγίσεις, το λεγόμενο Crypt-DB για κρυπτογράφηση βάσεων δεδομένων. Τα πειράματα καταδεικνύουν ότι πράγματι τέτοιες λύσεις είναι ρεαλιστικό να εφαρμοστούν, παρέχοντας συγκεκριμένες υπηρεσίες ασφαλείας οι οποίες δεν παρέχονται με συμβατικές μεθόδους, με κόστος – ως αναμενόταν – τη συνολική απόδοση, η οποία όμως πρέπει κάθε φορά να αξιολογείται στο πλαίσιο της διαχείρισης των κινδύνων που καλείται ένας οργανισμός να αντιμετωπίσει.

Summary

In the modern digital era, cryptography plays a vital role in ensuring secure communication between multiple entities, by providing data confidentiality, integrity and authentication services. Therefore, it also meets legal requirements with regard to data protection and security, since its use is provided for in many legal documents, so as to ensure that the above purposes are achieved. Current challenges have already triggered an ongoing research aimed at developing a next generation of encryption algorithms which are also analyzed in this paper.

However, apart from serving security purposes, cryptography plays a very important role also in enhancing privacy (Privacy Enhanced Cryptography). Indeed, there are advanced encryption techniques, such as searchable encryption, order-preserving encryption and homomorphic encryption, whose security properties have been mathematically established and which can provide solutions to issues that cannot be solved by classic cryptography. These techniques allow calculations over encrypted data, without needing the decryption key (and without having access to the original data).

This paper focuses in particular on advanced encryption techniques aimed at enhancing privacy, which could be also used to address challenges arising from relevant legal requirements, such as those set by the General Data Protection Regulation. An overview and description of the most known such techniques is carried out in order to show their advantages and their possible applications. Subsequently, as a case study, the paper focuses on a practical example by studying a particular software tool that implements such approaches, the so-called Crypt-DB for database encryption. Experiments demonstrate that it is, indeed, feasible to implement such solutions, providing specific security services which are not provided by conventional methods; as expected, this comes along with the expense of the overall performance, which, however, must be assessed each time in the framework of the risk management that an organization has to address.

Ευχαριστίες

Θερμές ευχαριστίες στον επιβλέποντα καθηγητή της παρούσας διατριβής κ. Κωνσταντίνο Λιμνιώτη για την άψογη συνεργασία, το ενδιαφέρον και την καθοριστική συμβολή του στην ολοκλήρωση του παρόντος πονήματος .

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Είναι πλέον γεγονός ότι με την άνθηση της ψηφιακής τεχνολογίας τα δεδομένα τα οποία αποθηκεύονται σε βάσεις δεδομένων ή/και ανταλλάσσονται μεταξύ δικτύων ολοένα και αυξάνονται (εφαρμογές και υποδομές υπολογιστικού νέφους, Διαδίκτυο των Πραγμάτων κ.α.). Αυτό με τη σειρά του έχει ως φυσικό επακόλουθο τις ολοένα αυξανόμενες απαιτήσεις για ασφάλεια των δεδομένων αλλά ταυτοχρόνως και προάσπισης της ιδιωτικότητας των χρηστών, ακριβώς γιατί και οι αντίστοιχοι κίνδυνοι αυξάνονται συνεχώς. Η έννοια της αποτίμησης διαχείρισης κινδύνων ασφαλείας (security risk assessment) έχει κατά μία έννοια διευρυνθεί στην έννοια της εκτίμησης αντικτύπου ως προς την προστασία προσωπικών δεδομένων (data protection impact assessment), η οποία μάλιστα στην Ευρωπαϊκή Ένωση υφίσταται πλέον ως νομική υποχρέωση, προκειμένου να καταδείξει ότι, όταν πρόκειται για μία επεξεργασία προσωπικών δεδομένων, χρειάζεται μία ολιστική προσέγγιση εξ αρχής προκειμένου να αντιμετωπιστούν κίνδυνοι όχι μόνο για την ασφάλεια των δεδομένων (δηλαδή τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητάς τους) αλλά και για την προστασία προσωπικών δεδομένων και της ιδιωτικότητας: για παράδειγμα, θα πρέπει επιπλέον να εξετάζονται αν τυχόν συλλέγονται περισσότερα προσωπικά δεδομένα από ό,τι χρειάζεται, αν τυχόν η συλλογή δεδομένων που πραγματοποιείται «επιτρέπει» τη χρήση τους για άλλους σκοπούς αδιαφανείς προς τους χρήστες κτλ [1] , [2].

Παραδοσιακά, η κρυπτογράφηση θεωρείται ως ένα κατ' εξοχήν μέσο επίτευξης στόχων ασφάλειας δεδομένων και πληροφοριών, όπως η εμπιστευτικότητα και η αυθεντικοποίηση τους. Ωστόσο, οι ανωτέρω αναφερόμενες απαιτήσεις για προάσπιση και της ιδιωτικότητας (η οποία εμπεριέχει την έννοια της εμπιστευτικότητας των προσωπικών δεδομένων αλλά, κατ΄ουσίαν, είναι ευρύτερη) έχει οδηγήσει στο να αναπτυχθούν εξελιγμένες τεχνικές κρυπτογράφησης ούτως ώστε να καταπολεμηθεί όσο αυτό είναι δυνατόν η οποιαδήποτε παραβίαση ή τροποποίηση των δεδομένων αυτών, αλλά και να υλοποιηθούν και οι σχετικές νομικές απαιτήσεις. Για παράδειγμα, έχουν αναπτυχθεί διάφορα συστήματα όπως το Crypt-DB, το SPORC, το MONOMI κ.α [3], [4]τα οποία μπορούν να συνδυάσουν αυτές τις προηγμένες κρυπτογραφικές τεχνικές και να κρυπτογραφήσουν τα δεδομένα σε έναν Server έτσι ώστε να καλύπτονται ειδικότερες απαιτήσεις ασφάλειας και ιδιωτικότητας. Για παράδειγμα, τα δεδομένα που αποθηκεύονται από τους πελάτες στους ιστοτόπους των παρόχων υπηρεσιών πρέπει να προστατεύονται από διαρροές ασφαλείας. Ως εκ τούτου θα πρέπει οι ίδιοι οι πάροχοι υπηρεσιών να είναι σε θέση να παρέχουν κάποιο προηγμένο επίπεδο ασφάλειας στους κατόχους των δεδομένων για τη χρήση των προϊόντων τους. Γενικά η προσέγγισή των παρόχων υπηρεσιών επικεντρώνεται σε θεωρητικές αλλά και πρακτικές τεχνικές προκειμένου να αντιμετωπιστούν τα προαναφερθέντα προβλήματα απορρήτου. Αυτές οι τεχνικές βασίζονται στην εκτέλεση ερωτημάτων SQL σε κρυπτογραφημένα δεδομένα με πρωταρχικό στόχο την εκτέλεση όσο το δυνατόν περισσότερων από αυτά στον χώρο του διακομιστή (server) χωρίς να χρειάζεται να αποκρυπτογραφηθούν τα πραγματικά δεδομένα. Συνεπώς, στη παρούσα διατριβή θα ασχοληθούμε με προηγμένες τεχνικές κρυπτογραφίας, οι οποίες εκφεύγουν της παραδοσιακής της χρήσης για εμπιστευτικότητα των δεδομένων, αυθεντικοποίηση των χρηστών κτλ. και έρχονται να δώσουν λύσεις σε ζητήματα που ανακύπτουν από τις ειδικές απαιτήσεις προστασίας της ιδιωτικότητας. Η ιδιωτικότητα και η προστασία προσωπικών δεδομένων διέπονται από ένα αυστηρό νομικό πλαίσιο, η υλοποίηση του οποίου στην πράξη δεν αποτελεί πάντα μία εύκολη λύση.

1.1 Βασικά Ερευνητικά Ερωτήματα

Τα βασικά ερευνητικά ερωτήματα που προκύπτουν είναι τα παρακάτω:

- Ποια ζητήματα της νομοθεσίας για την προστασία προσωπικών δεδομένων μπορούν να επιλύσουν οι προηγμένες τεχνικές κρυπτογραφίας; Σε τι βαθμό έχουν ήδη εφαρμοστεί και ποιες είναι οι προοπτικές?

- Μπορεί ο συνδυασμός κάποιων από αυτών των τεχνικών να καταφέρει να πετύχει σημαντική ενίσχυση στην προστασία των προσωπικών δεδομένων?

- Πόσο αποτελεσματικές είναι αυτές οι τεχνικές, λαμβάνοντας υπόψη ότι σε επεξεργασίας προσωπικών δεδομένων με υψηλούς κινδύνους για τα δικαιώματα των προσώπων, η ασφάλεια και προστασία δεδομένων καθίσταται υψίστης σημασίας;

- Προγράμματα που υλοποιούν τέτοιες τεχνικές μπορούν να αξιοποιηθούν άμεσα από οργανισμούς; Σε τι βαθμό επηρεάζεται η απόδοση συνολικά;

1.2 Αναγκαιότητα και Σπουδαιότητα Έρευνας

Καθημερινά πλέον η τεχνολογία εξελίσσεται και έτσι χρησιμοποιώντας όλο και περισσότερο τη τεχνολογία τόσο περισσότερα προσωπικά μας δεδομένα βρίσκονται εκτεθειμένα στο διαδίκτυο. Το νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων θέτει ένα σύνολο απαιτήσεων, οι οποίες πολλές φορές φαίνεται ότι δεν μπορούν να ικανοποιηθούν απόλυτα γιατί εκλείπουν οι κατάλληλες τεχνολογίες. Ωστόσο, η αλήθεια είναι ότι υπάρχουν πολλές τεχνολογίες που μπορούν να δώσουν λύσεις σε προβλήματα που φαίνονται άλυτα. Για αυτό το λόγο κρίνεται αναγκαίο να υπάρξει ένας συστηματικός τρόπος μελέτης των προηγμένων τεχνικών κρυπτογράφησης που είναι προσανατολισμένες στην ιδιωτικότητα των χρηστών, έτσι ώστε να αποσαφηνιστούν τα πεδία εφαρμογής τους αλλά και οι τυχόν επεκτάσεις τους

1.3 Μεθοδολογία

Η μεθοδολογία που εφαρμόστηκε για την εκπόνηση της συγκεκριμένης μεταπτυχιακής διατριβής είναι η εξής:

- Βιβλιογραφική επισκόπηση κλασικών μεθόδων κρυπτογράφησης

- Έρευνα, καταγραφή και ανάλυση των προηγμένων τεχνικών κρυπτογράφησης που μπορούν να χρησιμοποιηθούν για προάσπιση της ιδιωτικότητας. Λεπτομερής αναφορά στα πλεονεκτήματα και στα μειονεκτήματά τους και αποτίμησή τους υπό το φώς του νομικού πλαισίου για την προστασία προσωπικών δεδομένων, οι βασικές πτυχές του οποίου επίσης μελετώνται..

- Πρακτική εφαρμογή, ως μελέτη περίπτωσης, κάποιων προηγμένων κρυπτογραφικών τεχνικών. Μελέτη τους σε συγκεκριμένο περιβάλλον (CryptDB) για την εξαγωγή αποτελεσμάτων ως προς την αποτελεσματικότητά τους. Ο λόγος που επελέγη το εν λόγω εργαλείο ως μελέτη περίπτωσης είναι ότι είναι ελεύθερα διαθέσιμο, έχει αναπτυχθεί από ερευνητές του Πανεπιστημίου MIT, έχει πολύ καλά θεμελιωμένες μαθηματικές ιδιότητες, ενώ η ασφάλειά του δεν έχει αμφισβητηθεί παρά το γεγονός ότι είναι γνωστό επί δέκα περίπου έτη.

1.4 Δομή της Διατριβής

Κεφάλαιο 2: Το δεύτερο κεφάλαιο παρουσιάζει μία επισκόπηση των κλασικών τεχνικών κρυπτογράφησης. Αναφέρει τα πλεονεκτήματα και τα μειονεκτήματα τους και γίνεται αναφορά στο πώς μπορούν να εξελιχθούν μακροπρόθεσμα.

Κεφάλαιο 3:Το τρίτο κατά σειρά κεφάλαιο της συγκεκριμένης μεταπτυχιακής διατριβής εστιάζει στη παρουσίαση του νομικού πλαισίου που υφίσταται για την προστασία των προσωπικών δεδομένων.

Κεφάλαιο 4:Το συγκεκριμένο κεφάλαιο αναφέρεται στις προηγμένες τεχνικές κρυπτογράφησης που έχουν στόχο την περαιτέρω ενίσχυση της ασφάλειας των προσωπικών δεδομένων.

Κεφάλαιο 5: Το κεφάλαιο αυτό παρουσιάζει μία μελέτη περίπτωσης, το εργαλείο Crypt-DB. Ειδικότερα, περιγράφει την εγκατάσταση του προγράμματος Crypt-Db σε λειτουργικό σύστημα Linux(Ubuntu), τα προβλήματα που ανέκυψαν κατά την εγκατάστασή του, καθώς και την εκτέλεση ερευνητικού πειράματος που παρουσιάζει την αποτελεσματικότητα αλλά και την απόδοση του συγκεκριμένου προγράμματος.

Κεφάλαιο 6: Τέλος, στο συγκεκριμένο κεφάλαιο παρουσιάζεται μια συνοπτική ανάλυση των αποτελεσμάτων του πειράματος του πέμπτου κεφαλαίου και τα συμπεράσματα που προκύπτουν.

Κεφάλαιο 2
Κλασική Κρυπτογραφία

Η κρυπτογραφία έχει τέσσερις κύριους στόχους: εμπιστευτικότητα, ακεραιότητα, ταυτοποίηση και μη αμφισβήτηση(non-repudiation). Με άλλα λόγια, οι στόχοι είναι η προστασία της εμπιστευτικότητας των δεδομένων (εμπιστευτική μεταχείριση), η αυθεντικότητα των δεδομένων (επαληθευμένη πηγή) και η ακεραιότητα των δεδομένων (πρωτότυπο και αμετάβλητο μήνυμα). Η μη αμφισβήτηση αναφέρεται στο συνδυασμό καθενός από αυτά τα τρία πράγματα για την απόδειξη της αδιαμφισβήτητης εγκυρότητας του μηνύματος ή των δεδομένων. Ένα παράδειγμα μη-αμφισβήτησης σε χρήση είναι μια υπηρεσία που χρησιμοποιείται για την πιστοποίηση της γνησιότητας ψηφιακών υπογραφών και για να διασφαλιστεί ότι ένα άτομο δεν μπορεί να αρνηθεί ότι έχει υπογράψει ένα έγγραφο (δηλαδή η υπογραφή του είναι αδιαμφισβήτητη) [4].

Υπάρχουν, γενικά, δύο τύποι κρυπτογραφικών σχημάτων που συνήθως χρησιμοποιούνται για την επίτευξη των στόχων της κρυπτογραφίας και βάσει αυτών ορίζεται ο όρος της κλασική κρυπτογραφίας. Αυτά τα δύο κρυπτογραφικά σχήματα είναι η κρυπτογραφία μυστικού κλειδιού (ή συμμετρική ή συμβατική) και η κρυπτογραφία δημόσιου κλειδιού (ή ασύμμετρη)

κρυπτογραφία. Στην κρυπτογραφία συμμετρικού κλειδιού, χρησιμοποιείται ένας αλγόριθμος για την κρυπτογράφηση των μηνυμάτων με τη χρήση ενός μυστικού κλειδιού με τέτοιο τρόπο ώστε να καθίσταται άχρηστο σε όλους εκτός από αυτούς που έχουν πρόσβαση σε αυτό το μυστικό κλειδί [5].

Στην κρυπτογραφία δημόσιου κλειδιού[6], οι αλγόριθμοι χρησιμοποιούν δύο διαφορετικά κλειδιά: ένα ιδιωτικό κλειδί και ένα δημόσιο. Ένα μήνυμα που κρυπτογραφείται με ένα ιδιωτικό κλειδί μπορεί να αποκρυπτογραφηθεί με το δημόσιο κλειδί (και αντίστροφα). Ο ιδιοκτήτης του ζεύγους κλειδιών κατέχει το ιδιωτικό κλειδί και μπορεί να διανέμει το δημόσιο κλειδί σε οποιονδήποτε. Κάποιος που θέλει να στείλει ένα μυστικό μήνυμα χρησιμοποιεί το δημόσιο κλειδί του προοριζόμενου παραλήπτη για να το κρυπτογραφήσει. Μόνο ο παραλήπτης που κατέχει το ιδιωτικό κλειδί μπορεί να το αποκρυπτογραφήσει.

Τα δύο βασικά δομικά στοιχεία της πλειοψηφίας των τεχνικών συμμετρικής κρυπτογράφησης είναι η αντικατάσταση και η μετατόπιση. Μια τεχνική αντικατάστασης είναι αυτή στην οποία τα σύμβολα του αρχικού μηνύματος αντικαθίστανται με άλλα σύμβολα. Η τεχνική μετάθεσης είναι ένα διαφορετικό είδος αντιστοίχισης, όπου η αντιστοίχιση επιτυγχάνεται με την εκτέλεση κάποιου είδους αντιμετάθεσης του αρχικού μηνύματος– ουσιαστικά [7], η έξοδος σε έναν αλγόριθμο αντιμετάθεσης αποτελεί μία αναδιάταξη των στοιχείων της εισόδου του.

2.1 Κρυπτοσυστήματα Συμμετρικού Κλειδιού

Ένα συμμετρικό ή συμβατικό σύστημα κρυπτογράφησης έχει πέντε συστατικά [8].

- Απλό κείμενο/μήνυμα: Αυτό είναι το αρχικό κατανοητό μήνυμα ή τα δεδομένα που εισάγονται στον αλγόριθμο ως είσοδο.

- Αλγόριθμος κρυπτογράφησης: Ο αλγόριθμος κρυπτογράφησης εκτελεί διάφορες αντικαταστάσεις και μετασχηματισμούς στο απλό κείμενο.

- Μυστικό κλειδί: Το μυστικό κλειδί είναι επίσης η είσοδος στον αλγόριθμο κρυπτογράφησης. Το κλειδί είναι μια τιμή ανεξάρτητη από το απλό κείμενο. Ο αλγόριθμος θα παράγει διαφορετική έξοδο ανάλογα με το συγκεκριμένο κλειδί που χρησιμοποιείται εκείνη τη στιγμή. Οι ακριβείς αντικαταστάσεις και μετασχηματισμοί που εκτελούνται από τον αλγόριθμο εξαρτώνται από το κλειδί.

- Κρυπτογραφημένο κείμενο: Αυτό είναι το κρυπτογραφημένο μήνυμα που παράγεται ως έξοδος. Εξαρτάται από το κείμενο και το μυστικό κλειδί. Για ένα δεδομένο μήνυμα, δύο διαφορετικά κλειδιά θα παράγουν δύο διαφορετικά κρυπτογραφημένα κείμενα.

- Αλγόριθμος αποκρυπτογράφησης: Πρόκειται ουσιαστικά για τον αλγόριθμο κρυπτογράφησης που εκτελείται αντίστροφα. Παίρνει το κρυπτογραφημένο κείμενο και το μυστικό κλειδί και παράγει το αρχικό απλό κείμενο.

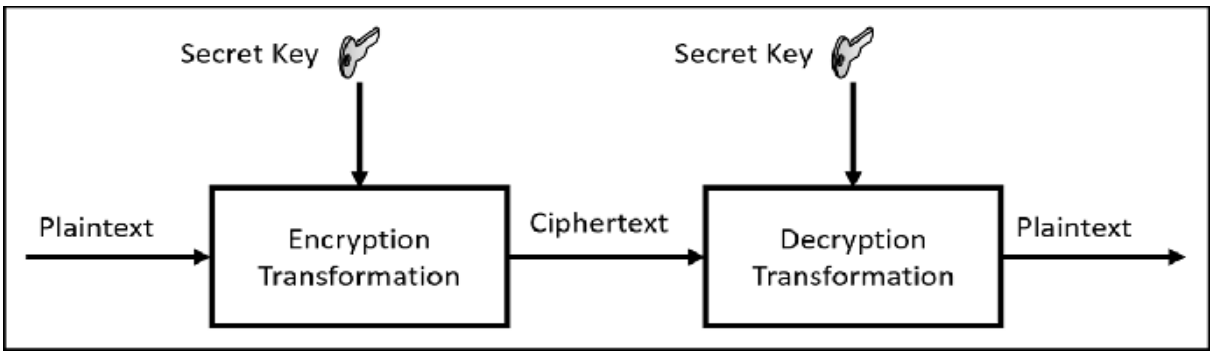
Υπάρχουν δύο απαιτήσεις για την ασφαλή χρήση συμμετρικού κλειδιού κρυπτογράφησης:

1. Ισχυρός αλγόριθμος κρυπτογράφησης: Κατ' ελάχιστο, ο αλγόριθμος πρέπει να είναι τέτοιος ώστε ένας αντίπαλος που γνωρίζει τον αλγόριθμο και έχει πρόσβαση σε ένα ή περισσότερα κρυπτογραφημένα κείμενα δεν θα είναι σε θέση να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο ή να βρει το κλειδί. Η απαίτηση αυτή διατυπώνεται συνήθως σε ισχυρότερη μορφή: Ο αντίπαλος δεν θα πρέπει να είναι σε θέση να αποκρυπτογραφήσει κρυπτογραφημένο κείμενο ή να ανακαλύψει το κλειδί ακόμη και αν έχει στην κατοχή του έναν αριθμό από κρυπτογραφημένα κείμενα μαζί με το απλό κείμενο που παρήγαγε κάθε κρυπτογραφημένο κείμενο.

2. Ο αποστολέας και ο παραλήπτης πρέπει να έχουν λάβει αντίγραφα του μυστικού κλειδιού με ασφαλές τρόπο και πρέπει να διατηρούν το κλειδί ασφαλές. Εάν κάποιος μπορεί να ανακαλύψει το κλειδί και γνωρίζει τον αλγόριθμο, όλες οι επικοινωνίες που χρησιμοποιούν αυτό το κλειδί είναι αναγνώσιμες.

2.1.1 Αρχές του Κρυπτοσυστήματος Συμμετρικού Κλειδιού

Στην κρυπτογραφία συμμετρικού κλειδιού, ένα μόνο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Όπως φαίνεται στο παρακάτω σχήμα (Εικόνα 2.1), ο αποστολέας χρησιμοποιεί το κλειδί (ή κάποιο σύνολο κανόνων) για να κρυπτογραφήσει το απλό κείμενο και να στείλει το κρυπτογραφημένο κείμενο στον παραλήπτη. Ο παραλήπτης εφαρμόζει το ίδιο κλειδί (ή σύνολο κανόνων) για την αποκρυπτογράφηση του μηνύματος και την ανάκτηση του απλού κειμένου. Επειδή ένα μόνο κλειδί χρησιμοποιείται και για τις δύο λειτουργίες, η κρυπτογραφία μυστικού κλειδιού ονομάζεται επίσης συμμετρική κρυπτογράφηση [9].



Εικόνα 2.1: Μοντέλο Κρυπτοσυστήματος συμμετρικού κλειδιού.

Με αυτή τη μορφή κρυπτογραφίας, είναι προφανές ότι το κλειδί πρέπει να είναι γνωστό και στους δύο, στον αποστολέα και στον παραλήπτη- και αυτό, στην πραγματικότητα, είναι το μυστικό. Η μεγαλύτερη δυσκολία με αυτή την προσέγγιση, φυσικά, είναι η ασφαλής διανομή του κλειδιού.

Τα συστήματα κρυπτογραφίας συμμετρικού κλειδιού κατηγοριοποιούνται γενικά ως εξής: κρυπτογράφηση ροής (streamcipher) ή κρυπτογράφηση μπλοκ (block),[11]. Το σύστημα κρυπτογράφησης ροής εφαρμόζει μια τεχνική κρυπτογράφησης που λειτουργεί byte προς byte για να μετατρέψει το απλό κείμενο σε κώδικα που δεν μπορεί να διαβαστεί από κανέναν χωρίς το κατάλληλο κλειδί. Οι κρυπτογραφήσεις ροής είναι γραμμικές (απλές δυαδικές προσθέσεις), οπότε το ίδιο κλειδί κρυπτογραφεί και αποκρυπτογραφεί μηνύματα. Οι κρυπταλγόριθμοι ροής βασίζονται σε:

- Απλό κείμενο. Ορίζεται το μήνυμα που πρέπει να κρυπτογραφηθεί.

- Κλειδοροή (key stream). Ένα σύνολο τυχαίων χαρακτήρων αντικαθιστά εκείνους του απλού κειμένου. Θα μπορούσαν να είναι αριθμοί, γράμματα ή σύμβολα.

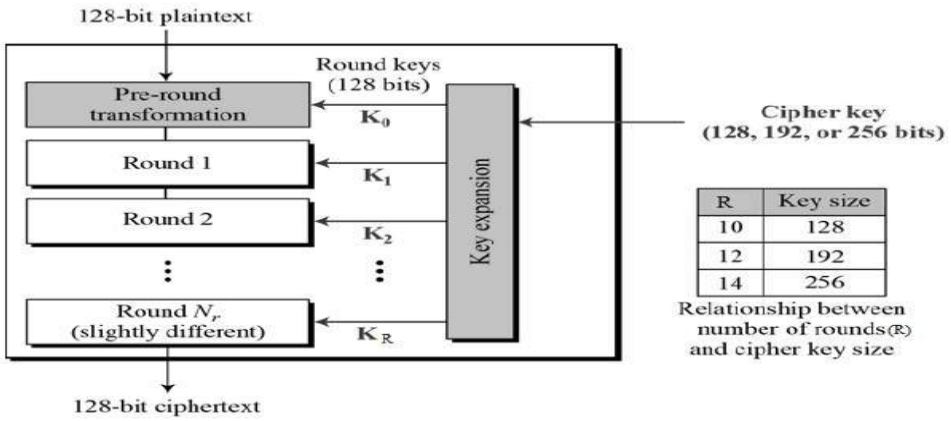
- Κρυπτογραφημένο κείμενο. Αυτό είναι το κωδικοποιημένο μήνυμα.

Η παραγωγή ενός κλειδιού είναι μια περίπλοκη μαθηματική διαδικασία. Τα bit του απλού κειμένου εισέρχονται στον αλγόριθμο και το κρυπτογράφημα επεξεργάζεται κάθε bit με τον μαθηματικό τύπο. Το κείμενο που προκύπτει είναι πλήρως κρυπτογραφημένο και ο παραλήπτης δεν μπορεί να το διαβάσει χωρίς το κατάλληλο κλειδί. Με το σωστό κλειδί, ο παραλήπτης μπορεί να ωθήσει το κρυπτογραφημένο κείμενο πίσω μέσω του κρυπτογράφου ροής και να μετατρέψει τα μετασχηματισμένα δεδομένα πίσω σε απλό κείμενο.

2.1.2 Κρυπταλγόριθμοι Τμήματος (block ciphers)

Οι κρυπτογραφικοί αλγόριθμοι τμήματος (blockciphers) επενεργούν σε τμήματα (blocks) του μηνύματος, αντί για bit-προς–bitή byte-προς –byte που λειτουργούν οι κρυπταλγόριθμοι ροής. Ειδικότερα, ένας κρυπταλγόριθμος τμήματος μπορεί να λειτουργήσει με έναν από διάφορους τρόπους- οι ακόλουθοι έξι είναι οι πιο σημαντικοί [12].

- Το Εξελιγμένο Πρότυπο Κρυπτογράφησης (Advanced Encryption Standard(AES)),αποτελεί την εξειδικευμένη εφαρμογή για την κρυπτογράφηση ηλεκτρονικών δεδομένων που καθιερώθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ το 2001 (Εικόνα 2.2). Το κλειδί του AES δύναται να είναι 128/192/256 bits. Το AES κρυπτογραφεί δεδομένα σε block των 128 bits/έκαστο. Αυτό σημαίνει ότι λαμβάνει 128 bit ως είσοδο και εξάγει 128 bit κρυπτογραφημένου κειμένου ως έξοδο. Το AES βασίζεται στην αρχή του δικτύου αντικατάστασης-μετάθεσης, που σημαίνει ότι εκτελείται χρησιμοποιώντας μία σειρά συνδεδεμένων λειτουργιών που περιλαμβάνει αντικατάσταση και ανακάτεμα των δεδομένων εισόδου.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

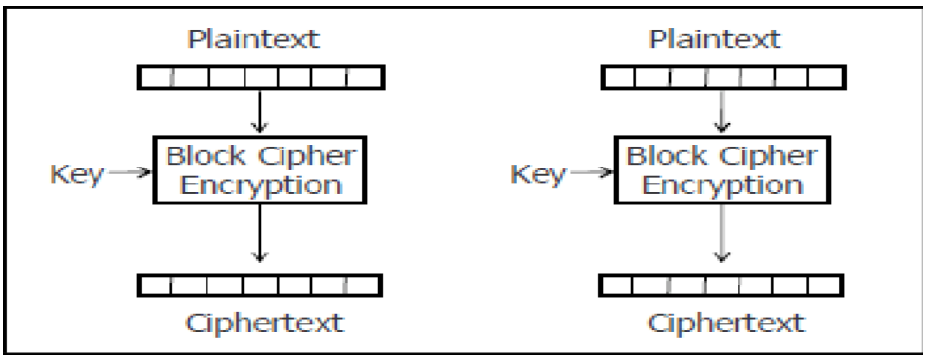
Εικόνα 2.2: Advanced Encryption Standard (AES).

- Το Ηλεκτρονικό κωδικοβιβλίο(Electronic Codebook (ECB))είναι η απλούστερη, πιο προφανής εφαρμογή: το μυστικό κλειδί χρησιμοποιείται για την κρυπτογράφηση του μπλοκ απλού κειμένου ώστε να σχηματιστεί ένα μπλοκ κρυπτογραφημένου κειμένου(Εικόνα 2.3). Δύο πανομοιότυπα μπλοκ απλού κειμένου, λοιπόν, θα δημιουργούν πάντα το ίδιο μπλοκ κρυπτογραφημένου κειμένου. Η τεχνική ECB είναι εύκολη στην υλοποίηση. Ωστόσο, αυτό είναι και το μεγαλύτερο μειονέκτημά της. Δύο όμοια μπλοκ

απλού κειμένου οδηγούν σε δύο αντίστοιχα όμοια μπλοκ κρυπτογραφημένου κειμένου, γεγονός που την καθιστά κρυπτογραφικά αδύναμη.

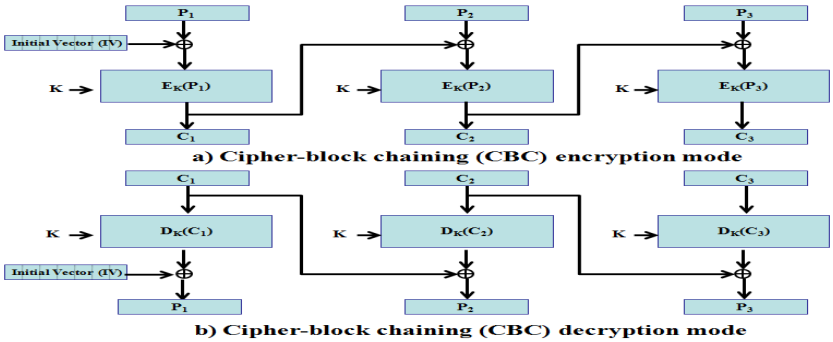
Η ECB δεν είναι καλό να χρησιμοποιείται με μικρά μεγέθη μπλοκ, για παράδειγμα για μπλοκ μικρότερα από 40 bit -- και πανομοιότυπους τρόπους κρυπτογράφησης. Σε μικρά μεγέθη μπλοκ ορισμένες λέξεις και φράσεις μπορεί να επαναχρησιμοποιούνται συχνά στο απλό κείμενο. Αυτό σημαίνει ότι το κρυπτογραφημένο κείμενο μπορεί να μεταφέρει (και να προδώσει) μοτίβα από το ίδιο απλό κείμενο και να προκύψουν τα ίδια επαναλαμβανόμενα τμήματα-μπλοκ του κρυπτογραφημένου κειμένου. Όταν τα μοτίβα του απλού κειμένου είναι προφανή, δημιουργούνται ευκαιρίες για κακόβουλους να μαντέψουν τα μοτίβα και να διαπράξουν μια επίθεση με κωδικοποιητή.

Η ασφάλεια του ECB είναι αδύναμη, αλλά μπορεί να βελτιωθεί με την προσθήκη τυχαίων σειρών από bits σε κάθε μπλοκ. Μεγαλύτερα μπλοκ (64-bit ή περισσότερα) πιθανόν να περιέχουν αρκετά μοναδικά χαρακτηριστικά (εντροπία) ώστε να καθιστούν απίθανη μια επίθεση τύπου code book (δηλαδή να δοθεί πρόσβαση σε μη κρυπτογραφημένα κείμενα σε ένα κακόβουλο).



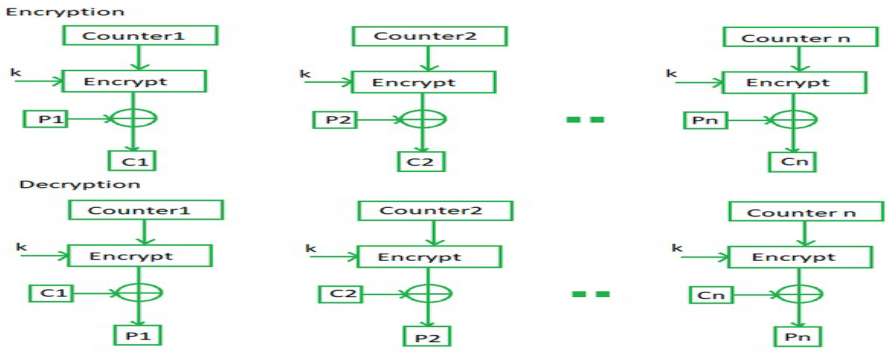
Εικόνα 2.3: Electronic Code Book (ECB)

- Ο Τρόπος Λειτουργίας Αλυσιδωτού Τμήματος (Cipher Block Chaining (CBC)),προσθέτει έναν μηχανισμό ανατροφοδότησης στην κρυπτογράφηση(Εικόνα 2.4). Στο CBC, το απλό κείμενο είναι αποκλειστικά OR (XOR) με το προηγούμενο μπλοκ κρυπτογραφημένου κειμένου πριν από την κρυπτογράφηση. Σε αυτή τη λειτουργία, δύο πανομοιότυπα μπλοκ απλού κειμένου δεν κρυπτογραφούνται ποτέ στο ίδιο κρυπτογραφημένο κείμενο.



