ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

«Προστασία ψηφιακών πόρων με τεχνολογίες κρυπτογραφίας βάσει χαρακτηριστικών»

Γιαννούλη Ευαγγελία

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Λιουδάκης
Εντεταλμένος Διδάσκων

ΣΥΝΕΠΙΒΛΕΠΩΝ
(εφόσον υπάρχει)

……..Ονοματεπώνυμο Υπεύθυνου……..
…….Βαθμίδα…….

Λαμία, 9 Μαρτίου 2023

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

«Προστασία ψηφιακών πόρων με τεχνολογίες κρυπτογραφίας βάσει χαρακτηριστικών»

Γιαννούλη Ευαγγελία

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Λιουδάκης
Εντεταλμένος Διδάσκων

ΣΥΝΕΠΙΒΛΕΠΩΝ
(εφόσον υπάρχει)

……..Ονοματεπώνυμο Υπεύθυνου……..
…….Βαθμίδα…….

Λαμία, 9 Μαρτίου 2023

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

Digital assets protection with Attribute-Based Encryption

Giannouli Evangelia

FINAL THESIS

ADVISOR

Georgios Lioudakis
Adjunct Lecturer

CO ADVISOR

.....Full Name.....
.....Position.....

Lamia, 9 March 2023

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 10/03/2023

Η Δηλ.

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία εστιάζει σε σύγχρονες κρυπτογραφικές τεχνολογίες, ειδικά στην κρυπτογραφία βάσει χαρακτηριστικών η οποία παρουσιάζει δυνατότητες που μπορούν να επιλύσουν κάποια ζητήματα που δημιουργούνται από λειτουργικές ελλείψεις των κλασικών μορφών κρυπτογραφίας, ήτοι της συμμετρικής κρυπτογραφίας και της κρυπτογραφίας δημοσίου κλειδιού. Η πτυχιακή συνδυάζει την κρυπτογραφία βάσει χαρακτηριστικών με την τεχνολογία ψηφιακών πιστοποιητικών υλοποιώντας έτσι τον κύκλο ζωής του ελέγχου πρόσβασης σε δεδομένα με βάση χαρακτηριστικά, από την ανάθεση των ιδιοτήτων του από την κρυπτογράφηση έως την αποκρυπτογράφηση. Η πτυχιακή παρουσιάζει αναλυτικά τους υποκείμενους μηχανισμούς καθώς και το σύστημα που υλοποιήθηκε.

ABSTRACT

This thesis is focused on modern cryptographic technologies, especially in attribute-based encryption which presents possibilities that can solve some issues that are created from functional deficiencies in classic cryptographic forms, namely symmetric cryptography and the public key cryptography. This thesis combines attribute-based encryption with digital certificate technology thus implementing the cycle of the access control to data based on attributes from the assignment of its properties from encryption to decryption. This thesis presents in detail the underlying mechanisms as well as the implemented system.

Table of Contents

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

Το βασικότερο πρόβλημα όπου παρουσιάζει η κλασσική ασύμμετρη κρυπτογραφία είναι η διαχείριση των χρηστών. Εάν θέλουμε να κρυπτογραφήσουμε ένα αρχείο με ασύμμετρη κρυπτογραφία, το οποίο απευθύνεται σε πολλούς δέκτες, θα πρέπει να κρυπτογραφηθεί ξεχωριστά για κάθε χρήστη με βάση το δημόσιο κλειδί του έτσι ώστε να μπορεί να αποκρυπτογραφήσει τα δεδομένα που τον αφορούν. Η διαδικασία αυτή έχει ζητήματα κλιμακοσιμότητας ενώ δεν επιτρέπει την εφαρμογή λεπτομερών κανόνων πρόσβασης στα δεδομένα. Λύση σε αυτό δίνει η Κρυπτογραφία Βάσει Χαρακτηριστικών, όπου η κρυπτογράφηση του αρχείου πραγματοποιείται με βάση μια πολιτική πρόσβασης. Στην πολιτική αυτή ορίζονται οι συνθήκες που πρέπει να ικανοποιούν τα χαρακτηριστικά που διαθέτει ο αποδέκτης έτσι ώστε να μπορεί να πραγματοποιήσει την αποκρυπτογράφηση. Ταυτόχρονα έχουμε την ύπαρξη τεχνολογιών κρυπτογραφικής πιστοποίησης χαρακτηριστικών. Στην παρούσα πτυχιακή εργασία πραγματοποιείται η λειτουργική ολοκλήρωση των δύο αυτών τεχνολογιών, ούτως ώστε τα κλειδιά αποκρυπτογράφησης να αντλούν τα χαρακτηριστικά που ενσωματώνουν από τα υποκείμενα ψηφιακά πιστοποιητικά.

Η πτυχιακή διαρθρώνεται ως εξής: Στο κεφάλαιο δύο παρουσιάζονται οι σύγχρονες τεχνολογίες κρυπτογραφίας, συμπεριλαμβανομένων των μηχανισμών συμμετρικής κρυπτογραφίας και κρυπτογραφίας δημοσίου κλειδιού, των ψηφιακών υπογραφών, των ψηφιακών πιστοποιητικών. Το τέταρτο μέρος του κεφαλαίου παρουσιάζεται η κρυπτογραφία βάσει χαρακτηριστικών. Στο τρίτο κεφάλαιο έχουμε την αναλυτική παρουσίαση του συστήματος που αναπτύχθηκε στο πλαίσιο της πτυχιακής, την αρχιτεκτονική του και τις τεχνολογίες που χρησιμοποιήθηκαν. Τέλος στο τελευταίο κεφάλαιο παρουσιάζονται τα συμπεράσματα της εργασίας.

ΚΕΦΑΛΑΙΟ 2 Κρυπτογραφία

(Υποκεφάλαιο 2.1) Κρυπτογραφία

(Ενότητα 2.1.α) Γενικές έννοιες

Η Κρυπτολογία είναι η μελέτη τεχνικών για την εξασφάλιση της μυστικότητας και/ή της αυθεντικότητας της πληροφορίας. Οι δύο υποκατηγορίες της κρυπτολογίας είναι οι εξής:
1. *Κρυπτογραφία*: Η υποκατηγορία αυτή μελετά τη σχεδίαση και την ανάπτυξη τεχνικών εξασφάλισης της μυστικότητας και/ή της αυθεντικότητας της πληροφορίας. Μπορούμε να την σκεφτούμε ως ένα μέσο για την δημιουργία μιας μεγάλης χρήσιμης εργαλειοθήκης, που περιέχει διαφορετικές τεχνικές σε εφαρμογές ασφάλειας.
2. *Κρυπτανάλυση*: Ασχολείται με δύο τομείς. Ο πρώτος είναι η ακύρωση των τεχνικών που δημιουργούνται, έτσι ώστε να ανακτώνται πληροφορίες. Ο δεύτερος σχετίζεται με την πλαστογράφηση πληροφοριών με τρόπο τέτοιο, ώστε να γίνονται αποδεκτές ως αυθεντικές. Η κρυπτανάλυση συνυπάρχει μαζί με την κρυπτογραφία. Η υποκατηγορία αυτή έχει ως πρόθεση να σπάσει την κρυπτογράφηση των δεδομένων, οπότε αξιοποιείται κατά τον σχεδιασμό των νέων κρυπτογραφικών τεχνικών για την δοκιμή των δυνάμεων της ασφάλειας.

Κύρια θεματική της συγκεκριμένης εργασίας είναι η πρώτη κατηγορία του κλάδου, η Κρυπτογραφία. Πιο συγκεκριμένα ως Κρυπτογραφία ορίζεται η μελέτη της σχεδίασης και της ανάπτυξης σχεδίων ή πρωτοκόλλων που μπορούν να υλοποιήσουν συγκεκριμένες διεργασίες ακόμα και στην ύπαρξη δυσκολίας [Coron, 2006]. Η βασική διεργασία της κρυπτογραφίας είναι η παροχή της δυνατότητας της κρυπτογράφησης αρχείων και της επικοινωνίας των χρηστών (πομπός –δέκτης) με ασφάλεια, μέσω ενός μη ασφαλούς καναλιού με τρόπο που να εγγυάται την ιδιωτικότητα και την αυθεντικότητα των μεταδόσεων – μηνυμάτων αλλά και των περιεχομένων τους.

Ο όρος προέρχεται από την ελληνική λέξη «Κρύπτος» όπου σημαίνει κρυφός. Η πρώτη καταγραφή της χρήσης της κρυπτογραφίας σε γραπτή μορφή εμφανίζεται περίπου το 1900π.Χ όταν οι Αιγύπτιοι γραφείς χρησιμοποιούσαν μη τυποποιημένα ιερογλυφικά στις επιγραφές. Μια μερίδα ειδικών υποστηρίζει πως η κρυπτογραφία εμφανίστηκε σε ανύποπτο χρόνο και με αυθόρμητο τρόπο κάποια στιγμή μετά την ανακάλυψη της, ενώ η χρήση ήταν διάχυτη σε πολλούς διάφορους τομείς που ξεκινούσαν από την διπλωματία μέχρι και τα πολεμικά σχέδια των λαών. Μεγαλύτερη ανάπτυξη της κρυπτογραφίας παρατηρήθηκε κατά

την διάρκεια της ανάπτυξης των ηλεκτρονικών επικοινωνιών. Στον τομέα των τηλεπικοινωνιών και της διαχείρισης των δεδομένων, η κρυπτογραφία είναι απαραίτητη για την επικοινωνία σε οποιοδήποτε μέσο που θεωρείται αναξιόπιστο, το οποίο περιλαμβάνει οποιοδήποτε δίκτυο, και ιδίως το διαδίκτυο.

Οι στόχοι της κρυπτογραφίας δηλαδή οι ειδικές απαιτήσεις ασφάλειας που πρέπει να τηρούνται είναι οι εξής:

1.Εμπιστευτικότητα: Οι μόνοι που μπορούν να είναι ενημερωμένοι για την μετάδοση της πληροφορίας είναι τα μέλη που τους αφορά, δηλαδή ο αποστολέας και ο παραλήπτης.

2.Εντιμότητα: Η πληροφορία που μεταδίδεται μπορεί να παραποιηθεί μόνο από τα εξουσιοδοτημένα μέλη της επικοινωνίας (αποστολέας- παραλήπτης).

3.Επικύρωση ταυτότητας: Η δυνατότητα να γίνεται η επαλήθευση της ταυτότητας ενός χρήστη.

4.Πιστοποίηση μηνύματος: Γίνεται η διασφάλιση πηγής/προορισμού της πληροφορίας.

5.Μη άρνηση: Ο αποστολέας και ο παραλήπτης της πληροφορίας πρέπει να αναλάβουν την ευθύνη για την δημιουργία και την μετάδοση αυτής και να μην αρνηθούν τίποτα από τα δύο.