Εικόνα 2.4: Cipher-block Chaining (CBC).

- Ο Τρόπος Λειτουργίας Μετρητή(Counter Mode(CTR)),είναι μια απλή υλοποίηση κρυπτογράφησης σε μπλοκ με βάση μετρητές(Εικόνα2.5). Κάθε φορά μια τιμή που ξεκινά από τον μετρητή κρυπτογραφείται και δίνεται ως είσοδος για XOR με το απλό κείμενο, το οποίο οδηγεί στο μπλοκ κρυπτογράφησης. Η λειτουργία CTR είναι ανεξάρτητη από τη χρήση ανατροφοδότησης και συνεπώς μπορεί να υλοποιηθεί παράλληλα. Δεδομένου ότι υπάρχει διαφορετική τιμή μετρητή για κάθε μπλοκ, αποφεύγεται η άμεση σχέση απλού κειμένου και κρυπτοκειμένου. Αυτό σημαίνει ότι το ίδιο απλό κείμενο μπορεί να αντιστοιχιστεί σε διαφορετικό κρυπτοκείμενο παράλληλη εκτέλεση της κρυπτογράφησης είναι δυνατή, καθώς οι έξοδοι από τα προηγούμενα στάδια δεν είναι αλυσιδωτές όπως στην περίπτωση της CBC.



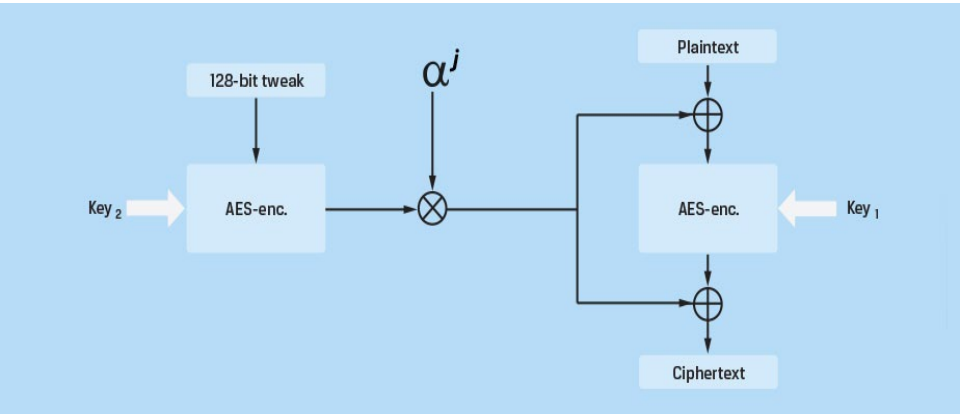
Εικόνα 2.5: Counter Mode (CTR).

- AES-XTS: Στο Εξελιγμένο Πρότυπο Κρυπτογράφησης Μορφής (Advanced Encryption Standard (AES)),ο NIST πρόσθεσε το XTSστον κατάλογο των τρόπων κρυπτογράφησης μπλοκ τύπου AES το 2010. Ο XTS είναι ο νεότερος τρόπος κρυπτογράφησης(Εικόνα 2.6). Σχεδιάστηκε ως ισχυρότερη εναλλακτική λύση σε σχέση με άλλους διαθέσιμους τρόπους

κρυπτογράφησης μπλοκ, όπως το CBC. Εξαλείφει τις πιθανές ευπάθειες που σχετίζονται με ορισμένες από τις πιο εξελιγμένες επιθέσεις πλευρικού καναλιού, οι οποίες θα μπορούσαν να χρησιμοποιηθούν για την εκμετάλλευση αδυναμιών άλλων τρόπων λειτουργίας.

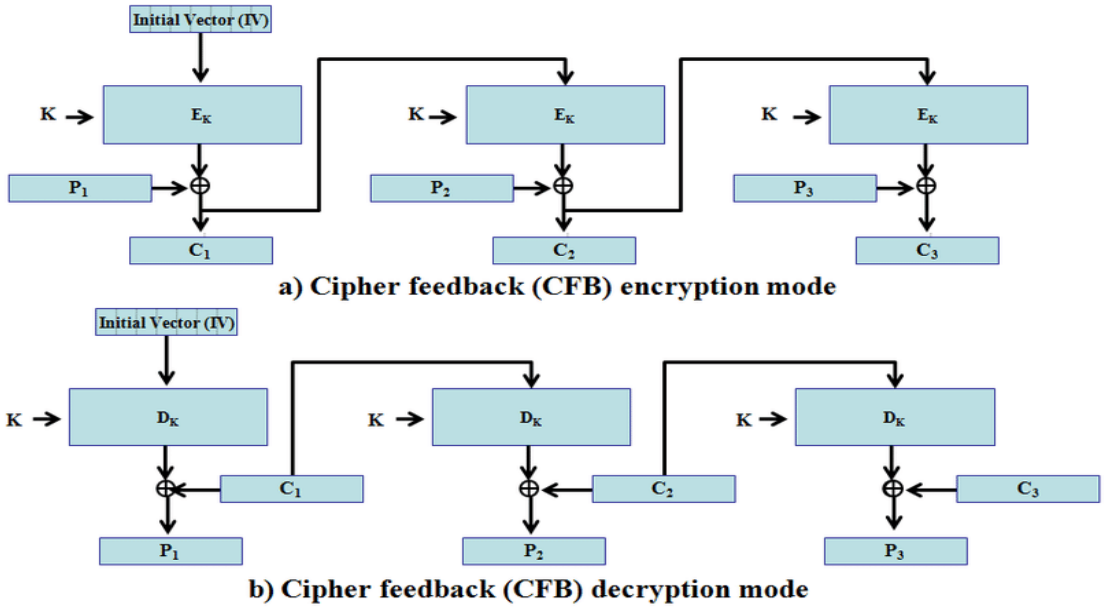
Ο XTS χρησιμοποιεί δύο κλειδιά AES. Το ένα κλειδί χρησιμοποιείται για την εκτέλεση της κρυπτογράφησης μπλοκ AES- το άλλο χρησιμοποιείται για την κρυπτογράφηση της λεγόμενης "τιμής τροποποίησης". Αυτή η κρυπτογραφημένη "tweak Value" τροποποιείται περαιτέρω με μια πολυωνυμική συνάρτηση Galois (GF) και γίνεται XOR τόσο με το απλό κείμενο όσο και με το κρυπτογραφημένο κείμενο κάθε μπλοκ. Η συνάρτηση GF παρέχει περαιτέρω διάχυση και διασφαλίζει ότι μπλοκ πανομοιότυπων δεδομένων δεν θα παράγουν πανομοιότυπο κρυπτογραφημένο κείμενο. Με τον τρόπο αυτό επιτυγχάνεται ο στόχος κάθε μπλοκ να παράγει μοναδικό κρυπτογραφημένο κείμενο με δεδομένο πανομοιότυπο απλό κείμενο χωρίς τη χρήση διανυσμάτων αρχικοποίησης και αλυσίδας.

Στην πραγματικότητα, το κείμενο είναι σχεδόν (αλλά όχι ακριβώς) διπλά κρυπτογραφημένο με τη χρήση δύο ανεξάρτητων κλειδιών. Η αποκρυπτογράφηση των δεδομένων επιτυγχάνεται με την αντιστροφή αυτής της διαδικασίας. Δεδομένου ότι κάθε μπλοκ είναι ανεξάρτητο και δεν υπάρχει αλυσιδωτή σύνδεση, εάν τα αποθηκευμένα κρυπτογραφημένα δεδομένα καταστραφούν και αλλοιωθούν, μόνο τα δεδομένα για το συγκεκριμένο μπλοκ δεν θα μπορούν να ανακτηθούν. Με τους τρόπους αλυσιδωτής λειτουργίας, τα σφάλματα αυτά μπορούν να μεταδοθούν σε άλλα μπλοκ κατά την αποκρυπτογράφηση.



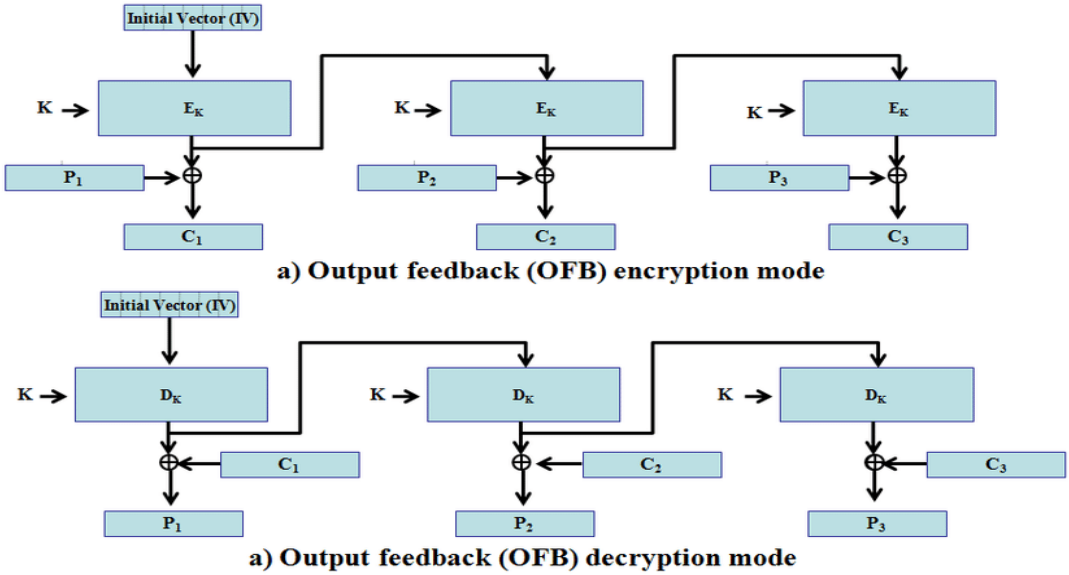
Εικόνα 2.6: AES-XTS.

- Ο Τρόπος Λειτουργίας Ανάδρασης Κρυπταλγορίθμου(Cipher Feedback (CFB)), είναι μια υλοποίηση κρυπτογράφησης μπλοκ ως σύστημα ροής που αυτοσυγχρονίζεται(Εικόνα 2.7). Η λειτουργία CFB επιτρέπει την κρυπτογράφηση δεδομένων σε μονάδες μικρότερες από το μέγεθος του μπλοκ, το οποίο μπορεί να είναι χρήσιμο σε ορισμένες εφαρμογές, όπως η κρυπτογράφηση της εισόδου δεδομένων από τερματικό. Στην περίπτωση της λειτουργίας CFB 1 byte, για παράδειγμα, κάθε εισερχόμενος χαρακτήρας τοποθετείται σε έναν καταχωρητή μετατόπισης ίδιου μεγέθους με το μπλοκ, κρυπτογραφείται και το μπλοκ μμεταδίδεται. Στην πλευρά λήψης, το κρυπτογραφημένο κείμενο αποκρυπτογραφείται και τα επιπλέον bits στο μπλοκ (δηλαδή, όλα όσα υπερβαίνουν το ένα byte) απορρίπτονται.



Εικόνα 2.7: Cipher-Feedback(CFB).

- Ο Τρόπος Λειτουργίας Ανάδρασης Εξόδου (Output Feedback(OFB)),είναι μια υλοποίηση κρυπτογράφησης μπλοκ εννοιολογικά παρόμοια με ένα σύγχρονο σύστημα κρυπτογράφησης ροής(Εικόνα 2.8) . Η OFB αποτρέπει το ίδιο μπλοκ απλού κειμένου από το να παράγει το ίδιο μπλοκ κρυπτογραφημένου κειμένου με τη χρήση ενός εσωτερικού μηχανισμού ανατροφοδότησης που είναι ανεξάρτητος τόσο από τις ροές bit του απλού κειμένου όσο και από τις ροές bit του κρυπτογραφημένου κειμένου.



Εικόνα 2.8: Output Feedback (OFB).

2.1.3 Κρυπταλγόριθμοι Ροών (Stream Ciphers)

Μία κρυπτογράφηση ροής κρυπτογραφεί μια συνεχή συμβολοσειρά δυαδικών ψηφίων εφαρμόζοντας μετασχηματισμούς που μεταβάλλονται χρονικά σε δεδομένα απλού κειμένου. Επομένως, αυτός ο τύπος κρυπτογράφησης λειτουργεί κομμάτι-κομμάτι, χρησιμοποιώντας ροές κλειδιών για τη δημιουργία κρυπτογραφημένου κειμένου για αυθαίρετα μήκη απλών μηνυμάτων κειμένου. Ο κρυπταλγόριθμος συνδυάζει ένα κλειδί (128/256 bit) και ένα ψηφίο nonce (64-128 bit) για να παράγει τη ροή κλειδιών — και έναν ψευδοτυχαίο αριθμό XOR με το απλό κείμενο για την παραγωγή κρυπτογραφημένου κειμένου. Ενώ το κλειδί και το nonce μπορούν να επαναχρησιμοποιηθούν, η ροή κλειδιών πρέπει να είναι μοναδική για κάθε επανάληψη κρυπτογράφησης για να διασφαλιστεί η ασφάλεια. Η κρυπτογράφηση ροής το επιτυγχάνει αυτό χρησιμοποιώντας καταχωρητές μετατόπισης ανατροφοδότησης για τη δημιουργία ενός μοναδικού nonce (αριθμός που χρησιμοποιείται μόνο μία φορά) για τη δημιουργία της ροής κλειδιών. Βασικοί τύποι τέτοιων αλγορίθμων είναι οι παρακάτω:

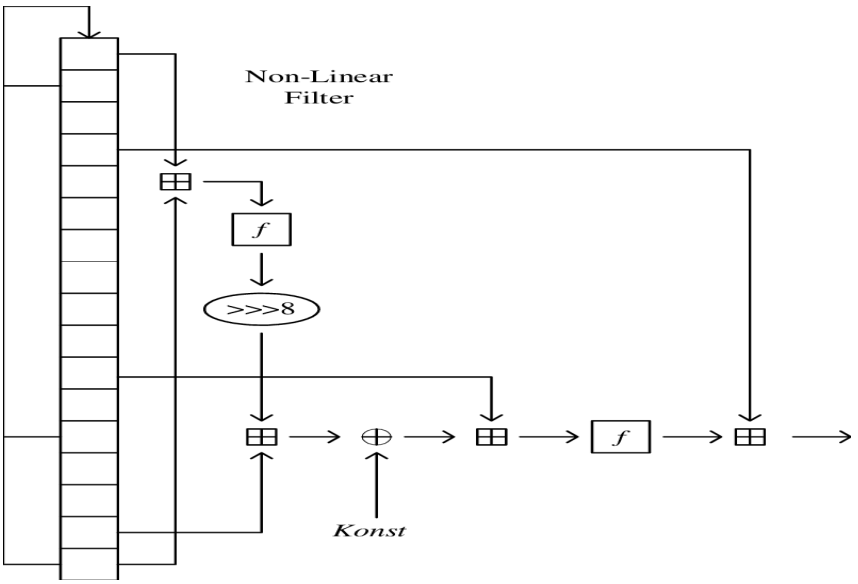
- Ο Κρυπταλγόριθμος ροής HC-256 χαρακτηρίζεται ως ένα απλός και ασφαλής κρυπτογραφικός αλγόριθμος ο οποίος βρίσκει εφαρμογή σε λογισμικά και είναι ελεύθερα διαθέσιμος στην αγορά. Ο HC-256 αποτελείται από δύο μυστικούς πίνακες που καθένας τους αποτελείται από 1024 στοιχεία των 32 bit. Σε πρώτη φάση ενημερώνουμε ένα στοιχείο ενός πίνακα με συνάρτηση μη γραμμικής ανάδρασης. Κάθε 2048 βήματα ενημερώνονται όλα τα στοιχεία των δύο πινάκων. Σε κάθε βήμα το HC-256 δημιουργεί μία

έξοδο 32 bit χρησιμοποιώντας την 32bit σε 32bit αντιστοίχηση. Στη συνέχεια εφαρμόζεται η γραμμική κάλυψη πριν δημιουργηθεί η έξοδος.

$$
\begin{aligned}
f_1(x) &= (x \ggg 7) \oplus (x \ggg 18) \oplus (x \gg 3) \\
f_2(x) &= (x \ggg 17) \oplus (x \ggg 19) \oplus (x \gg 10) \\
g_1(x,y) &= ((x \ggg 10) \oplus (y \ggg 23)) + Q[(x \oplus y) \bmod 1024] \\
g_2(x,y) &= ((x \ggg 10) \oplus (y \ggg 23)) + P[(x \oplus y) \bmod 1024] \\
h_1(x) &= Q[x_0] + Q[256 + x_1] + Q[512 + x_2] + Q[768 + x_3] \\
h_2(x) &= P[x_0] + P[256 + x_1] + P[512 + x_2] + P[768 + x_3]
\end{aligned}
$$

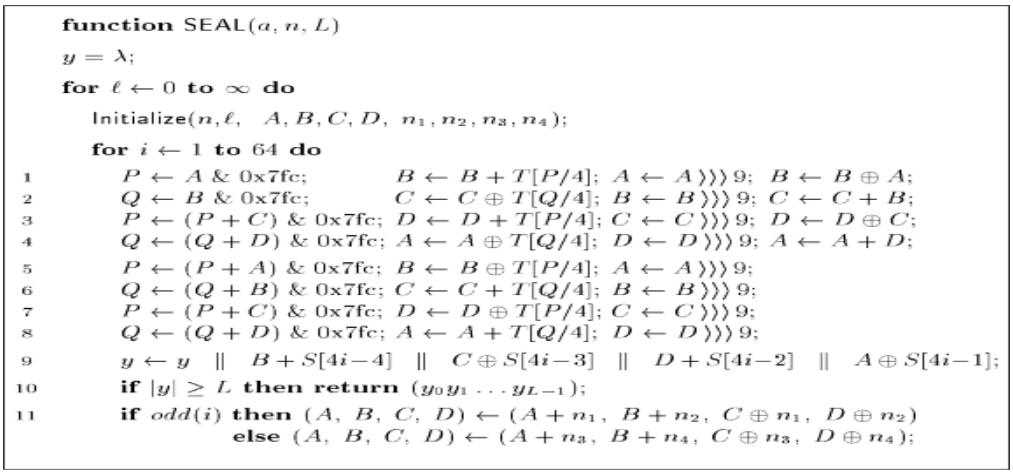
Εικόνα 2.9: Συναρτήσεις του HC-256 (HC-256 Functions).

- Ο SOBER-128 είναι ένα σύγχρονος κρυπταλγόριθμος ροής ο οποίος είναι σχεδιασμένος για ένα μυστικό κλειδί μήκους έως 128bit. Η κρυπτογράφηση εξάγει τη ροή κλειδιού σε block 32bit(Εικόνα 2.10). OSOBER-128 χαρακτηρίζεται ως ένας προσαρτημένος στο εκάστοτε λογισμικό κρυπταλγόριθμος που βασίζεται σε λειτουργίες των 32 bit (όπως 32bitXOR πράξεις καθώς και προσθήκες modulo 232) καθώς και αναφορές σε μικρές σταθερές συστοιχίες. Κατά συνέπεια, ο SOBER-128 στο σπίτι σε πολλά υπολογιστικά περιβάλλοντα, από έξυπνες κάρτες μέχρι μεγάλους υπολογιστές. Ο πηγαίος κώδικας του SOBER-128 είναι δωρεάν διαθέσιμος και η χρήση του επιτρέπεται δωρεάν για οποιοδήποτε σκοπό.



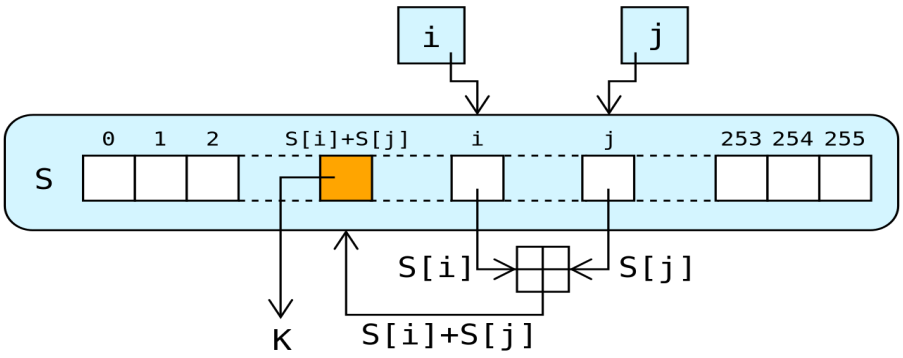
Εικόνα 2.10: SOBER-128.

- Στην κρυπτογραφία, ο SEAL (Software-Optimized Encryption Algorithm)είναιένας κρυπταλγόριθμος ροής βελτιστοποιημένος για μηχανήματα με μέγεθος λέξης 32bit και άφθονη μνήμη RAM με αναφερόμενη απόδοση περίπου 4 κύκλων ανά byte. Ο SEAL είναι στη πραγματικότητα μια ψευδοτυχαία οικογένεια συναρτήσεων καθώς πρέπει εύκολα να δημιουργήσει αυθαίρετα τμήματα της ροής κλειδιών χωρίς να χρειάζεται να ξεκινήσει από την αρχή. Αυτό το καθιστά κατάλληλο για εφαρμογές όπως κρυπτογράφηση σκληρών δίσκων.



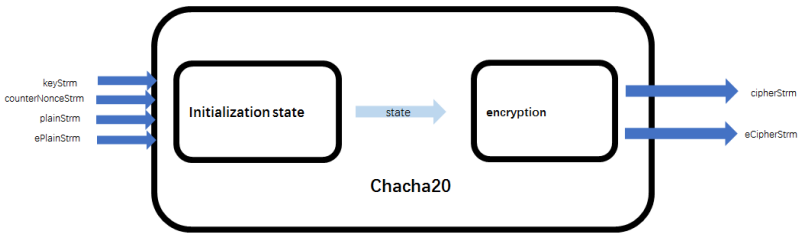
Εικόνα 2.11: SEAL-FUNCTION.

- Το RC4 (επίσης γνωστό ως Rivest Cipher 4) είναι ένα αλγόριθμος κρυπτογράφησης ροής και κλειδιού μεταβλητού μήκους(Εικόνα 2.12). Αυτός ο αλγόριθμος κρυπτογραφεί ένα byte κάθε φορά(ή μεγαλύτερες μονάδες κάθε φορά). Μία είσοδος κλειδιού είναι μια ψευδοτυχαία γεννήτρια bit που παράγει έναν αριθμό ροής 8-bit που είναι απρόβλεπτος χωρίς γνώση του κλειδιού εισόδου. Ο RC4 ήταν ο πιο ευρέως διαδεδομένος κρυπταλγόριθμος ροής επί σχεδόν δύο δεκαετίες, αλλά πια δεν θεωρείται ασφαλής.



Εικόνα 2.12: RC4.

- Ο Cha-Cha20 είναι ένας κρυπταλγόριθμος ροής ο οποίος σχεδιάστηκε από τον Daniel J. Bernstein με στόχο τη διασφάλιση υψηλών περιθωρίων ασφαλείας, επιτυγχάνοντας παράλληλα υψηλές επιδόσεις σε ένα ευρύ φάσμα πλατφόρμων λογισμικού(Εικόνα 2.13).Χρησιμοποιείται μέχρι και σήμερα στο TLS 1.3. Η είσοδός του περιλαμβάνει ένα κλειδί 256 bit, έναν μετρητή 32 bit, ένα nonce96 bit και απλό κείμενο. Η αρχική του κατάσταση είναι ένας πίνακας 4*4 με λέξεις 32bit. Η πρώτη σειρά είναι μία σταθερή συμβολοσειρά 32 byte που κόβεται σε λέξεις 4*32 bit. Η δεύτερη και η Τρίτη γεμίζουν με κλειδί 256-bit. Η πρώτη λέξη στην τελευταία σειρά είναι μετρητής 32 bit και οι άλλες είναι 96 bit nonce. Δημιουργεί ροή κλειδιού 512 bit σε κάθε επανάληψη για να κρυπτογραφήσει ένα γράμμα 512 bit απλού κειμένου.



Εικόνα 2.13: Cha-Cha20.

2.1.4Συναρτήσεις Κατακερματισμού

Η συνάρτηση αυτή (cryptographic hash function) είναι ένας σύνθετος αλγόριθμος που χρησιμοποιείται στη κρυπτογραφία. Μία συνάρτηση κατακερματισμού είναι μια ντετερμινιστική διαδικασία που λαμβάνει ως είσοδο ένα αυθαίρετο μπλοκ από δεδομένα και επιστρέφει μια συμβολοσειρά bit σταθερού μεγέθους, την τιμή κατακερματισμού, έτσι ώστε μια τυχαία ή σκόπιμη αλλαγή στα δεδομένα θα αλλάξει την τιμή κατακερματισμού. Τα δεδομένα προς κωδικοποίηση συχνά ονομάζονται μήνυμα. Η τιμή κατακερματισμού μερικές φορές ονομάζεται αποτύπωμα (message digest ή απλά digest) [**13**].

Βασικά χαρακτηριστικά των συναρτήσεων κατακερματισμού:

- Είναι εύκολος ο υπολογισμός της τιμής κατακερματισμού για οποιοδήποτε δεδομένο μήνυμα.

- Οι συναρτήσεις κατακερματισμού είναι ανέφικτο να δημιουργήσουν ένα μήνυμα που έχει δεδομένο αποτύπωμα.

- Δεν είναι δυνατή η τροποποίηση ενός μηνύματος χωρίς να αλλάξει η κατακερματισμένη τιμή στις συναρτήσεις κατακερματισμού.

- Στις συναρτήσεις κατακερματισμού, δύο διαφορετικά μηνύματα δεν μπορούν να έχουν την ίδια τιμή κατακερματισμού (αποτύπωμα).

Μερικές από τις δημοφιλείς κρυπτογραφικές συναρτήσεις κατακερματισμού είναι οι εξής:

- Secure Hash Algorithms: SHA-2, SHA-3. Η οικογένεια SHA-2 έχει τέσσερις παραλλαγές SHA, SHA-224, SHA-256, SHA-384 και SHA-512, ανάλογα με τον αριθμό των bits στην τιμή κατακερματισμού τους. Τον Οκτώβριο του 2012, το NIST επέλεξε τον αλγόριθμο Keccak ως το νέο πρότυπο SHA-3. Ο Keccak προσφέρει πολλά πλεονεκτήματα, όπως αποδοτικές επιδόσεις και καλή αντοχή στις επιθέσεις.

- RIPEMD (RACE Integrity Primitives Evaluation Message Digest). Αυτό το σύνολο συναρτήσεων κατακερματισμού σχεδιάστηκε από την ανοικτή ερευνητική κοινότητα και είναι γενικά γνωστό ως οικογένεια ευρωπαϊκών συναρτήσεων κατακερματισμού. Το σύνολο περιλαμβάνει τις RIPEMD, RIPEMD-128 και RIPEMD-160. Υπάρχουν επίσης εκδόσεις 256 και 320 bit αυτού του αλγορίθμου. Ο αρχικός RIPEMD (128 bit) βασίζεται στις αρχές σχεδιασμού που χρησιμοποιήθηκαν στον MD4 και διαπιστώθηκε ότι παρέχει αμφισβητήσιμη ασφάλεια. Η έκδοση RIPEMD 128-bit ήρθε ως άμεση αντικατάσταση για να ξεπεραστούν τα τρωτά σημεία του αρχικού RIPEMD. Το RIPEMD-160 είναι μια βελτιωμένη έκδοση και η πιο ευρέως χρησιμοποιούμενη έκδοση της οικογένειας αυτής. Οι εκδόσεις 256 και 320 bit μειώνουν την πιθανότητα τυχαίας σύγκρουσης, αλλά δεν έχουν υψηλότερα επίπεδα ασφάλειας σε σύγκριση με το RIPEMD-128 και το RIPEMD-160 αντίστοιχα.

- Whirlpool: Πρόκειται για μια συνάρτηση κατακερματισμού 512-bit που προέρχεται από την τροποποιημένη έκδοση του Advanced Encryption Standard (AES). Έχουν κυκλοφορήσει τρεις εκδόσεις του Whirlpool, συγκεκριμένα οι WHIRLPOOL-0, WHIRLPOOL-T και WHIRLPOOL.

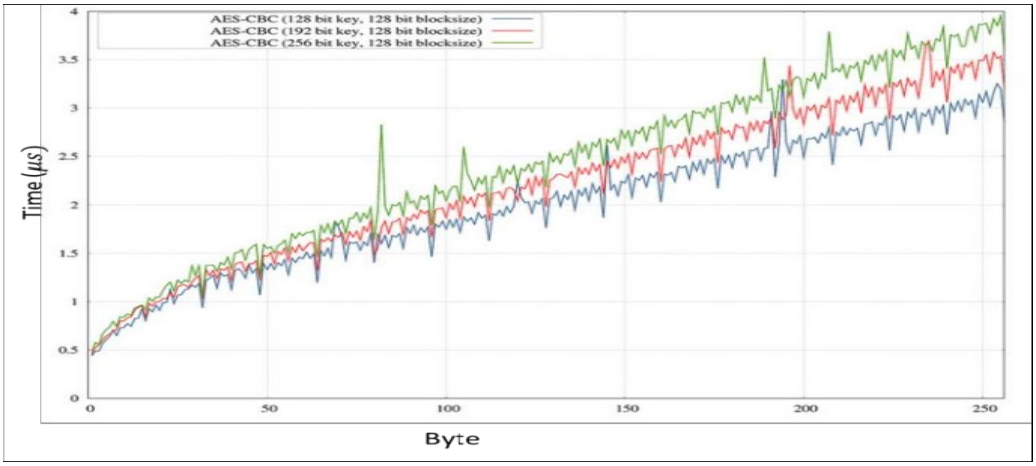
Εφαρμογές των συναρτήσεων κατακερματισμού:

- Χρησιμοποιούνται στην επαλήθευση της ακεραιότητας μηνυμάτων
- Επιτρέπουν τη γρήγορη αναζήτηση των δεδομένων σε έναν πίνακα κατακερματισμού
- Χρησιμοποιούνται στα δίκτυα ανταλλαγής αρχείων peer-to-peer για τον εντοπισμό αρχείων.
- Χρησιμοποιούνται σε περιβάλλοντα όπου είναι απαραίτητο για τους χρήστες να προστατεύονται από την πιθανότητα πλαστογράφησης.
- Χρησιμοποιούνται επίσης στη δημιουργία ψευδοτυχαίων bits, για την εξαγωγή νέων κλειδιών ή κωδικών πρόσβασης από ένα ενιαίο, ασφαλές κλειδί ή κωδικό πρόσβασης.
- Χρησιμοποιούνται ευρέως στην αυθεντικοποίηση πληροφοριών
- Χρησιμοποιούνται για τη διατήρηση του απορρήτου του πελάτη
- Παρέχουν ασφάλεια για τα συστήματα ηλεκτρονικού ταχυδρομείου και μεταφοράς αρχείων.

2.1.5Σύγχρονες Προκλήσεις για τα Κρυπτοσυστήματα Συμμετρικού Κλειδιού

Οι περισσότεροι αλγόριθμοι κρυπτογράφησης λειτουργούν αποτελεσματικότερα όταν υλοποιούνται σε υλικό συνήθως με έναν μόνο επεξεργαστή, από ό,τι σε λογισμικό. Ωστόσο, τα συστήματα που χρησιμοποιούν υλοποιήσεις υλικού έχουν σημαντικά μειονεκτήματα: δεν είναι σε θέση να ανταποκριθούν σε ατέλειες που ανακαλύπτονται στον υλοποιημένο αλγόριθμο ή σε αλλαγές στα πρότυπα. Ως εναλλακτική λύση, είναι δυνατή η υλοποίηση αλγορίθμων κρυπτογραφίας σε λογισμικό που εκτελείται σε πολλαπλούς επεξεργαστές.

Ένα σύγχρονο σύστημα κρυπτογράφησης πρέπει να εγγυάται σαφώς την ασφάλεια αλλά και την ταχύτητα.



Εικόνα 2.14: Ταχύτητα του AESστα 128,192 και 256-bitμεγέθη κλειδιών.

Γενικότερα, υπάρχουν δύο βασικές προκλήσεις για την κρυπτογραφία συμμετρικού κλειδιού.

1. Εγκαθίδρυση κλειδιού - Πριν από κάθε επικοινωνία, τόσο ο αποστολέας όσο και ο παραλήπτης πρέπει να συμφωνήσουν σε ένα μυστικό συμμετρικό κλειδί. Απαιτείται η ύπαρξη ενός ασφαλούς μηχανισμού εγκαθίδρυσης κλειδιού.

2. Πρόβλημα εμπιστοσύνης - Εφόσον ο αποστολέας και ο παραλήπτης χρησιμοποιούν το ίδιο συμμετρικό κλειδί, υπάρχει μια σιωπηρή απαίτηση ότι ο αποστολέας και ο παραλήπτης "εμπιστεύονται" ο ένας τον άλλον. Για παράδειγμα, μπορεί να συμβεί ότι ο παραλήπτης έχει χάσει το κλειδί από κάποιον επιτιθέμενο και ο αποστολέας δεν έχει ενημερωθεί.

Αυτές οι δύο προκλήσεις είναι ιδιαίτερα περιοριστικές για τη σύγχρονη επικοινωνία. Σήμερα, οι άνθρωποι πρέπει να ανταλλάσσουν πληροφορίες με μη οικεία και μη έμπιστα μέρη. Για παράδειγμα, μια επικοινωνία μεταξύ διαδικτυακού πωλητή και πελάτη. Αυτοί οι περιορισμοί της κρυπτογράφησης συμμετρικού κλειδιού οδήγησαν στα συστήματα κρυπτογράφησης ασύμμετρου κλειδιού.

2.2 Κρυπτοσυστήματα Ασύμμετρου Κλειδιού

Η ασύμμετρη κρυπτογραφία, γνωστή και ως κρυπτογραφία δημόσιου κλειδιού, είναι πιο αργή από τη συμμετρική κρυπτογραφία. Απαιτούνται διαφορετικά κλειδιά για την κρυπτογράφηση

και την αποκρυπτογράφηση δεδομένων. Ωστόσο, είναι πιο κλιμακούμενη , δεδομένου ότι έχει σχεδιαστεί για να επιτρέπει την ασφαλή ανταλλαγή κλειδιών μεταξύ πολλών χρηστών [10].