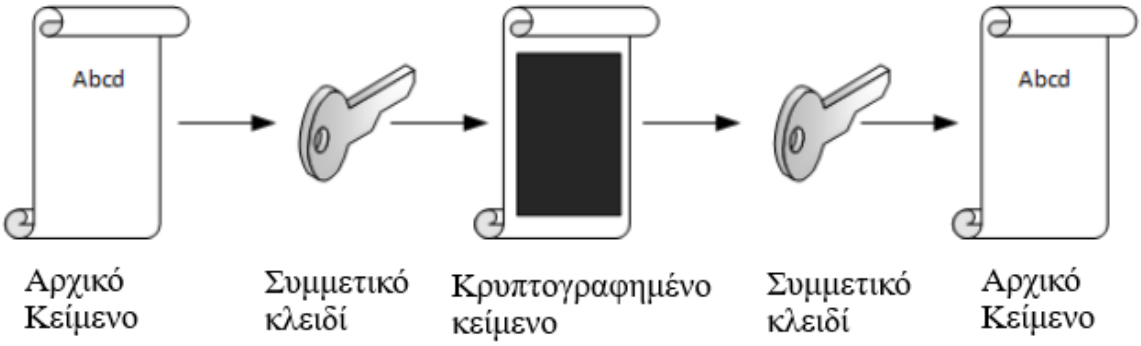
(Ενότητα 2.1.β) Μηχανισμοί κρυπτογράφησης

Το Computer Security Resource Center (CSRC) ορίζει την κρυπτογράφηση ως «η κρυπτογραφική μετατροπή δεδομένων σε μια μορφή που αποκρύπτει την αρχική σημασία των δεδομένων για την αποφυγή να γνωστοποιηθούν ή να χρησιμοποιηθούν» [CSRC, n.d.]. Γίνεται κατανοητό λοιπόν πως η κρυπτογράφηση προστατεύει τα ευαίσθητα δεδομένα από τα αδιάκριτα μάτια, μέσω της κωδικοποίησης του κειμένου (αρχικό κείμενο-plaintext) σε μορφή (κρυπτοκείμενο-ciphertext) που είναι αδύνατον να διαβαστεί, χωρίς την κατοχή του κατάλληλου κλειδιού αποκρυπτογράφησης.

Για την υλοποίηση της διαδικασίας της κρυπτογράφησης είναι απαραίτητα ένας αλγόριθμος και ένα κλειδί. Η μετατροπή του αρχικού κειμένου στο κρυπτοκείμενο και αντίστροφα ορίζεται από τον αλγόριθμο. Ως παράμετρο του αλγόριθμου έχουμε το κλειδί, όπου είναι μια τυχαία σειρά δεδομένων και περιλαμβάνει όλη την ασφάλεια της διαδικασίας. Το κλειδί είναι εξέχουσας σημασίας για την επιτυχία της διαδικασίας. Για αυτό το λόγο είναι αναγκαία η ασφαλή αποθήκευση του. Παρόλο που οι αλγόριθμοι είναι τόσο σημαντικοί, αυτό δεν σημαίνει ότι οι λεπτομέρειες αυτών είναι κρυφές. Αντιθέτως είναι διαθέσιμες στο ευρύ κοινό.

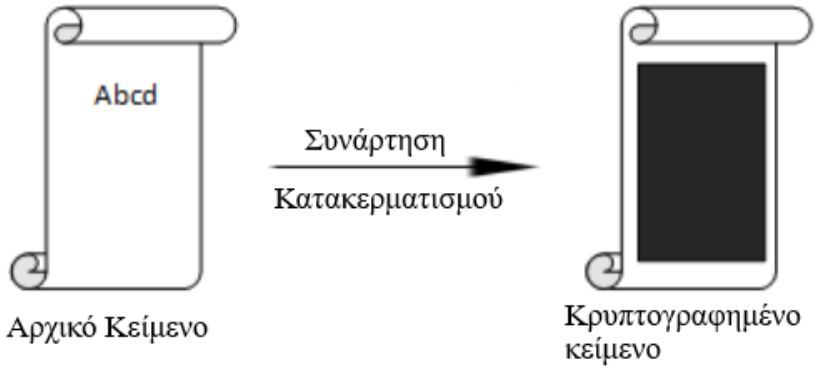
Υπάρχουν διάφοροι τρόποι που είναι δυνατόν να κατηγοριοποιήσουν τους τύπους κρυπτογράφησης. Η κατηγοριοποίηση θα πραγματοποιηθεί με βάση τα κλειδιά που χρησιμοποιούνται για τις διαδικασίες της κρυπτογράφησης αλλά και αποκρυπτογράφησης. Επομένως προκύπτει η διάκριση 3 τύπων κρυπτογράφησης:

1. Συμμετρική Κρυπτογράφηση, ή κρυπτογραφία ιδιωτικού κλειδιού : Σε αυτό τον τύπο κρυπτογράφησης χρησιμοποιείται ένα κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Με την παροχή ενός κλειδιού επιτυγχάνεται η ασφαλής επικοινωνία μεταξύ των μελών της και ένα αδιαπέραστο στρώμα κρυπτογράφησης από την αρχή της διαδικασίας έως και το τέλος της. Το κοινό-συμμετρικό κλειδί θα μπορούσε να έχει τη μορφή κωδικού ή μια τυχαία σειρά αριθμών. Σημαντική δε είναι και η διαβίβαση του συμμετρικού κλειδιού στον δέκτη, η οποία πρέπει να γίνεται με ασφαλή τρόπο. Η μεταβίβαση αυτή αποτελεί τον μεγαλύτερο κίνδυνο ασφάλειας όπου υπάρχει σε αυτόν τύπο κρυπτογράφησης. Μερικά από τα πιο δημοφιλή συστήματα συμμετρικής κρυπτογράφησης είναι: Advanced Encryption Standard (AES), Data Encryption Standard (DES) και Triple Data Encryption Algorithm (3DEA- 3DES) [Marget, 2022].



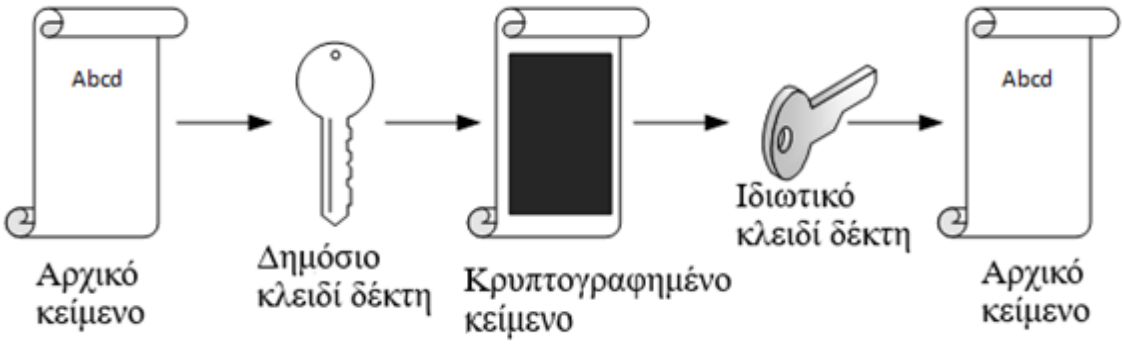
Σχήμα 2.1.1:Συμμετρική κρυπτογράφηση

2. Συναρτήσεις Κατακερματισμού : Στον συγκεκριμένο τύπο κρυπτογράφησης δεν έχουμε χρήση κλειδιού. Γίνεται η χρήση μιας τιμής κατακερματισμού, που έχει σταθερό μήκος και υπολογίζεται σύμφωνα με το αρχικό κείμενο, το οποίο καθιστά αδύνατη την δυνατότητα επαναφοράς του περιεχόμενου του απλού κειμένου. Πολλά λειτουργικά συστήματα χρησιμοποιούν αυτού του είδους κρυπτογράφησης έτσι ώστε να επιτύχουν την αποθήκευση διάφορων δεδομένων, όπως για παράδειγμα τους κωδικούς πρόσβασης.



Σχήμα 2.1.2:Κρυπτογραφία με συναρτήσεις κατακερματισμού

3. Ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημοσίου κλειδιού : Σε αυτό τον τρόπο κρυπτογράφησης χρησιμοποιείται ένα ζευγάρι κλειδιών, τα οποία είναι μαθηματικά συνδεδεμένα μεταξύ τους, ώστε να υλοποιηθεί η κρυπτογράφηση και η αποκρυπτογράφηση της πληροφορίας. Για την κρυπτογράφηση των δεδομένων γίνεται η χρήση ενός δημοσίου κλειδιού, ενώ για την αποκρυπτογράφηση των δεδομένων χρησιμοποιείται ένα ιδιωτικό κλειδί. Τα δύο αυτά κλειδιά μπορεί να είναι μαθηματικά συνδεδεμένα αλλά είναι διαφορετικά μεταξύ τους. Στην περίπτωση που υπάρχει επίγνωση του περιεχομένου του δημοσίου κλειδιού, μόνο ο κατάλληλός χρήστης-δέκτης μπορεί να αποκρυπτογραφήσει το κείμενο, διότι μόνο εκείνος έχει στην διάθεση του το κατάλληλο ιδιωτικό κλειδί. Η συγκεκριμένη μορφή κρυπτογραφίας προσφέρει καλύτερη ασφάλεια μέσω της επαλήθευσης της πηγής των δεδομένων και της μη-φήμης (δηλαδή ο δημιουργός δεν μπορεί να αμφισβητήσει το συντάκτη του). Ωστόσο, έχουμε την αύξηση του χρόνου της διαδικασίας μεταφοράς της πληροφορίας, την ταχύτητα του δικτύου και τις επιδόσεις του. Υπάρχουν πολλά δημοφιλή συστήματα ασύμμετρης κρυπτογράφησης, με δημοφιλέστερο παράδειγμα το εξής: κρυπταλγόριθμος Rivest–Shamir–Adleman (RSA) [Marget, 2022].



Σχήμα 2.1.3:Ασύμμετρη κρυπτογράφηση

(Υποκεφάλαιο 2.2) Ψηφιακές Υπογραφές

(Ενότητα 2.2.α) Γενικές έννοιες

Ένα από τα σημαντικότερα παρακλάδια της εφαρμοσμένης Κρυπτογραφίας θεωρούνται οι ψηφιακές υπογραφές, οι οποίες ενδεχομένως να αποτελούν καθοριστικό μέρος για την εξέλιξης της ιστορίας της Κρυπτογραφίας. Η πλήρης ονομασία των υπογραφών αυτών είναι «Σχήματα Ψηφιακών Υπογραφών (Digital Signature Schemes) – Σχήματα Υπογραφών», των οποίων η ιδέα και η αξία αναγνωρίστηκαν πριν γίνει εφικτή η οποιαδήποτε πρακτική εφαρμογή τους. Όπως έχει ήδη αναφερθεί σε προηγούμενο υποκεφάλαιο, η κρυπτογράφηση τοποθετείται χρονικά στα αρχαία χρόνια, οι υπογραφές ωστόσο έγιναν πραγματικότητα γύρω στο 1970 και αυτό οφείλετε στην Κρυπτογραφία με δημόσιο κλειδί (PKI--Public-Key Cryptography). Η μέθοδος που επινοήθηκε πρώτη ήταν το σχήμα υπογραφής RSA (Rivest–Shamir–Adleman) όπου αναπτύχθηκε το 1970, το οποίο αποτελεί μέχρι και σήμερα μια από τις πιο διαδομένες, πρακτικές τεχνικές όπου διαθέτουμε.