Η ασύμμετρη κρυπτογραφία βασίζεται σε ένα ζεύγος κλειδιών που δημιουργείται για κάθε χρήστη. Το ένα από τα κλειδιά παραμένει πάντα ιδιωτικό και είναι γνωστό μόνο στον χρήστη, ενώ το άλλο είναι δημόσιο και μοιράζεται με οποιαδήποτε συσκευή του χρήστη με την οποία θα ήθελε να ανταλλάξει με ασφάλεια δεδομένα. Μια θεμελιώδης αρχή της ασύμμετρης κρυπτογραφίας είναι ότι το δημόσιο και το ιδιωτικό κλειδί στο ζεύγος κλειδιών μπορούν τόσο να κρυπτογραφήσουν όσο και να αποκρυπτογραφήσουν τα δεδομένα. Ωστόσο, κατά τη διάρκεια μιας ανταλλαγής δεδομένων μόνο ένα από τα κλειδιά (είτε το δημόσιο είτε το ιδιωτικό) χρησιμοποιείται για την κρυπτογράφηση των δεδομένων και το άλλο κλειδί χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων και αντίστροφα.

Όταν ένας χρήστης θέλει να μοιραστεί δεδομένα, θα κρυπτογραφήσει τις πληροφορίες χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη. Η ασύμμετρη κρυπτογραφία εξασφαλίζει στη συνέχεια ότι μόνο το ιδιωτικό κλειδί του παραλήπτη μπορεί να αποκρυπτογραφήσει το μήνυμα. Με αυτόν τον τρόπο, πολλά μέρη μπορούν να έχουν τα εργαλεία για την ασφάλεια των δεδομένων, αλλά μόνο ένας παραλήπτης μπορεί να αποκρυπτογραφήσει τις πληροφορίες. Λόγω αυτής της λειτουργίας, η ασύμμετρη κρυπτογραφία χρησιμοποιείται συνήθως για την προστασία δεδομένων κατά τη μεταφορά. Στον σημερινό συνδεδεμένο κόσμο, αυτό περιλαμβάνει εξαιρετικά συνηθισμένες περιπτώσεις χρήσης, όπως το ηλεκτρονικό ταχυδρομείο, η σύνδεση σε έναν ιστότοπο ή η ανταλλαγή μηνυμάτων σε πλατφόρμες, καθώς και εφαρμογές ψηφιακών νομισμάτων όπως η αποστολή και η λήψη Bitcoin[10].

Το άλλο σημαντικό πλεονέκτημα της ασύμμετρης κρυπτογράφησης είναι η δυνατότητα επαλήθευσης της πηγής των δεδομένων ή επικοινωνιών. Σε αυτή την περίπτωση, χρησιμοποιείται ένα ιδιωτικό κλειδί για την κρυπτογράφηση πληροφοριών και οποιαδήποτε οντότητα με το αντίστοιχο δημόσιο κλειδί μπορεί να επαληθεύσει τον αποστολέα των πληροφοριών. Χρησιμοποιώντας αυτή τη ροή, οποιοσδήποτε λαμβάνει δεδομένα γνωρίζει ότι τα δεδομένα πράγματι προήλθαν από μία συγκεκριμένη, επαληθευμένη πηγή, επειδή μόνο το δημόσιο κλειδί της πηγής μπορεί να αποκαλύψει το υποκείμενο κείμενο. Ψηφιακές υπογραφές και ψηφιακά πιστοποιητικά εκμεταλλεύονται αυτό το χαρακτηριστικό των ασύμμετρων κλειδιών για να επαληθεύσουν ότι τα δεδομένα προέρχονται από μία αξιόπιστη και επαληθευμένη πηγή.

Η συμμετρική και η ασύμμετρη κρυπτογραφία αποτελούν τη ραχοκοκαλιά του σύγχρονου διαδικτύου. Χρησιμοποιείται μια ποικιλία πρωτοκόλλων για να καταστεί δυνατή η ασφαλής αποστολή μηνυμάτων, και η πιστοποίηση της ταυτότητας χρήστη.

2.2.1 Αλγόριθμοι Ασύμμετρης Κρυπτογράφησης

Το 1978, οι RonRivest, AdiShamir και LeonardAdleman εισήγαγαν έναν κρυπτογραφικό αλγόριθμο που μπορεί και υλοποιεί ένα κρυπτοσύστημα δημόσιου κλειδιού, καθώς και ψηφιακές υπογραφές, τον RSA. Ο RSA (Εικόνα 2.15) παρακινείται από τη δημοσιευμένη εργασία των Diffie και Hellman από λίγα χρόνια πριν, που περιέγραψαν την ιδέα ενός τέτοιου αλγόριθμου, αλλά ποτέ δεν τον ανέπτυξαν πραγματικά [14]

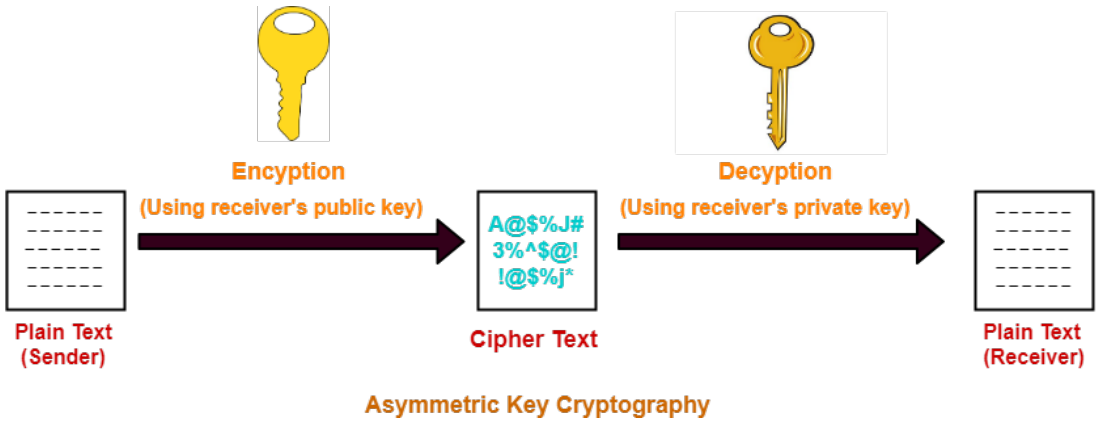
Εισήχθη την εποχή που αναμενόταν να δημιουργηθεί σύντομα το ηλεκτρονικό ταχυδρομείο(email) και υλοποίησε δύο σημαντικές ιδέες:

1. Κρυπτογράφηση δημοσίου κλειδιού. Αυτή η ιδέα παραλείπει την ανάγκη για έναν 'ταχυμεταφορέα' που θα παραδίδει τα κλειδιά στους παραλήπτες μέσο ασφαλούς καναλιού πριν λάβουν το προβλεπόμενο μήνυμα. Στο RSA, τα κλειδιά κρυπτογράφησης είναι δημόσια, ενώ τα κλειδιά αποκρυπτογράφησης δεν είναι. Επομένως μόνο το άτομο με το σωστό κλειδί αποκρυπτογράφησης μπορεί να αποκρυπτογραφήσει ένα κρυπτογραφημένο μήνυμα. Ο καθένα έχει τα δικά του κλειδιά κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα. Τα κλειδιά πρέπει να γίνουν με τέτοιο τρόπο ώστε το κλειδί αποκρυπτογράφησης να μην μπορεί να συναχθεί εύκολα με το δημόσιο κλειδί [14].

2. Ψηφιακές Υπογραφές: Ο παραλήπτης μπορεί να χρειαστεί να επαληθεύσει ότι ένα μεταδιδόμενο μήνυμα πραγματικά προέρχεται από τον εκάστοτε αποστολέα (έλεγχος ταυτότητας). Αυτό γίνεται χρησιμοποιώντας το κλειδί αποκρυπτογράφησης του αποστολέα για τη δημιουργία ψηφιακής υπογραφής στο μήνυμα, η οποία υπογραφή μπορεί αργότερα να επαληθευτεί από οποιονδήποτε, χρησιμοποιώντας το αντίστοιχο κλειδί κρυπτογράφησης. Επομένως οι υπογραφές δεν μπορούν να πλαστογραφηθούν. Επίσης δεν μπορεί κανένας που έχει υπογράψει να αρνηθεί ότι υπέγραψε [14].

   Ο RSA δεν είναι μόνο χρήσιμος για το ηλεκτρονικό ταχυδρομείο, αλλά και για άλλες ηλεκτρονικές συναλλαγές και μεταδόσεις, όπως μεταφορές κεφαλαίων. Η ασφάλεια του αλγορίθμου RSA έχει επικυρωθεί μέχρι στιγμής, καθώς καμία γνωστή απόπειρα

διάσπασης του δεν ήταν ακόμα επιτυχής, κυρίως λόγω της δυσκολίας παραγοντοποίησης μεγάλων αριθμών n = p*q όπου p και q είναι μεγάλοι πρώτοι αριθμοί [14].



Εικόνα 2.15: RSA Αλγόριθμος.

Η Κρυπτογραφία Ελλειπτικής Καμπύλης(Elliptic Curve Cryptography(ECC)), είναι μία σύγχρονη τεχνική κρυπτογράφησης δημοσίου κλειδιού γνωστή ως μικρότερη, ταχύτερη και πιο αποτελεσματική από τους κατεστημένους φορείς. Η κρυπτογραφία ECC θεωρήθηκε φυσικός σύγχρονος διάδοχος του κρυπτοσυστήματος RSA, επειδή το ECC χρησιμοποιεί μικρότερα κλειδιά και υπογραφές από το RSA για το ίδιο επίπεδο ασφάλειας και παρέχει πολύ γρήγορη παραγωγή κλειδιών, γρήγορη συμφωνία κλειδιών και γρήγορες υπογραφές. Μία κοινή χρήση του ECCείναι η κρυπτογράφηση δεδομένων έτσι ώστε μόνο εξουσιοδοτημένα μέρη να μπορούν να τα αποκρυπτογραφούν. Αυτό έχει πολλές προφανείς περιπτώσεις χρήσης, αλλά χρησιμοποιείται πιο συχνά για την κρυπτογράφηση τη κίνησης στο διαδίκτυο. Τελικά η ECCδεν αντικατέστησε τον RSA – ωστόσο συνυπάρχουν και τα δύο (πολλές εφαρμογές/πρωτόκολλα έχουν υιοθετήσει τον RSA και άλλες την ECC).

2.3 Σημασία της Κρυπτογραφίας Συμμετρικού & Δημοσίου Κλειδιού

Το κύριο πλεονέκτημα της κρυπτογραφίας δημόσιου κλειδιού ότι τα ιδιωτικά κλειδιά δεν χρειάζεται ποτέ να μεταδοθούν ή να κοινοποιηθούν σε κανέναν. Σε ένα σύστημα συμμετρικού κλειδιού, αντίθετα, τα συμμετρικά κλειδιά πρέπει να μεταδίδονται (είτε χειροκίνητα ή μέσω ενός

καναλιού επικοινωνίας), και μπορεί να υπάρχει η πιθανότητα ότι ένας εχθρός να ανακαλύψει τα συμμετρικά κλειδιά κατά τη μετάδοσή τους [6].

Ένα άλλο σημαντικό πλεονέκτημα των συστημάτων δημόσιου κλειδιού είναι ότι μπορούν να παρέχουν μια μέθοδο για ψηφιακές υπογραφές. Η πιστοποίηση ταυτότητας μέσω συστημάτων συμμετρικών κλειδιών απαιτεί την κοινή χρήση ορισμένων συμμετρικών κλειδιών και μερικές φορές απαιτεί επίσης την εμπιστοσύνη ενός τρίτου μέρους. Ως αποτέλεσμα, ένα αποστολέας μπορεί να αποκηρύξει ένα προηγουμένως αυθεντικοποιημένο μήνυμα ισχυριζόμενος ότι το κοινόχρηστο συμμετρικό κλειδί παραβιάστηκε με κάποιο τρόπο από ένα από τα μέρη που μοιράζονται το συμμετρικό κλειδί. Η αυθεντικοποίηση δημόσιου κλειδιού, από την άλλη πλευρά, αποτρέπει αυτόν τον τύπο απόρριψης, κάθε χρήστης έχει την αποκλειστική ευθύνη για την προστασία του ιδιωτικού του κλειδιού. Αυτή η ιδιότητα της αυθεντικοποίησης δημόσιου κλειδιού ονομάζεται συχνά μη αποκήρυξη [15].

Ένα μειονέκτημα της χρήσης κρυπτογραφίας δημόσιου κλειδιού για κρυπτογράφηση είναι η ταχύτητα. Δημοφιλείς μέθοδοι κρυπτογράφησης συμμετρικού κλειδιού είναι σημαντικά ταχύτερες από οποιαδήποτε διαθέσιμη σήμερα μέθοδος κρυπτογράφησης δημόσιου κλειδιού. Παρ' όλα αυτά, η κρυπτογράφηση δημόσιου κλειδιού μπορεί να χρησιμοποιηθεί συνδυαστικά με την κρυπτογραφία συμμετρικού κλειδιού. Πράγματι, για την κρυπτογράφηση, η καλύτερη λύση είναι ο συνδυασμός των συστημάτων δημόσιου - και συμμετρικού κλειδιού, ώστε να επιτυγχάνονται τόσο τα πλεονεκτήματα ασφάλειας των συστημάτων δημόσιου κλειδιού όσο και η ταχύτητα των συστημάτων συμμετρικού κλειδιού. Το σύστημα δημόσιου κλειδιού μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση ενός συμμετρικού κλειδιού το οποίο χρησιμοποιείται για την κρυπτογράφηση του μεγαλύτερου μέρους ενός αρχείου ή μηνύματος. Ένα τέτοιο πρωτόκολλο ονομάζεται ψηφιακός φάκελος [15].

Σε ορισμένες περιπτώσεις, η κρυπτογράφηση δημόσιου κλειδιού δεν είναι απαραίτητη και η κρυπτογράφηση συμμετρικού κλειδιού είναι επαρκής. Αυτό περιλαμβάνει περιβάλλοντα όπου η ασφαλής συμμετρική συμφωνία κλειδιών μπορεί να πραγματοποιηθεί, για παράδειγμα από χρήστες που συναντώνται ιδιωτικά. Περιλαμβάνει επίσης περιβάλλοντα στα οποία μία και μόνη αρχή γνωρίζει και διαχειρίζεται όλα τα κλειδιά (π.χ. ένα κλειστό τραπεζικό σύστημα). Δεδομένου ότι η αρχή γνωρίζει ήδη τα κλειδιά όλων, δεν υπάρχουν πολλά πλεονεκτήματα για ορισμένα να είναι "δημόσια" και άλλα "ιδιωτικά". Επίσης, η κρυπτογραφία δημόσιου κλειδιού δεν είναι συνήθως απαραίτητη σε περιβάλλον ενός χρήστη. Γενικά, η κρυπτογράφηση δημόσιου κλειδιού είναι καταλληλότερη για ένα ανοικτό περιβάλλον πολλαπλών χρηστών [16].

Συγκεντρωτικά τα πλεονεκτήματα & τα μειονεκτήματα της συμμετρικής και της ασύμμετρης κρυπτογραφίας είναι τα εξής:

Πλεονεκτήματα της κρυπτογραφίας συμμετρικού κλειδιού

- Οι κρυπτογραφήσεις συμμετρικού κλειδιού μπορούν να σχεδιαστούν ώστε να έχουν υψηλούς ρυθμούς απόδοσης δεδομένων.

- Τα κλειδιά για τη κρυπτογράφηση συμμετρικού κλειδιού είναι σχετικά μικρά, συγκρινόμενα με αυτά της ασύμμετρης κρυπτογράφησης.

- Οι κρυπτογραφήσεις συμμετρικού κλειδιού μπορούν να χρησιμοποιηθούν ως πρωτόκολλα για την κατασκευή διαφόρων κρυπτογραφικών μηχανισμών, όπως γεννήτριες ψευδοτυχαίων αριθμών, συναρτήσεις κατακερματισμού, και υπολογιστικά αποδοτικά συστήματα ψηφιακής υπογραφής.

- Οι κρυπτογραφήσεις συμμετρικού κλειδιού μπορούν να συντίθενται για την παραγωγή ισχυρότερων κρυπτογραφήσεων. Απλή μετασχηματισμοί που είναι εύκολοι στην ανάλυση, αλλά από μόνοι τους αδύναμοι, μπορούν να χρησιμοποιηθούν για να κατασκευάσουν ισχυρές λύσεις κρυπτογράφησης.

Μειονεκτήματα της κρυπτογραφίας συμμετρικού κλειδιού

- Σε μια αμφίδρομη επικοινωνία, το κλειδί πρέπει να παραμείνει μυστικό και στα δύο άκρα.

- Σε ένα μεγάλο δίκτυο, υπάρχουν πολλά ζεύγη κλειδιών που πρέπει να διαχειριστούν. Κατά συνέπεια, η αποτελεσματική διαχείριση κλειδιών απαιτεί τη χρήση ενός άνευ όρων αξιόπιστου τρίτου μέρους.

- Σε μια αμφίδρομη επικοινωνία μεταξύ οντοτήτων Α και Β, η υγιής κρυπτογραφική πρακτική υπαγορεύει ότι το κλειδί πρέπει να αλλάζει συχνά και ίσως για κάθε συνεδρία επικοινωνίας. Οι μηχανισμοί ψηφιακής υπογραφής που προκύπτουν από την κρυπτογράφηση συμμετρικού κλειδιού συνήθως απαιτούν είτε μεγάλα κλειδιά για τη δημόσια επαλήθευση είτε τη χρήση ενός τρίτου μέρους.

Πλεονεκτήματα της κρυπτογραφίας δημόσιου κλειδιού

- Μόνο το ιδιωτικό κλειδί πρέπει να διατηρείται μυστικό (η αυθεντικότητα των δημόσιων κλειδιών πρέπει, ωστόσο, να διασφαλίζεται).

- Ανάλογα με τον τρόπο χρήσης, ένα ζεύγος ιδιωτικού κλειδιού/δημόσιου κλειδιού μπορεί να παραμείνει αμετάβλητο για σημαντικά χρονικά διαστήματα, π.χ. πολλές συνεδρίες (ακόμη και για πολλά χρόνια).

- Πολλά σχήματα δημόσιου κλειδιού αποδίδουν σχετικά αποδοτικούς μηχανισμούς για ψηφιακές υπογραφές. Το κλειδί που χρησιμοποιείται για την περιγραφή της δημόσιας συνάρτησης επαλήθευσης είναι τυπικά πολύ μικρότερο από ό,τι για το αντίστοιχο συμμετρικού κλειδιού.

- Σε ένα μεγάλο δίκτυο, ο αριθμός των αναγκαίων κλειδιών μπορεί να είναι σημαντικά μικρότερος από ό,τι στο σενάριο του συμμετρικού κλειδιού.

Μειονεκτήματα της κρυπτογράφησης δημόσιου κλειδιού

- Τα ποσοστά απόδοσης για τις πιο δημοφιλείς μεθόδους κρυπτογράφησης δημόσιου κλειδιού είναι αρκετές τάξεις μεγέθους πιο αργές από τις πιο γνωστές μεθόδους συμμετρικού κλειδιού.

- Τα μεγέθη κλειδιών είναι συνήθως πολύ μεγαλύτερα από εκείνα που απαιτούνται για τη κρυπτογράφηση συμμετρικού κλειδιού, και το μέγεθος των υπογραφών δημόσιου κλειδιού είναι μεγαλύτερο από εκείνο των ετικετών που παρέχουν πιστοποίηση της προέλευσης των δεδομένων από τεχνικές συμμετρικού κλειδιού.

Συνεπώς,

- Η κρυπτογραφία δημόσιου κλειδιού διευκολύνει τις αποδοτικές υπογραφές και τη διαχείριση κλειδιών.

- Η κρυπτογραφία συμμετρικού κλειδιού είναι αποτελεσματική για την κρυπτογράφηση και την ακεραιότητα ορισμένων εφαρμογών διαχείρισης δεδομένων.

2.4 Προς Επόμενη Γενιά Αλγορίθμων Κρυπτογράφησης

Στη σύγχρονη εποχή, το IoT έχει δημιουργήσει νέες αξίες συνδέοντας διάφορες συσκευές στο δίκτυο, αλλά έχει επίσης οδηγήσει σε απειλές ασφαλείας και έχουν προκαλέσει σημαντικά ζητήματα, όπως φαίνεται στις πρόσφατες αναφορές για παράνομη χειραγώγηση καμερών παρακολούθησης και παραβίαση αυτοκινήτων κ.λπ. Η κρυπτογράφηση είναι ένα αποτελεσματικό αντίμετρο, και το IoT απαιτείται πλέον να εφαρμόζει κρυπτογράφηση σε συσκευές αισθητήρων σε περιβάλλοντα με διάφορους περιορισμούς που προηγουμένως δεν είχαν υποβληθεί σε κρυπτογράφηση. Η κρυπτογραφία χαμηλών πόρων (lightweight cryptography)είναι κλάδος της κρυπτογραφίας που ερευνήθηκε και αναπτύχθηκε για να ανταποκριθεί σε αυτό το ζήτημα. Απαιτούνται οι ακόλουθοι παράγοντες για την υλοποίηση του lightweight cryptography: μέγεθος (μέγεθος κυκλώματος, μεγέθη ROM/RAM), ισχύς, κατανάλωση ισχύος, ταχύτητα επεξεργασίας (απόδοση, καθυστέρηση).

Τα τελευταία χρόνια, έχει επίσης πραγματοποιηθεί σημαντική έρευνα σχετικά με τους κβαντικούς υπολογιστές - μηχανές που εκμεταλλεύονται τα κβαντομηχανικά φαινόμενα για την επίλυση μαθηματικών προβλημάτων που είναι δύσκολα ή δυσεπίλυτα για τους συμβατικούς υπολογιστές. Εάν ποτέ κατασκευαστούν κβαντικοί υπολογιστές μεγάλης κλίμακας, θα είναι σε θέση να «σπάσουν» πολλά από τα κρυπτοσυστήματα δημόσιου κλειδιού που χρησιμοποιούνται σήμερα. Αυτό θα έθετε σε σοβαρό κίνδυνο την εμπιστευτικότητα και την ακεραιότητα των ψηφιακών επικοινωνιών στο Διαδίκτυο και αλλού. Ο στόχος της μετα-κβαντικής κρυπτογραφίας (post-quantum cryptography) είναι η ανάπτυξη κρυπτογραφικών συστημάτων που είναι ασφαλή τόσο έναντι κβαντικών όσο και έναντι κλασικών υπολογιστών και μπορούν να διαλειτουργούν με τα υπάρχοντα πρωτόκολλα και δίκτυα επικοινωνιών.

Κεφάλαιο 3

Γενικός Κανονισμός Προσωπικών Δεδομένων(GDPR)

Τόσο η ιδιωτικότητα όσο και η προστασία προσωπικών δεδομένων αποτελούν θεμελιώδη ατομικά δικαιώματα στην Ευρωπαϊκή Ένωση (και όχι μόνο), όπως προβλέπεται στη Χάρτα Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Για την προάσπισή τους υπάρχει σαφές νομικό πλαίσιο, το οποίο θέτει συγκεκριμένες υποχρεώσεις σε όσους οργανισμούς επεξεργάζονται προσωπικά δεδομένα αλλά και δικαιώματα για όλους όσους τα δεδομένα τους υφίστανται επεξεργασία.

Βασική νομοθεσία στην Ευρωπαϊκή Ένωση (ΕΕ) για την προστασία προσωπικών δεδομένων είναι ο Γενικός Κανονισμός Προσωπικών Δεδομένων – (ΓΚΠΔ) – ευρέως γνωστός και με το ακρωνύμιο GDPR (General Data Protection Regulation). Κύριος στόχος του GDPR είναι η προστασία των πολιτών της ΕΕ από οργανισμούς που επεξεργάζονται πληροφορίες προσωπικού χαρακτήρα. Οι κυρώσεις για παραβιάσεις προσωπικών δεδομένων έχουν επίσης αυξηθεί, και οι οργανισμοί έχουν νέες απαιτήσεις π.χ. για τις κοινοποιήσεις περιστατικών παραβίασης δεδομένων. Οι οργανισμοί που δεν συμμορφώνονται με τον ΓΚΠΔ ενδέχεται να αντιμετωπίσουν κυρώσεις ύψους έως 20 εκατ. Ευρώ ή το 4% του παγκόσμιου ετήσιου κύκλου εργασιών τους.

Οι κανόνες του ΓΚΠΔ, ο οποίος είναι σε εφαρμογή από το Μάιο του 2018,επικαιροποίησησαν το προηγούμενο συναφές νομικό πλαίσιο στην ΕΕ και είχε ως στόχο, μεταξύ άλλων, να βοηθήσει τους οργανισμούς να προετοιμάσουν σωστές πολιτικές και διαδικασίες για τη διαχείριση περιστατικών ασφάλειας στον κυβερνοχώρο. Επιπλέον, ο ΓΚΠΔ αλλάζει τον τρόπο με τον οποίο οι οργανισμοί επεξεργάζονται και αποθηκεύουν προσωπικές πληροφορίες.. Τα δικαιώματα των πολιτών στην ΕΕ έχουν επεκταθεί και ο ΓΚΠΔ εφαρμόζεται σε όλους τους οργανισμούς που επεξεργάζονται δεδομένα κατοίκων χωρών στην ΕΕ[17].

Με τον ΓΚΠΔ, για κάθε επεξεργασία δεδομένων, ένας οργανισμός μπορεί να έχει έναν εκ δύο ρόλων:

- ο υπεύθυνος επεξεργασίας και
- αυτός που εκτελεί την επεξεργασία των δεδομένων.

Ο υπεύθυνος επεξεργασίας πρέπει να καθορίσει πώς και γιατί τα προσωπικά δεδομένα υφίστανται επεξεργασία (δηλαδή καθορίζει το σκοπό, τα μέσα και κάθε άλλη ουσιώδη πτυχή της επεξεργασίας), ενώ ο εκτελών την επεξεργασία τα επεξεργάζεται για λογαριασμό του υπευθύνου επεξεργασίας. Ο υπεύθυνος επεξεργασίας μπορεί να είναι μια εταιρεία, ίδρυμα ή κυβερνητικός

οργανισμός. Ο εκτελών την επεξεργασία μπορεί να είναι, για παράδειγμα, μια εταιρεία πληροφορικής που της ανατίθεται, από κάποιον υπεύθυνο επεξεργασίας, μία επεξεργασία δεδομένων. Ακόμη και οργανισμοί εκτός της Ευρωπαϊκής Ένωσης που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση πρέπει να εφαρμόζουν τις απαιτήσεις του Κανονισμού. Μετά τη θέσπιση της νομοθεσίας GDPR, κάθε οργανισμός πρέπει να χειρίζεται τα δεδομένα προσωπικού χαρακτήρα νόμιμα και με διαφάνεια, ακολουθώντας πολύ συγκεκριμένους κανόνες. Επιπλέον, η επεξεργασία των προσωπικών δεδομένων πρέπει να έχει έναν σαφή και νόμιμο σκοπό. Όταν πληροφορίες που ταυτοποιούν ένα φυσικό πρόσωπο δεν είναι πλέον απαραίτητες, οι οργανισμοί πρέπει να τις διαγράφουν [18].

3.1 Ορισμός των Προσωπικών Πληροφοριών σύμφωνα με τον ΓΚΠΔ

Κάθε δεδομένο που σχετίζεται άμεσα ή έμμεσα με ένα ταυτοποιήσιμο φυσικό πρόσωπο είναι δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα. Παραδείγματα προσωπικών δεδομένων είναι το όνομα ενός φυσικού προσώπου, ο αριθμός ταυτότητας, δεδομένα σχετικά με τη τοποθεσία, κάποιο διαδικτυακό αναγνωριστικό (διευθύνσεις ηλεκτρονικού ταχυδρομείου ή διεύθυνση IP), δεδομένα υγείας, φυσικά, γενετικά ή βιομετρικά δεδομένα, δεδομένα σχετικά με την ψυχική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του φυσικού προσώπου.

3.2 Αρχές του GDPRγια Νόμιμη Επεξεργασία Προσωπικών Δεδομένων.

Το άρθρο 5 του κανονισμού περιγράφει τις αρχές τις οποίες οι υπεύθυνοι επεξεργασίας θα πρέπει να τηρούν κατά την επεξεργασία των προσωπικών δεδομένων. Παρακάτω παρατίθεται η λίστα με τις θεμελιώσεις αυτές αρχές:

- Η επεξεργασία των προσωπικών δεδομένων πρέπει να είναι νόμιμη, θεμιτή και με διαφάνεια. Τα προσωπικά δεδομένα πρέπει να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και όχι να υποβάλλονται σε επεξεργασία με τρόπο που δεν είναι συμβατός με τους σκοπούς αυτούς

- Τα προσωπικά δεδομένα πρέπει να είναι επαρκή, συναφή και περιορισμένα στους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία (αρχή της ελαχιστοποίησης των δεδομένων).

- Τα προσωπικά δεδομένα πρέπει να είναι ακριβή, να ενημερώνονται και οι οργανισμοί πρέπει να διασφαλίζουν ότι τα δεδομένα δεν είναι ανακριβή (αρχή της ακρίβειας των δεδομένων).

- Τα προσωπικά δεδομένα πρέπει να τηρούνται σε μορφή που να επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το χρονικό διάστημα που είναι απαραίτητο.

- Η επεξεργασία των προσωπικών δεδομένων πρέπει να γίνεται με τρόπο που να διασφαλίζεται και να προστατεύεται από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και να μην χάνονται, καταστρέφονται ή να έχουν υποστεί ζημιά.

- Ο υπεύθυνος επεξεργασίας είναι υπεύθυνος για την απόδειξη της συμμόρφωσης των δεδομένων με τον κανονισμό.

Η παρακάτω εικόνα (Εικόνα 3.1) παρουσιάζει τις έξι αρχές για νόμιμη επεξεργασία προσωπικών δεδομένων του ΓΚΠΔ[19].

Εικόνα 3.1: Αρχές Προστασίας των Προσωπικών Δεδομένων του ΓΚΠΔ.

Η αρχή του περιορισμού του σκοπού υποδηλώνει ότι τα προσωπικά δεδομένα μπορούν να υποβάλλονται σε επεξεργασία για καθορισμένους, σαφείς και νόμιμους σκοπούς, και όχι να χρησιμοποιούνται εκ των υστέρων για άλλον σκοπό. Το υποκείμενο των δεδομένων (δηλαδή το φυσικό πρόσωπο του οποίου τα δεδομένα υφίστανται επεξεργασία) γνωρίζει τους προαναφερθέντες σκοπούς και τα δεδομένα του δεν χρησιμοποιούνται γιαπεραιτέρω ενέργειες Συλλέγονται μόνο τα δεδομένα που είναι απαραίτητα και τίποτα περισσότερο (ελαχιστοποίηση δεδομένων).

Η αρχή της ακρίβειας υποδηλώνει ότι τα προσωπικά δεδομένα πρέπει να διατηρούνται ενημερωμένα και ακριβή. Περιορισμοί αποθήκευσης σημαίνει ότι τα δεδομένα θα αποθηκεύονται μόνο για το χρονικό διάστημα που είναι απαραίτητο και όχι περισσότερο. Όταν δεν υπάρχει πλέον σκοπός για την αποθήκευση των προσωπικών δεδομένων τα δεδομένα θα πρέπει να διαγράφονται. Η ακεραιότητα και η εμπιστευτικότητα σημαίνουν ότι τα προσωπικά δεδομένα θα πρέπει να αντιμετωπίζονται με τρόπο που να διασφαλίζεται από παράνομη επεξεργασία ή από καταστροφή ή ζημιά [19].

Το έκτο άρθρο του ΓΚΠΔ ορίζει τις νομικές βάσεις, μία εκ των οποίων πρέπει να έχει εφαρμογή για να είναι επιτρεπτή η επεξεργασία. Αυτές είναι οι εξής:

- Το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών του πληροφοριών για τουλάχιστον έναν ή περισσότερους σκοπούς.

- Η επεξεργασία δεδομένων είναι απαραίτητη στο πλαίσιο σύμβασης, μέλος της οποία είναι το υποκείμενο των δεδομένων.

- Η επεξεργασία είναι απαραίτητη γιατί επιβάλλεται από νόμο. Η επεξεργασία είναι απαραίτητη για τη διαφύλαξη των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.

- Η επεξεργασία είναι αναγκαία από την άποψη του δημόσιου συμφέροντος ή του δημόσιου καθήκοντος κάποιας της επίσημης αρχής.

- Η επεξεργασία είναι απαραίτητη για την προάσπιση έννομων συμφερόντων του υπευθύνου επεξεργασίας ή τρίτου, τα οποία υπερτερούν έναντι των δικαιωμάτων των φυσικών προσώπων. είναι απαραίτητα για να προστατευθούν.

Απαγορεύεται η επεξεργασία ειδικών κατηγοριών προσωπικών πληροφοριών εξ ορισμού σύμφωνα με το άρθρο 9 του ΓΚΠΔ. Η φυλετική, εθνική καταγωγή, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, γενετικά δεδομένα, βιομετρικά δεδομένα, δεδομένα υγείας ή σεξουαλικής ζωής ή ο γενετήσιος προσανατολισμός ενός φυσικού προσώπου μπορούν να θεωρηθούν ευαίσθητα δεδομένα. Ο ΓΚΠΔ απαριθμεί ορισμένες περιπτώσεις που επιτρέπουν στους οργανισμούς να επεξεργάζονται μια ειδική κατηγορία προσωπικών δεδομένων [20].

Το άρθρο 32 του ΓΚΠΔ εξειδικεύει τις απαιτήσεις για ασφάλεια της επεξεργασίας. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία οφείλουν να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσουν επίπεδο ασφάλειας ανάλογο του κινδύνου, μεταξύ άλλων και κατά περίπτωση:

1. την ψευδωνυμοποίηση και την κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα,

2. την ικανότητα να διασφαλίζεται η συνεχής εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των συστημάτων και υπηρεσιών επεξεργασίας,

3. την ικανότητα έγκαιρης αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε περίπτωση φυσικού ή τεχνικού συμβάντος,

4. διαδικασία για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

Κατά την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας λαμβάνονται υπόψη ιδίως οι κίνδυνοι που ενέχει η επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη κοινοποίηση ή πρόσβαση σε δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται σε άλλη επεξεργασία.

Το άρθρο 32 αναφέρει επίσης ότι ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα για να διασφαλίσουν ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εξουσία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία και έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα δεν τα επεξεργάζεται παρά μόνο κατόπιν οδηγιών του υπευθύνου

επεξεργασίας, εκτός εάν υποχρεούται να το πράξει βάσει του δικαίου της Ένωσης ή του κράτους μέλους.

3.3 Δικαιώματα Φυσικού Προσώπου Σύμφωνα με τον ΓΚΠΔ

Τα υποκείμενα των δεδομένων έχουν κάποια δικαιώματα αναφορικά με την επεξεργασία προσωπικών τους δεδομένων, τα οποία προδιαγράφονται ρητώς στο ΓΚΠΔ. Μία επεξεργασία λοιπόν θα πρέπει να γίνεται με τέτοιο τρόπο ώστε να μπορούν να ικανοποιούνται τα εν λόγω δικαιώματα. Κάποια εκ των βασικών δικαιωμάτων (όχι εξαντλητική λίστα) είναι τα εξής:

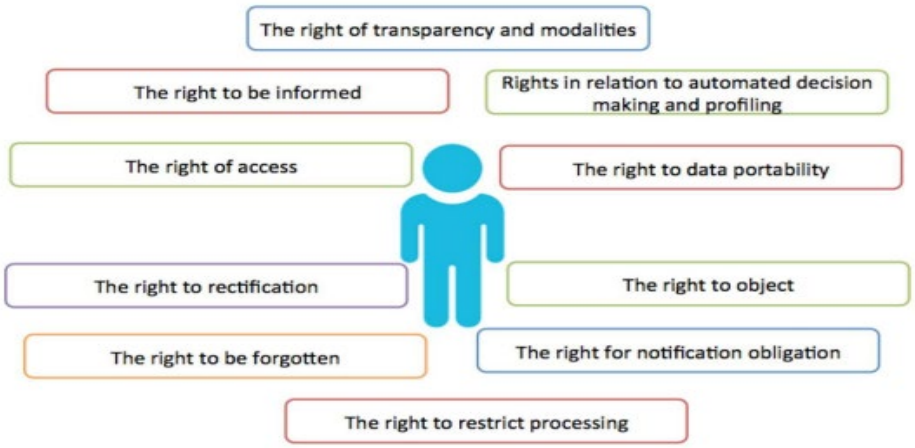
- Το δικαίωμα ενημέρωσης: τα φυσικά πρόσωπα πρέπει να γνωρίζουν αναλυτικά κάθε πτυχή σχετικά με την επεξεργασία των δεδομένων τους(ποιος την κάνει, για ποιο σκοπό, τι δεδομένα αφορά, πώς γίνεται, ποιοι είναι οι αποδέκτες κ.α.)

- Το δικαίωμα πρόσβασης: τα φυσικά πρόσωπα μπορούν ανά πάσα στιγμή να ζητήσουν να μάθουν πληροφορίες αναλυτικά για την επεξεργασία των δεδομένων τους, καθώς και να λάβουν αντίγραφο των δεδομένων αυτών.

- Το δικαίωμα διόρθωσης: τα φυσικά πρόσωπα μπορούν ανά πάσα στιγμή να ζητήσουν διόρθωση για τις εσφαλμένες πληροφορίες που τυχόν τηρεί και επεξεργάζεται ο υπεύθυνος επεξεργασίας.

- Το δικαίωμα διαγραφής: τα φυσικά πρόσωπα μπορούν ανά πάσα στιγμή να ζητήσουν από τους υπευθύνους επεξεργασίας να διαγράψουν τα ληγμένα προσωπικά τους δεδομένα. Επιπλέον, ένα πρόσωπο έχει επίσης το δικαίωμα να αναιρέσει τυχόν συγκατάθεσή του για την επεξεργασία δεδομένων.

Η παρακάτω εικόνα (Εικόνα 3.2) απεικονίζει τα δικαιώματα του φυσικού προσώπου σύμφωνα με τον ΓΚΠΔ.



Εικόνα 3.2: Τα δικαιώματα του φυσικού προσώπου σύμφωνα με το GDPR [21].

3.4 Προκλήσεις του ΓΚΠΔ

Στην ενότητα αυτή παρουσιάζουμε κάποια ειδικά θέματα του ΓΚΠΔ, τα οποία αποτελούν προκλήσεις για τους οργανισμούς και τα οποία σχετίζονται με το αντικείμενο της παρούσας διατριβής.

3.4.1 Κοινοποίηση Παραβίασης Δεδομένων

Το άρθρο 33 του ΓΚΠΔ αναφέρει: "Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας οφείλει χωρίς αδικαιολόγητη καθυστέρηση και, εφόσον είναι εφικτό, το αργότερο εντός 72 ωρών αφότου έχει λάβει γνώση, γνωστοποιεί την παραβίαση δεδομένων προσωπικού χαρακτήρα στην αρμόδια εποπτική αρχή σύμφωνα με το άρθρο 55, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα είναι απίθανο να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η κοινοποίηση στην εποπτική αρχή δεν γίνεται εντός 72 ωρών, συνοδεύεται από τους λόγους της καθυστέρησης [20].

Στις ΗΠΑ υπάρχουν πάνω από 48 διαφορετικοί νόμοι για την κοινοποίηση παραβιάσεων. Η συντομότερη προθεσμία κοινοποίησης είναι 30 ημέρες στη Φλόριντα, και για παράδειγμα, η Νότια Ντακότα απαιτεί 60 ημέρες από την ανακάλυψη της παραβίασης [22]. Η απαίτηση του GDPR είναι

72 ώρες, γεγονός που μετατρέπει τον εντοπισμό ενός προβλήματος σε αγώνα δρόμου ενάντια στο χρόνο από τη στιγμή που ανακαλύφθηκε η παραβίαση. Οι παραβιάσεις ασφαλείας μπορούν να κατηγοριοποιηθούν με τους ακόλουθους τρόπους.

- Παραβίαση εμπιστευτικότητας: μη εξουσιοδοτημένη ή τυχαία πρόσβαση σε δεδομένα.

- Παραβίαση διαθεσιμότητας: τυχαία ή μη εξουσιοδοτημένη απώλεια πρόσβασης σε δεδομένα ή καταστροφή τους.

- Παραβίαση ακεραιότητας: μη εξουσιοδοτημένη ή τυχαία αλλοίωση δεδομένων προσωπικού χαρακτήρα.

Μια παραβίαση δεδομένων μπορεί να αφορά όλες τις προαναφερθείσες κατηγορίες ταυτόχρονα ή οποιοδήποτε συνδυασμό τους.

Περαιτέρω, μία από τις υποχρεώσεις των υπευθύνων επεξεργασίας που επιβάλλει ο ΓΚΠΔ είναι ότι, σε περίπτωση περιστατικού παραβίασης δεδομένων, αν προκύπτουν υψηλοί κίνδυνοι για τα θιγόμενα φυσικά πρόσωπα τότε αυτά θα πρέπει να ενημερωθούν σχετικά. Η υποχρέωση αυτή ισχύει εάν η παραβίαση προκαλεί μεγάλους κινδύνους για τα δικαιώματα και την ελευθερία ενός ατόμου. Οι προαναφερόμενοι κίνδυνοι είναι, για παράδειγμα, οι κλοπές ταυτότητας, οι απάτες με πιστωτικές κάρτες ή άλλες εγκληματικές δραστηριότητες. Η κοινοποίηση δεν είναι υποχρεωτική εάν οι πληροφορίες προσωπικού χαρακτήρα που διέρρευσαν ήταν κρυπτογραφημένες και τα κλειδιά κρυπτογράφησης δεν διέρρευσαν [20].

3.4.2 Προστασία των Δεδομένων ήδη από το σχεδιασμό (Data Protection Design)

Για την προστασία των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων, στη περίπτωση επεξεργασίας δεδομένων προσωπικού χαρακτήρα, απαιτείται η λήψη κατάλληλων μέτρων τεχνικού και οργανωτικού χαρακτήρα, ώστε να διασφαλίζεται η τήρηση των απαιτήσεων του ΓΚΠΔ.

Ο υπεύθυνος επεξεργασίας των δεδομένων θα πρέπει να εφαρμόζει μέτρα τα οποία να ανταποκρίνονται ειδικότερα στις αρχές τις προστασίας των δεδομένων ήδη από το σχεδιασμό. Τέτοια μέτρα μπορούν να περιλαμβάνουν για παράδειγμα :

- Την ελαχιστοποίηση δεδομένων προσωπικού χαρακτήρα.

- Την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα.

- Την διαφάνεια όσον αφορά τις λειτουργίες και την επεξεργασία παρόμοιων δεδομένων.

Βάσει των παραπάνω το υποκείμενο των δεδομένων θα μπορεί να παρακολουθεί την επεξεργασία τους και ο υπεύθυνος επεξεργασίας θα μπορεί να βελτιώνει τα χαρακτηριστικά ασφαλείας.

Οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών θα πρέπει να λαμβάνουν υπόψιν τους το δικαίωμα προστασίας των δεδομένων ήδη από των σχεδιασμό, ώστε βάση των τελευταίων εξελίξεων, τόσο οι υπεύθυνοι επεξεργασίας όσο και οι εκτελούντες την επεξεργασία θα είναι σε θέση να εκπληρώσουν τις υποχρεώσεις τους ως προς την προστασία των δεδομένων.

Τα συστήματα που είναι εξαρχής σχεδιασμένα λανθασμένα, πιθανόν να είναι δύσκολο να μετατραπούν κατάλληλα εκ των υστέρων ώστε να είναι συμβατά με τις απαιτήσεις προστασίας δεδομένων. Όταν σχεδιάζονται και υλοποιούνται χαρακτηριστικά σε μία εφαρμογή, ο ΓΚΠΔ και οι έλεγχοι ασφάλειας πληροφοριών θα πρέπει να λαμβάνονται υπόψιν. Πολλοί οργανισμοί, προγραμματιστές και αναλυτές δεν γνωρίζουν την ύπαρξη προηγμένων κρυπτογραφικών εργαλείων και τεχνικών (PEC) τα οποία μπορούν να δώσουν λύσεις για την προστασία των δεδομένων. Συνεπώς, η εξ αρχής υιοθέτηση και ενσωμάτωση των πλέον κατάλληλων τεχνικών, αν και ουσιαστικά αποτελεί πλέον υποχρέωση βάσει του άρθρου 25 του ΓΚΠΔ, παραμένει στην πράξη μία πρόκληση.

Κεφάλαιο 4
Προηγμένες Κρυπτογραφικές Τεχνικές για Ενίσχυση Ιδιωτικότητας

Ένας όρος που χρησιμοποιείται στο χώρο της ασφάλειας και προστασίας προσωπικών δεδομένων είναι το PET (Privacy Enhancing Technology). PET ονομάζουμε εκείνα τα τεχνικά μέτρα που έχουν ως σκοπό την προστασία των προσωπικών δεδομένων και την προστασία της ιδιωτικότητας, αποτρέποντας έτσι την περιττή ή ανεπιθύμητη επεξεργασία τους και χωρίς να υποβαθμίζεται η λειτουργικότητας ενός πληροφοριακού συστήματος [23].

Συνεπώς όταν χρησιμοποιείται ειδικότερη κρυπτογραφία ως PET τότε μιλάμε για Κρυπτογραφία Ενίσχυσης της Ιδιωτικότητας (PEC), που είναι νέος όρος που εισήγαγε το σχετικό εγχειρίδιο του NIST(Privacy-Enhancing Cryptography CSRC (nist.gov)).Η Ομάδα Τεχνολογιών Κρυπτογραφίας (CTG) στο Τμήμα Ασφάλειας Υπολογιστών (CSD) του NIST ασχολείται με σχετικές τεχνολογίες στον τομέα της κρυπτογραφίας που ενισχύει την ιδιωτικότητα (PEC). Στο πλαίσιο των τεχνολογιών PEC επιδιώκεται η ανάπτυξη εγχειριδίου στο οποίο μπορούν να αναφερθούν οργανισμοί που ασχολούνται με την ανάπτυξη σύγχρονων κρυπτογραφικών εργαλείων για την προστασία των προσωπικών δεδομένων σε αμέτρητες εφαρμογές.

Πράγματι, οι τεχνολογίες κρυπτογράφησης με έμφαση στην ενίσχυση της ιδιωτικότητας (PET) είναι πρωτόκολλα, εφαρμογές και μηχανισμοί που διασφαλίζουν την ιδιωτικότητα των δεδομένων του χρήστη. Οι τεχνολογίες αυτές αποτρέπουν την περιττή επεξεργασία προσωπικών δεδομένων χωρίς να χάνεται η λειτουργικότητα των πληροφοριακών συστημάτων και επικοινωνιών. Οι χρήστες αυτών των συστημάτων προστατεύονται από τη διαρροή των προσωπικών τους δεδομένων και των προσωπικών τους πληροφοριών, ενώ – αναλόγως την τεχνολογία – μπορούν να ικανοποιούνται και πρόσθετες απαιτήσεις, όπως ελαχιστοποίηση των δεδομένων, μη δυνατότητα αναγνώρισης χρήστη κ.α. Τα PET μπορούν να προστατεύουν την

ιδιωτικότητα σε διάφορα επίπεδα, κυρίως στο επίπεδο δικτύου, στο επίπεδο μεταφοράς και στο επίπεδο εφαρμογής [24].

Ουσιαστικά, η κλασική κρυπτογραφία που είδαμε στο Κεφάλαιο 2 εστιάζει σε πτυχές της ασφάλειας επικοινωνιών, όπως η εμπιστευτικότητα, η ακεραιότητα δεδομένων και η αυθεντικοποίηση. Οι προηγμένες κρυπτογραφικές τεχνικές που εντάσσονται στην κατηγορία PEC εστιάζουν (και) σε άλλους στόχους οι οποίοι είναι προσανατολισμένοι στην προστασία προσωπικών δεδομένων και στην ιδιωτικότητα: για παράδειγμα, διασφαλίζουν ότι αποκαλύπτεται η απολύτως απαραίτητη πληροφορία σε νόμιμους παραλήπτες και όχι περισσότερη από ό,τι χρειάζεται. Πιο συγκεκριμένα, υπάρχουν περιπτώσεις όπου μία οντότητα πρέπει να κάνει μαθηματικούς υπολογισμούς για να παράγει ένα αποτέλεσμα (π.χ. άθροισμα ή μέσο όρο), αλλά δεν θέλουμε η οντότητα αυτή να αποκτήσει πρόσβαση στις τιμές εκείνες οι οποίες υπεισέρχονται στους υπολογισμούς: ένα τέτοιο πρόβλημα δεν μπορεί να λυθεί με την κλασική κρυπτογραφία.

Άλλο παράδειγμα, το οποίο σχετίζεται με την απόκρυψη της ταυτότητας ενός χρήστη, είναι οι κοινόχρηστοι λογαριασμοί. Αυτή η απλή μέθοδος μπορεί να υλοποιηθεί εύκολα με τη δημιουργία ενός ψεύτικου διαδικτυακού λογαριασμού που είναι κοινή προς χρήση από μια ομάδα χρηστών. Ο δημιουργός του λογαριασμού συμπληρώνει μια φόρμα με τις απαιτούμενες πληροφορίες με ψεύτικα στοιχεία για το όνομα, τη διεύθυνση, τον αριθμό τηλεφώνου, τις προτιμήσεις κ.λπ. Στη συνέχεια, ο δημιουργός στέλνει το αναγνωριστικό χρήστη (π.χ. Login) και τον κωδικό πρόσβασης στους χρήστες. Οι χρήστες που χρησιμοποιούν αυτόν τον κοινόχρηστο λογαριασμό δεν αποκαλύπτουν την ταυτότητά τους και τις προσωπικές τους πληροφορίες.

Γενικά, ως τεχνολογίες ενίσχυσης της ιδιωτικότητας, μπορούν να εφαρμοστούν μέθοδοι που εστιάζουν στην ελάχιστη χρήση δεδομένων αλλά διασφαλίζουν την ορθή λειτουργία των συστημάτων. Κρατούν στο ελάχιστο τα προσωπικά δεδομένα που συλλέγονται σε ηλεκτρονικά συστήματα και χρησιμοποιούνται από τους παρόχους διαφόρων υπηρεσιών. Τα δεδομένα διαγράφονται αυτόματα εντός ορισμένου χρονικού διαστήματος και οι χρήστες μπορούν να διαπραγματευτούν τα είδη των προσωπικών δεδομένων που αποστέλλονται στα συστήματα.

Μερικές φορές, οι χρήστες μπορούν να επιθεωρούν, να διαγράφουν και να διορθώνουν τα προσωπικά τους δεδομένα, αλλά σύμφωνα με τους συμφωνηθέντες όρους.

Περαιτέρω, η εισαγωγή «θορύβου» («θόλωμα») είναι μία τεχνική που χρησιμοποιείται ιδιαίτερα στις υπηρεσίες που βασίζονται στην τοποθεσία. Για παράδειγμα, η τοποθεσία χρησιμοποιείται ευρύτερα από εφαρμογές και υπηρεσίες μέσω κινητών τηλεφώνων. Ο εντοπισμός της πραγματικής θέσης των χρηστών μπορεί να παραβιάσει την ιδιωτική τους ζωή. Η τεχνική του «θολώματος» ενισχύει ελαφρώς την ιδιωτικότητα των χρηστών και δεν επιβαρύνει τις εφαρμογές που κάνουν χρήση του εντοπισμού θέσης. Από την άλλη πλευρά, οι χρήστες δεν μπορούν να εντοπιστούν με ακρίβεια λόγω αυτής της προσέγγισης.

Στη συνέχεια περιγράφονται συγκεκριμένοι τομείς στους οποίους μπορούν να εφαρμοστούν τεχνολογίες ενίσχυσης της ιδιωτικότητας, με αναφορά στα βασικά χαρακτηριστικά των τεχνολογιών αυτών.

4.1 PEC Εργαλεία

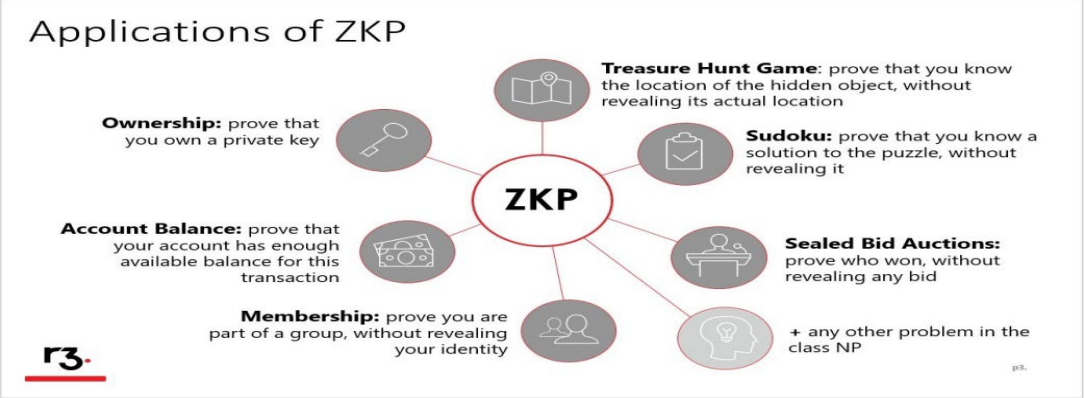
Υπάρχουν διάφορα κρυπτογραφικά πρωτόκολλα, τεχνικές και πρωτόκολλα που ενδιαφέρουν τις εφαρμογές ενίσχυσης της ιδιωτικότητας. Μπορούν να συμβάλλουν στην ιδιωτικότητα σε περιπτώσεις όπου αυτό θα ήταν δύσκολο να γίνει, σε περιβάλλοντα όπου διαφορετικά (χωρίς PEC) μπορεί να μην υπάρχει εμπιστοσύνη για τη συμμετοχή σε τέτοιες διαδικασίες, ή να μην είναι σε θέση να ανταποκριθούν στις κανονιστικές απαιτήσεις προστασίας της ιδιωτικής ζωής.

Για παράδειγμα, οι αποδείξεις μηδενικής γνώσης (ZKPs) επιτρέπουν σε ένα μέρος (τον ελεγκτή) να αποδείξει σε ένα άλλο μέρος (τον επαληθευτή) ότι μια δεδομένη δήλωση είναι αληθής ή/και ότι η λύση κάποιου μαθηματικού προβλήματος είναι γνωστή στον ελεγκτή, χωρίς να αποκαλύπτει καμία πληροφορία για την ίδια τη λύση.

Οι αποδείξεις μηδενικής γνώσης (Zero Knowledge Proofs–ZKPs) είναι ένα από τα παραδείγματα των καλύτερων τεχνολογιών ενίσχυσης της ιδιωτικότητας στη σημερινή εποχή. Τα ZKPs είναι στην πραγματικότητα κρυπτογραφικές μέθοδοι που επιτρέπουν σε ένα μέρος να αποδείξει ότι γνωρίζει ένα γεγονός σε ένα άλλο μέρος. Είναι ενδιαφέρον ότι το πρώτο μέλος δεν χρειάζεται να αποκαλύψει στο δεύτερο μέλος καμία πρόσθετη πληροφορία σχετικά με το γεγονός.

Για παράδειγμα, τα ZKPs θα μπορούσαν να βοηθήσουν στην απόδειξη της ηλικίας ενός ατόμου (ότι δηλαδή, π.χ., είναι πάνω από ένα ελάχιστο επιτρεπτό όριο) χωρίς να αποκαλύπτουν τις

προσωπικές του πληροφορίες, όπως η ημερομηνία γέννησης. Υποστηρίζουν την ελαχιστοποίηση αλλά και την εμπιστευτικότητα των δεδομένων. Επιπλέον, τα ZKPs εξασφαλίζουν επίσης την ενσωμάτωση της ιδιωτικότητας ως προεπιλεγμένου στοιχείου στο σχεδιασμό συναλλαγών σε τεχνολογίες blockchain (για παράδειγμα, ένα μέλος μπορεί να αποδεικνύει ότι είναι σε θέση να πραγματοποιήσει μία συναλλαγή χωρίς να αποκαλύπτει κάτι περισσότερο όπως, π.χ., το πραγματικό ποσό που διαθέτει).



Εικόνα 4.1: Εφαρμογές του ZKP[25].

Μία άλλη κατηγορία προηγμένης κρυπτογράφησης για ενίσχυση της ιδιωτικότητας είναι τα πρωτόκολλα, ο ασφαλούς υπολογισμού πολλαπλών μερών SMPC (Secure Multiparty Computation) ή MPC (Multiparty Computation) : τα πρωτόκολλα αυτά επιτρέπουν σε πολλαπλά μέρη, συχνά χωρίς αμοιβαία εμπιστοσύνη, να υπολογίζουν κάποια ιδιότητα των κοινών δεδομένων τους, σαν να είχε υπολογιστεί από ένα αξιόπιστο τρίτο μέρος χωρίς να αποκαλύπτουν αυτά καθαυτά τα δεδομένα τους [26].

Ειδικότερα, τα SMPC είναι πρωτόκολλα που επιτρέπουν σε δύο ή περισσότερα μέρη να εκτελέσουν έναν υπολογισμό που περιλαμβάνει και τα δύο σύνολα δεδομένων τους με τέτοιο τρόπο ώστε κανένα μέρος να μην χρειάζεται να παραδώσει ρητά ένα σύνολο δεδομένων σε κάποιο από τα άλλα. Επειδή τα πρωτόκολλα SMPC επιτρέπουν τον υπολογισμό ερωτημάτων χωρίς την ανάγκη για την αποθήκευση όλων των δεδομένων να είναι συγκεντρωτική, μειώνει τη ζημία από την παραβίαση των δεδομένων και επιτρέπει υπολογισμούς μεταξύ μερών που δεν εμπιστεύονται πλήρως το ένα το άλλο. Θεωρητικά, μπορεί να συνδυαστεί με διάφορες άλλες τεχνολογίες ενίσχυσης ιδιωτικότητας.

Αυτό σημαίνει ότι ο υπολογισμός γίνεται χωρίς να μοιράζονται τις παραμέτρους και εξασφαλίζοντας ταυτόχρονα έγκυρο αποτέλεσμα μίας διαδικασίας.

Ως άλλο παράδειγμα τεχνολογίας PEC, η πλήρως ομομορφική κρυπτογράφηση FHE (Fully Homomorphic Encryption) επιτρέπει την εκτέλεση υπολογισμών σε κρυπτογραφημένα δεδομένα χωρίς να χρειάζεται να γίνει αποκρυπτογράφηση, η οποία με τη σειρά της μπορεί να χρησιμοποιηθεί για την ανάθεση υπολογισμών σε μη αξιόπιστα μέρη. Άλλα εργαλεία PEC περιλαμβάνουν ομαδικές υπογραφές, κρυπτογράφηση με δυνατότητα αναζήτησης, ανάκτηση ιδιωτικών πληροφοριών, διασταύρωση ιδιωτικών συνόλων και λειτουργική κρυπτογράφηση.

Η έννοια των συστημάτων ομαδικής υπογραφής (group signatures)έχει προταθεί από τους Chaum and Van Heyst(Heyst, 1991)και επιτρέπει στα μέλη μιας προκαθορισμένης ομάδας να υπογράφουν ανώνυμα μηνύματα για λογαριασμό της ομάδας. Με τον τρόπο αυτό, οι υπογράφοντες αποδεικνύουν σιωπηρά και ανώνυμα την ιδιότητα του μέλους της ομάδας αλλά όχι την πραγματική τους ταυτότητα. Οι επαληθευτές με τη σειρά τους μπορούν να προσδιορίσουν αν μια υπογραφή έχει πράγματι παραχθεί από μέλος της ομάδας, αλλά δεν είναι σε θέση να προσδιορίσουν την πραγματική ταυτότητα ενός υπογράφοντος. Ωστόσο, σε περίπτωση διαφωνίας, ο λεγόμενος διαχειριστής ομάδας (GM) είναι σε θέση να ανοίξει μια δεδομένη υπογραφή ομάδας(GS) προκειμένου να προσδιορίσει την ταυτότητα του πραγματικού υπογράφοντος.

Τα σημερινά μειονεκτήματα των ομαδικών υπογραφών είναι το υπολογιστικό κόστος και οι μεγάλες υπογραφές. Οι βασικές φάσεις, δηλαδή η υπογραφή και η επαλήθευση, των σχημάτων ομαδικών υπογραφών είναι πιο δαπανηρές από ό,τι οι φάσεις των κοινών σχημάτων ψηφιακής υπογραφής, όπως τα RSA, DSA ή ECDSA. Είναι δύσκολο να υλοποιηθούν τα σχήματα ομαδικής υπογραφής σε υπολογιστικά περιορισμένες συσκευές.

4.2 Προηγμένες Τεχνικές Κρυπτογράφησης

Στην Ενότητα αυτή δίνεται μία περαιτέρω έμφαση σε κάποιες προηγμένες τεχνικές κρυπτογράφησης που μπορούν να δώσουν απαντήσεις σε προκλήσεις όχι μόνο ασφάλειας αλλά και προστασίας προσωπικών δεδομένων.

4.2.1 Κρυπτογράφηση με Δυνατότητα Αναζήτησης (Searchable Encryption)

Η κρυπτογράφηση με δυνατότητα αναζήτησης (Searchable Encryption - SE) δίνει στον χρήστη τη δυνατότητα να εκτελέσει ένα ερώτημα αναζήτησης χωρίς να αποκρυπτογραφήσει τα περιεχόμενα του αρχείου. Η βασική ιδέα πίσω από μια SE είναι η εξαγωγή των λέξεων – κλειδιών από τα αρχεία απλού κειμένου. Με βάση τις εξαγόμενες λέξεις-κλειδιά δημιουργείται ένα ευρετήριο. Τα αρχεία κρυπτογραφούνται μαζί με το σχετικό ευρετήριο και αποστέλλονται και τα δύο στο χώρο αποθήκευσης. Αργότερα, όταν ο χρήστης θέλει να αναζητήσει μια λέξη – κλειδί, δημιουργεί μια παράμετρο (trapdoor) με βάση τη λέξη – κλειδί αναζήτησης, έτσι ώστε ο διακομιστής να μην μάθει τη λέξη – κλειδί που αναζητείται. Αυτή η παράμετρος trapdoor στη συνέχεια αποστέλλεται στον διακομιστή. Ο διακομιστής αναζητά την παράμετρο trapdoor στο ασφαλές ευρετήριο και επιστρέφει τα αντίστοιχα κρυπτογραφημένα αρχεία [27].

Η ασφάλεια προς τα εμπρός και προς τα πίσω (forward and backward security) είναι μία σημαντική ιδιότητα της κρυπτογράφησης με δυνατότητα αναζήτησης για τον μετριασμό των επιθέσεων που αποσκοπούν στη κλοπή δεδομένων, διασφαλίζοντας ότι[27]:

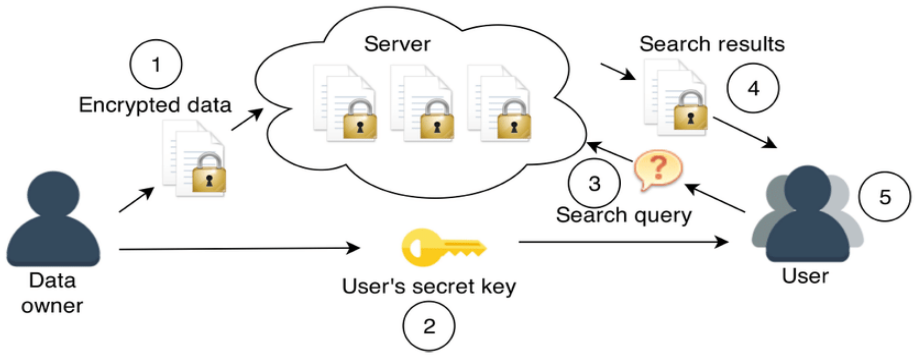
1. Οι νέες ενημερωμένες καταχωρήσεις δεν μπορούν να συνδεθούν με την προηγούμενη ενημέρωση και τα ερωτήματα αναζήτησης (που ονομάζεται ασφάλεια προς τα εμπρός), και

2. Οι διαγραμμένες καταχωρήσεις δεν μπορούν να βρεθούν από τα επόμενα ερωτήματα αναζήτησης (και ονομάζεται ασφάλεια προς τα πίσω).

Συγκεκριμένα, η προς τα πίσω ασφάλεια αντιμετωπίζει τρεις διαφορετικούς τύπους διαρροής δεδομένων (Τύπος I έως Τύπος-III με σειρά από το πιο ασφαλές προς το λιγότερο ασφαλές). Η ασφάλεια προς τα εμπρός απαιτεί την προσθήκη ενός νέου αρχείου για να μην αποκαλυφθεί η παρουσία μιας λέξης – κλειδιού που έχει ήδη αναζητηθεί. Η ασφάλεια προς τα πίσω απαιτεί η αναζήτηση να μην επιστρέφει κανένα αναγνωριστικό αρχείου, προερχόμενο από αρχείο που είχε διαγραφεί προηγουμένως. Με βάση αυτές τις αρχές σχεδιάστηκαν στο παρελθόν ορισμένα γνωστά συστήματα κρυπτογράφησης με δυνατότητα αναζήτησης για την επίτευξη ασφάλειας προς τα εμπρός και προς τα πίσω, ενώ επιτυγχάνοντας ταυτόχρονα όσο το δυνατόν μεγαλύτερη αποδοτικότητα(π.χ.Moneta, Fides, Diana, Janus, MITRA, ORION, HORUS, FB-DSSE, SD, QOS, Aura, ROSE, κ.α) [27].

Πολλά σχήματα SE έχουν προταθεί, συμπεριλαμβανομένων σχημάτων συμμετρικής κρυπτογράφησης με δυνατότητα αναζήτησης (SSE) και σχημάτων κρυπτογράφησης δημόσιου

κλειδιού με αναζήτηση λέξεων-κλειδιών (PEKS). Ωστόσο, αυτά τα σχήματα περιορίζονται κυρίως στη ρύθμιση ενός χρήστη, η οποία επιτρέπει μόνο σε έναν χρήστη να πραγματοποιεί αναζήτηση λέξεων – κλειδιών και να έχει πρόσβαση στα κρυπτογραφημένα δεδομένα. Αυτά τα σχήματα τα ονομάζουμε «κρυπτογράφηση με δυνατότητα αναζήτησης ενός χρήστη (SUSE)». Στην πραγματικότητα, η αναζήτηση λέξεων – κλειδιών σε ρύθμιση πολλών χρηστών είναι ένα πιο συνηθισμένο σενάριο, π.χ. ένας χρήστης που κατέχει μια συλλογή εγγράφων θα ήθελε να τα μοιραστεί με μια ομάδα εξουσιοδοτημένων χρηστών. Την αναζήτηση λέξεων – κλειδιών σε ρύθμιση πολλών χρηστών την αποκαλούμε ως «κρυπτογράφηση με δυνατότητα αναζήτησης πολλών χρηστών (MUSE)» [28].



Εικόνα 4.2: Τεχνική Συμμετρικής Κρυπτογράφησης με Δυνατότητα Αναζήτησης

Τα αρχικά προτεινόμενα σχήματα SE ήταν στατικής φύσης. Μόλις δημιουργείται το ασφαλές ευρετήριο, ο χρήστης δεν μπορούσε να προσθέσει ή να διαγράψει ένα αρχείο χωρίς να αναδημιουργήσει ολόκληρο το ευρετήριο. Αργότερα αναπτύχθηκαν σχήματα δυναμικής κρυπτογράφησης με δυνατότητα αναζήτησης (Dynamic Searchable Encryption - DSE) που έδιναν στον κάτοχο των δεδομένων τη δυνατότητα να προσθέσει ή να διαγράψει ένα αρχείο μετά τη δημιουργία του ασφαλούς ευρετηρίου. Η ενημέρωση ενός αρχείου σε αυτά τα σχήματα δεν απαιτεί την εκ νέου δημιουργία του ασφαλούς ευρετηρίου [28].

Οι επικρατέστερες τεχνικές για τον εμπλουτισμό των ερωτημάτων περιλαμβάνουν τη τεχνική της συζευκτικής αναζήτησης με λέξεις-κλειδιά ή συζευκτικής αναζήτησης με φράσεις. Σε σχετικές επεκτάσεις σε περιβάλλον πολλαπλών χρηστών, μπορούν μόνο οι εξουσιοδοτημένοι χρήστες να εκτελούν SE αναζήτηση [29].

Επιπρόσθετα, τα σχήματα κρυπτογράφησης με δυνατότητα αναζήτησης σε περιβάλλον πολλαπλών χρηστών πρέπει να χειριστούν το πρόβλημα της δυναμικής εισαγωγής και διαγραφής

χρήστη. Αυτό πρέπει να συμβεί για να υπάρχει η βεβαιότητα ότι η διαγραφή ενός χρήστη δεν θα προκαλέσει ζητήματα ασφαλείας, όπως διαρροή μυστικού κλειδιού. Πιο πρόσφατα, προτάθηκε ένας λεπτομερής έλεγχος πρόσβασης με χρήση αξιόπιστου τρίτου μέρους για την επίλυση αυτού του ζητήματος, που ωστόσο αυξάνει την πολυπλοκότητα διαχείρισης για τη διατήρηση μαζικών πληροφοριών ελέγχου ταυτότητας των χρηστών [29].