Η Ψηφιακή υπογραφή είναι ένας τύπος ηλεκτρονικής υπογραφής, που έχει ως σκοπό τη χρήση αυτής, για την επαλήθευση της ταυτότητας του αποστολέα ενός αρχείου/εγγράφου και τη κατοχύρωση της μη παραποίησης του αρχικού περιεχομένου του αρχείου/εγγράφου, που έχει φτάσει στο δέκτη. Η μεταφορά της υπογραφής είναι μια εύκολη διαδικασία, η οποία χαρακτηρίζεται από τη μη δυνατή μίμηση από τρίτους και την αυτόματη εισαγωγή χρονοσφραγίδας (timestamp «Ένα δείγμα πληροφοριών που χρησιμοποιείται για τη διασφάλιση του χρονοδιαγράμματος»[Barker,2006]). Με την εξασφάλιση του αρχικού αρχείου/εγγράφου που έφτασε στον δέκτη, το οποίο φέρει την υπογραφή, έχουμε ως αποτέλεσμα την μη δυνατή άρνηση από τον αποστολέα σε δεύτερο χρόνο. Οι ψηφιακές υπογραφές θεωρούνται πιο ασφαλισμένες από άλλες μορφές ηλεκτρονικών υπογραφών.

(Ενότητα 2.2.β) Ιδιότητες και απαιτήσεις ψηφιακών υπογραφών.

Όταν δεν υπάρχει απόλυτη εμπιστοσύνη μεταξύ του αποστολέα και του παραλήπτη, θα πρέπει να παρέχεται κάτι περισσότερο από την αυθεντικοποίηση. Λύση σε αυτό το πρόβλημα δίνει η ψηφιακή υπογραφή, η οποία είναι ανάλογη της χειρόγραφης υπογραφής. Για να θεωρηθεί όμως αξιόπιστη, θα πρέπει να διαθέτει τις εξής ιδιότητες :

- Κατά την στιγμή της υπογραφής πρέπει να αυθεντικοποιούνται τα δεδομένα-περιεχόμενα.

- Για να μην είναι δυνατή η ύπαρξη αμφισβητήσεων, θα πρέπει η υπογραφή να είναι επαληθεύσιμη από τρίτους.
- Πρέπει να πιστοποιείται όχι μόνο ο υπογράφοντας αλλά και η χρονική στιγμή (ημερομηνία-ώρα) της υπογραφής.

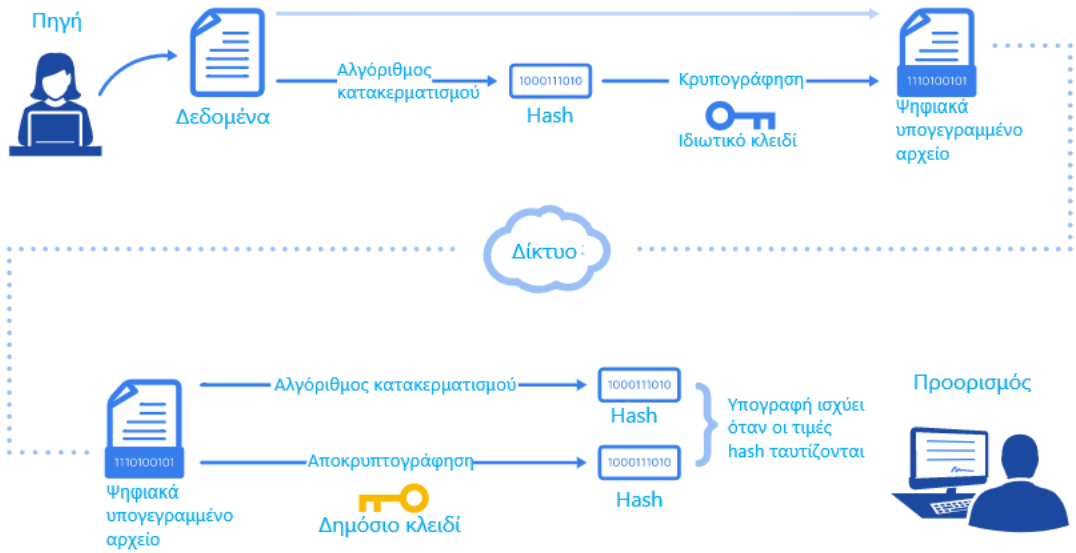
Βάσει των ιδιοτήτων που μόλις αναφέραμε, μπορούμε να συμπεράνουμε και να απαριθμήσουμε τις εξής απαιτήσεις που αφορούν μια ψηφιακή υπογραφή :

1. Για την αποφυγή της πλαστογράφησης και της αποποίησης, η υπογραφή πρέπει να περιέχει κάποιες ξεχωριστές πληροφορίες για τον αποστολέα.
2. Πρέπει η παραγωγή, η ανάγνωση, αλλά και η πιστοποίηση να είναι σχετικά εύκολες.
3. Πρέπει η υπογραφή να είναι μια ακολουθία από bit που να συνδέεται από το μήνυμα που υπογράφεται.
4. Πρέπει να υπάρχει η δυνατότητα της διατήρησης αντιγράφου της ψηφιακής υπογραφής.
5. Δεν πρέπει να είναι με κανέναν τρόπο και από κανέναν δυνατόν να γίνεται η πλαστογράφηση μιας ψηφιακής υπογραφής, είτε με την δημιουργία ενός άλλου μηνύματος για μια συγκεκριμένη ψηφιακή υπογραφή ή η δημιουργία μίας ψεύτικης ψηφιακής υπογραφής για ένα συγκεκριμένο μήνυμα.

(Ενότητα 2.2.γ) Τρόπος λειτουργείας.

Όταν η πηγή (ο δημιουργός-ο υπογράφων) ηλεκτρονικά υπογράφει ένα αρχείο/έγγραφο, η δημιουργία της υπογραφής γίνεται με την χρήση του ιδιωτικού κλειδιού της πηγής, το οποίο φυλάσσεται από την πηγή. Ο μαθηματικός αλγόριθμος ενεργεί σαν ένας κρυπταλγόριθμος, ο οποίος δημιουργεί δεδομένα. Τα δεδομένα αυτά αντιστοιχούν στο αρχείο/έγγραφο που έχει υπογραφεί, το οποίο και ονομάζεται hash (κατακερματισμός), και κρυπτογραφούνται τα δεδομένα αυτά. Ως συνέπεια της διαδικασίας αυτής (κρυπτογραφημένα δεδομένα) είναι η ψηφιακή υπογραφή. Στην υπογραφή αναφέρεται και συνδέεται η χρονική στιγμή όπου το αρχείο/έγγραφο υπογράφθηκε. Εάν το αρχείο/έγγραφο έχει τροποποιηθεί για τον οποιοδήποτε λόγο μετά την υπογραφή του, η ψηφιακή υπογραφή που υπάρχει ακυρώνεται.

Στο παρακάτω σχήμα έχουμε ένα σχεδιάγραμμα και μια σύντομη επεξήγηση αυτού, ώστε να καταστεί ευκολότερη η κατανόηση της συγκεκριμένης διαδικασίας:



Σχήμα 2.2.1:Διαδικασία ψηφιακής υπογραφής

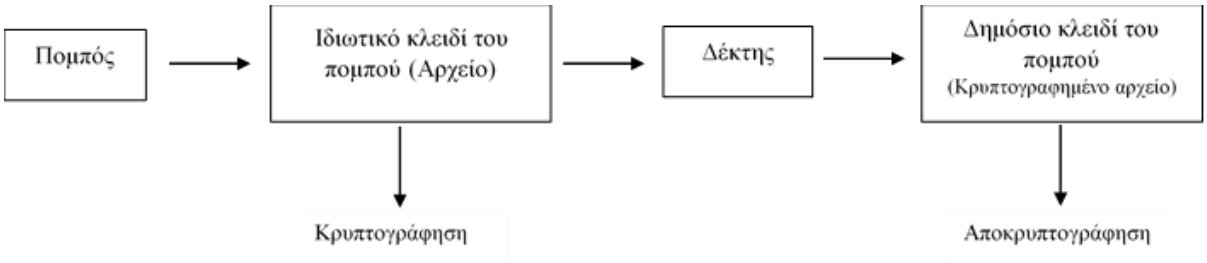
Τα δεδομένα που θέλει να μεταφέρει η πηγή, αρχικά περνάνε από μια συνάρτηση κατακερματισμού και έτσι δημιουργείται ένα hash. Στην συνέχεια κρυπτογραφείται με βάση το ιδιωτικό κλειδί της πηγής και έτσι έχουμε την δημιουργία του ψηφιακού υπογεγραμμένου αρχείου. Το αρχείο αυτό αποστέλλεται στον προορισμό μέσω του δικτύου. Στο ψηφιακά υπογεγραμμένο αρχείο γίνονται δυο διαδικασίες. Στην πρώτη εφαρμόζεται ένας αλγόριθμος κατακερματισμού και δημιουργείται ένα hash (hash1), ενώ στη δεύτερη με την χρήση του δημοσίου κλειδιού της πηγής, πραγματοποιείται η αποκρυπτογράφηση και ως αποτέλεσμα έχουμε ένα δεύτερο hash (hash2). Εάν οι 2 τιμές που συγκρίνονται (hash1-hash2) ταυτίζονται, τότε έχουμε την εξασφάλιση της ακεραιότητας και η ψηφιακή υπογραφή θεωρείται έγκυρη.

(Ενότητα 2.2.δ) Κατηγορίες ψηφιακών υπογραφών.

Με τη συνεχή έρευνα έχουν προταθεί πάρα πολλές προσεγγίσεις για την συνάρτηση της ψηφιακής υπογραφής. Για την καλύτερη μελέτη αυτών έχουν κατηγοριοποιηθεί στις εξής δύο κατηγορίες: 1.στις άμεσες και 2.σε αυτές με διαμεσολάβηση.

Άμεση ψηφιακή υπογραφή

Στην άμεση ψηφιακή υπογραφή (direct digital signature) περιλαμβάνονται μόνο τα δύο μέλη της επικοινωνίας, ο πομπός και ο δέκτης. Αυτό γίνεται διότι θεωρείται, πως ο δέκτης των δεδομένων (ψηφιακή υπογραφή) γνωρίζει ήδη το δημόσιο κλειδί του πομπού. Από την άλλη ο πομπός εμπιστεύεται τον δέκτη ότι δεν θα τροποποιήσει το αρχείο.



Σχήμα 2.2.2:Άμεση ψηφιακή υπογραφή

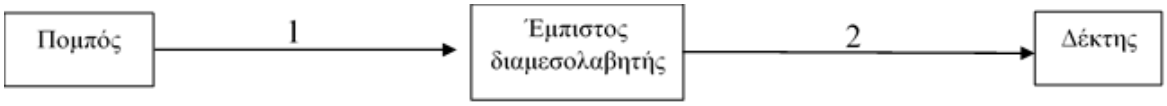
Μειονεκτήματα :

• Είναι αναγκαία η εμπιστοσύνη μεταξύ των μελών, εξαιτίας της μη ύπαρξης ανεξάρτητης διαδικασία πιστοποίησης.