Η κρυπτογράφηση με δυνατότητα αναζήτησης επιτρέπει στον χρήστη να πραγματοποιήσει αναζήτηση στα κρυπτογραφημένα αρχεία που περιέχουν ορισμένες λέξεις-κλειδιά, αλλά αποκαλύπτει όσο το δυνατόν λιγότερες πληροφορίες στον χρήστη. Καθώς το υπολογιστικό νέφος (cloudcomputing) γίνεται διαδεδομένο, όλο και περισσότερες ευαίσθητες πληροφορίες συγκεντρώνονται στο σύννεφο. Για αυτό το λόγο η κρυπτογράφηση με δυνατότητα αναζήτησης χρησιμοποιείται ευρέως για την προστασία του απορρήτου των δεδομένων του χρήστη στο cloud [28].

4.2.2 Συμμετρική Κρυπτογράφηση που Διατηρεί τη Διάταξη(Order Preserving Encryption)

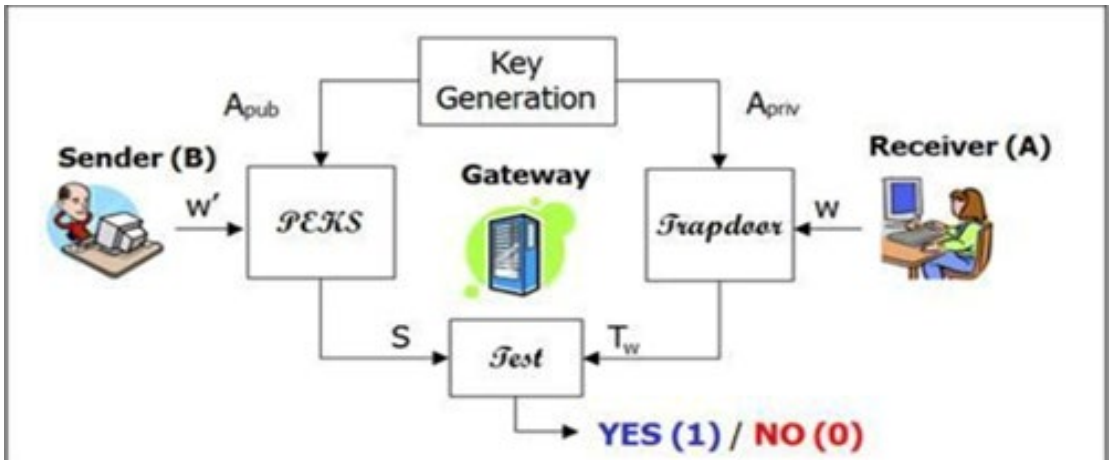
Ένα σχήμα συμμετρικής κρυπτογράφησης που διατηρεί τη διάταξη (Order Preserving Encryption - OPE) είναι ένα ντετερμινιστικό σχήμα συμμετρικής κρυπτογράφησης του οποίου ο αλγόριθμος κρυπτογράφησης παράγει κρυπτογραφημένα κείμενα που διατηρούν την αριθμητική σειρά των απλών κειμένων. Η πρώτη επίσημη κρυπτογραφική επεξεργασία της OPE εμφανίστηκε στην εργασία των Boldyreva and Chenette. Οι συγγραφείς επισημοποίησαν μια απαίτηση ασφαλείας για την OPE και πρότειναν ένα αποτελεσματικό σύστημα που βασίζεται σε μπλοκ κρυπτογράφησης που αποδεδειγμένα ανταποκρίνεται στον ορισμό ασφαλείας τους [30].

Εφαρμογές:

Η OPE τεχνική έχει πολλές εφαρμογές. Κύρια εφαρμογή είναι οι βάσεις δεδομένων που προσφέρονται ως υπηρεσία DAS(Database as a service). Στο DAS η βάση δεδομένων ανατίθεται σε εξωτερικούς συνεργάτες στο υπολογιστικό νέφος και οι αποθηκευμένες τιμές κρυπτογραφούνται πριν σταλούν σε αυτό. Στη συνέχεια, η βάση δεδομένων εκτελεί τα ερωτήματά της σε κρυπτογραφημένα δεδομένα. Συνεπώς, ο πάροχος του αποθηκευτικού μέσου μπορεί να ανταποκρίνεται σε ερωτήματα επί της βάσης δεδομένων που τηρεί, χωρίς να έχει πρόσβαση στο περιεχόμενο της βάσης. Η OPE επιτρέπει την εκτέλεση ερωτημάτων εύρους σε μια

κρυπτογραφημένη βάση δεδομένων χωρίς αλλαγές στο σύστημα διαχείρισης της βάσης δεδομένων [30].

Εκτός από τις βάσεις δεδομένων, η OPE τεχνική έχει πολλές εφαρμογές σε γενικά λογισμικά στο υπολογιστικό νέφος ως υπηρεσίες και εφαρμογές διαδικτύου, π.χ. επιχειρηματικό λογισμικό και ηλεκτρονικό ταχυδρομείο [30].



Εικόνα 4.3: Order Preserving Encryption (OPE).

4.2.3 Ομομορφική Κρυπτογράφηση (Homomorphic Encryption)

Η χρήση του υπολογιστικού νέφους έχει αυξηθεί γρήγορα σε πολλούς οργανισμούς καθώς προσφέρει οφέλη στους χρήστες, όσον αφορά την άμεση διαθεσιμότητα, την επεκτασιμότητα και την κοινή χρήση πόρων. Πολλοί οργανισμοί διστάζουν να αξιοποιήσουν πλήρως τα οφέλη του υπολογιστικού νέφους, επικαλούμενοι ανησυχίες σχετικά με την απώλεια δεδομένων και τη μη εξουσιοδοτημένη πρόσβαση και διστάζουν να βασιστούν σε παρόχους στο υπολογιστικό νέφος για την επίλυση αυτών των προκλήσεων [31].

Η ανάπτυξη συστημάτων αποθήκευσης στο υπολογιστικό νέφος, όπως το Dropbox και οι πλατφόρμες υπολογιστών, δίνει τη δυνατότητα στους χρήστες να αναθέτουν σε τρίτους την αποθήκευση και τους υπολογισμούς των δεδομένων τους και στην συνέχεια να επιτρέπουν στις επιχειρήσεις να αναθέτουν σε υπηρεσίες στο υπολογιστικό νέφος τον αυξανόμενο όγκο

αποθήκευσης και διαχείρισης δεδομένων. Αν και συνεχώς κερδίζουν έδαφος αυτά τα πλεονεκτήματα της χρήσης του υπολογιστικού νέφους, οι χρήστες πρέπει να γνωρίζουν τα πιθανά μειονεκτήματα της χρήσης των υπηρεσιών στο υπολογιστικό νέφος που είναι η απώλεια του ιδιωτικού απορρήτου και η επιχειρηματική αξία των εμπιστευτικών δεδομένων.

Μια αποτελεσματική μέθοδος αντιμετώπισης αυτών των προβλημάτων είναι η κρυπτογράφηση όλων των δεδομένων που είναι αποθηκευμένα στο σύννεφο και η εκτέλεση λειτουργιών στα κρυπτογραφημένα δεδομένα χωρίς ο πάροχος του σύννεφου να μάθει τίποτα για τα δεδομένα των χρηστών. Για την αντιμετώπιση αυτών των ζητημάτων, έχουν επινοηθεί ορισμένα προηγμένα κρυπτογραφικά σχήματα. Μία από αυτές τις τεχνικές είναι η ομομορφική κρυπτογράφηση [31].

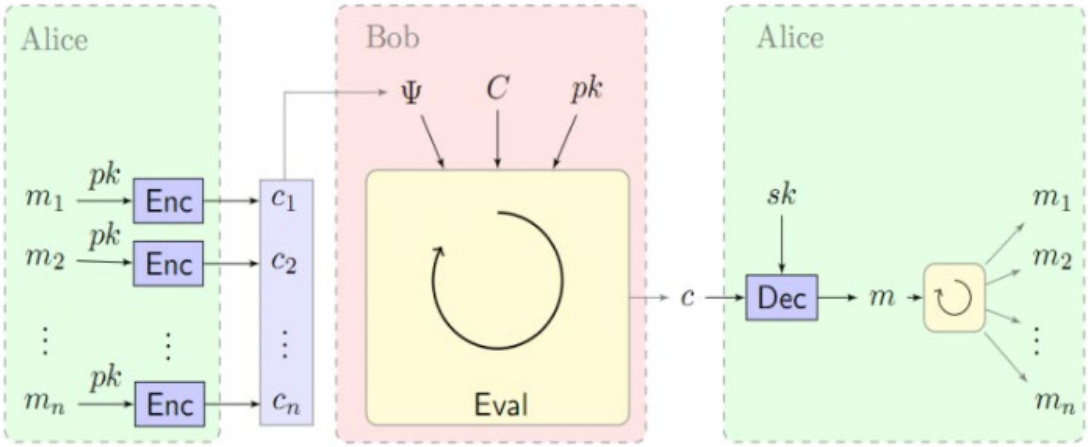
Κατηγορίες Ομομορφικής Κρυπτογράφησης:

Οι τρεις γενικές κατηγορίες ομομορφικής κρυπτογράφησης είναι οι εξής

- Μερικώς Ομομορφική Κρυπτογράφηση (Partially Homomorphic Encryption (PHE)): είναι το σχήμα κρυπτογράφησης που έχει ομομορφική ιδιότητα που υποστηρίζει έναν και μόνο έναν τύπο πράξεων είτε πρόσθεσης είτε πολλαπλασιασμού.

- Εν μέρει ομομορφική κρυπτογράφηση(Somewhat Homomorphic Encryption (SHE)): είναι το σχήμα κρυπτογράφησης που έχει την ομομορφική ιδιότητα που υποστηρίζει περιορισμένο αριθμό προσθηκών και πράξεων πολλαπλασιασμού.

- Πλήρως ομομορφική κρυπτογράφηση(Fully Homomorphic Encryption (FHE)): είναι ένα σχήμα ομομορφικής κρυπτογράφησης που μπορεί να εκτελέσει έναν αυθαίρετο αριθμό πράξεων πρόσθεσης και πολλαπλασιασμού.



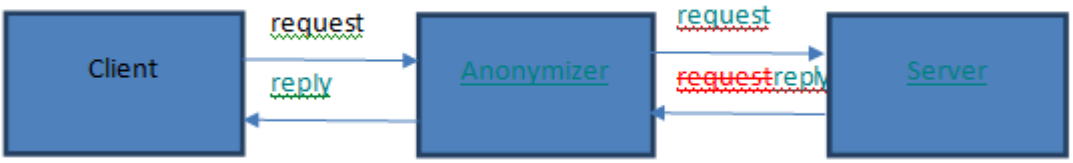
Εικόνα 4.4: Σχήμα Ομομορφικής Κρυπτογράφησης.

4.3 Τεχνικές Δρομολόγησης και Επικοινωνίας με Ενίσχυση Ιδιωτικότητας

Η διαδικτυακή επικοινωνία έχει γίνει πλήρως διαδραστική και σε πραγματικό χρόνο με τη χρήση τεχνολογιών ΤΠΕ όπως τα άμεσα μηνύματα, ο παγκόσμιος ιστός, οι απομακρυσμένες συνδέσεις, το Voice-Over-IP (VoIP), παιχνίδια, κοινωνικές και γεωκοινωνικές διαδικτυακές υπηρεσίες. Οι λεγόμενοι ανωνυμοποιητές επικοινωνίας(communication anonymizer) αποκρύπτουν την πραγματική διαδικτυακή ταυτότητα, όπως μια διεύθυνση ηλεκτρονικού ταχυδρομείου, μια διεύθυνση IP κ.λπ. Οι πραγματικές ταυτότητες των χρηστών αντικαθίστανται από μη ανιχνεύσιμες ταυτότητες, όπως email διευθύνσεις μιας χρήσης, ψευδώνυμα, μια τυχαία IP ενός κεντρικού υπολογιστή από ένα ανώνυμο δίκτυο κ.λπ. Η ανωνυμοποίηση μπορεί να γίνει στο επίπεδο δικτύου και στο επίπεδο εφαρμογής .Η ανωνυμοποίηση στο επίπεδο δικτύου βασίζεται συνήθως στην ανώνυμη δρομολόγηση. Εκεί υπάρχουν συστήματα όπως το TOR που παρέχουν ανώνυμη δρομολόγηση και προστατεύουν το απόρρητο των πηγών. Εκτός από τη μονόδρομη ανώνυμη επικοινωνία, κατά την οποία ο αποστολέας μηνύματος μιας επικοινωνίας δεν μπορεί να αναγνωριστεί, υπάρχει και η αμφίδρομη ανώνυμη επικοινωνία όπου τόσο ο αποστολέας όσο και ο παραλήπτης δεν μπορούν να αναγνωριστούν[32].

Μία απλή προσέγγιση είναι η χρήση Proxy Anonymizer και βασίζεται στη χρήση διακομιστών μεσολάβησης. Ένας διακομιστής μεσολάβησης λειτουργεί ως μεσάζων που αποστέλλει εκ νέου

μηνύματα από έναν πελάτη σε έναν παραλήπτη. Η πηγή του πελάτη αντικαθίσταται από τη διεύθυνση προέλευσης του μεσάζοντα. Με τον τρόπο αυτό, ο διακομιστής μεσολάβησης δημιουργεί ένα ιδιωτικό κανάλι, ώστε ο παραλήπτης να μην είναι σε θέση να διακρίνει ποιος είναι ο αποστολέας του λαμβανόμενου μηνύματος και ποιος στέλνει μηνύματα στον διακομιστή μεσολάβησης. Ο διακομιστής μεσολάβησης (proxy anonymizer) αποστέλλει εκ νέου τις απαντήσεις στους πελάτες. Για να αυξηθεί η ασφάλεια, η επικοινωνία μεταξύ των πελατών και των διακομιστών μεσολάβησης μπορεί επιπροσθέτως να είναι κρυπτογραφημένη [33].



Εικόνα 4.5: Πρότυπο του Proxy Anonymizer.

Ο διακομιστής μεσολάβησης πρέπει να είναι μια έμπιστη οντότητα επειδή είναι σε θέση να συνδέει συνεδρίες και να διαβάζει το περιεχόμενο των μηνυμάτων. Αυτή η ιδιότητα αποτελεί αδυναμία αυτής της προσέγγισης που μπορεί να καλυφθεί με τη χρήση μεθόδων όπως τα « Crowd systems». Τα συστήματα αυτά βασίζονται στην ομάδα πολλών χρηστών. Ένας χρήστης μπορεί απλά να συμπεριληφθεί σε ένα πλήθος χρηστών. Τα μηνύματα αποστέλλονται ανώνυμα από τους αποστολείς στους παραλήπτες λόγω του γεγονότος ότι τα μηνύματα αναμεταδίδονται από τους χρήστες που ανήκουν στο ίδιο πλήθος. Η διαδρομή του αναμεταδιδόμενου μηνύματος είναι τυχαία αλλά μπορεί να είναι και άμεση. Ένας επιτιθέμενος δεν είναι σε θέση να εντοπίσει τον αποστολέα του μηνύματος – το μόνο που μπορεί να εντοπίσει είναι το πλήθος των χρηστών, ένας εκ των οποίων έστειλε το μήνυμα, χωρίς να ξέρει ποιος [33].

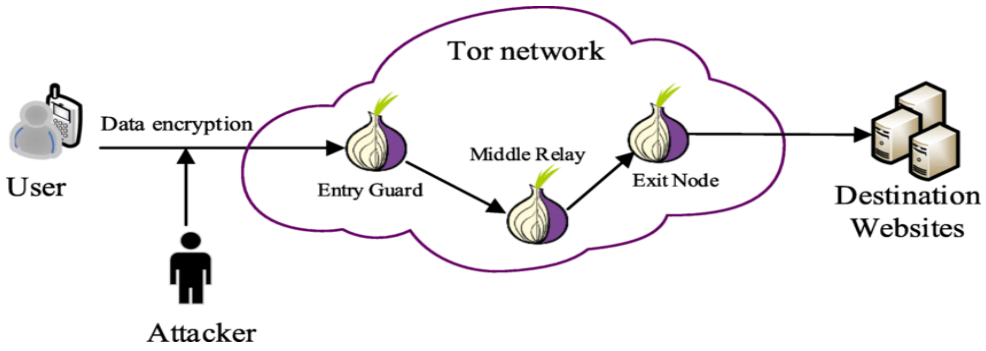
Μια μεγαλύτερη ομάδα χρηστών παρέχει ισχυρότερη ανωνυμία. Στο σενάριο αυτό, οι χρήστες δεν χρειάζεται να εμπιστεύονται μία μόνο οντότητα (π.χ. έναν διακομιστή μεσολάβησης). Από την άλλη πλευρά, αυτός ο μηχανισμός επιβαρύνει την επικοινωνία στην υποδομή του δικτύου επειδή ένα μήνυμα αναμεταδίδεται σε πολλά μονοπάτια. Ο μηχανισμός του πλήθους μπορεί να εφαρμοστεί, για παράδειγμα, στις συναλλαγές στο διαδίκτυο.

Ένας εναλλακτικός μηχανισμός για συναλλαγές στο διαδίκτυο που ονομάζεται Web Mixes, παρέχει ανωνυμία και μη παρατηρησιμότητα. Η μη παρατηρησιμότητα εξασφαλίζει ότι κανείς, ούτε καν το δίκτυο μεταφοράς, δεν είναι σε θέση να προσδιορίσει ποιος επικοινωνεί με ποιον. Το

σύστημα αυτό είναι μια δομή από διάφορες οντότητες MIX, οι οποίες ελέγχονται από διαφορετικούς οργανισμούς. Μια οντότητα MIX μπορεί να είναι ένας απλός υπολογιστής συνδεδεμένος μέσω του Διαδικτύου. Η οντότητα MIX κωδικοποιεί και αναδιατάσσει την κυκλοφορία. Οι αποστολείς κρυπτογραφούν τα δεδομένα τους σταθερού μεγέθους και τα αποστέλλουν σεμια οντότητα MIX. Η οντότητα MIX λαμβάνει δεδομένα από όλους τους αποστολείς, αποκρυπτογραφεί και τα αναδιατάσσει. Στη συνέχεια, τα δεδομένα αυτά περνούν από μια κλιμάκωση (αλυσίδα) οντοτήτων MIX. Κατά τη διάρκεια αυτής της διαδικασίας, αυτές οι οντότητες MIX πραγματοποιούν κάποιες κρυπτογραφικές πράξεις. Η τελευταία οντότητα MIX αποστέλλει τα δεδομένα σε έναν διακομιστή cache-proxy, ο οποίος επικοινωνεί με παραλήπτες, όπως webservers. Για την ενίσχυση της ιδιωτικότητας, οι αποστολείς μπορούν να προσθέσουν εικονικά μηνύματα (τυχαία δεδομένα)εάν δεν έχουν μηνύματα να στείλουν.

Από την άλλη πλευρά, εφαρμόζεται συχνά στις μέρες μας το πρωτόκολλο TOR. Το πρωτόκολλο TOR είναι μια πρακτική εφαρμογή που χρησιμοποιεί τη λεγόμενη «onion» δρομολόγηση. Τα μηνύματα αναμεταδίδονται από μια ακολουθία κόμβων δικτύου που ονομάζονται onion δρομολογητές που λειτουργούν ως πληρεξούσιοι. Για την αποτροπή της υποκλοπής, τα μηνύματα κρυπτογραφούνται μεταξύ των onion δρομολογητών με τη χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας. Δύο κόμβοι, οι οποίοι επικοινωνούν απευθείας μεταξύ τους, δημιουργούν ένα κλειδί συνόδου για κρυπτογράφηση μέσω ασύμμετρης κρυπτογραφίας [7].

Για να ενισχυθεί η απόδοση, ολόκληρη η αλληλογραφία μεταξύ αυτών των κόμβων κρυπτογραφείται με συμμετρική κρυπτογραφία η οποία χρησιμοποιεί τα μυστικά κλειδιά σε επίπεδο συνεδρίας. Με την αύξηση των κόμβων αναμετάδοσης, τα επίπεδα της κρυπτογράφησης αυξάνονται επίσης. Η διαδρομή του μηνύματος είναι τυχαία μεταξύ του αποστολέα και του παραλήπτη. Το TOR προσφέρει ανωνυμία στις υπηρεσίες επικοινωνίας που χρησιμοποιούν το TCP/IP, μικρή καθυστέρηση, ακεραιότητα από άκρο σε άκρο και μεταβλητές πολιτικές εξόδου για τους δρομολογητές. Παρ' όλα αυτά, η δρομολόγηση με αυτή τη τεχνική και το TOR έχουν αδυναμίες, όπως η ανάλυση χρονισμού που επιτρέπει το να προσδιοριστεί εάν ένας κόμβος επικοινωνεί με μια υπηρεσία λόγω χαμηλής καθυστέρησης. Το TOR μπορεί να παρέχει βέβαια ανώνυμα κανάλια Διαδικτύου σε πιο σύνθετες λύσεις ασφαλείας που χρησιμοποιούνται σε δίκτυα IP [34].



Εικόνα 4.6: Παράδειγμα Χρήσης του Δικτύου TOR

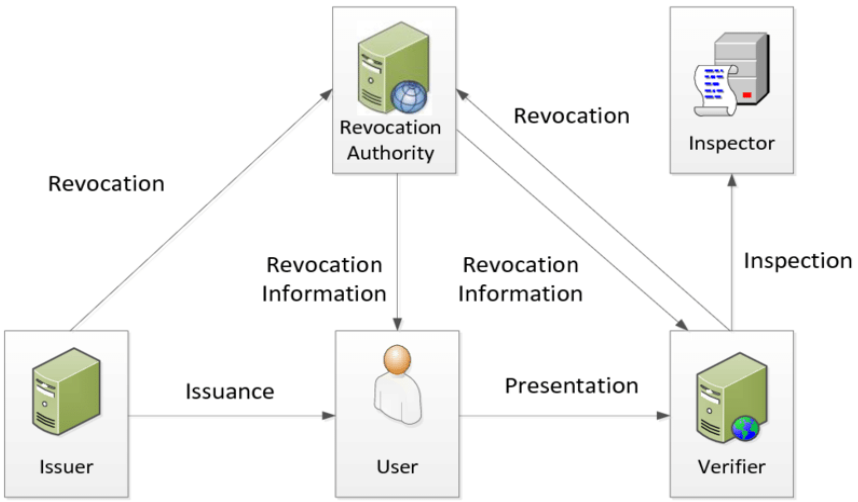
4.4 Μηχανισμοί Ταυτοποίησης με Ανώνυμο Τρόπο

Τα πρωτόκολλα ταυτοποίησης με ανώνυμο τρόπο (anonymity-based authentication protocols) λειτουργούν στην κορυφή των μεθόδων δρομολόγησης που προστατεύουν την ανωνυμία που περιγράψαμε στη προηγούμενη παράγραφο. Εγγυώνται τόσο την ανωνυμία των χρηστών (αφαίρεση των πληροφοριών αναγνώρισης τους κατά τις διάφορες συνεδρίες) όσο και τη μη συνδεσιμότητα (οι συνεδρίες πολλαπλών χρηστών που εκτελούνται σε έναν διακομιστή είναι αξεχώριστες μεταξύ τους – αν ο ίδιος χρήστης επικοινωνήσει σε δύο διαφορετικές συνεδρίες, δεν μπορεί κάποιος τρίτος να αντιληφθεί έστω ότι σε αυτές τις δύο συνεδρίες υπεισέρχεται ο ίδιος χρήστης). Τα συστήματα ανώνυμης ταυτοποίησης μπορούν να βασίζονται στην έννοια των πρωτοκόλλων μηδενικής γνώσης, των ομαδικών υπογραφών, τυφλών υπογραφών, δεσμεύσεων και ηλεκτρονικών νομισμάτων. Τα ηλεκτρονικά νομίσματα μπορούν να γενικευτούν σε ανώνυμα σημεία ή συστήματα εξασφάλισης διαπιστευτηρίων. Ένας χρήστης που έχει έγκυρο κουπόνι (ή διαπιστευτήριο) μπορεί να πιστοποιηθεί και να αποκτήσει πρόσβαση σε προστατευόμενες υπηρεσίες [29].

Τα συστήματα ανώνυμης ταυτοποίησης χρησιμοποιούν συνήθως στοιχεία ελέγχου ταυτότητας, όπως έξυπνες κάρτες, προστατευμένες αποθήκες δεδομένων και ούτω καθεξής. Τα στοιχεία αυτά χρησιμοποιούνται για την πρόσβαση σε προστατευμένους χώρους (κτίρια, δωμάτια, εργαστήρια κ.λπ.). Τα αντικείμενα μπορούν επίσης να συνδεθούν σε έναν υπολογιστή μέσω ενός αναγνώστη, και να χρησιμοποιούνται για πρόσβαση σε διαδικτυακές υπηρεσίες, λειτουργικά συστήματα κ.λπ. Το στοιχείο ελέγχου ταυτότητας που φέρει δεδομένα ταυτοποίησης ενός χρήστη μπορεί να συνδυαστεί με άλλες μεθόδους, όπως κωδικοί πρόσβασης, κωδικοί pin κλπ.

Έτσι διακρίνουμε δύο ειδών σχήματα: τα σχήματα βασισμένα σε χαρακτηριστικά (attribute-based schemes) και τα σχήματα βασισμένα σε διαπιστευτήρια (credentials-based schemes) [29].

Στη πρώτη περίπτωση, έχουμε κρυπτογραφικά σχήματα, τα οποία έχουν σχεδιαστεί για να ενισχύσουν την ιδιωτικότητα των χρηστών [35].Τα σχήματα αυτά παρέχουν ανώνυμες αποδείξεις της κατοχής συγκεκριμένων προσωπικών χαρακτηριστικών ενός χρήστη. Το προσωπικό χαρακτηριστικό αντιπροσωπεύει μια συγκεκριμένη πληροφορία σχετικά με έναν χρήστη, π.χ. την ηλικία, την άδεια οδήγησης ή τον τόπο γέννησης. Ο χρήστης που ζητά μια υπηρεσία καλείται πρώτα να αποδείξει την κατοχή του χαρακτηριστικού σε ένα σύστημα επαλήθευσης. Οι χρήστες ενός πληροφοριακού συστήματος που χρησιμοποιεί ένα τέτοιο σχήμα ταυτοποιούνται ανώνυμα χωρίς να διαρρέουν οποιαδήποτε άλλη πληροφορία. Για παράδειγμα, αν για τη χρήση μίας υπηρεσίας απαιτείται ο χρήστης να είναι τουλάχιστον 16 ετών, με τέτοιες τεχνολογίες ο χρήστης μπορεί να αποδεικνύει την ηλικία του χωρίς να αποκαλύπτει την ταυτότητά του.

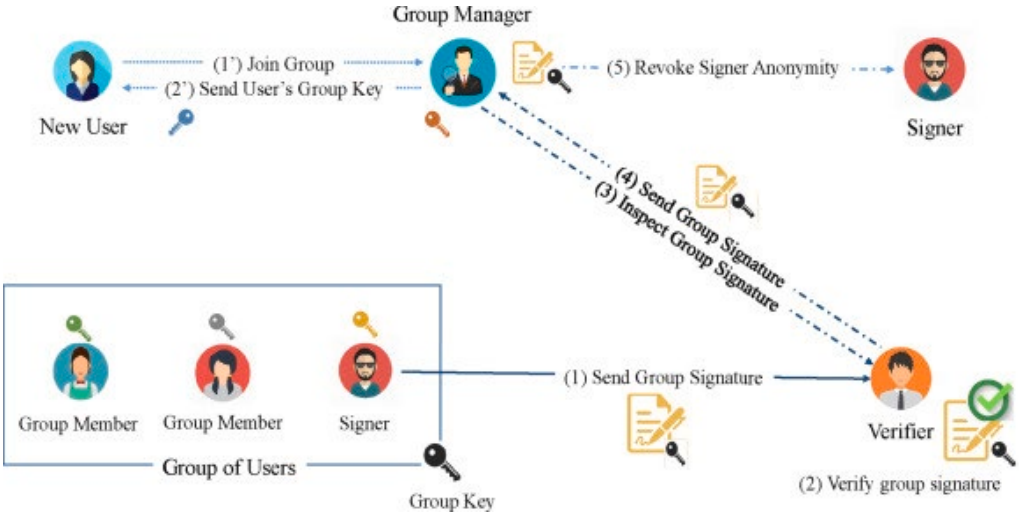


Εικόνα 4.7: Attribute Based Systems.

Τα συστήματα διαπιστευτηρίων όπως για παράδειγμα το σύστημα Idemix [36]και το σύστημα U-Prove[37], παρέχουν ταυτοποίηση των χρηστών με ανώνυμο τρόπο. Ένα τέτοιο σύστημα μπορεί να χρησιμοποιεί tokens για την ανώνυμη επαλήθευση των χαρακτηριστικών του χρήστη. Οι ταυτότητες των χρηστών δεν αποκαλύπτονται όταν οι χρήστες παρουσιάζουν τα χαρακτηριστικά τους βάσει των οποίων αυθεντικοποιούνται. Παρ' όλα αυτά, οι συνεδρίες του ίδιου χρήστη μπορούν να συνδεθούν μεταξύ τους, και αυτό μειώνει την ιδιωτικότητα του χρήστη.

Σε ανάλογα συστήματα οι χρήστες παρέχουν αποδείξεις κατοχής διαπιστευτηρίων και αποδείξεις κατοχής ορισμένων χαρακτηριστικών χωρίς να αποκαλύπτουν την ταυτότητά τους

Το πρόβλημα των συστημάτων διαπιστευτηρίων θα μπορούσε να είναι η πρακτική ανάκληση κακόβουλων ή ληγμένων χρηστών, εάν χρησιμοποιούνται αργές off-line συσκευές (π.χ. έξυπνες κάρτες) για την αποθήκευση των χαρακτηριστικών. Παρ' όλα αυτά, τα συστήματα ελέγχου ταυτότητας που βασίζονται σε κάρτες, όπως οι ηλεκτρονικές ταυτότητες, οι έξυπνες κάρτες υπαλλήλων, οι κάρτες πρόσβασης σε βιβλιοθήκες κ.λπ. απαιτούν πρακτική ανάκληση [35].



Εικόνα 4.8: Διαδικασία Ανάκλησης Πιστοποιητικού Ανωνύμου Χρήστη [35].

4.5 Πρωτόκολλα και Συστήματα με Επίγνωση Ιδιωτικότητας

Αυτά τα σχήματα και πρωτόκολλα παρέχουν ορισμένες βασικές ιδιότητες ασφάλειας, π.χ. εμπιστευτικότητα, ακεραιότητα δεδομένων, ταυτοποίηση, και ορισμένες ενισχυμένες ιδιότητες ασφάλειας, για παράδειγμα ψευδωνυμοποίησης, ανωνυμία, μη συνδεσιμότητα, ανάκληση και μη ανιχνευσιμότητα. Τα τρέχοντα κρυπτογραφικά συστήματα προσπαθούν να είναι ασφαλή, υπολογιστικά αποδοτικά και να διατηρούν χαμηλή επιβάρυνση στην επικοινωνία (σύντομες υπογραφές, δημόσια κλειδιά). Όμως, οι προηγμένες ιδιότητες διατήρησης της ιδιωτικότητας μπορεί να αυξήσουν την επικοινωνία και την υπολογιστική επιβάρυνση. Εκτός από τα σχήματα που βασίζονται στη παραγοντοποίηση ακεραίων αριθμών, το πρόβλημα RSA ή το πρόβλημα του

διακριτού λογαρίθμου, υπάρχουν σχήματα που βασίζονται σε ελλειπτικές καμπύλες (elliptic curves) και διγραμμικές παραστάσεις (bilinear maps) που μπορούν να προσφέρουν αποδοτικά και νέα κρυπτογραφικά σχήματα [38].

Επί του παρόντος, έχουν προκύψει διάφορα κρυπτογραφικά συστήματα που παρέχουν προστασία της ιδιωτικής ζωής. Αυτά τα σχήματα έχουν εφαρμοστεί σε λύσεις ελέγχου ταυτότητας και πρόσβασης με διατήρηση της ιδιωτικότητας του χρήστη. Για το σχεδιασμό λύσεων ασφάλειας σε συστήματα επικοινωνίας που διασφαλίζουν την ιδιωτικότητα των χρηστών και την ασφάλεια των δεδομένων, ένα σχήμα ομαδικής υπογραφής μπορεί να αποτελέσει κατάλληλο κρυπτογραφικό εργαλείο.

Σε άλλα πρωτόκολλα, όπως τα πιστοποιητικά μιας χρήσης (One Time Password-OTP) , υλοποιούνται χαρακτηριστικά με επίκεντρο το απόρρητο, όπως ότι ο κάτοχος του πιστοποιητικού έχει τον έλεγχο των χαρακτηριστικών και είναι δυνατό για έναν χρήστη να δώσει διαδραστικά ή μη αποδείξεις ότι τα χαρακτηριστικά που κωδικοποιούνται στο πιστοποιητικό διαθέτουν μια δεδομένη ιδιότητα. Αυτό γίνεται χωρίς να αποκαλυφθεί η πραγματική τιμή του ηχαρακτηριστικού. Το κύριο μειονέκτημα αυτών των πιστοποιητικών είναι ότι η χρήση του ίδιου πιστοποιητικού δύο φορές κάνει τις δύο συναλλαγές να συνδέονται, παρόλο που τα χαρακτηριστικά εξακολουθούν να είναι κρυφά. Το ίδιο ισχύει, για παράδειγμα, στην ανώνυμη ηλεκτρονική έκδοση εισιτηρίων για σκοπούς ελέγχου πρόσβασης.

Έτσι, σε αντίθεση με τα πιστοποιητικά ίδιας χρήσης, τα πιστοποιητικά πολλαπλών χρήσεων μπορούν να χρησιμοποιηθούν πολλές φορές και εξακολουθούν να εγγυώνται τη μη σύνδεση. Ο ίδιος ο κάτοχος ενός πιστοποιητικού πολλαπλής χρήσης μπορεί να κατασκευάσει άλλα πιστοποιητικά κατά περίπτωση, με ένα ή περισσότερα από τα ίδια χαρακτηριστικά από το αρχικό πιστοποιητικό, έτσι ώστε να μην είναι δυνατή η σύνδεση. Ωστόσο, αυτά τα πιστοποιητικά δεν επιτρέπουν στον χρήστη να αποδείξει, για παράδειγμα με χρήση αποδείξεων μηδενικής γνώσης, τις ιδιότητες των χαρακτηριστικών του πιστοποιητικού του [25].

Τα Ανώνυμα Διαπιστευτήρια είναι άλλη μία σημαντική κατηγορία πρωτοκόλλων ενίσχυσης της ιδιωτικότητας. Σε παγκόσμιο επίπεδο, σε ένα ανώνυμο σύστημα διαπιστευτηρίων επιτρέπεται στους χρήστες να λαμβάνουν ανώνυμα διαπιστευτήρια από αρμόδιες έμπιστες αρχές, να αποδεικνύουν ανώνυμα την κατοχή αυτών των διαπιστευτηρίων και να κάνουν διαφορετικές χρήσεις των ίδιων διαπιστευτηρίων ασύνδετα, έτσι ώστε οι οντότητες επαλήθευσης ακόμα και εάν ενώσουν τις δυνάμεις τους να μην μπορούν να διακρίνουν έναν χρήστη από τον άλλο.

Το 1986 οι Chaum και Evertse παρουσίασαν το πρώτο μη μεταβιβάσιμο ανώνυμο σύστημα διαπιστευτηρίων. Αυτό το σύστημα βασίστηκε στη χρήση ψευδωνύμων. Το 2001 προτάθηκε ένα πιο αποτελεσματικό και πρακτικό ανώνυμο σύστημα διαπιστευτηρίων από τους Camenisch και Lysyanskaya. Τα περισσότερα ανώνυμα συστήματα διαπιστευτηρίων βασίζονται σε αποτρεπτικούς παράγοντες για την εκχώρηση διαπιστευτηρίων, συνδέοντας τα διαπιστευτήρια με οποιοδήποτε σύνολο πολύτιμων μυστικών του χρήστη. Ωστόσο, ορισμένες αιτήσεις απαιτούν ισχυρότερη εγγύηση μη μεταβίβασης, π.χ. τα ανώνυμα διαπιστευτήρια για την ιθαγένεια της χώρας. Ο ανώνυμος βιομετρικός έλεγχος ταυτότητας είναι ένας τρόπος επιβεβαίωσης της ταυτότητας ενός ατόμου με ισχυρή εγγύηση μη μεταβίβασης.

Από την άλλη πλευρά, ένας χρήστης επαληθεύεται χρησιμοποιώντας κάποια αλυσίδα διαπιστευτηρίων, π.χ. ένας κεντρικός οργανισμός δίνει ένα διαπιστευτήριο σε ένα ενδιάμεσο μέρος που μπορεί με τη σειρά του να το χρησιμοποιήσει για να εκδώσει διαπιστευτήρια σε άλλους χρήστες. Ένας χρήστης μπορεί να αποδείξει ότι έχει μια έγκυρη αλυσίδα διαπιστευτηρίων δεδομένου μήκους χωρίς να αποκαλύψει άλλες πληροφορίες ή χαρακτηριστικά αναγνώρισης..

4.6 Εφαρμογές Τεχνολογιών PEC

Στην συνέχεια θα παρουσιάσουμε ορισμένες περιπτώσεις χρήσης των PEC τεχνικών μαζί με τα αντίστοιχα δομικά στοιχεία που χρησιμοποιούνται.

4.6.1 Σενάριο Περίπτωσης: Αποκάλυψη Ιδιοτήτων

Θεωρούμε το σενάριο όπου ένα άτομο διαθέτει ένα διαπιστευτήριο, π.χ. ενσωματωμένο σε μια έξυπνη κάρτα, που εκδίδεται και ψηφιακά υπογεγραμμένο από μια αρχή πιστοποίησης (CA), και περιέχει πληροφορίες προσωπικών δεδομένων. Τα πιστοποιημένα δεδομένα μπορεί να περιλαμβάνουν κάποια αλφαριθμητικά αναγνωριστικά, όπως το ονοματεπώνυμο, την ημερομηνία γέννησης, τη διεύθυνση, κάποιο αριθμό ταυτότητας ή άδειας (για κάποια δραστηριότητα) και επαγγελματικό τίτλο (ή τίτλους), και ενδεχομένως και κάποια ψηφιοποιημένα βιομετρικά δεδομένα (π.χ. φωτογραφία προσώπου και δακτυλικό αποτύπωμα).

Σε μια πιθανή εφαρμογή, το πρόσωπο που κατέχει το διαπιστευτήριο το χρησιμοποιεί για να αποδείξει κάποια ιδιότητα η οποία απορρέει από τα προσωπικά του δεδομένα. Για παράδειγμα, θα μπορούσε να αποδείξει ότι μια ψηφιοποίηση του προσώπου του ατόμου σε πραγματικό χρόνο

ταιριάζει με την πιστοποιημένη φωτογραφία και ότι τα σχετικά δεδομένα συνάδουν με την ηλικία ψήφου και την εγγεγραμμένη διεύθυνση σε μια συγκεκριμένη διαδικασία ψηφοφορίας.

Χρησιμοποιώντας ένα πρακτικό πρωτόκολλο PEC, π.χ. βασισμένο σε ZKPs, το πρόσωπο θα πρέπει να είναι σε θέση να πείσει έναν ελεγκτή ότι μία ιδιότητα ικανοποιείται με συνέπεια με τα αναγνωριστικά και τα χαρακτηριστικά για τα οποία έχει εγγυηθεί η CA, χωρίς όμως να αποκαλύπτει πρόσθετα δεδομένα και χωρίς αλληλεπίδραση με την αρχή πιστοποίησης (CA).

4.6.2 Έλεγχος Ταυτότητας και Μεσολάβηση

Οι πάροχοι υπηρεσιών ταυτοποίησης (IDPs) μπορούν να επιτρέπουν στους χρήστες να πιστοποιούνται στους παρόχους υπηρεσιών (SPs).Ορισμένες ρυθμίσεις απαιτούν τη χρήση ενός διαμεσολαβητή για τη συναλλαγή αυτή, ώστε να επιτρέπεται η πιστοποίηση ταυτότητας ενός παθητικού χρήστη (που δεν διαθέτει εξειδικευμένο λογισμικό) μεταξύ των IDP και των SP, ενώ παράλληλα ο ένας IDP και ο SP δεν θα γνωρίζει ο ένας την ύπαρξη του άλλου.

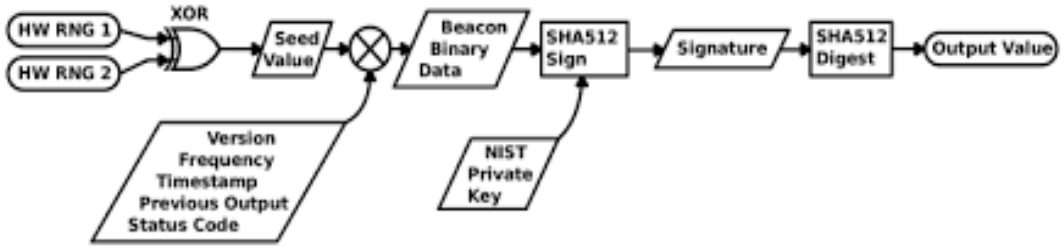
Μία τεχνολογία PEC μπορεί να χρησιμοποιηθεί για να αποτρέψει περαιτέρω τον διαμεσολαβητή από το να μάθει τα χαρακτηριστικά του χρήστη, να ταυτοποιήσει τον χρήστη, και να τον συνδέσει σε διάφορες πιστοποιήσεις. Ενώ ταυτόχρονα διασφαλίζονται χαρακτηριστικά δυνατότητας ελέγχου για την επαλήθευση της εγκυρότητας των συναλλαγών. Διάφορες προηγμένες τεχνικές κρυπτογράφησης μπορούν να χρησιμοποιηθούν για ναβοηθήσουντη διατήρηση της ιδιωτικότητας της ταυτότητας με μεσολάβηση. Για παράδειγμα, το SMPC μπορεί να επιτρέψει στον μεσολαβητή να επαληθεύει ότι τα χαρακτηριστικά και η ταυτότητα ενός χρήστη, όπως κατέχονται από έναν IDP, ικανοποιούν κάποιες συνθήκες που απαιτούνται από έναν SP, αλλά χωρίς ο IDP να μαθαίνει τι είναι αυτό το κατηγόρημα, και χωρίς ο μεσολαβητής να μαθαίνει τα χαρακτηριστικά και την ταυτότητα.

4.6.3 Δημόσιος Έλεγχος

Το Randomness Beacon είναι μία τεχνική που δημοσιεύει έναν τυχαίο αριθμό 512 bit κάθε λεπτό, καθιστώντας τον δημόσια διαθέσιμο δωρεάν με ψηφιακή υπογραφή και χρονοσήμανση, και μέρος μιας αλυσίδας που δεν μπορεί να αλλάξει προς τα πίσω. Αυτή η δημόσια τυχαιότητα μπορεί να χρησιμοποιηθεί για να βοηθήσει πολυάριθμα μέρη να συντονιστούν σχετικά με τυχαίους

αριθμούς που θα χρησιμοποιήσουν, ενώ παράλληλα επιτρέπει τη μεταγενέστερη δημόσια επαλήθευση ότι χρησιμοποιήθηκαν οι σωστοί τυχαίοι αριθμοί.

Αυτό μπορεί να ταιριάζει σε εφαρμογές όπου η πιθανολογική κατανομή του αποτελέσματος πρέπει να εξαρτάται, σε μια δημόσια γνωστή διαδικασία, από δεσμευμένα ιδιωτικά χαρακτηριστικά. Χρησιμοποιώντας PEC, π.χ. ZKPs, είναι δυνατόν να επιτραπεί τέτοια δημόσια δυνατότητα ελέγχου, ικανοποιώντας παράλληλα τις απαιτήσεις ιδιωτικότητας. Για παράδειγμα, αυτό μπορεί να επιτρέψει τη δημόσια ελέγξιμη επεξεργασία κλινικών δοκιμών με τυχαίο τρόπο που εξαρτώνται από δεδομένων ασθενών, ενώ παράλληλα προστατεύει τα προσωπικά δεδομένα των ασθενών.



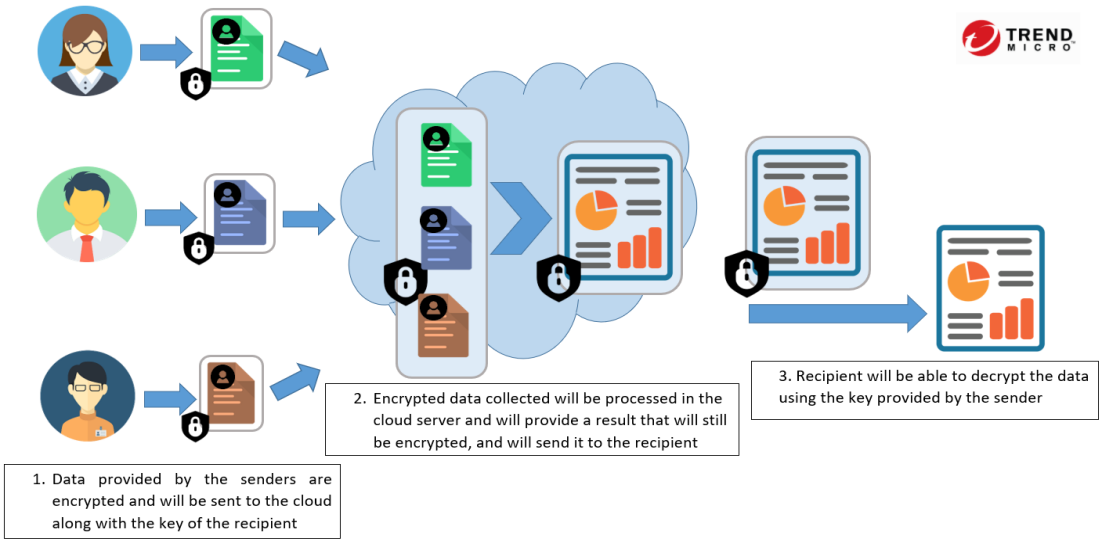
Εικόνα 4.9: Διαδικασία Κρυπτογράφησης Προσωπικών Δεδομένων προς Διάθεση στο Ευρύτερο Κοινό.

4.6.4 Μεγάλη Ποικιλία Εφαρμογών

Τα θέματα των εφαρμογών PEC είναι πιθανό να δίνουν έμφαση στην τεχνολογία πληροφοριών, τόσο σε επιχειρηματικούς όσο και σε μη επιχειρηματικούς τομείς. Για παράδειγμα, οι εφαρμογές μπορούν να σχετίζονται με το ηλεκτρονικό εμπόριο, τις τράπεζες, την υγεία, την εκπαίδευση, τη γεωγραφική τοποθεσία, τις μετρήσεις, την ηλεκτρονική ψηφοφορία, την επαλήθευση συνθηκών, τα μέσα κοινωνικής δικτύωσης και τα ιδιωτικά μηνύματα. Μπορούν να σχετίζονται με τη διευκόλυνση της αυτονομίας των ιδιωτών ή ομάδων, καθώς και με τη διευκόλυνση καλών πρακτικών από συλλογικές οντότητες. Επίσης, το εύρος των ιδιοκτησιών που αναζητούνται μαζί με το απόρρητο μπορεί να είναι ποικίλο, συμπεριλαμβανομένης της δυνατότητας ελέγχου και των στατιστικών στοιχείων.

Οι περιπτώσεις χρήσης μπορούν να υποκινούνται από γενικές αρχές απορρήτου και από τον αντιληπτό κοινωνικό αντίκτυπο των λύσεων. Σε ορισμένες άλλες περιπτώσεις, οι απαιτήσεις απορρήτου ενδέχεται να προκύψουν πιο άμεσα από τους υφιστάμενους κανονισμούς. Ανάλογα

με τη δικαιοδοσία ενδέχεται να υπάρχουν κανονισμοί σε επίπεδο κράτους που σχετίζονται με τα δικαιώματα των καταναλωτών σχετικά με τα προσωπικά τους δεδομένα που συλλέγονται από την επιχείρηση. Επίσης, η μετάδοση δεδομένων μεταξύ των χωρών ενδέχεται να απαιτεί συμμόρφωση με διάφορους διεθνείς κανονισμούς.



Εικόνα 4.10: Περιπτώσεις Χρήσης των PEC.

Τα ανωτέρω σε καμία περίπτωση δεν εξαντλούν το πλήθος των εφαρμογών στην πράξη για τις οποίες οι τεχνολογίες PEC μπορούν να δώσουν λύσεις σε προκλήσεις που ανακύπτουν και από τις απαιτήσεις του νομικού πλαισίου προστασίας δεδομένων. Καταδεικνύουν ωστόσο, ως ενδεικτικά παραδείγματα, τις δυνατότητες και το μεγάλο εύρος εφαρμογών που υπάρχουν. Μία επισκόπηση των διαφόρων τέτοιων τεχνολογιών και των εφαρμογών τους υπάρχει στο [39].

Κεφάλαιο 5

Crypt-DB: Ένα Πρακτικό Κρυπτογραφημένο Σύστημα Διαχείρισης Σχεσιακών Βάσεων Δεδομένων

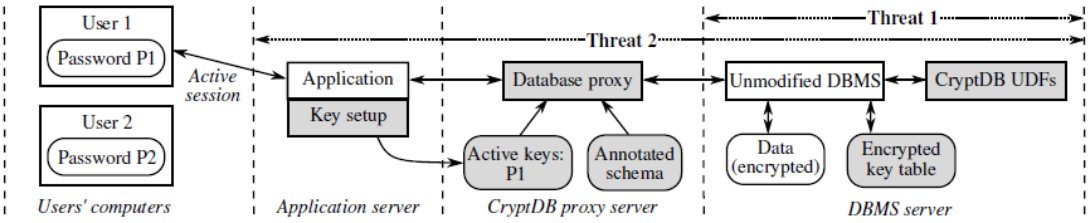
Ενόψει της απειλής κατάχρησης προνομίων από διαχειριστές βάσεων δεδομένων (DBA) αλλά και της αντιμετώπισης απειλών από εισβολείς, πρέπει να ληφθούν αυξημένα μέτρα ασφάλειας για την εμπιστευτικότητα στα Συστήματα Διαχείρισης Βάσεων Δεδομένων (DBMS). Για αυτό το λόγο η συγκεκριμένη μεταπτυχιακή διατριβή διερευνά, ως μελέτη περίπτωσης, και δοκιμάζει εκτενώς έναν τρόπο ασφάλειας βάσεων δεδομένων παρουσία των δύο απειλών που αναφέρονται παραπάνω. Αυτή ή τεχνική ονομάζεται Crypt-DB: πρόκειται για ένα σύστημα που λειτουργεί ως διακομιστής μεσολάβησης για την ασφάλεια της επικοινωνίας μεταξύ του διακομιστή βάσης δεδομένων(Database Server) και του διακομιστή εφαρμογών(Application Server) [40].

Το Crypt-DB λαμβάνει ερωτήματα από τον διακομιστή εφαρμογών, τα «προστατεύει» (κρυπτογραφεί) και τα στέλνει στον διακομιστή της βάσης δεδομένων. Στη συνέχεια, θα λάβει κρυπτογραφημένα δεδομένα από τη βάση δεδομένων, θα τα αποκρυπτογραφήσει και θα τα αποστείλει στον διακομιστή εφαρμογής για να σταλούν στον αιτούντα [40].

Με λίγα λόγια, το Crypt-DB επιτρέπει στο DBMS να εκτελεί ερωτήματα SQL σε κρυπτογραφημένα δεδομένα βάσης δεδομένων, όπως θα μπορούσε να κάνει σε απλό κείμενο. Η υπόθεση που γίνεται είναι ότι ο διακομιστής εφαρμογής και ο διακομιστής βάσης δεδομένων είναι διαφορετικοί και ένας διακομιστής μεσολάβησης μπορεί να υποκλέψει την επικοινωνία τους – ενώ επίσης θεωρούμε, όπως προαναφέρθηκε, ότι δεν είναι «έμπιστος» ούτε ο πάροχος/διαχειριστής της βάσης δεδομένων, δηλαδή δεν επιθυμούμε να είναι σε θέση να διαβάζει τα δεδομένα – χαρακτηριστικό πεδίο εφαρμογής είναι η περίπτωση τήρησης της βάσης δεδομένων σε έναν τρίτο πάροχο υπολογιστικού νέφους. Το CryptDB μπορεί να εφαρμοστεί σε μια σειρά DBMS όπως MySQL και Postgres [40].

5.1 Αρχές και Τεχνικές Σχεδίασης του Crypt-DB

Το CryptDB έχει σχεδιαστεί από ερευνητές του MIT για να αντιμετωπίζει τις αδυναμίες των ήδη προϋπάρχουσων λύσεων που είτε είναι πολύ αργές είτε δεν παρέχουν την απαραίτητη εμπιστευτικότητα. Το CryptDB προσθέτει έναν διακομιστή μεσολάβησης και ορισμένα άλλα στοιχεία στην τυπική δομή των εφαρμογών που υποστηρίζονται από βάση δεδομένων, η οποία αποτελείται από έναν διακομιστή DBMS και έναν ξεχωριστό διακομιστή εφαρμογών, όπως φαίνεται στη παρακάτω εικόνα (Εικόνα 5.1)[40].



Εικόνα 5.1:Δομή του Crypt-DB.

Υπάρχουν τρεις προσεγγίσεις που χρησιμοποιεί το Crypt-DB για να λύσει τα προβλήματα των ήδη υφισταμένων προσεγγίσεων. Η προσέγγιση κρυπτογράφησης με επίγνωση της SQL χρησιμοποιεί το γεγονός ότι τα ερωτήματα SQL έχουν μια πολύ γνωστή δομή που αποτελείται από τελεστές

όπως συγκρίσεις παραγγελιών, έλεγχος ισότητας και συγκεντρωτικά στοιχεία όπως ενώσεις αθροίσματος και πινάκων. Στη συνέχεια, το CryptDB χρησιμοποιεί κρυπτογραφικές μεθόδους για συνδέσεις για να μετατρέψει τα ερωτήματα σε μια φόρμα που μπορεί να επιτρέψει στο DBMS να τα εκτελεί σε κρυπτογραφημένα δεδομένα[40].

Από την άλλη πλευρά, η ρυθμιζόμενη κρυπτογράφηση βάσει ερωτημάτων (adjustable query-based encryption**)** λύνει το πρόβλημα που παρατηρήθηκε στις πρώτες τεχνικές όπου ορισμένα κρυπτογραφικά σχήματα διαρρέουν περισσότερα δεδομένα από τα απαιτούμενα. Ωστόσο, επειδή εξακολουθούν να χρειάζονται, απαιτούνται ενώσεις κρυπτογράφησης για την προσεκτική προσαρμογή των ερωτημάτων για την ελαχιστοποίηση της διαρροής δεδομένων[40].

Η τρίτη προσέγγιση, η οποία θεωρείται ότι προστατεύει τους χρήστες που δεν είναι συνδεδεμένοι σε ένα σύστημα, είναι η αλυσίδα των κρυπτογραφικών κλειδιών σε κωδικούς πρόσβασης χρηστών για να ενεργοποιηθεί η αποκρυπτογράφηση δεδομένων σε χρήστες με δικαιώματα πρόσβασης[40].

5.2 Queries(Ερωτήματα) για Κρυπτογραφημένα Δεδομένα

Για την ασφάλεια των δεδομένων, το κανονικό σχήμα βάσης δεδομένων αλλάζει προκειμένου να αποκρύψει τυχόν σχέσεις που μπορούν να διαβαστούν από τη βάση δεδομένων και στη συνέχεια να αποθηκευτούν στον διακομιστή μεσολάβησης του Crypt-DB. Στην πραγματικότητα, τα ονόματα πινάκων και στηλών είναι κρυπτογραφημένα. Η κρυπτογράφηση στηλών εξαρτάται από τα δεδομένα που διατηρεί αυτή η στήλη και τον τύπο των ερωτημάτων που θα εκτελεστούν από τον DBMS[40].

Ανάλογα με τον τύπο των δεδομένων που αποθηκεύει μια στήλη, υπάρχουν έξι μέθοδοι κρυπτογράφησης. Τη Random(RND) η οποία παράγει ένα κρυπτογραφημένο κείμενο από ένα όνομα στήλης χρησιμοποιώντας ένα τυχαία δημιουργημένο αρχικό διάνυσμα. Λόγω της τυχαιότητας, η RND παρέχει ισχυρή κρυπτογράφηση και είναι κατάλληλη κατά το χειρισμό ευαίσθητων δεδομένων[40].

Ο δεύτερος τρόπος κρυπτογράφησης είναι ο Ντετερμινιστικός (DET).Παρέχει ασθενέστερη ασφάλεια λόγω της διαρροής που προκαλείται από την παραγωγή του ίδιου κρυπτογραφημένου κειμένου για το ίδιο κείμενο[40].

Ο τρίτος τρόπος είναι η Κρυπτογράφηση Διατήρησης Σειράς (Order-Preserving-Encryption, OPE).Η OPE όπως υποδηλώνει το όνομα, διατηρεί τη σειρά του κρυπτογραφημένου κειμένου ούτως ώστε να παραμείνει όπως ήταν στο απλό κείμενο. Η OPE είναι συγκριτικά πιο αδύναμη από τη DET καθώς αποκαλύπτει τη σειρά[40].

Ο τέταρτος τρόπος κρυπτογράφησης είναι η Ομομορφική Κρυπτογράφηση ,(Homomorphic ,HOM), η οποία είναι εύχρηστη για κάθε δεδομένο που απαιτεί υπολογισμό. Χρησιμοποιώντας την είναι δυνατοί σύνθετοι μαθηματικοί υπολογισμοί καθώς θα μπορούσαν να γίνουν με απλό κείμενο[40].

Ένας άλλος τρόπος κρυπτογράφησης είναι ο (JOIN και OPE-JOIN), ο οποίος χρησιμοποιείται για τη σύνδεση στηλών για την απόκρυψη της συσχέτισης μεταξύ τους .Αυτό συμβαίνει επειδή χρησιμοποιούνται διαφορετικά κλειδιά DET. Οι ενώσεις γίνονται για ελέγχους ισότητας και σειράς[40].

Τέλος, οι έλεγχοι λέξεων (SEARCH) είναι μια μέθοδος που χρησιμοποιείται για την αναζήτηση κρυπτογραφημένων λέξεων. Αυτή η μέθοδος χρησιμοποιείται σε ερωτήματα με λειτουργίες SQL όπως το LIKE .Το SEARCH είναι ασφαλές ως τυχαίο, επειδή δεν επιτρέπει στο DBMS να δει εάν ορισμένες λέξεις-κλειδιά επαναλαμβάνονται σε πολλές σειρές[40].

Το Crypt-DB υποστηρίζει όλες τις ανωτέρω κρυπτογραφικές λειτουργίες..

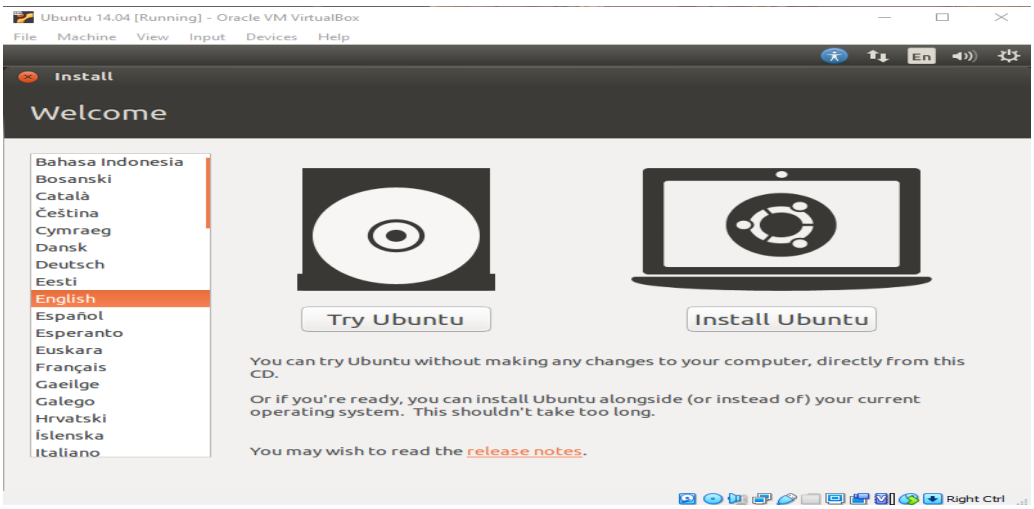
5.3 Εγκατάσταση του Crypt-DB

Στη συγκεκριμένη μεταπτυχιακή διατριβή πραγματοποιήθηκε εγκατάσταση του προγράμματος Crypt-DBσε σύστημα Linux (Ubuntu 14.04).

Αναλυτικά:

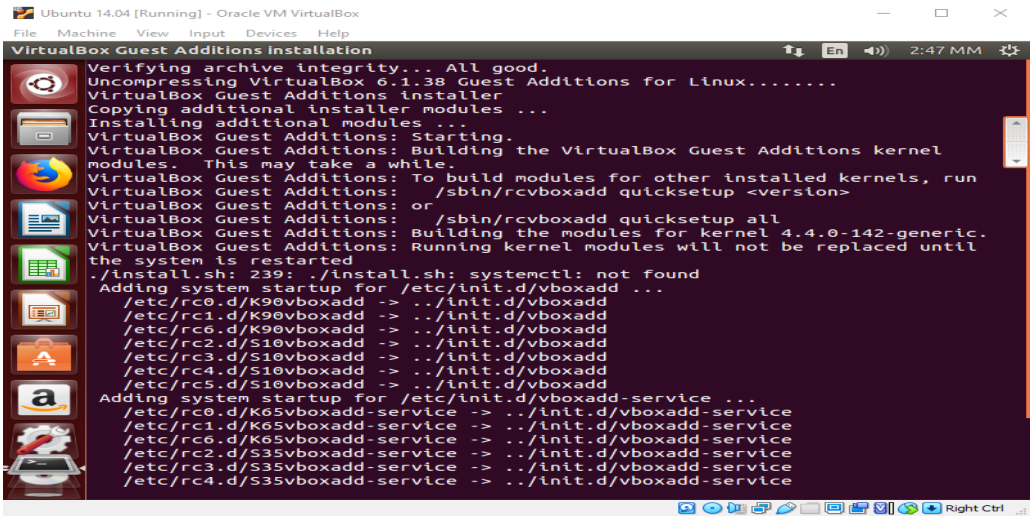
1. Εγκατάσταση του Προγράμματος Oracle VM VirtualBox (Έκδοση 6.1): Το Oracle VM VirtualBox είναι λογισμικό εικονικοποίησης πολλαπλών πλατφορμών το οποίο μας επέτρεψε να τρέξουμε το λειτουργικό σύστημα Ubuntu 14.04.

2. Εγκατάσταση του λειτουργικού Ubuntu 14.04:



Εικόνα 5.2: Εγκατάσταση Ubuntu στο VirtualBox.

3. Αφότου πραγματοποιήθηκε η εγκατάσταση του λειτουργικού συστήματος στη συνέχεια πραγματοποιήθηκε εγκατάσταση κάποιον πρόσθετων πακέτων του Virtual Box ούτως ώστε να ενεργοποιήσουμε την ανταλλαγή αρχείων μεταξύ του δικού μας λειτουργικού συστήματος (Windows 10) και του λειτουργικού συστήματος που έχουμε εγκαταστήσει στο VirtualBox (Ubuntu 14.04).



Εικόνα 5.3: Εγκατάσταση των Virtual Box Additions.

4. Στη συνέχεια αφότου ολοκληρωθεί η εγκατάσταση των Virtual Box Additions ξεκινήσαμε την εγκατάσταση του Crypt-DB και της MySQL ακολουθώντας τη παρακάτω διαδικασία:

Εκτέλεση των εντολών:

```
1.sudo apt-get update
2.sudo apt-get install automake bison bzr cmake flex g++ git gtk-doc-tools
libaio-dev libbsd-dev libevent-dev libglib2.0-dev libgmp-dev liblua5.1-0-dev
libmysqlclient-dev libncurses5-dev libntl-dev libssl-dev
```

Οι παραπάνω εντολές αποτελούν την ενημέρωση των απαραίτητων πακέτων του συστήματος (sudo-apt-get update) καθώς και την εγκατάσταση συγκεκριμένων πακέτων τα οποία είναι απαραίτητα για τη σωστή εγκατάσταση του Crypt-DB.

Στη συνέχεια ακολουθούν οι παρακάτω εντολές οι οποίες απεγκαθηστούν τα πακέτα δεδομένων libbison & bison.

```
3.sudo apt-get remove --auto-remove libbison-dev
4.sudo apt-get remove --auto-remove bison
```

Ακολουθεί η απόκτηση των πακέτων libbison της έκδοσης 2.7 καθώς και της αντίστοιχης έκδοσης του bison.

```
5.wget http://launchpadlibrarian.net/140087283/libbison-
dev_2.7.1.dfsg-1_amd64.deb
6.wget http://launchpadlibrarian.net/140087282/bison_2.7.1.dfsg-1_amd64.deb
```

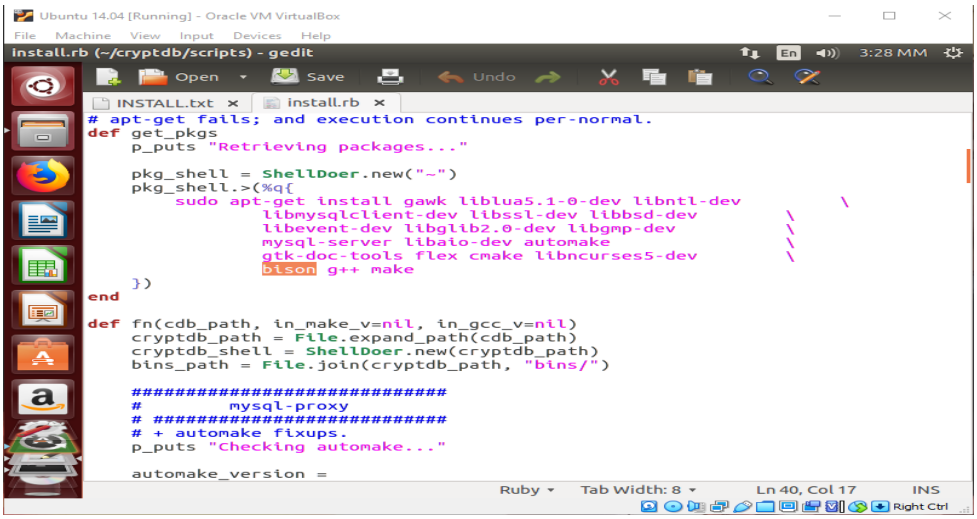
Έπειτα ακολουθεί η εγκατάσταση των συγκεκριμένων πακέτων.

```
7.sudo dpkg -i libbison-dev_2.7.1.dfsg-1_amd64.deb
8.sudo dpkg -i bison_2.7.1.dfsg-1_amd64.deb
```

Αφού εγκατασταθούν τα συγκεκριμένα πακέτα και βιβλιοθήκες, στη συνέχεια γίνεται εγκατάσταση του πακέτου ruby καθώς γίνεται και η απόκτηση του αρχείου εγκατάστασης του Crypt-DBαπό τον σχετικό ιστότοπο του MIT.

```
9.sudo apt-get install git ruby
10.git clone -b public git://g.csail.mit.edu/cryptdb
```

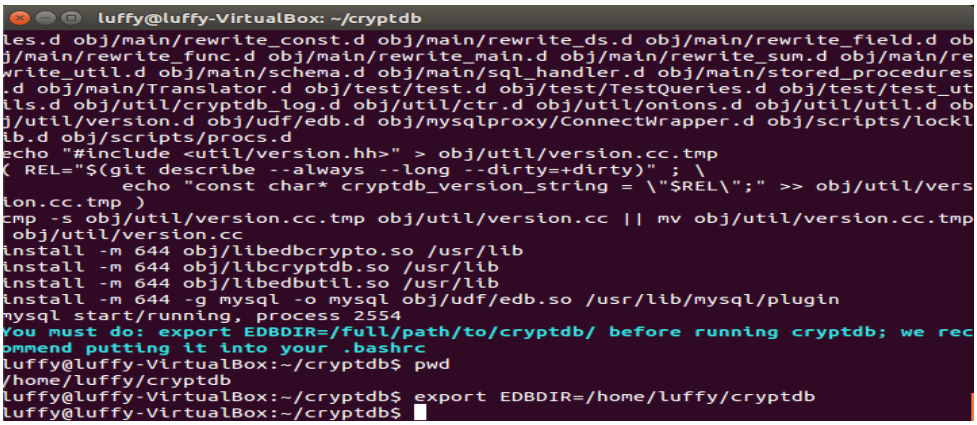
Για να εγκατασταθεί σωστά το Crypt-DBθα πρέπει να παραμετροποιήσουμε το αρχείο install.rb με τέτοιο τρόπο(διαγραφή της βιβλιοθήκης bison) όπως φαίνεται στη παρακάτω εικόνα ούτως ώστε να μην πραγματοποιήσει ενημέρωση στη βιβλιοθήκη bison καθώς το Crypt-DBδεν τρέχει στην ενημερωμένη έκδοση της συγκεκριμένης βιβλιοθήκης.