• Στο συγκεκριμένο σχήμα θεωρείται δεδομένο ότι ο πομπός έχει-γνωρίζει το ιδιωτικό του κλειδί και το δημόσιο κλειδί του δέκτη, ενώ ο δεκτής μονο το δημόσιο του κλειδί. Στην περίπτωση όπου το ιδιωτικό κλειδί κλαπεί υπάρχει η περίπτωση πλαστογράφησης αυτού αλλά και της ψηφιακής υπογραφής. Η έκβαση αυτή όμως μπορεί να οδηγήσει σε πιθανό κίνδυνο της ασφάλειας.

Ψηφιακή Υπογραφή με Διαμεσολάβηση

Υπάρχει μεγάλη ποικιλία σχημάτων ψηφιακής υπογραφής με διαμεσολαβητή (arbitrated digital signature). Σε γενικές γραμμές όμως τα σχήματα αυτά ακολουθούν μια κοινή διαδικασία. Η υπογραφή αυτή εκτός από τα δύο βασικά μέλη της επικοινωνίας (πομπό-δέκτη), έχει και ένα τρίτο μέλος που αποκαλείται έμπιστός διαμεσολαβητής, ο οποίος εισχωρεί ανάμεσα στα άλλα δυο μέλη. Σκοπός του διαμεσολαβητή είναι να επαληθεύει την αρτιμέλεια των υπογεγραμμένων δεδομένων, να «βάζει» την χρονοσφραγίδα στα δεδομένα και να πραγματοποιεί την μετάδοση των πλέον υπογεγραμμένων δεδομένων στον τελικό δέκτη.



Σχήμα 2.2.3: Ψηφιακή υπογραφή με διαμεσολαβητή

Η διαδικασία είναι η εξής :

1. Το υπογεγραμμένο μήνυμα το οποίο στέλνει ο πομπός πρώτα περνάει από τον διαμεσολαβητή, όπου εκεί το μήνυμα και η υπογραφή ελέγχονται για την προέλευση και το περιεχόμενο τους.

2.Με το πέρας της διαδικασίας αυτής το υπογεγραμμένο μήνυμα αποστέλλετε στον δέκτη μαζί με την χρονοσφραγίδα του, η οποία πιστοποιεί στον δέκτη, ότι το αρχείο έχει πιστοποιηθεί από τον διαμεσολαβητή.

Μειονεκτήματα :

• Με την χρήση του διαμεσολαβητή πρέπει και τα δύο βασικά μέλη να δείξουν εμπιστοσύνη στο γεγονός ότι ο διαμεσολαβητής όχι μόνο θα καταστήσει εφικτή την χρονολόγηση και την μετάδοση των δεδομένων, όπως του έχει ανατεθεί, αλλά και ότι δεν θα επιτρέψει να υποστούν οποιαδήποτε τροποποίηση τα δεδομένα αυτά.

• Ενδέχεται και η δημιουργία κάποιας «συμμαχίας» μεταξύ του διαμεσολαβητή με κάποιο από τα δύο κύρια μέλη για την εξυπηρέτηση κάποιου απώτερου σκοπού. (πομπός- απόρριψη ενός υπογεγραμμένου μηνύματος, δέκτης- πλαστογραφία υπογραφής πομπού)

(Υποκεφάλαιο 2.3) Ψηφιακά Πιστοποιητικά τύπου X.509

(Ενότητα 2.3.α) Το πρότυπο X.509

Η σύσταση X.509 είναι μέρος της σειράς συστάσεων X.500, η οποία έχει ως σκοπό τον ορισμό μιας υπηρεσίας καταλόγου (directory). Ο κατάλογος αυτός είναι ένας εξυπηρετητής ή ένα κατανεμημένο σύνολο εξυπηρετητών, ο οποίος διατηρεί μια βάση δεδομένων πληροφοριών για τους χρήστες. Στις πληροφορίες αυτές συμπεριλαμβάνεται και η αντιστοίχιση ονομάτων χρηστών με τις ανάλογες διευθύνσεις δικτύων, χαρακτηριστικών και πληροφοριών.

Η X.509 είναι υπεύθυνη για την παροχή υπηρεσιών αυθεντικοποίησης του καταλόγου X.500 στους χρήστες. Η μορφή αυτού του ψηφιακού πιστοποιητικού είναι ένα πρότυπο ευρέως χρησιμοποιημένο στην ασύμμετρη κρυπτογραφία. Ο κατάλογος μπορεί να περιέχει πιστοποιητικά δημοσίου κλειδιού, τα οποία σχετίζονται με την ταυτότητα του χρήστη (π.χ. ένα hostname, ένας οργανισμός, ένα άτομο). Σε κάθε πιστοποιητικό περιέχεται το δημόσιο κλειδί του χρήστη, δημιουργείται και υπογράφεται με το ιδιωτικό κλειδί από μια έμπιστη αρχή πιστοποίησης (Certification Authority – CA) και τοποθετείται στον κατάλογο από την αρχή πιστοποίησης ή από τον ίδιο τον χρήστη. Ο ίδιος ο εξυπηρετητής καταλόγου δεν είναι

υπεύθυνος για την δημιουργία δημόσιων κλειδιών ή για την λειτουργία πιστοποίησης. Η ιδιότητα του είναι η παροχή δυνατότητας εύκολης πρόσβασης των χρηστών στα πιστοποιητικά. Η X.509 παραθέτει εναλλακτικά πρωτόκολλα αυθεντικοποίησης, τα οποία βασίζονται στη χρήση πιστοποιητικών δημοσίου κλειδιού.

Η σύσταση X.509 αποτελεί ένα σημαντικό πρότυπο, διότι η δομή του, όσο και τα πρωτόκολλα αυθεντικοποίησης του χρησιμοποιούνται σε μεγάλο εύρος εφαρμογών, τα οποία βρίσκονται σε ευρεία χρήση από τους ανθρώπους και ιδιαιτέρως στις εφαρμογές για την ασφάλεια των δικτύων.

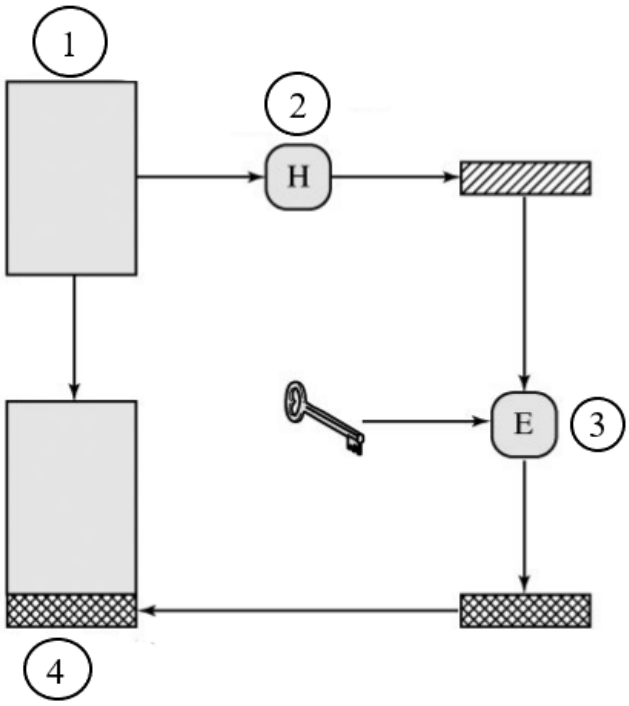
Μερικά από αυτά είναι τα εξής:

1. Web Server Security με πιστοποιητικά Secure Socket Layer (SSL)/ Transport Layer Security (TLS) και Hypertext Transfer Protocol Security (HTTPS) για την επικύρωση και την κρυπτογράφηση του περιηγητή ιστού.
2. Υπογεγραμμένα και κρυπτογραφημένα μηνύματα (e-mail) μέσω του πρωτοκόλλου S/MIME(Secure MIME –Πρότυπο ασφαλούς ηλεκτρονικού ταχυδρομείου S/MIME)
3. Ψηφιακές υπογραφές και υπογραφή εγγράφου
4. IPsec – IP Security (Ασφάλεια Πρωτοκόλλου Internet)
5. Κλειδιά Security Shell Protocol (SSH)
6. Υπογραφή κώδικα
7. Πρωτόκολλο Secure Electronic Transaction(SET)
8. Ψηφιακές ταυτότητες

Η πρώτη σύσταση του X.509 δημοσιεύτηκε το 1988. Το πρότυπο αυτό στην συνέχεια αναθεωρήθηκε έτσι ώστε να αντιμετωπίσει κάποια προβλήματα ασφάλειας. Το 1996 παρουσιάστηκε μια 3^{η} έκδοση, στην οποία προστέθηκαν κάποιες σημαντικές επεκτάσεις, οι οποίες υποστηρίζουν εφαρμογές της χρήσης του διαδικτύου. Μέχρι και σήμερα έχουν δημοσιευτεί αρκετές εκδόσεις με την τελευταία να είναι η έκδοση 9, όπου και δημοσιεύτηκε το 2019.

Η X.509 βασίζεται στη χρήση της μορφής κρυπτογράφησης δημοσίου κλειδιού και των ψηφιακών υπογραφών. Το πρότυπο δεν υπαγορεύει τη χρήση κάποιου συγκεκριμένου αλγόριθμου αλλά συνιστά τον αλγόριθμο River- Shamir- Adleman (RSA) [Stallings, 2006]. Όπως έχουμε ήδη προαναφερθεί, το σχήμα ψηφιακής υπογραφής επίσης απαιτεί τη χρήση μιας συνάρτησης κατακερματισμού. Σε αυτή την περίπτωση το πρότυπο δεν υπαγορεύει την χρήση κάποιου συγκεκριμένου αλγόριθμου .

Το παρακάτω σχήμα απεικονίζει την δημιουργία ενός πιστοποιητικού δημόσιου κλειδιού.