Εικόνα 5.4: Διαγραφή της Βιβλιοθήκης bison στο αρχείο Install.Rb.

Τέλος, πραγματοποιείται εκτέλεση του αρχείου Install.rb ούτως ώστε να πραγματοποιηθεί εγκατάσταση του Crypt-DB καθώς και της MySQL.

```
11. cd cryptdb
12. sudo ./scripts/install.rb .
```



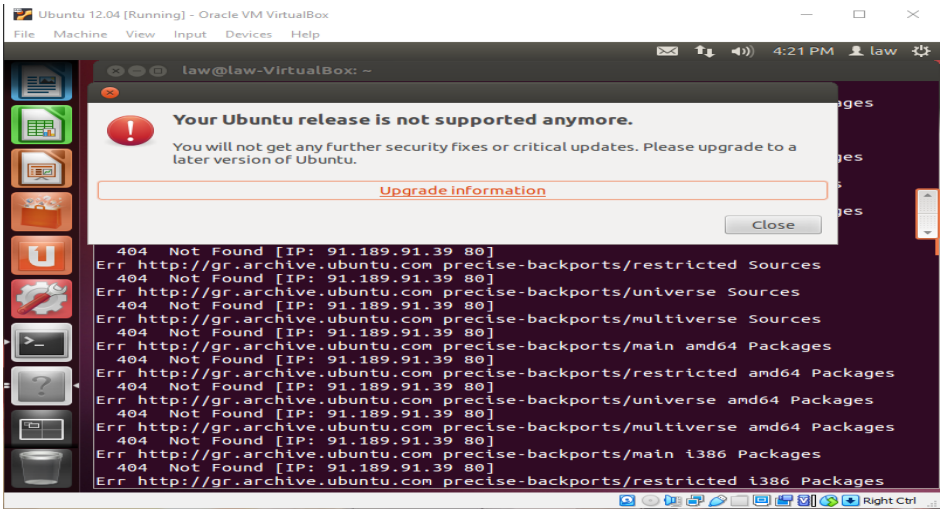
Εικόνα 5.5: Επιτυχής Εγκατάσταση του Crypt_DB.

5.4 Προβλήματα κατά την Εγκατάσταση του Προγράμματος Crypt-DB

Κατά την διάρκεια της προσπάθειας να εγκατασταθεί το Crypt-DBσε περιβάλλον Ubuntu, προέκυψαν πολλά και δυσεπίλυτα προβλήματα λόγω μη ενημερωμένων εκδόσεων για νεότερες εκδόσεις του λειτουργικού συστήματος Ubuntu. Κρίνεται σκόπιμη η λεπτομερής παρουσίαση των προβλημάτων πού ανέκυψαν κατά την προσπάθεια εγκατάστασης του Crypt-DB, με απώτερο στόχο τη διευκόλυνση όσων θα επιθυμούσαν στο μέλλον να ασχοληθούν με το συγκεκριμένο πρόγραμμα.

Για Ubuntu 12.04:

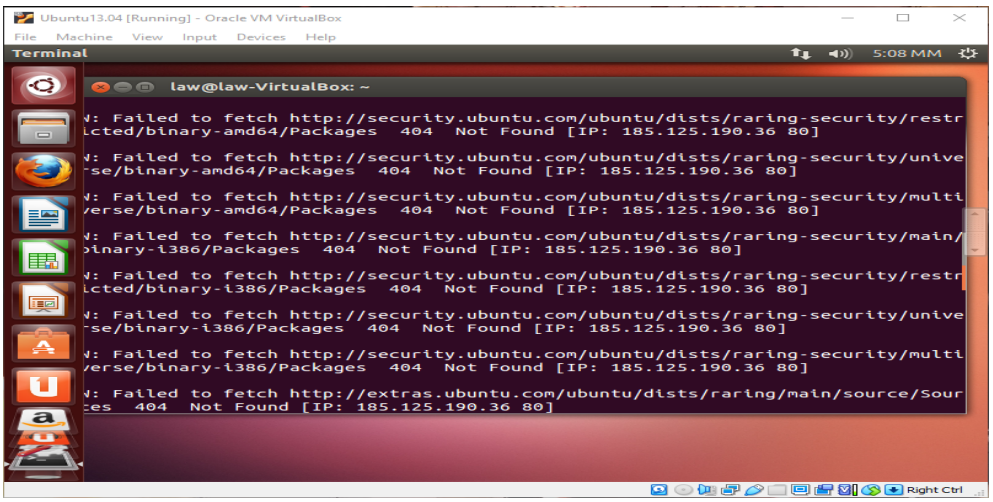
Η συγκεκριμένη έκδοση των Ubuntu αποτελεί και την έκδοση στην οποία αναπτύχθηκε το Crypt-DBαλλά όπως βλέπουμε και στη παρακάτω εικόνα(Εικόνα 5.6),πλέον η συγκεκριμένη έκδοση δεν υποστηρίζεται.



Εικόνα 5.6: Ubuntu 12.04 not supported anymore.

Για Ubuntu 13.04

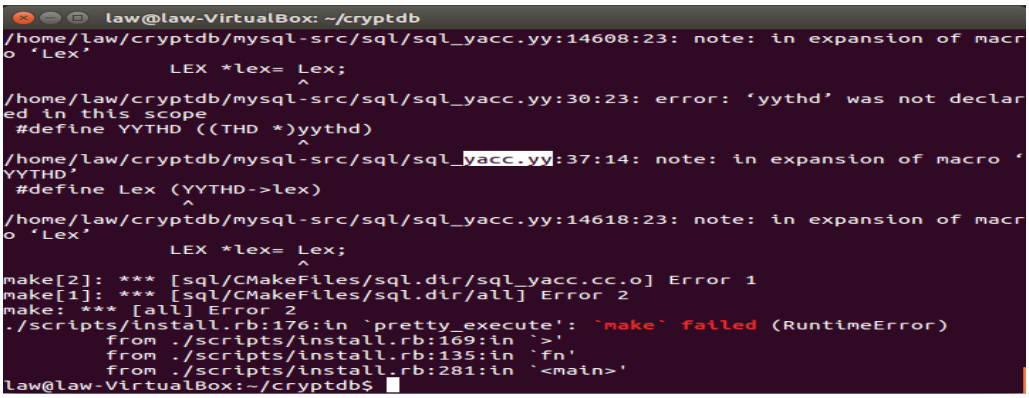
Ακριβώς το ίδιο συμβαίνει και σε αυτή την έκδοση των Ubuntu καθώς βλέπουμε (Εικόνα 5.7) ότι δε μπορεί να πραγματοποιηθεί ορθά το update των πακέτων δεδομένων. Συγκεκριμένα παρατηρείται αδυναμία στην ενημέρωση πακέτων που αφορά την ασφάλεια του συγκεκριμένου λειτουργικού συστήματος.



Εικόνα 5.7: Ubuntu 13.04(sudo apt-get update failed).

Για Ubuntu 14.04

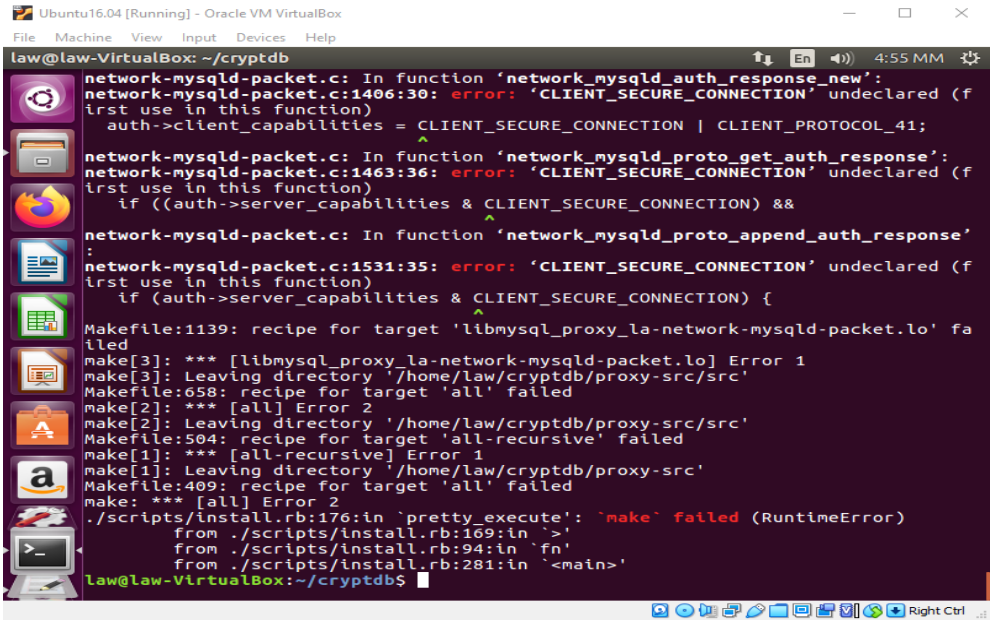
Η συγκεκριμένη έκδοση των Ubuntu είναι αυτή στη οποία κατάφερε να εγκατασταθεί τελικός το Crypt-DB. Παρόλα αυτά και στη συγκεκριμένη έκδοση παρατηρήθηκαν δυσκολίες όπως φαίνεται στην παρακάτω εικόνα (Εικόνα 5.8) .Τοσυγκεκριμένο σφάλμα (error)συμβαίνει επειδή το αρχείο εγκατάστασης του Crypt-DB (Install.rb) εμπεριέχει ενημέρωση συγκεκριμένων βιβλιοθηκών. Μία από αυτές τις βιβλιοθήκες είναι η βιβλιοθήκη libbison η οποία εμπεριέχει το πακέτο δεδομένων bison.Το Crypt-DB λειτουργεί με την έκδοση 2.7 του bison.Το αρχείο Install.rb εμπεριέχει την εγκατάσταση της τελευταίας έκδοσης της συγκεκριμένης βιβλιοθήκης η οποία είναι η 3.0 και κατ' επέκταση συμβαίνει το παρακάτω error το οποίο διορθώθηκε όπως περιγράφεται αναλυτικά στη ενότητα 5.3.



Εικόνα 5.8: Ubuntu 14.04 error (bison 3.0 error).

Για Ubuntu 16.04

Σε αυτή την έκδοση των Ubuntu παρατηρηθήκαν 2 σημαντικά errors κατά την εγκατάσταση του Crypt-DB. Το πρώτο erroreίναι το ίδιο που παρατηρήθηκε και στην έκδοση 14.04και διορθώθηκε με τον ίδιο τρόπο. Το δεύτερο όμως (Εικόνα 5.9) ήταν αυτό στο οποίο παρότι βρέθηκε μία λύση (Εικόνα 5.10) στην ουσία η συγκεκριμένη λύση δεν λειτούργησε και έτσι δε μπόρεσε να ολοκληρωθεί η εγκατάσταση του προγράμματος.



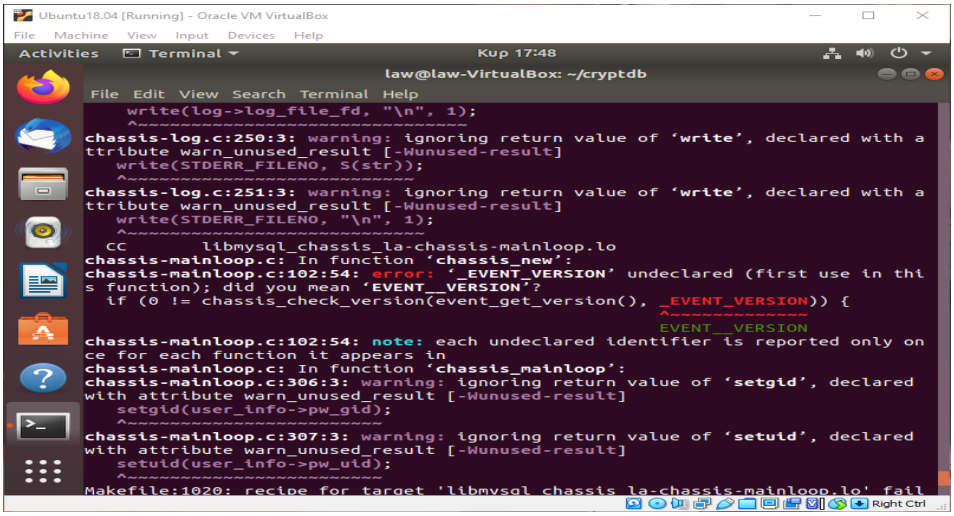
Εικόνα 5.9: Ubuntu 16.04 CLIENT_SECURE_CONNECTION error.

```
##############
error: 'CLIENT_SECURE_CONNECTION' undeclared (first use in this function)
##############

after /home/user/Downloads/cryptdb/proxy-src/plugins/admin/admin-plugin.c:97 add
#define CLIENT_SECURE_CONNECTION 32768 /* New 4.1 authentication for MySQL5.6 */

after /home/user/Downloads/cryptdb/proxy-src/tests/unit/t_network_mysqld_packet.c:37 add
#define CLIENT_SECURE_CONNECTION 32768 /* New 4.1 authentication for MySQL5.6 */

after /home/user/Downloads/cryptdb/proxy-src/src/network_mysqld_packet.c:33 add
#define CLIENT_SECURE_CONNECTION 32768 /* New 4.1 authentication for MySQL5.6 */
```

Εικόνα 5.10: Ubuntu 16.04 CLIENT_SECURE_CONNECTION error (Solution).

Για Ubuntu 18.04

Παρατηρήθηκε ότι κατά την προσπάθεια εγκατάστασης του Crypt-DB σε λειτουργικά Ubuntu επόμενης γενιάς όπως η έκδοση 18.04 τόσο αυξάνονται τα προβλήματα που παρατηρούνται με τα πακέτα δεδομένων που χρησιμοποιεί το Crypt-DB, καθώς βγαίνουν errors στα οποία δεν έχει βρεθεί ακόμα κάποια λύση(Εικόνα 5.11), καθιστώντας αδύνατη την εγκατάστασή του.



Εικόνα 5.11: Ubuntu 18.04 EVENT_VERSION error.

Άρα, ένα βασικό εύρημα που ανέκυψε ήδη κατά την παραμετροποίηση του περιβάλλοντος δοκιμών είναι ότι η μη επικαιροποίηση του λογισμικού δημιουργεί σοβαρά προβλήματα εγκατάστασης (στο επόμενο κεφάλαιο με τα συμπεράσματα και τη μελλοντική έρευνα συζητείται περαιτέρω το εν λόγω εύρημα).

5.5 Πειραματικός Μέρος

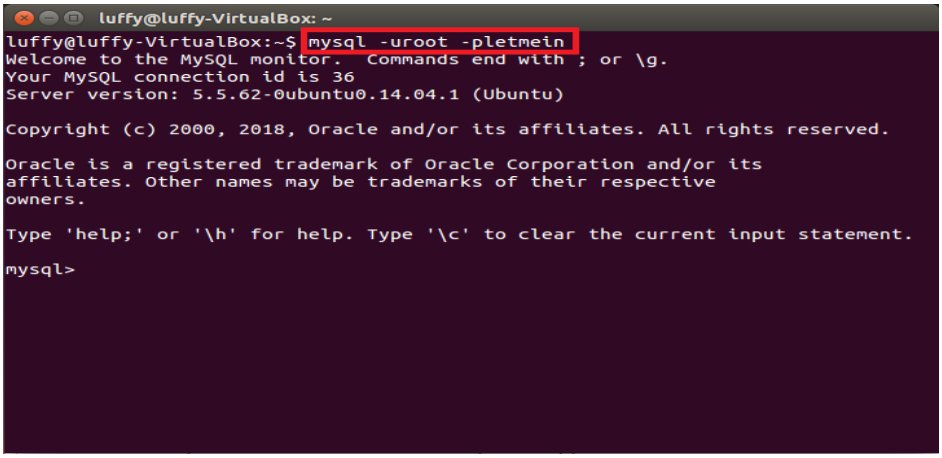
Στο πειραματικό μέρος παρουσιάζεται η εκτέλεση του προγράμματος Crypt_DBτο οποίο πραγματοποιεί κρυπτογράφηση σε πέντε πίνακες διαφορετικών βάσεων δεδομένων κάθε φορά. Επελέγη ένα απλό σενάριο βάσης δεδομένων, όπου η κάθε βάση έχει απλά έναν πίνακα.

Οι πίνακες εμπεριέχουν στοιχεία υπαλλήλων μισθοδοσίας και αποτελούνται από τρία πεδία, Όνομα (Name), IBAN, Μισθός(Amount) και διαφορετικό πλήθος υπαλλήλων. Οι ίδιοι οι πίνακες θα εισαχθούν και σε διαφορετικές βάσεις δεδομένων εκτός Crypt_DB, με σκοπό μέσω τις επιλογής

(SELECT) της MySQL να παρατηρήσουμε το χρόνο που γίνεται η επιλογή ενός πίνακα δεδομένων με κρυπτογράφηση Crypt_DB αλλά και χωρίς αυτή.

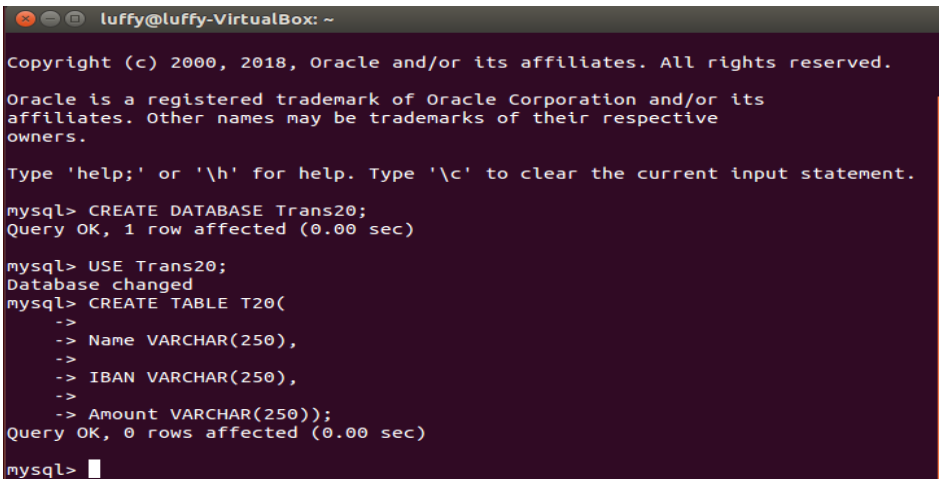
Πιο αναλυτικά:

Εκτέλεση της MySQL: Για την είσοδό μας στη MySQL μέσα από το τερματικό των Linux εκτελέστηκε η παρακάτω εντολή όπως φαίνεται στη παρακάτω εικόνα (Εικόνα 5.12).



Εικόνα 5.12: Είσοδο στη MySQL.

Δημιουργία Βάσης Δεδομένων και Πίνακα: Η δημιουργία μίας βάσης δεδομένων και ενός πίνακα γίνεται με τις παρακάτω τρεις εντολές (CREATEDATABASE *Name of the Database;*, USE *Name of the Database;* CREATE TABLE *Name of the Table;)* όπως φαίνεται στη παρακάτω εικόνα (Εικόνα 5.13).



Εικόνα 5.13: Δημιουργία βάσης δεδομένων (CREATEDATABASE) Trans20, Χρήση (USE) της συγκεκριμένης βάσης και δημιουργία πίνακα (CREATETABLE) με όνομα T20.

Εκτέλεση της Εντολής Εισαγωγής Δεδομένων σε Πίνακα: Για την εισαγωγή δεδομένων σε πίνακα χρησιμοποιείται η εντολή INSERT INTO Name of the Table (Name of the column1, Nameofthecolumn2, Nameofthecolumn3,….) VALUES (value1, value 2 value 3,…); όπως φαίνεται στη παρακάτω εικόνα(Εικόνα 5.14).

```
mysql> INSERT INTO T20 (Name,IBAN,Amount)  VALUES  ('Victor Cobb','GB34BARC20040
442936671','1000'),  ('Aaron Fox','GB67BARC20038453925469','1500'),  ('Rodney Ma
ck','GB28BARC20039517783759','600'),  ('Phil Lewis','GB30BARC20040446312634','16
00'),  ('Blanche Waters','GB67BARC20035364364986','2000'),  ('Lucia Nguyen','GB8
0BARC20031843859556','700'),  ('Tabitha Williams','GB12BARC20040192491312','500'
),  ('Laverne Romero','GB53BARC20031865283268','1200'),  ('Teresa Simon','GB14BA
RC20040486334831','1300'),  ('Ivan Mendez','ES6420387648748781475286','2500'),
('Herbert Lamb','GB26BARC20040161113985','3000'),  ('Lynn Maxwell','GB45BARC2004
0439967497','2100'),  ('Rita Sutton','GB97BARC20040141673519','2300'),  ('Dawn H
aynes','GB15BARC20037817685751','450'),  ('Dwayne Frank','GB33BARC20031815778126
','600'),  ('Gladys Gray','GB93BARC20031865695865','750'),  ('Connie Perry','GB8
4BARC20037859982135','900'),  ('Celia Romero','GB40BARC20037861346941','1700'),
 ('Percy Fields','GB33BARC20040464953264','2600'),  ('Clifton Tucker','GB44BARC2
0040441453264','4000');
Query OK, 20 rows affected (0.01 sec)
Records: 20  Duplicates: 0  Warnings: 0

mysql>
```

Εικόνα 5.14: Εισαγωγή στοιχείων 20 υπαλλήλων στο πίνακα T20 με χρήση της εντολής INSERT INTO.

Εκτέλεση της εντολής επιλογής SELECT: Εφόσον πραγματοποιηθεί η εισαγωγή μεταβλητών στον εκάστοτε πίνακα στην συνέχεια εκτελείται η εντολή επιλογής SELECT η οποία μας επιλέγει τα στοιχεία του εκάστοτε πίνακα και μας δείχνει το χρόνο εκτέλεσής της (Εικόνα 5.15).

```
mysql> SELECT*FROM T20;
+------------------+--------------------------+--------+
| Name             | IBAN                     | Amount |
+------------------+--------------------------+--------+
| Victor Cobb      | GB34BARC20040442936671   | 1000   |
| Aaron Fox        | GB67BARC20038453925469   | 1500   |
| Rodney Mack      | GB28BARC20039517783759   | 600    |
| Phil Lewis       | GB30BARC20040446312634   | 1600   |
| Blanche Waters   | GB67BARC20035364364986   | 2000   |
| Lucia Nguyen     | GB80BARC20031843859556   | 700    |
| Tabitha Williams | GB12BARC20040192491312   | 500    |
| Laverne Romero   | GB53BARC20031865283268   | 1200   |
| Teresa Simon     | GB14BARC20040486334831   | 1300   |
| Ivan Mendez      | ES6420387648748781475286 | 2500   |
| Herbert Lamb     | GB26BARC20040161113985   | 3000   |
| Lynn Maxwell     | GB45BARC20040439967497   | 2100   |
| Rita Sutton      | GB97BARC20040141673519   | 2300   |
| Dawn Haynes      | GB15BARC20037817685751   | 450    |
| Dwayne Frank     | GB33BARC20031815778126   | 600    |
| Gladys Gray      | GB93BARC20031865695865   | 750    |
| Connie Perry     | GB84BARC20037859982135   | 900    |
| Celia Romero     | GB40BARC20037861346941   | 1700   |
| Percy Fields     | GB33BARC20040464953264   | 2600   |
| Clifton Tucker   | GB44BARC20040441453264   | 4000   |
+------------------+--------------------------+--------+
20 rows in set (0.00 sec)
```

Εικόνα 5.15: Εκτέλεση της εντολής επιλογής SELECTπου επιλέγει όλα τα δεδομένα του πίνακα T20 και εμφάνισης του χρόνου εκτέλεσής της.

Εκτέλεση ενεργοποίησης του Query Profiler: Όπως μπορούμε να δούμε και στη παραπάνω εικόνα (Εικόνα 5,15) με την εκτέλεση της εντολής SELECT δεν μπορούμε να έχουμε σαφή εικόνα του χρόνου εκτέλεσής της καθώς το αποτέλεσμα που έχουμε είναι 0,00sec. Για αυτό το λόγο ενεργοποιούμε το Query Profiler (Εικόνα 5.16)το οποίο μας βοηθά να μετρήσουμε με μεγαλύτερη ακρίβεια το κάθε ερώτημα (query)που εκτελείται στη βάση δεδομένων.

```
mysql> SET PROFILING=1;
Query OK, 0 rows affected (0.00 sec)
```

Εικόνα 5.16: Ενεργοποίηση του Query Profiler.

Με αυτό τον τρόπο εκτελώντας ξανά την εντολή SELECT μπορούμε να δούμε τον ακριβή χρόνο εκτέλεσής της εκτελώντας την εντολή SHOWPROFILES(Εικόνα 5.17).

```
mysql> SHOW PROFILES;
+----------+------------+------------------+
| Query_ID | Duration   | Query            |
+----------+------------+------------------+
|        1 | 0.00013525 | SELECT*FROM T20 |
+----------+------------+------------------+
1 row in set (0.00 sec)
```

Εικόνα 5.17: Εντολή SHOW PROFILESγια πίνακα 20 υπαλλήλων.

Η ίδια διαδικασία εκτελέστηκε ξανά για άλλους 4 πίνακες με διαφορετικά πλήθη εγγραφών και τα αποτελέσματα των χρόνων εκτέλεσης αυτών είναι τα εξής:

```
mysql> SHOW PROFILES;
+----------+------------+-----------------+
| Query_ID | Duration   | Query           |
+----------+------------+-----------------+
|        1 | 0.00015725 | SELECT*FROM T40 |
+----------+------------+-----------------+
1 row in set (0.00 sec)
```

Εικόνα 5.18: Εντολή SHOWPROFILESγια πίνακα 40 υπαλλήλων.

```
mysql> SHOW PROFILES;
+----------+------------+-----------------+
| Query_ID | Duration   | Query           |
+----------+------------+-----------------+
|        1 | 0.00015975 | SELECT*FROM T60 |
+----------+------------+-----------------+
1 row in set (0.00 sec)
```

Εικόνα 5.19: Εντολή SHOW PROFILESγια πίνακα 60 υπαλλήλων.

```
mysql> SHOW PROFILES;
+----------+------------+-----------------+
| Query_ID | Duration   | Query           |
+----------+------------+-----------------+
|        1 | 0.00024950 | SELECT*FROM T80 |
+----------+------------+-----------------+
1 row in set (0.00 sec)
```

Εικόνα 5.20: Εντολή SHOW PROFILESγια πίνακα 80 υπαλλήλων.

```
mysql> SHOW PROFILES;
+----------+------------+------------------+
| Query_ID | Duration   | Query            |
+----------+------------+------------------+
|        1 | 0.00026650 | SELECT*FROM T100 |
+----------+------------+------------------+
1 row in set (0.00 sec)
```

Εικόνα 5.21: Εντολή SHOW PROFILESγια πίνακα 100 υπαλλήλων.

Έπειτα πραγματοποιήθηκε η ίδια διαδικασία(με εξαίρεση τη μη χρησιμοποίηση του Query Profiler) χρησιμοποιώντας όμως το Crypt_DB:

Έναρξη του Προγράμματος Crypt_DB: Για την έναρξη του proxy του Crypt_DB χρησιμοποιούμε τις παρακάτω εντολές όπως φαίνεται στην παρακάτω εικόνα(Εικόνα 5.22).

```
luffy@luffy-VirtualBox:~$ export EDBDIR=/home/luffy/cryptdb
luffy@luffy-VirtualBox:~$ /home/luffy/cryptdb/bins/proxy-bin/bin/mysql-proxy
    \
>                           --plugins=proxy --event-threads=4             \
>                           --max-open-files=1024                         \
>                           --proxy-lua-script=$EDBDIR/mysqlproxy/wrapper.lua \
>                           --proxy-address=127.0.0.1:3307                \
>                           --proxy-backend-addresses=localhost:3306
2022-11-10 17:46:32: (critical) plugin proxy 0.8.4 started
```

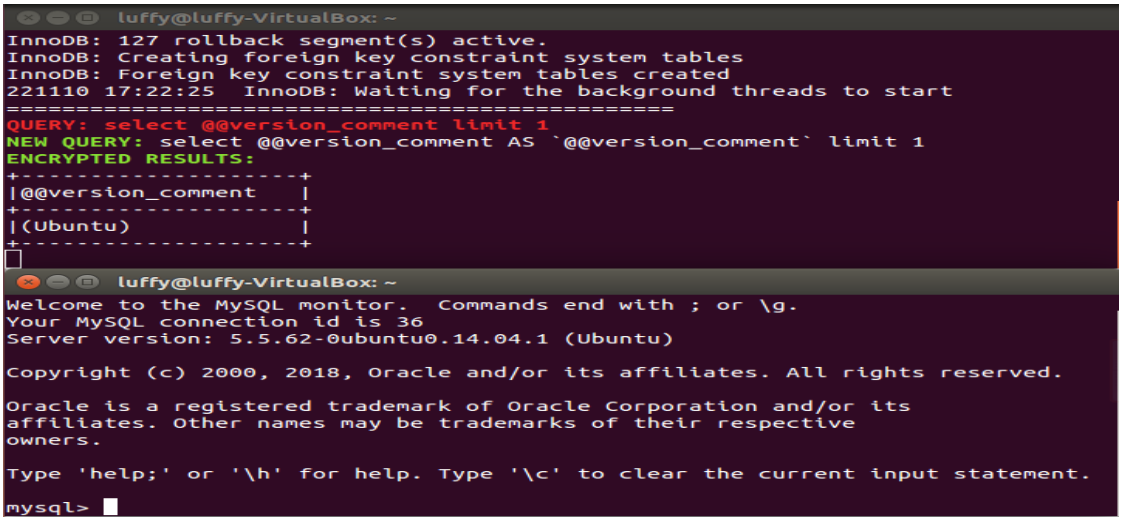
Εικόνα 5.22: Έναρξη του Crypt-DB proxy.

Στη συνέχεια χρησιμοποιήθηκε καινούργιο τερματικό για την είσοδο σε διαφορετικό port στη MySQL για να συνδεθεί με το Crypt-DB proxy (Εικόνα 5.23).

```
luffy@luffy-VirtualBox: ~
luffy@luffy-VirtualBox:~$ export EDBDIR=/home/luffy/cryptdb
luffy@luffy-VirtualBox:~$ /home/luffy/cryptdb/bins/proxy-bin/bin/mysql-proxy
    \
>                           --plugins=proxy --event-threads=4             \
>                           --max-open-files=1024                         \
>                           --proxy-lua-script=$EDBDIR/mysqlproxy/wrapper.lua \
>                           --proxy-address=127.0.0.1:3307                \
>                           --proxy-backend-addresses=localhost:3306
2022-11-11 21:38:50: (critical) plugin proxy 0.8.4 started

luffy@luffy-VirtualBox: ~
luffy@luffy-VirtualBox:~$ mysql -u root -pletmein -h 127.0.0.1 -P 3307
```

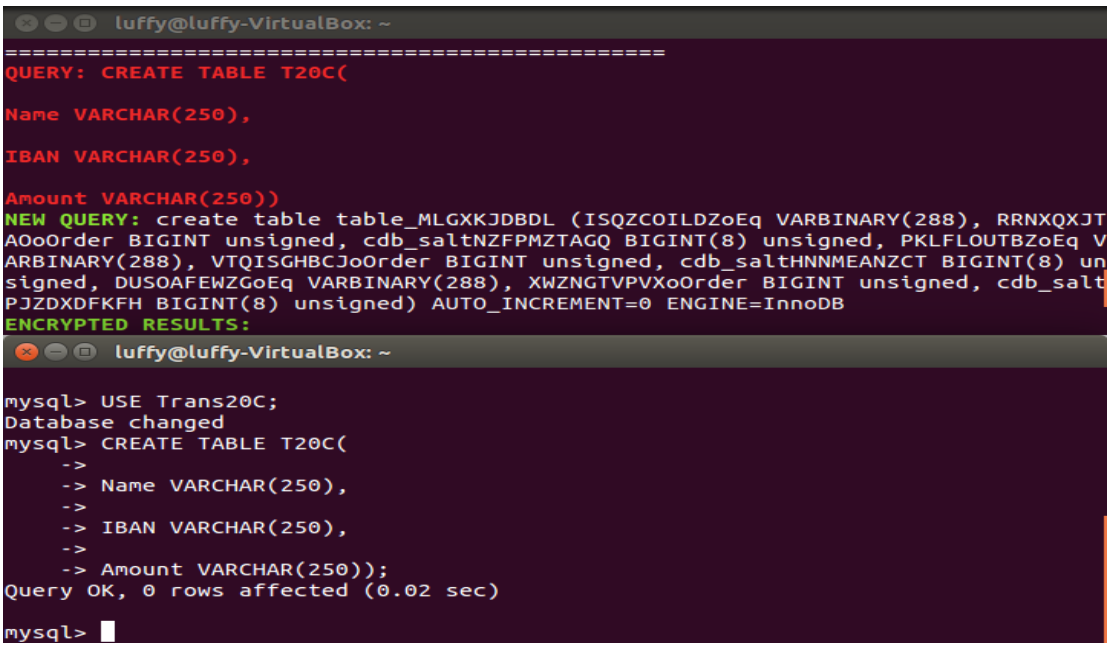
Εικόνα 5.23: Εκτέλεση εισόδου MySQL: *mysql-uroot-pletmein-h 127.0.0.1 –P 3007*.

Με την εκτέλεση είσόδου στη MySQL πραγματοποιείται ταυτόχρονη είσοδος και στον Crypt_DB proxy (Εικόνα 5.24).