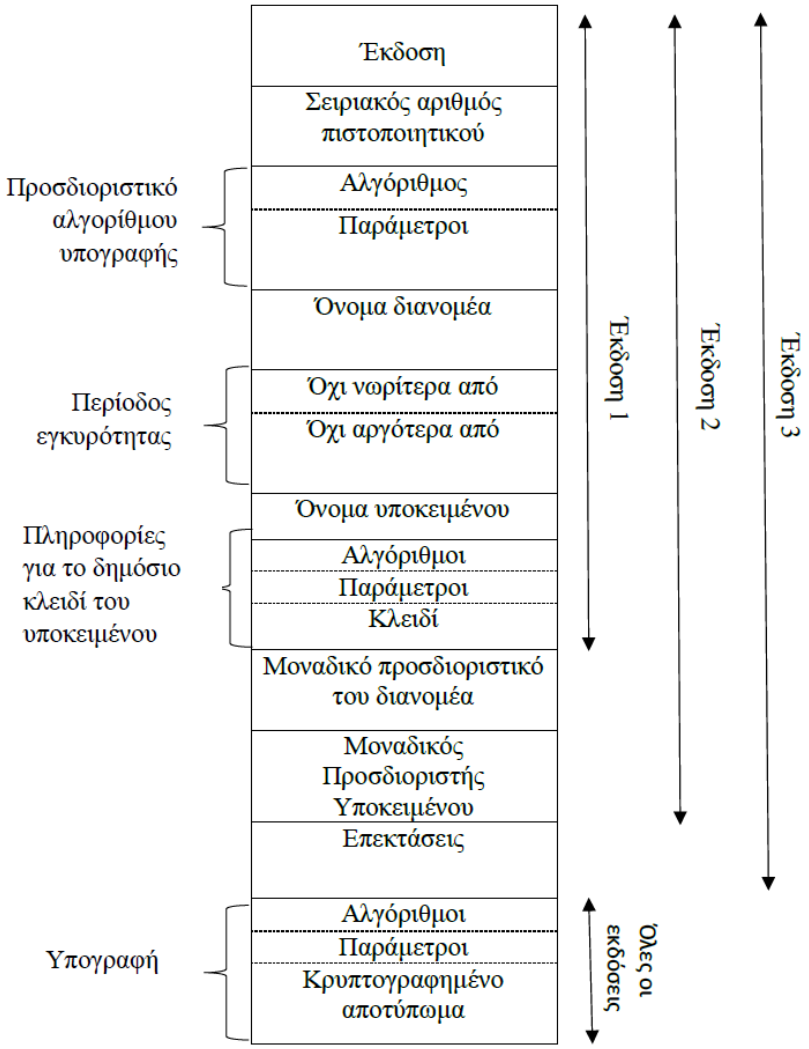


Σχήμα 2.3.1: Χρήση πιστοποιητικού δημοσίου κλειδιού

1. Μη υπογεγραμμένο πιστοποιητικό: σε αυτό περιλαμβάνεται το αναγνωριστικό ταυτότητας (ID) του χρήστη, και το δημόσιο κλειδί του.
2. Παραγωγή κώδικα κατακερματισμού για μη υπογεγραμμένο πιστοποιητικό.
3. Κρυπτογράφηση του κώδικα κατακερματισμού με το ιδιωτικό κλειδί της έμπιστης αρχής πιστοποίησης για το σχηματισμό υπογραφής.
4. Υπογεγραμμένο πιστοποιητικό: ο δέκτης έχει την δυνατότητα πιστοποίησής της υπογραφής, χρησιμοποιώντας το δημόσιο κλειδί της CA.

(Ενότητα 2.3.β) Γενική Μορφή X.509

Το ακόλουθο σχήμα απεικονίζει την γενική μορφή ενός πιστοποιητικού και στην συνέχεια θα αναλυθεί κάθε πεδίο του διεξοδικώς:



Σχήμα 2.3.2: Μορφή X.509

- **Έκδοση** : Η έκδοση διαφοροποιείται ανάμεσα στις εκδόσεις της μορφοποίησης του πιστοποιητικού κατά εξ ορισμού έκδοση είναι η $1^{η}$. Για να είναι η $2^{η}$ έκδοση θα πρέπει το πιστοποιητικό να περιέχει τουλάχιστον ένα από τα επόμενα δύο, $1^{ον}$ να περιέχει το μοναδικό προσδιοριστικό της ταυτότητας του διανομέα ή $2^{ον}$ το μοναδικό προσδιοριστικό ταυτότητας του υποκειμένου. Εάν υπάρχουν μία ή περισσότερες επεκτάσεις, η τιμή της έκδοσης πρέπει να είναι η $3^{η}$.
- **Σειριακός αριθμός πιστοποιητικού**: Είναι μια ακέραια, μοναδική τιμή για τη έμπιστη αρχή πιστοποίησης, η οποία καταμερίζει τα πιστοποιητικά και συνδέεται μοναδικά με αυτό το πιστοποιητικό.

- **Προσδιοριστικό αλγορίθμου υπογραφής** : Σε αυτό το μέρος του πιστοποιητικού βρίσκεται ο αλγόριθμος που χρησιμοποιείται για να υπογράφει το πιστοποιητικό, άλλα και οποιεσδήποτε άλλες σχετικές παράμετροι. Το πεδίο αυτό έχει μικρή έως και μηδενική χρησιμότητα, εφόσον οι πληροφορίες αυτές επαναλαμβάνονται στο πεδίο της υπογραφής στο τέλος του πιστοποιητικού αυτού.
- **Όνομα διανομέα** : Το όνομα X.500 της έμπιστης αρχής πιστοποίησης, το οποίο δημιούργησε και υπέγραψε το συγκεκριμένο πιστοποιητικό.
- **Περίοδος εγκυρότητας** : Χωρίζεται σε δύο μικρότερα υπό-πεδία και το καθένα αποτελείται από μία ημερομηνία: την ημερομηνία έναρξης και λήξης της ισχύος, την οποία έχει το συγκεκριμένο πιστοποιητικό .
- **Όνομα υποκειμένου** : Το όνομα του χρήστη στον οποίο αναφέρεται το πιστοποιητικό αυτό. Αναλυτικότερα, το πιστοποιητικό βεβαιώνει το δημόσιο κλειδί του υποκειμένου, που κατέχει το αντίστοιχο ιδιωτικό κλειδί.
- **Πληροφορίες δημοσίου κλειδιού υποκειμένου** : Το πεδίο αυτό αναφέρεται στο δημόσιο κλειδί του υποκειμένου και ένα προσδιοριστικό αλγόριθμου κρυπτογράφησης, στον οποίο έχει σκοπό να χρησιμοποιηθεί αυτό το κλειδί, μαζί με όλες τις ανάλογες παραμέτρους.
- **Μοναδικό προσδιοριστικό του διανομέα:** Το πεδίο αυτό είναι προαιρετικό και είναι μια ακολουθία από bit που χρησιμοποιείται για να διευκρινίσει μοναδικά την έμπιστη αρχή πιστοποίησης, έτσι ώστε να μην υπάρχει σύγχυση στην περίπτωση επαναχρησιμοποίησης του πιστοποιητικού από διαφορετικές οντότητες.
- **Μοναδικό προσδιοριστικό του υποκειμένου:** Είναι ένα προαιρετικό πεδίο bit ακολουθίας, το οποίο χρησιμοποιείται για τον μοναδικό προσδιορισμό του υποκειμένου που πιστοποιείται, για την αποτροπή σύγχυσης εάν έχει επαναχρησιμοποιηθεί για διαφορετικές οντότητες το όνομά του.
- **Επεκτάσεις:** Οι επεκτάσεις ορίζονται ως το σύνολο από ένα ή περισσότερα πεδία που περιέχουν διάφορες επεκτάσεις . Επεκτάσεις προστέθηκαν στην έκδοση 3. Αναφορικά οι επεκτάσεις χωρίζονται σε τρείς κύριες κατηγορίες: πληροφορίες κλειδιού και πολιτικής, χαρακτηριστικά υποκειμένου και διανομέα, και περιορισμοί στην διαδρομή του πιστοποιητικού.
- **Υπογραφή :** Εφαρμόζεται και στις τρεις εκδοχές του πιστοποιητικού που παρουσιάζεται στο Σχήμα 2.3.2. Το πεδίο αυτό περιέχει τον κώδικα κατακερματισμού όλων των υπολοίπων πεδίων, κρυπτογραφημένο με το ιδιωτικό

κλειδί της έμπιστης αρχής πιστοποίησης. Επομένως στο πεδίο αυτό περιλαμβάνεται το προσδιοριστικό του αλγόριθμου υπογραφής.

Τα πεδία των μοναδικών προσδιοριστικών διανομέα/υποκειμένου προστέθηκαν στην έκδοση 2 για να χειριστούν την πιθανή επαναχρησιμοποίηση ονόματος υποκειμένου και/ή ονομάτων διανομέων των πιστοποιητικών. Τα πεδία αυτά χρησιμοποιούνται σπάνια.

(Ενότητα 2.3.γ) Οφέλη πιστοποιητικών X.509

Με την χρήση των πιστοποιητικών X.509 παρέχονται τα εξής οφέλη:

- **Εμπιστοσύνη:** Με την χρήση των ψηφιακών πιστοποιητικών δίνεται η δυνατότητα σε άτομα, οργανισμούς και σε άλλα να θεωρούνται έμπιστα στον ψηφιακό κόσμο. Τα X.509 μπορούν παντού να συναντηθούν, σε κάθε συνδεδεμένη διαδικασία από διαδικτυακούς τόπους, σε εφαρμογές, σε συσκευές τελικού χρήστη μέχρι και σε έγγραφα που υπάρχουν στον παγκόσμιο ιστότοπο.

- **Επεκτασιμότητα :** Η Αρχιτεκτονική Υποδομής Δημοσίου Κλειδιού (Public Key Infrastructure – PKI) όπου χρησιμοποιεί το X.509 είναι τόσο επεκτάσιμη, ώστε να προσφέρει τη δυνατότητα εξασφάλισης της καθημερινής ανταλλαγής όγκων μηνυμάτων από οργανισμούς μέσω των δικών τους δικτύων αλλά και μέσω του διαδικτύου.

(Υποκεφάλαιο 2.4) Κρυπτογραφία Βάσει Χαρακτηριστικών

(Ενότητα 2.4.α) Τι είναι η Κρυπτογραφία Βάσει Χαρακτηριστικών.

Η Κρυπτογραφία Βάσει Χαρακτηριστικών (Attribute-based Encryption - ABE) ανήκει στην «οικογένεια» σχημάτων κρυπτογραφίας ιδιωτικού κλειδιού. Ο συγκεκριμένος τύπος κρυπτογραφίας αναπτύχθηκε και παρουσιάστηκε πρώτη φορά το 2005 από τους Sahai και Waters[(Sahai and Waters, 2005)] ενώ έχει βελτιωθεί σε άλλες αναφορές [(Bethencourt, Sahai and Waters, 2007), (Goyal et al., 2006)].

Η Κρυπτογραφία Βάσει Χαρακτηριστικών είναι ένας πιο αναλυτικός τύπος κρυπτογράφησης, ο οποίος επιτρέπει το πιο ευέλικτο έλεγχο προσπέλασης, με βάση τις κρυπτογραφικές πολιτικές που επιβάλλονται. Μάλιστα δίνεται η δυνατότητα ταυτόχρονης κρυπτογράφησης για πολλούς χρήστες, αντί για έναν μόνο χρήστη, και ο λόγος θα αναπτυχθεί παρακάτω.

Στο συγκεκριμένο σχήμα κρυπτογράφησης έχουμε 3 κύριες οντότητες: η πρώτη είναι η οντότητα της κρυπτογράφησης με σκοπό την κρυπτογράφηση, η δεύτερη είναι η οντότητα της αποκρυπτογράφησης όπου έχει σκοπό, όπως αποδεικνύεται και από το όνομα της, την αποκρυπτογράφηση, και η τρίτη, την Αρχή κλειδιού όπου έχει ως σκοπό την δημιουργία κλειδιών.

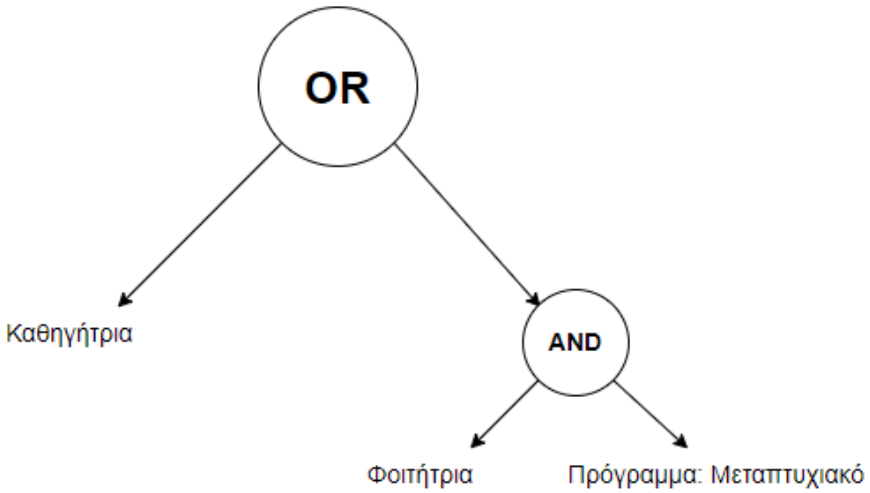
Στο σχέδιο της Κρυπτογραφίας Βάσει Χαρακτηριστικών το οποίο μελετάται υπάρχουν τρεις διαφορετικοί τύποι κλειδιών: Το κύριο κρυφό κλειδί (secret master key), το δημόσιο κλειδί (public key), το ιδιωτικό κλειδί (private key).

Η Αρχή κλειδιού (key authority) έχει στόχο τη δημιουργία ενός κύριου κρυφού κλειδιού (secret master key) και ενός συνδεδεμένου σε αυτό δημόσιο κλειδί (public key). Η Αρχή κλειδιού είναι μια αξιόπιστη οντότητα, που έχει τη δυνατότητα δημιουργίας των ιδιωτικών κλειδιών (private keys) και αποτελεί βασικό αρωγό των ανθρώπων για τη διασφάλιση της εμπιστοσύνης στο σύστημα. Τα δύο κλειδιά που δημιουργούνται έχουν το καθένα ένα σκοπό. Το ιδιωτικό κλειδί χρειάζεται για την αποκρυπτογράφηση των δεδομένων, ενώ σε αντίθεση το δημόσιο κλειδί αξιοποιείται για την κρυπτογράφηση των δεδομένων, αλλά και την διάδοση σε άλλους. Τα ζεύγη των κλειδιών που έχουν δημιουργηθεί είναι συνδεδεμένα με τα χαρακτηριστικά που έχει ο κάθε χρήστης και όχι απευθείας με αυτούς.

Η Κρυπτογραφία Βάσει Χαρακτηριστικών είναι ένα σχήμα κρυπτογράφησης, που μπορεί να επιβάλει την πολιτική του λεπτομερούς ελέγχου προσπέλασης των δεδομένων (fine-grained access control policy) μέσω των κρυπτογραφικών τεχνικών. Αυτό μπορεί να επιτευχθεί μέσω της χρήσης των συνόλων χαρακτηριστικών (attribute sets). Το κάθε μυστικό κύριο κλειδί έχει ένα μοναδικό πακέτο χαρακτηριστικών, που προσδιορίζει μοναδικά ένα χρήστη και αυτό με τη σειρά του συνδέεται με το μοναδικό ιδιωτικό κλειδί που φανερώνει τα χαρακτηριστικά του.

Κατά την διάρκεια της κρυπτογράφησης, ο κρυπτογράφος έχει ορίσει μια πολιτική (policy) στην οποία προδιαγράφεται ποια πρέπει να είναι η συνθήκη χαρακτηριστικών του αποκρυπτογράφου, για να είναι εφικτή η αποκρυπτογράφηση. Εάν αυτός που προσπαθεί να αποκρυπτογραφήσει, ικανοποιεί την πολιτική που έχει δοθεί στην οντότητα κρυπτογράφησης, μπορεί να προχωρήσει η διαδικασία της αποκρυπτογράφησης, εάν όχι δεν συνεχίζεται. Ως πολιτική ορίζουμε μια Boolean μορφή, η οποία ορίζει ποια είναι τα χαρακτηριστικά που αποτελούν προϋπόθεση για τους χρήστες, ώστε να είναι δυνατή η ολοκλήρωση της αποκρυπτογράφησης.

Για παράδειγμα εάν έχουμε την πολιτική (καθηγήτρια OR (φοιτήτριες AND πρόγραμμα μεταπτυχιακό)) για την καλύτερη κατανόηση της την αναπαριστούμε ένα διάγραμμα (δένδρο) AND-OR και θα είναι της εξής μορφής :



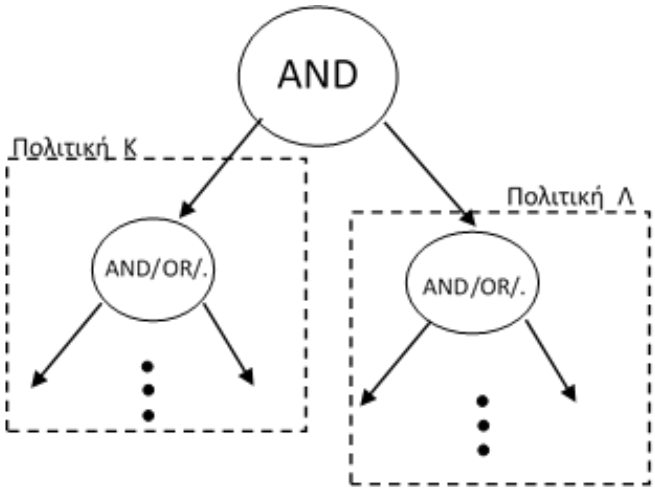
Σχήμα 2.4.1: Πολιτική

Η συγκεκριμένη πολιτική περιγράφει πως το κρυπτογραφημένο αρχείο είναι διαθέσιμο για ανάγνωση μόνο από δύο ειδών χρήστες. Οι πρώτοι πρέπει να έχουν το χαρακτηριστικό «καθηγήτρια», ενώ οι δεύτεροι πρέπει να έχουν τα χαρακτηριστικά ότι είναι φοιτήτριες ΚΑΙ ότι ανήκουν στο μεταπτυχιακό πρόγραμμα. Εάν παραδείγματος χάρη είναι φοιτήτριες και ανήκουν στο προπτυχιακό πρόγραμμα σπουδών, δεν θα μπορέσουν να έχουν πρόσβαση στην πληροφορία. Επομένως εάν το πακέτο χαρακτηριστικών του ιδιωτικού κλειδιού ικανοποιεί την Boolean μορφή, η οποία ισχύει για το κάθε σύστημα, χορηγείται η πρόσβαση στο αρχικό-μη κρυπτογραφημένο κείμενο (ή μήνυμα)(plaintext).

Ένα από τα βασικότερα και σημαντικότερα πλεονεκτήματα αυτής της μορφής κρυπτογράφησης είναι ότι η παραγωγή των ιδιωτικών κλειδιών και η διαδικασία της αποκρυπτογράφησης δεν είναι συνδεδεμένες. Τα ιδιωτικά κλειδιά παράγονται με βάση συγκεκριμένα χαρακτηριστικά, τα οποία πάντα θα είναι ικανά να αποκρυπτογραφούν δεδομένα, για τα οποία μπορούν να ικανοποιούν την Boolean σχέση που έχει δημιουργηθεί, χωρίς να επικοινωνούν ξανά με την Αρχή κλειδιού. Σε αυτό το σημείο πρέπει να σημειωθεί, πως υπάρχει μια νεότερη εκδοχή της κρυπτογραφίας βάσει χαρακτηριστικών, η οποία μπορεί να λάβει υπόψη το πρόβλημα αυτό με ανάκληση, μέσω κάποιου διακομιστή μεσολάβησης (proxy server) ή μέσω της ανάθεσης των πολιτικών (policy delegation), με την οποία παρέχεται η δυνατότητα της ενημέρωσης της δεδομένης πολιτικής που απαιτεί ένα μόνο

δημόσιο κλειδί. Τα χαρακτηριστικά ωστόσο είναι στατικά, συνεπώς μπορούν να αλλάξουν μόνο με την δημιουργία και το μοίρασμα ενός νέου, ιδιωτικού κλειδιού.

Ένα από τα σημαντικότερα χαρακτηριστικά – πλεονεκτήματα που έχει ο συγκεκριμένος τρόπος κρυπτογράφησης είναι η πρόληψη των επιθέσεων συγκρούσεων (collusion attacks-resistance). Για την επεξήγηση αυτού, θα παραθέσουμε το ακόλουθο παράδειγμα. Έχουμε ένα αρχείο το οποίο είναι κρυπτογραφημένο με την πολιτική (Κ and Λ), και το κρυπτογραφημένο αρχείο στέλνεται σε δύο χρήστες.



Σχήμα 2.4.2: Πολιτική (Κ and Λ)