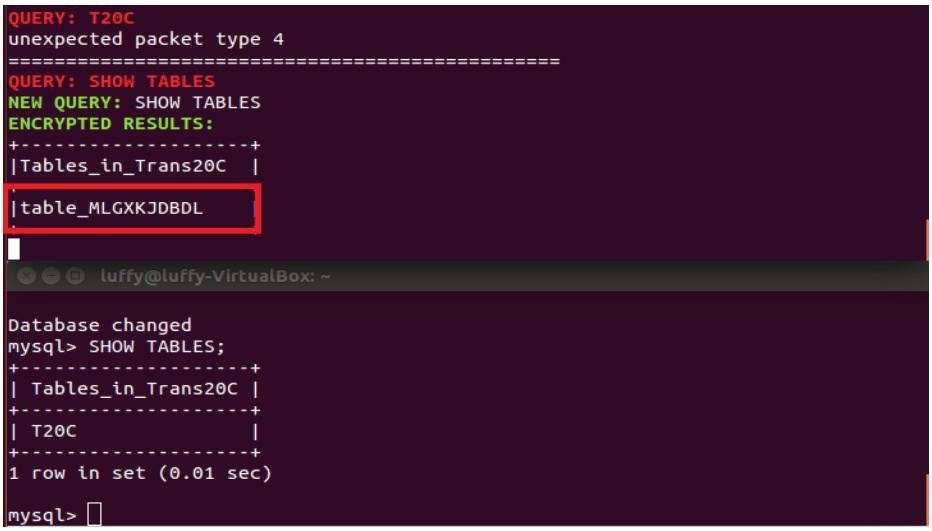
Εικόνα 5.24: Crypt-DB proxy Interface.

Δημιουργία Βάσης Δεδομένων και Πίνακα με ταυτόχρονη κρυπτογράφηση του Πίνακα από το Crypt DB: Στη παρακάτω εικόνα βλέπουμε τη δημιουργία του πίνακα T20Cπαρατηρώντας την κρυπτογράφηση του μέσω του Crypt-DB proxy (Εικόνα 5.25).



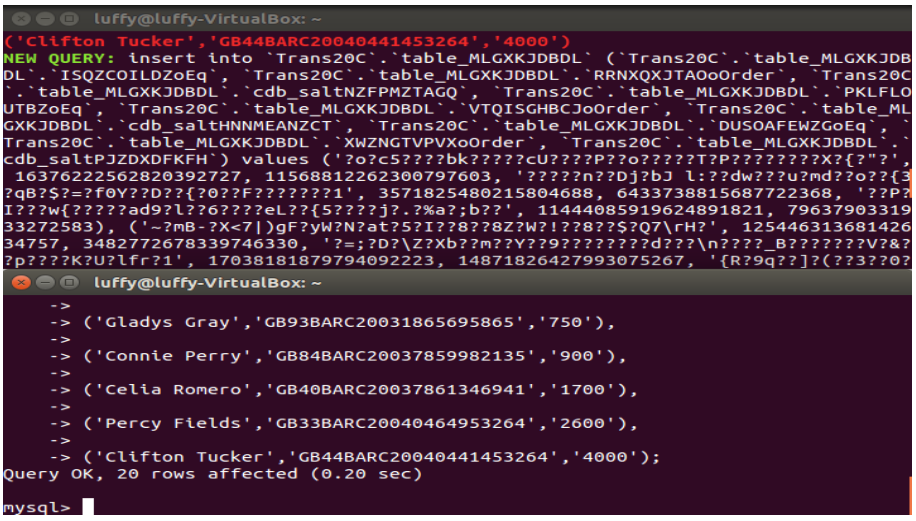
Εικόνα 5.25: Δημιουργία Πίνακα (CREATETABLE) T20Cμε παράλληλη κρυπτογράφηση μέσω Crypt-DB proxy.

Εκτέλεση εντολής SHOW TABLES; : Με την εκτέλεση της συγκεκριμένης εντολής μπορούμε να δούμε πόσους πίνακες διαθέτη μία βάση δεδομένων και πώς ονομάζονται. Παρατηρούμε όμως στο Crypt-DB χρησιμοποιώντας τη συγκεκριμένη εντολή το όνομα του εκάστοτε πίνακα κρυπτογραφείται και αυτό όπως φαίνεται στη παρακάτω εικόνα(Εικόνα 5.26).



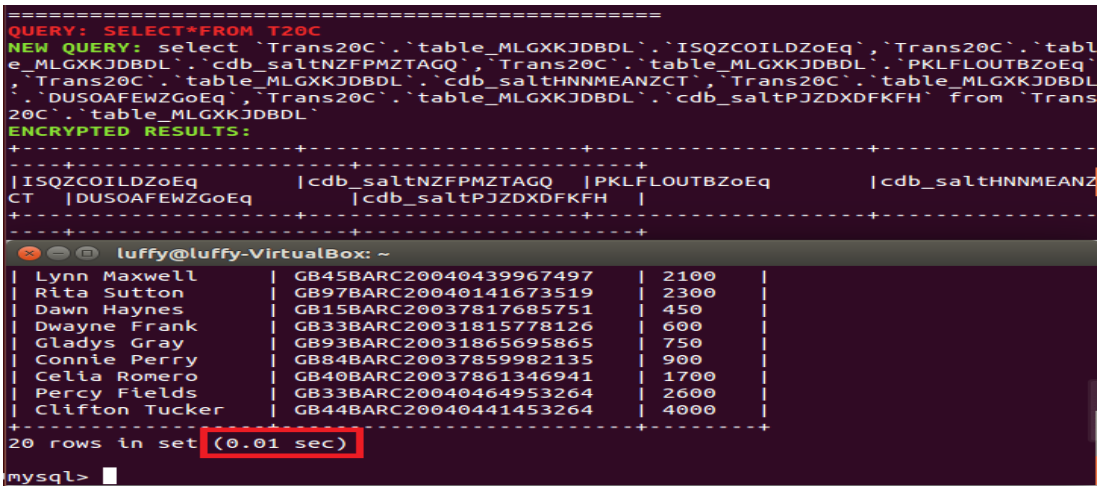
Εικόνα 5.26: Χρήση της εντολής SHOWTABLES; στη βάση δεδομένων Trans20C.

Εκτέλεση εντολής εισαγωγής δεδομένων σε Πίνακα χρησιμοποιώντας την εντολή INSERT INTO με ταυτόχρονη κρυπτογράφηση των δεδομένων μέσω του Crypt DB: Κατά την εκτέλεση της εντολής INSERT INTO παρατηρούμε μέσω του Crypt-DB proxy και την κρυπτογράφηση των δεδομένων που εισέρχονται στο συγκεκριμένο πίνακα(Εικόνα 5.27).



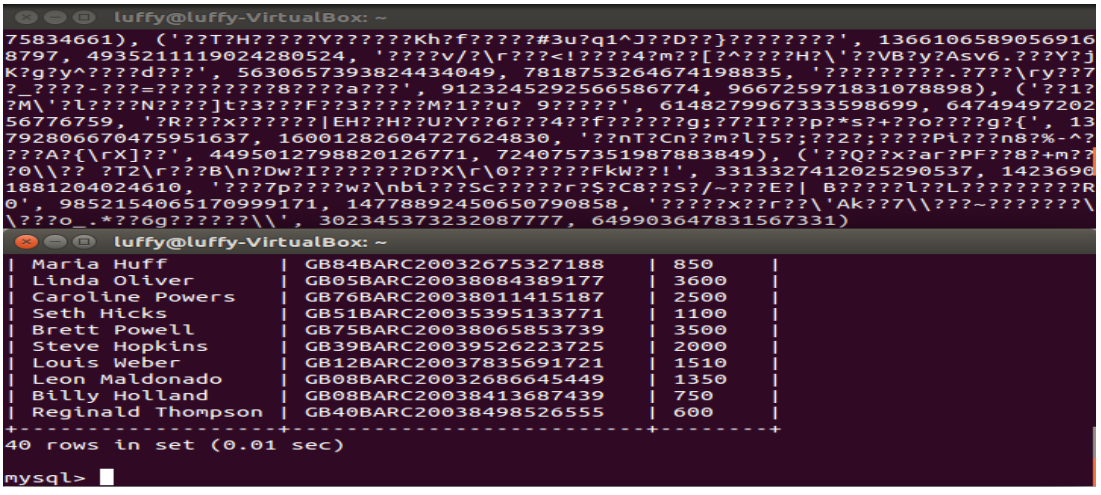
Εικόνα 5.27: Εκτέλεση εντολής INSERTINTOμε ταυτόχρονη κρυπτογράφηση των εισαγόμενων δεδομένων μέσω του Crypt-DB.

Εκτέλεση Εντολής Επιλογής SELECT με κρυπτογράφηση Crypt-DB: Με την εκτέλεση της εντολής SELECT παρατηρούμε την κρυπτογράφηση του εκάστοτε πίνακα καθώς και το χρόνο εκτέλεσης του συγκεκριμένου Query. Μπορούμε να δούμε τον χρόνο εκτέλεσης του συγκεκριμένου Query όπως φαίνεται στη παρακάτω εικόνα(Εικόνα 5.28) αλλά δε μπορούμε να χρησιμοποιήσουμε για περισσότερη ακρίβεια το Query Profiler καθώς δε λειτουργεί σε έτοιμες functions (UDF) που χρησιμοποιεί το Crypt-DB.

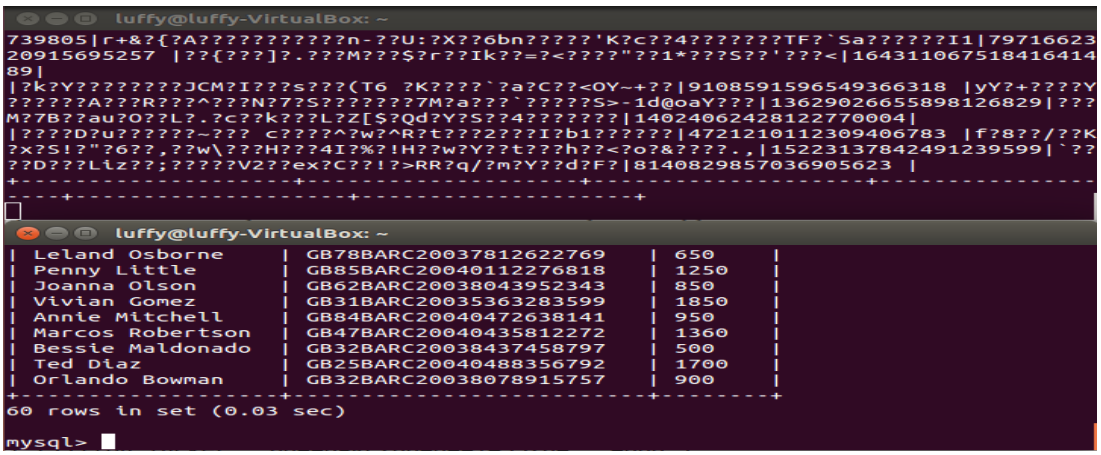


Εικόνα 5.28: Εκτέλεση εντολής επιλογής SELECT στο πίνακα T20C που αποτελείται από 20 υπαλλήλους με ταυτόχρονη κρυπτογράφησή του.

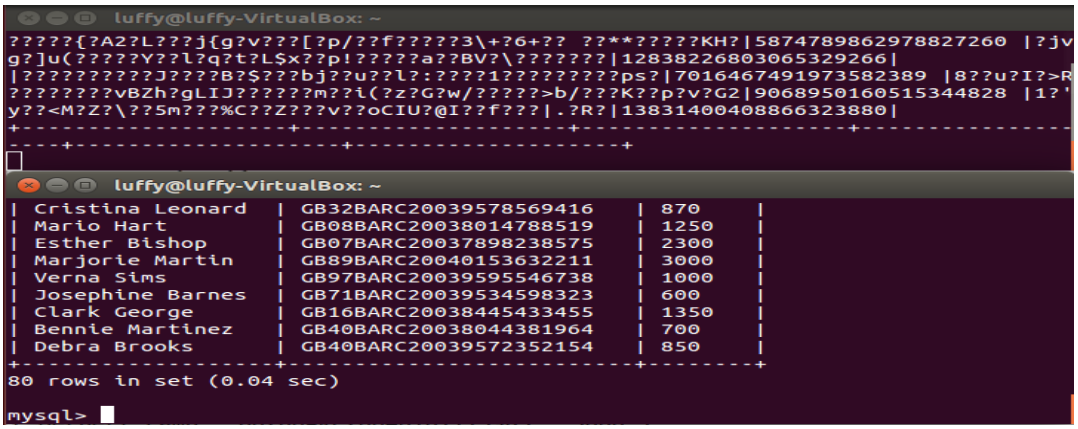
Στη συνέχεια πραγματοποιήθηκε η ίδια διαδικασία άλλες τέσσερις φορές σε άλλους τέσσερις πίνακες με διαφορετικό αριθμών υπαλλήλων:



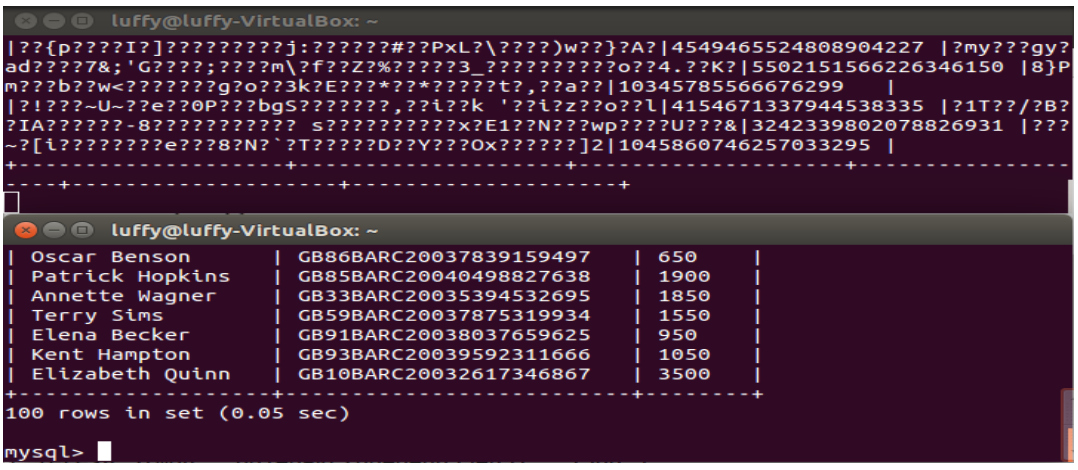
Εικόνα 5.29: Εκτέλεση εντολής επιλογής SELECTστο πίνακα T40Cπου αποτελείται από 40 υπαλλήλους με ταυτόχρονη κρυπτογράφησή του.



Εικόνα 5.30: Εκτέλεση εντολής επιλογής SELECTστο πίνακα T60Cπου αποτελείται από 60 υπαλλήλους με ταυτόχρονη κρυπτογράφησή του.



Εικόνα 5.31: Εκτέλεση εντολής επιλογής SELECTστο πίνακα T80C που αποτελείται από 80 υπαλλήλους με ταυτόχρονη κρυπτογράφησή του.



Εικόνα 5.32: Εκτέλεση εντολής επιλογής SELECT στο πίνακα T100C που αποτελείται από 100 υπαλλήλους με ταυτόχρονη κρυπτογράφησή του.

Στη συνέχεια ακολουθεί ένας πίνακας ο οποίος εμπεριέχει αναλυτικά τους χρόνους εκτέλεσης των queries(εντολή SELECT) για όλες τι βάσεις δεδομένων αλλά και η διαφορά ταχύτητας που παρατηρείται μεταξύ της εκτέλεσης των queries σε απλή MySQL(χωρίς Crypt-DB) και σε MySQL με Crypt-DB. Να σημειωθεί ότι η βασική μνήμη της εικονικής μηχανής (Virtual Box) ανέρχεται στο 1GBκαθώς και χρησιμοποιήθηκε ένας πυρήνας του επεξεργαστή (AMD Ryzen 7 3700X).

Πίνακες Βάσεων δεδομένων Trans	**MySQL-Without Crypt-DB(A)**	**MySQL-With Crypt-DB(B)**	**Speed Difference (B-A)/A *100%**
T20,T20C	0,00013525sec	0,01 sec	72,937%
T40,T40C	0,00015725sec	0,01 sec	62.593%
T60,T60C	0,00015975sec	0,03 sec	186,79%
T80,T80C	0,00024950sec	0,04 sec	159,32%
T100,T100C	0,00026650sec	0,05 sec	186,61%

Πίνακας 5.1: Αναλυτικός πίνακας εκτέλεσης Queries(εντολή SELECT) στη My SQLμε και χωρίς το Crypt-DB καθώς και υπολογισμός της διαφοράς ταχύτητας μεταξύ των δύο αυτών περιπτώσεων.

Οι χρόνοι εκτέλεσης αφορούν, όπως είδαμε, την εκτέλεση της πιο απλής select εντολής, προκειμένου να επιστραφούν όλες οι εγγραφές ενός πίνακα. Ήδη όμως από αυτές τις εντολές διαφαίνεται ότι η υποκείμενη κρυπτογράφηση που υλοποιεί το λογισμικό Crypt-DB εισάγει καθυστέρηση στην εκτέλεση των υπολογισμών (αν και σαφέστατα τα πειράματα που υλοποιήθηκαν δεν είναι εκτεταμένα).Μία καθυστέρηση στο χρόνο εκτέλεσης των ερωτημάτων ήταν σαφώς αναμενόμενο να διαφανεί, ενώ για τον ακριβή προσδιορισμό της σε ρεαλιστικές συνθήκες απαιτείται πολύ εκτεταμένο εύρος πειραμάτων, σε πιο σύνθετες βάσεις δεδομένων και με ερωτήματα που απαιτούν «συνδέσεις» (joins) μεταξύ πινάκων, σε διαφορετικά υπολογιστικά περιβάλλοντα. Σε κάθε δε περίπτωση, θα πρέπει συμπερασματικά να ειπωθούν τα εξής:

1. Αν και η απόδοση είναι ένας πολύ σημαντικός παράγοντας, θα πρέπει να ανακαλέσουμε ότι ο ΓΚΠΔ προκρίνει τη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων στο πλαίσιο μίας διαχείρισης κινδύνων, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και

τους κινδύνους για τα φυσικά πρόσωπα. Συνεπώς, αν από μία επεξεργασία προσωπικών δεδομένων μέσω βάσεων δεδομένων ελλοχεύουν πολύ υψηλοί κίνδυνοι για τα φυσικά πρόσωπα, είναι εξαιρετικά πιθανό η υιοθέτηση αντίστοιχων λύσεων να είναι αναγκαία προϋπόθεση για την αντιμετώπιση των κινδύνων αυτών (με αποδεκτό «κόστος» μία υποβάθμιση στην απόδοση).

2. Οι περιπτώσεις όπου εργαλεία όπως το Crypt-DB αφορούν σαφώς και υπηρεσίες υπολογιστικού νέφους. Σε τέτοιες περιπτώσεις, οι πάροχοι των υπηρεσιών αυτών διαθέτουν πολύ σημαντική υπολογιστική ισχύ, με αποτέλεσμα να μειώνεται η επίδραση της καθυστέρησης πραγματοποίησης των υπολογισμών στη συνολική απόδοση της προσφερόμενης υπηρεσίας.

Κεφάλαιο 6
Συμπεράσματα-Επίλογος

Η παρούσα διατριβή εστίασε σε προηγμένες κρυπτογραφικές τεχνικές, οι οποίες μπορούν να παρέχουν λύσεις σε περιπτώσεις για τις οποίες αποτυγχάνουν εκ των πραγμάτων οι παραδοσιακές κρυπτογραφικές μέθοδοι. Λαμβάνοντας υπόψη και τις νομικές απαιτήσεις αναφορικά με την προστασία προσωπικών δεδομένων, διαφαίνεται πράγματι ότι οι εν λόγω τεχνικές μπορούν να αποτελούν την «απάντηση» σε πολλές περιπτώσεις, επιτρέποντας έτσι τους οργανισμούς να υλοποιούν την απαίτηση για «προστασία των δεδομένων ήδη από το σχεδιασμό» (data protection by design). Παρόλο που ακαδημαϊκά οι εν λόγω προηγμένες κρυπτογραφικές τεχνικές είναι γνωστές εδώ και πολλά έτη, και συνεχίζουν να αποτελούν ενεργό αντικείμενο έρευνας, εν τούτοις φαίνεται ότι η υιοθέτησή τους στην πράξη δεν είναι ακόμη αρκετά εκτεταμένη: συναντώνται μεν, αλλά όχι στον αναμενόμενο βαθμό, αφού διαφαίνεται ένα κενό μεταξύ των ακαδημαϊκών λύσεων και των τελικών προϊόντων λογισμικού που αναπτύσσονται.

Η διατριβή επίσης εστίασε σε ένα ελεύθερα διαθέσιμο εργαλείο λογισμικού, το Crypt-DB, το οποίο υλοποιεί πολλές από αυτές τις τεχνικές και προσφέρει λύσεις για περιπτώσεις προστασίας βάσεων δεδομένων. Ο λόγος που επελέγη το εν λόγω εργαλείο ως μελέτη περίπτωσης είναι ότι έχει αναπτυχθεί από ερευνητές του Πανεπιστημίου MIT, έχει πολύ καλά θεμελιωμένες

μαθηματικές ιδιότητες, ενώ η ασφάλειά του δεν έχει αμφισβητηθεί παρά το γεγονός ότι είναι ήδη ελεύθερα διαθέσιμο επί δέκα περίπου έτη. Παρόλα αυτά διαπιστώθηκε ότι το εργαλείο δεν επικαιροποιείται πλέον, με αποτέλεσμα να μην είναι καθόλου ευχερής η υιοθέτησή του (βλ. τη σχετική ανάλυση στο Κεφάλαιο 5). Αυτή η παρατήρηση ενισχύει τον προηγούμενο ισχυρισμό σχετικά με τη μη ευρεία υιοθέτηση προηγμένων τεχνικών κρυπτογράφησης σε πραγματικά συστήματα, παρόλο που αντίστοιχες λύσεις δεν μπορούν να παρασχεθούν από παραδοσιακές κρυπτογραφικές τεχνικές.

Τα κύρια συμπεράσματα τα οποία απορρέουν από την παρούσα διατριβή είναι τα εξής:

1. Υπάρχει πληθώρα κρυπτογραφικών τεχνικών οι οποίες επιτρέπουν «πράξεις» επί κρυπτογραφημένων δεδομένων και οι οποίες δεν είναι ευρέως διαδεδομένες. Ωστόσο, στο πλαίσιο μίας διαχείρισης κινδύνων, διαφαίνεται ότι η υιοθέτηση τέτοιων λύσεων σε πολλές περιπτώσεις θα κρινόταν απαραίτητη. Θα μπορούσε δε να ειπωθεί ότι η μη υιοθέτησή τους μπορεί, σε συγκεκριμένες περιπτώσεις, να παραβιάζει και τη θεμελιώδη αρχή του «data protection by design».

2. Ένας λόγος που δεν υιοθετούνται τέτοιες λύσεις φαίνεται να είναι ότι δεν είναι πάντα ευχερώς διαθέσιμες σε έτοιμα προϊόντα λογισμικού. Ένας οργανισμός αναζητά λύσεις λογισμικού από τις ήδη διαθέσιμες προκειμένου να ενισχύσει την ασφάλεια και προστασία των δεδομένων του και δεν «επενδύει» στο να αναπτύξει κάτι εκ του μηδενός ή έστω να υιοθετήσει μία λύση που προσφέρεται από την ακαδημαϊκή κοινότητα.

3. Για να αρθεί ο ανωτέρω περιορισμός, είναι ανάγκη για περαιτέρω ενέργειες όλων των εμπλεκομένων, συμπεριλαμβανομένων των εταιρειών παραγωγής λογισμικού, των ερευνητικών/ακαδημαϊκών κέντρων, των οργανισμών/επιχειρήσεων, των αρχών προστασίας δεδομένων και των εθνικών αρχών κυβερνοασφάλειας, αλλά και του ευρωπαίου νομοθέτη προς την κατεύθυνση ενσωμάτωσης τέτοιων λύσεων στην πράξη. Για παράδειγμα, κρίνεται σκόπιμο να αναπτυχθούν πρότυπα (standards) που να βασίζονται σε τέτοιες λύσεις, τα οποία με τη σειρά τους αναμένεται να δώσουν ώθηση στην περαιτέρω εξάπλωσή τους. Περαιτέρω, οι αρμόδιες αρχές θα πρέπει να προκρίνουν σαφώς τη χρήση τους.

Αν αναλογιστεί κανείς ότι, αν δεν υιοθετηθεί η καλύτερη δυνατή λύση εξ αρχής, πολλές φορές δεν μπορεί εύκολα να «εμφυτευτεί» εκ των υστέρων και απαιτείται εκ βάθρων ανασχεδίαση ενός

συστήματος επεξεργασίας δεδομένων, γίνεται σαφής η σημασία της έγκαιρης ενσωμάτωσης τεχνολογικών λύσεων που διασφαλίζουν τις θεμελιώδεις αρχές προστασίας δεδομένων.

Βιβλιογραφία

[01] Manuel A. Serano and Eduardo Fernández-Medina Julio Moreno, "Main Issues inn Big Data Security," *Specria Issue: Security in Cloud Computing and Big Data*, pp. 44; https://doi.org/10.3390/fi8030044, 2016.

[02] Michael Friedewald, Marit Hansen, Hannah Obersteller & Martin Rost Felix Bieker, "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation," in *Privacy Technologies and Policy*. Frankfurt: Springer, 2016, pp. 21–37.

[03] Stephen Lyle Tu, M. Frans Kaashoek, Samuel R. Madden, and Nickolai Zeldovich, "Processing Analytical Queries over Encrypted Data," *Proceedings of the 39th international conference on Very Large Data Bases (PVLDB '13)*, pp. http://hdl.handle.net/1721.1/87023, 2013.

[04] William P. Zeller, Michael J. Freedman, and Edward W. Felten. Ariel J. Feldman, "SPORC: Group collaboration using untrusted cloud resources. ," *In Proceedings of the 9th Symposium on Operating Systems Design and Implementation*, 2010.

[05] Jonathan Katz Moti Yung, *Digital Signatures (Advances in Information Security)*. Berlin: Springer-Verlag, 2005.

[06] Mohammed. Al-Shabi, "A Survey on Symmetric and Asymmetric Cryptography Algorithms in Information Security.," *International Journal of Scientific and Research Publications(IJSRP)*, pp. 9, p8779, 10.29322/IJSEP.9.03.2019.p8779., 2019.

[07] M.Helman W.Diffie, "Multiuser Cryptographic Techniques, proceedings of AFIPS National Computer Conference ," pp. 109-112, 1976.

|[09] V.Rijmen J.Daemon, "The Rijndael Block Cipher: AES Proposal, NIST, Version 2," 1999.

|[11] W.Stallings, "Cryptography and Network Security," *Principle and Practices , Fourth Edition , Pearson Education*, 2006.

|[13] T.P Innokentievich and M.V Vasilevich, "The Evaluation of the cryptographic strength of asymmetric encryption algorithms.," in *2017 Second Russia and Pacific Conference on Computer Technologyy and Application(RPC)*, 2017, pp. 180-183.

|[15] A.J, Van Oorschot, P.C, & Vanston, S.A Menezes, "Handbook of Applied Cryptography(1st ed)," in *Handbook of Applied Cryptography(1st ed)*.: CRS Press, 1997, p. 10.1201/9780429466335.

|[17] C.Sanchez-Avila and R.Sanchez-Reillol, "The Rijndael block cipher (AES proposal): a comparison with DES," in *Proceedings IEEE 35th Annual 2001 Internation Carnahan Conference on Security Technology*, 2001, pp. 229-234, 10.1109/CCST.2001.962837.

|[19] J, Lindell,A.Y Katz, "Agreegate Message Authentication Codes, CT-RSA 2008:Topics in Cryptology in CT-RSA.2008.," in *Lecture Notes In Computer Sciences, vol 4964*. Berlin: Springer, 2008, pp. 10.1007/978-3-540-79263-5_10.

|[21] Evgeny Milanov, "The RSA Algorithm," 2009.

[22] K & Arivazhagan,D Gameshkumar, "Generating A Digital Signature Based On New Cryptographic Scheme For User Authentication And Security.," *Indian Journal of Science and Technology*, pp. 7. 1-5. 10.17485/ijst/2014/v7sp6.1, 2014.

[23] NIST. (2006, May) https://csrc.nist.gov. [Online]. https://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1.pdf

[24] Bob & Whittington, Mark Duncan, *The Complexities of Auditing and Securing Systems in the Cloud- is there a Solution and will the GDPR move it up the Corporate Agenda?*, 2018.

[25] Curtis. (2018) Privacy notice relating to data protection. [Online]. https://www.curtis.com/legal-notices/privacy-notice-relating-to-data-protection

[26] M Goddard, "The EU General Data Protection Regulation(GDPR): European Regulation that has a Global Impact," *International Journal of Market Research* , pp. 59(6), 703-705, https://doi.org/10.2501/IJMR-2017-050, 2017.

[27] EU Regulation. (2016) Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Diractive 95/46/EC(General Data Protection Regulation). [Online]. https://www.eumonitor.eu/9353000/1/j4nvk6yhcbpeywk_j9vvik7m1c3gyxp/vk3t7p3lbczq#:~:text=Regulation%20(EU)%202016%2F679%20of%20the%20European%20Parliament%20and,(OJ%20L%20119%2C%204.5.

[28] Gunathunga.S. (2017) Defining a Winning GDPR Strategy Part1 - Introduction to GDPR. [Online]. https://wso2.com/library/article/2017/12/introduction-to-gdpr/

[29] Biscoe. (2018) Resolving conflicts between the security team and the rest of the businees. [Online]. https://www.itgovernance.eu/blog/en/author/cbiscoe

[30] John j.Borking, and J.G Eddy Olk Gilles W. van Blarkom, "The Case of Inteliigent Software Agents," in *Handbook of Privacy and Privacy-Enhancing Technologies.*: Bescherming Persoonsgegevens, 2003.

[31] C.Troncoso, "Design and Analysis Methods for Privacy Technologies," *Dissertation presented in partial fulfillment of the requierements for the degree of Doctor in Electrical Engineering.Arenberg Doctoral School of Science, Engineering & Technology Faculty of Enginnering Department of Electrical Engineering (ESAT)*, 2011.

[32] Sommer.D, Zimmermann.R Camenisch.J, "A General Certification Framework with Applications to Privacy-Enhacning Certificate Infrastructures.," in *Security and Privacy in Dynamic Enviroments.SEC 2006. IFIP International Federation for Information Processing vol 201*. Boston, MA: Springer, 2006, pp. htts://doi.org/10.1007/0-387-33406-8_3.

[33] M.et.al Lepinski, "Privacy-Enhacned Android for Smart Cities Applications. In: et al. Smart City 360. Smart City 360 2016-2015," in *Lecture Notes of the Institute of Computer Sciences, Social Informatics and Telecommunications Engineering vol 166.*: Springer, 2016, pp. https://doi.org/10.1007/978-3-319-33681-7_6.

[34] P.Xuteal, "ROSE: Robust Searchable Encryption With Forward and Backward Security," *Transactions on Information Forensics and Security vol 17*, pp. 1115-1130, doi:10.1109/TIFS.2022.3155977, 2022.

[35] J.Wang,S.Sun,M.Miao and X.Chen Y.Wang, "Toward Forward Secure SSE Supporting Conjunctive Keyword Search," *IEEE Access, Vol 7*, pp. 142762-142772, doi: 10.1109/ACCESS.2019.2944246., 2019.

[36] Peter Zimmermann, Thomas Neubauer, Stefan Fenz Johannes Heurix, "A Taxanomy for privacy enhancing technologies.," *Computers & Security, Volume 53*, pp. 1-17, 2015.

[37] Chenette.N, O'Neill.A Boldyreva.A, "Order-Preserving Encryption Revisited: Improved Security Analysis and Alternative Solutions," in *Advances in Cryptology-CRYPTO 2011. CRYPTO 2011.Lecture Notes in Computer Science, vol*

6842. Berlin, Heidelberg: Springer, 2011, pp. https://doi.org/10.1007/978-3-642-22792-9 33.

[38] Hidayet Aksu, A.Selcuk Uluagac and Mauro Conti Abbas Acar, "A Survey on Homomorphic Ecryption Schemes: Theory and Implemetation," *ACM Comput. Surv 51,4 Article 79(July 2019)*, pp. 35, https://doi.org/10.1145/3214303, 2018.

[39] Siani Pearson Yun Shen, "Privacy Enhancing Technologies: A Review. HP Laboratories HPL," p. 113, 2011.

[40] Gritzalis S, Kioulafas.C Argyrakis.J, "Privacy Enhancing Technologies :A Review In: Traunmuller.R(eds) Electronic Goverment EGOV 2003.," in *Lecture Notes in Computer Science vol 2739*. Berllin,Heidelberg: Science , 2003, pp. https://doi.org/10.1007/10929179_51.

[41] The Tor Project. (2018) The Tor Project. [Online]. https://www.torproject.org

[42] Maryline Laurent, Sana Belguith Nesrine Kaaniche, "Privacy enhancing technologies of solving the privacy-personalization paradox," *Taxonomy and survey ,Journey of Network and Computer Applications, Volume 171*, pp. 102807,ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2020.102807, 2020.

[43] Peter Berlich,Jan Camenisch,Sebestian Clauβ, Andreas Pfitzmann, Michael Wainder Marit Hansen, "Privacy-enhancing identity managment," *Information Security Technical Report Volume 9, Issue 1*, pp. 35-44, ISSN 1363-4127, https://doi.org/10.1016/S1363-4127(04)00014-7, 2004.

[44] Krenn.S, Lehmann.A, Mikkelsen, G.L, Neven.G, Pedersen.MO. Camenisch.J, "Formal Treathment of Privacy-Enhancing Credential Systems," in *Selected Areas in Cryptography-SAC 2015. SAC 2015 Lecture Notes in Computer Science(), vol 9566.*: Springer, 2016, pp. https://doi.org/10.1007/978-3-319-31301-6_1.

[45] S.- Y.Huang and Y.-L.Lai C-I Fan, "Privacy-Enhanced Data Aggresion Schemme Against Internal Attackers in Smart Grid," *IEEE Transactions on Industrial Informatics, vol 10, no 1*, pp. 666-675, Feb.2014 ,doi: 10.1109/TII.2013.2277938., 2014.

[46] Konstantinos Limniotis, "Cryptography as the Means to Protect Fundamental," *Cryptography 2021*, pp. https://doi.org/10.3390/, 2021.

[47] Yi Jiang Dhaval Pate, "Overview of CryptDB," *CPSC 5670 Term Paper*, 2013.