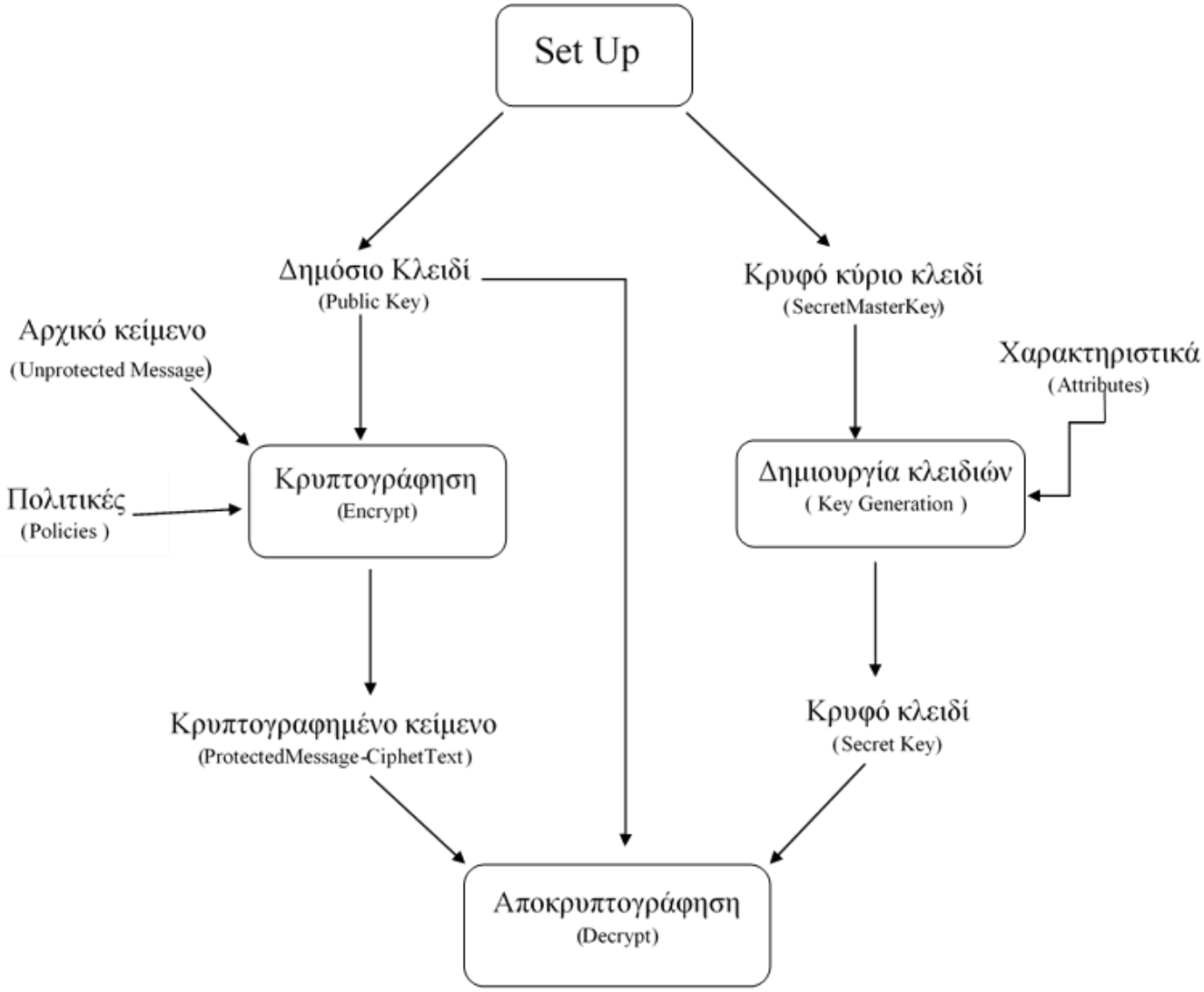
Ο πρώτος χρήστης με βάσει τα χαρακτηριστικά του έχει το ιδιωτικό κλειδί με την πολιτική Κ, ενώ ο δεύτερος χρήστης έχει το ιδιωτικό κλειδί με την πολιτική Λ. Ούτε ο πρώτος αλλά ούτε και ο δεύτερος χρήστης δεν θα μπορούσε να αποκρυπτογραφήσει το αρχείο που τους στάλθηκε, εφόσον τα χαρακτηριστικά που έχουν ο καθένας τους ατομικά, δεν ικανοποιούν την σχέση της πολιτικής. Για να μπορεί να πραγματοποιηθεί η αποκρυπτογράφηση, θα πρέπει οι χρήστες να κατέχουν και τις δύο πολιτικές. Η κρυπτογραφία αυτή έχει την εξής ιδιότητα: οι χρήστες να μην μπορούν να συνδυάσουν τα ιδιωτικά κλειδιά τους έτσι ώστε να δημιουργηθεί ένα ενιαίο-κοινό κλειδί, το οποίο θα μπορούσε να αποκρυπτογραφήσει το αρχείο το οποίο τους στάλθηκε. Στην συνέχεια θα παρατεθούν με αναλυτικό τρόπο και άλλα πλεονεκτήματα της κρυπτογράφησης αυτής.

Η Κρυπτογραφία Βάσει Χαρακτηριστικών χωρίζεται σε δύο βασικές κατηγορίες.
Η Key-Policy ABE (KP-ABE) παρουσιάστηκε το 2009 από τους Chase, S.S.M. Chow. Στο σχήμα αυτό το μήνυμα κρυπτογραφείται με ένα πακέτο χαρακτηριστικών και το ιδιωτικό κλειδί του χρήστη είναι συνδεδεμένο με την πολιτική που εφαρμόζεται. Εάν τα χαρακτηριστικά ικανοποιούν την πολιτική, μπορεί να γίνει η αποκρυπτογράφηση. Στην

Ciphertext-Policy ABE (CP-ABE), η οποία παρουσιάστηκε από τους J. Bethencourt, A. Sahai, B. Waters το 2007, το μήνυμα είναι κρυπτογραφημένο με βάσει την πολιτική και το ιδιωτικό κλειδί είναι συνδεδεμένο με τα χαρακτηριστικά του χρήστη.

(Ενότητα 2.4.β) Βασικές λειτουργίες

Το σχήμα της CP-ABE συνήθως περιέχει τις 4 βασικότερες διαδικασίες SetUp, Encrypt, Key Generation και Decrypt όπως και φαίνεται και στο παρακάτω σχήμα :



Σχήμα 2.4.3: CP-ABE

Ποιο συγκεκριμένα :

1. Setup: Η συγκεκριμένη λειτουργία δημιουργεί ένα δημόσιο κλειδί και ένα συνδεδεμένο κρυφό κύριο κλειδί.

2.Κρυπτογράφηση (Encrypt): Το αρχείο κρυπτογραφείται με ένα δημόσιο κλειδί και μία συγκεκριμένη πολιτική.

3. Δημιουργία των κλειδιών (Key Generation): Δημιουργείται ένα ιδιωτικό κλειδί με συγκεκριμένα χαρακτηριστικά, το οποίο επιτυγχάνεται με την χρήση του κρυφού κύριου κλειδιού. Τα τρία κλειδιά (ιδιωτικό –δημόσιο –κρυφό κύριο) είναι συνδεδεμένα μεταξύ τους.

4.Αποκρυπτογράφηση (Decrypt): Αυτή η λειτουργία δέχεται το κρυπτογραφημένο κείμενο και το ιδιωτικό κλειδί. Η αποκρυπτογράφηση μπορεί να ολοκληρωθεί μόνο και μόνο εάν τα χαρακτηριστικά των ιδιωτικών κλειδιών ικανοποιούν την πολιτική και το ιδιωτικό κλειδί είναι συνδεδεμένο με το δημόσιο κλειδί που έχει χρησιμοποιηθεί στην αρχή της κρυπτογράφησης.

(Ενότητα 2.4.γ) Εφαρμογές και Θετικά χρήσης ABE

Η Κρυπτογραφία Βάσει Χαρακτηριστικών έχει πολλές εφαρμογές σε διάφορους τομείς που χρησιμοποιούνται καθημερινώς όπως στο ηλεκτρονικό ταχυδρομείο (e-mail), στις υπηρεσίες αποθήκευσης προσωπικών δεδομένων, στα συστήματα επικοινωνίας οχημάτων, στις βάσεις δεδομένων, στο σύστημα υγείας, στον στρατό και σε άλλα.

Πέρα από την πρόληψη των επιθέσεων συγκρούσεων, όπως και περιγράψαμε στην παραπάνω υποενότητα, υπάρχουν και άλλα θετικά πλεονεκτήματα της χρήσης της Κρυπτογραφίας Βάσει Χαρακτηριστικών :

1. Επεκτασιμότητα: Είναι η ικανότητα χειρισμού του φορτίου του χρήστη που υποστηρίζεται,(αριθμός συναλλαγών, όγκος δεδομένων κτλ.). Όσο οι εξουσιοδοτημένοι χρήστες αυξάνονται, τόσο το σύστημα είναι σε θέση να λειτουργεί αποτελεσματικά χωρίς να υπάρχει πρόβλημα, δηλαδή το πλήθος των χρηστών δεν θα επηρεάζει την επίδοση του συστήματος .
2. Εμπιστευτικότητα των δεδομένων: Η εμπιστευτικότητα των δεδομένων θεωρείται το σύνολο κανόνων που έχει ως στόχο τον περιορισμό της πρόσβασης ή τον περιορισμό σε συγκεκριμένους τύπους πληροφοριών με την υποβολή περιορισμών. Τα δεδομένα στο εκάστοτε σύστημα είναι κρυπτογραφημένα από τον ιδιοκτήτη και οι μη εξουσιοδοτημένοι χρήστες συμπεριλαμβανόμενου και του ίδιου του συστήματος, δεν μπορούν να γνωρίζουν τις πληροφορίες που σχετίζονται με τα κρυπτογραφημένα δεδομένα. Με αυτόν τον τρόπο επιτυγχάνεται η διατήρηση της εμπιστευτικότητας των δεδομένων.

3. Ασφαλής έλεγχος πρόσβασης: Ορίζεται ως ο οποιοδήποτε μηχανισμός, μέσω του οποίου το σύστημα χορηγεί ή ανακαλεί το δικαίωμα πρόσβασης σε ορισμένα δεδομένα, ή το δικαίωμα εκτέλεσης δράσεων.

ΚΕΦΑΛΑΙΟ 3 Ανάπτυξη συστήματος προστασίας πόρων με χρήση ABE

(Υποκεφάλαιο 3.1) Απαιτήσεις–Περιπτώσεις χρήσης συστήματος

Κατά τη διάρκεια της κατασκευής του συστήματος για την καλύτερη κατανόηση και την πιο εύκολη ολοκλήρωση αυτού, έγινε χρήση της τεχνικής της «σύνταξης-απαρίθμησης» των περιπτώσεων χρήσεων (use cases) και των απαιτήσεων (requirements) του συστήματος.

(Ενότητα 3.1.α) Περιπτώσεις χρήσης συστήματος

Με βάση τον Βεσκούκη, ως περίπτωση χρήσης ορίζεται ως «η αλληλουχία ενεργειών που εκτελεί το λογισμικό αλληλοεπιδρώντας με τον χρήστη ή με εξωτερικά συστήματα, προκειμένου να ικανοποιήσει μία λειτουργική απαίτηση.» [Veskoukis, V. (2015)]. Η κάθε μια από αυτή μπορεί να προσδιορίζεται με περισσότερη ή λιγότερη λεπτομέρεια.
Στο σύστημα της συγκεκριμένης εργασίας υπάρχουν οι εξής περιπτώσεις χρήσης:

Δημιουργία ψηφιακών χαρακτηριστικών

Για την υλοποίηση του συστήματος έχουμε την δημιουργία κάποιων χαρακτηριστικών μοναδικών για κάθε χρήστη τα οποία χρησιμοποιεί και χρειάζεται το σύστημα για την πιστοποίηση των χρηστών και κατά συνέπεια την συνέχιση του συστήματος. Η δημιουργία των χαρακτηριστικών γίνεται μέσω συγκεκριμένων αξιόπιστων ψηφιακών πιστοποιητικών.(X.509).

Δημιουργία κρυπτογραφικού κλειδιού αποκρυπτογράφησης με βάση τα χαρακτηριστικά

Το σύστημα δέχεται κάποια αξιόπιστα ψηφιακά πιστοποιητικά τα οποία ελέγχονται με βάσει τα χαρακτηριστικά (attributes), που είναι προκαθορισμένα από το σύστημα. Εάν τα πιστοποιητικά είναι αξιόπιστα και τηρούν τα attributes η διαδικασία της δημιουργίας κρυπτογραφικού κλειδιού αποκρυπτογράφησης συνεχίζεται, ενώ εάν δεν είναι αξιόπιστα το σύστημα σταματάει την διαδικασία.

Δημιουργία των policies

Με βάση τις ανάγκες του συστήματος δημιουργούμε τις πολιτικές-policies οι οποίες και καθορίζουν ποιος μπορεί να κάνει χρήση αυτού. Προκύπτει δηλαδή η δημιουργία ενός συνόλου μεταβλητών, οι οποίες αλλάζουν με βάσει τις ανάγκες του προγράμματος .

Δημιουργία κλειδιών κρυπτογράφησης

Το σύστημα αρχικά θα δημιουργήσει το δημόσιο κλειδί και το κύριο ιδιωτικό κλειδί. Έπειτα ο Key Generator (γεννήτρια κλειδιών) με βάσει το κύριο ιδιωτικό κλειδί που έχει δημιουργηθεί νωρίτερα και τα χαρακτηριστικά τα οποία παρέχονται, δημιουργεί το μοναδικό ιδιωτικό κλειδί.

Κρυπτογράφηση

Στην συγκεκριμένη περίπτωση χρήσης γίνεται η κρυπτογράφηση του αρχείου σύμφωνα με την πολιτική που έχουμε ως δεδομένη και το αρχικό μη κρυπτογραφημένο κείμενο-αρχείο

Αποκρυπτογράφηση

Τελευταίο μέρος του συστήματος είναι η αποκρυπτογράφηση της πληροφορίας. Για την υλοποίηση της διαδικασίας αυτής παίρνουμε ως παραμέτρους το ιδιωτικό κλειδί, το οποίο είναι συνδεδεμένο με τα χαρακτηριστικά που ικανοποιούν τις πολιτικές και το αποτέλεσμα της διαδικασίας της κρυπτογράφησης, δηλαδή το κρυπτογραφημένο κείμενο-αρχείο (ciphertext).

(Ενότητα 3.1.β) Απαιτήσεις Συστήματος

Ο Βεσκούκης δίνει τον ορισμό για την απαίτηση του συστήματος ως «μια λειτουργία που αυτό θα πρέπει να επιτελεί ή μια συνθήκη που θα πρέπει να ικανοποιεί όταν θα έχει ολοκληρωθεί η κατασκευή του.» [Veskoukis, V. (2015)]. Η διαδικασία είναι μείζονος σημασίας, διότι ο σωστός προσδιορισμός των διεργασιών οδηγεί στην αποφυγή δημιουργίας λογισμικού όπου δεν θα καλύπτει τον σκοπό δημιουργίας του.
Στο δικό μας σύστημα οι απαιτήσεις που πρέπει να καλύπτει είναι οι εξής:

- Δημιουργία ψηφιακών πιστοποιητικών τύπου X.509.
- Εξαγωγή χαρακτηριστικών από ένα ψηφιακό πιστοποιητικό τύπου X.509 και εισαγωγή αυτών στο σύστημα μας .
- Δημιουργία δημοσίου κλειδιού (Public Key) και κύριου κρυφού κλειδιού (Master Secret Key).

- Συνδυασμός χαρακτηριστικών (attributes) έτσι ώστε να μπορεί να γίνεται η δημιουργία του κρυφού κλειδιού (secret key).
- Δημιουργία πολιτικών (policies).
- Εισαγωγή του αρχείου στο σύστημα, συνδυασμού αυτού με τις πολιτικές και εξαγωγή του αποτελέσματος (ciphertext) για τη χρήση του στην συνέχεια .
- Συνδυασμός κρυφού κλειδιού και κρυπτοκειμένου για την αποκρυπτογράφηση.

(Υποκεφάλαιο 3.2) Αρχιτεκτονική συστήματος

Ο στόχος της παρούσας πτυχιακής είναι η δημιουργία ενός συστήματος το οποίο δέχεται ένα αρχείο/κείμενο το οποίο και το κρυπτογραφεί. Στην αρχή δημιουργείται για κάθε χρήστη, με βάση τα μοναδικά του χαρακτηριστικά έμπιστα ψηφιακά πιστοποιητικά τύπου X.509. Στην συνέχεια κατά τη διάρκεια της κρυπτογράφησης, δίνεται μια σχέση πολιτικής στην οποία αναφέρονται τα χαρακτηριστικά τα οποία πρέπει ο κάθε χρήστης να κατέχει, έτσι ώστε να είναι σε θέση το σύστημα να αποκρυπτογραφήσει τα κρυπτογραφημένα δεδομένα. Τα χαρακτηριστικά αυτά παρέχονται από τα X.509 ψηφιακά πιστοποιητικά. Τέλος εάν ο χρήστης με βάσει τα χαρακτηριστικά του ικανοποιεί την πολιτική, έχουμε την ολοκλήρωση του συστήματος, δηλαδή την αποκρυπτογράφηση των δεδομένων. Αντίθετα, εάν όχι το σύστημα μας ενημερώνει για την «αποτυχία» της αποκρυπτογράφησης.

Για την ολοκλήρωση του συστήματος μας έχουμε 4 οντότητες οι οποίες έχουν ως σκοπό τη διευκόλυνση των διαδικασιών όπου θα δούμε παρακάτω. Οι 4 οντότητες είναι οι εξής:

•Αρχή Πιστοποιητικών, είναι μια έμπιστη οντότητα η οποία εξάγει πιστοποιητικά τα οποία είναι αρχεία δεδομένων που συνδυάζουν την κρυπτογραφική οντότητα με ένα δημόσιο κλειδί. Η οντότητα αυτή βοηθάει για την εξασφάλιση της εμπιστοσύνης επικοινωνίας μεταξύ των χρηστών και του δικτύου, την επαλήθευση ταυτότητας και την διατήρηση καταλόγου ανάκλησης πιστοποιητικών.

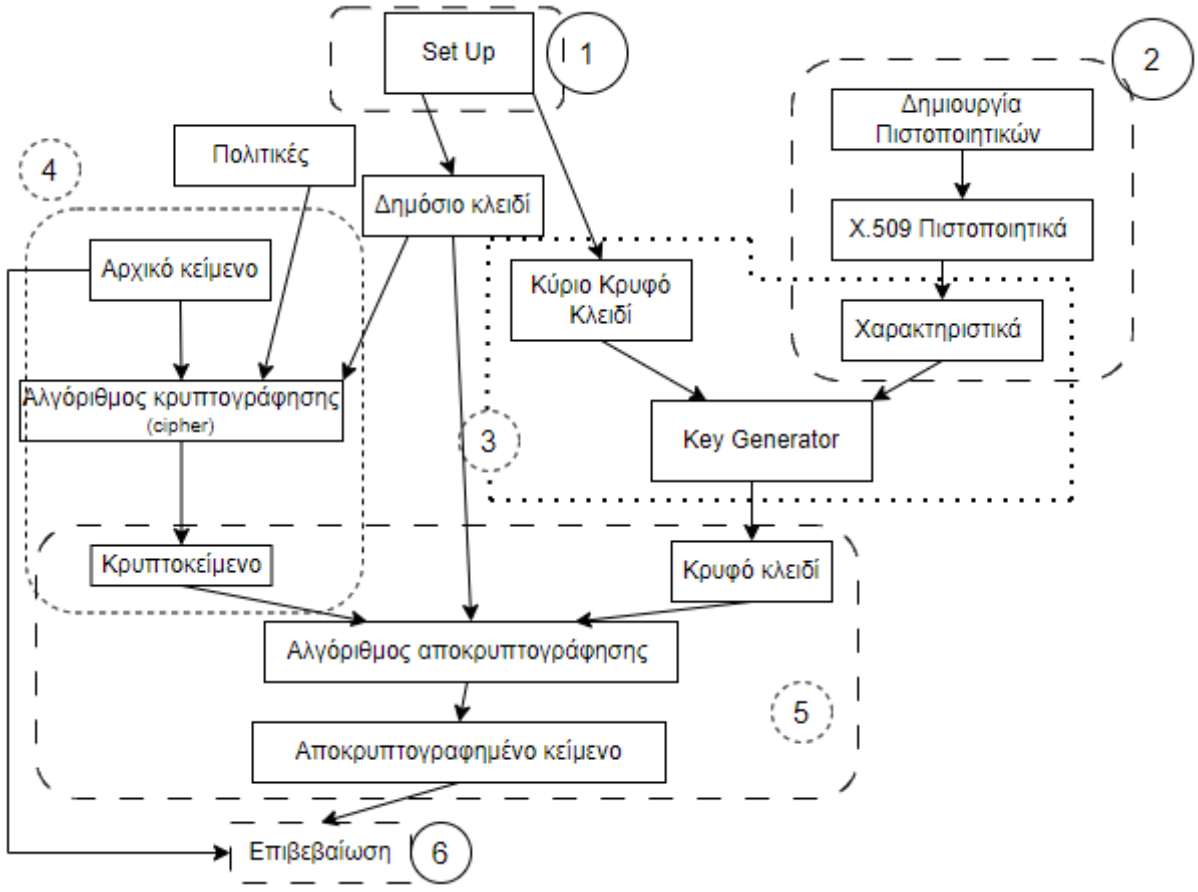
•Αρχικοποίηση, η οντότητα αυτή έχει ως σκοπό, όπως αποκαλύπτει και το όνομα της την αρχικοποίηση του συστήματος δηλαδή την παραγωγή συγκεκριμένων παραμέτρων που βασίζεται το κάθε σύστημα στο οποίο χρησιμοποιείται.

•Κρυπτογράφηση, η οντότητα αυτή είναι υπεύθυνη για την προστασία των δεδομένων με την χρήση μαθηματικών μοντέλων και τη δημιουργία αυτών σε ακατάλληλη μορφή έτσι ώστε μόνο οι εξουσιοδοτημένοι χρήστες να έχουν πρόσβαση.

•Αποκρυπτογράφηση, η οντότητα αυτή συνδέεται άμεσα με την κρυπτογράφηση, σκοπός της είναι η μετατροπή των δεδομένων ακατάλληλης μορφής σε μια ευανάγνωστη μορφή, εφόσον ο χρήστης θεωρείται εξουσιοδοτημένος.

Για την υλοποίηση του συστήματος που μόλις περιγράψαμε έχουμε τη δημιουργία έξι διαφορετικών διαδικασιών. Οι διαδικασίες αυτές μπορεί να είναι διαφορετικές μεταξύ τους, αλλά η μία είναι η συνέχεια της άλλης, για την οποία και αποτελεί βασικό ρόλο για την υλοποίηση της επόμενης και ως συνέπεια την ολοκλήρωση του συστήματος.

Στο παρακάτω σχεδιάγραμμα παρατίθονται σχεσιακά οι διαδικασίες και εξηγείται η κάθε μια ξεχωριστά.



Σχήμα 3.2.1: Αρχιτεκτονική συστήματος

Η 1η διαδικασία είναι αυτή της αρχικοποίησης του συστήματος. Σε αυτήν, όπως φανερώνει και το όνομα της, γίνεται η αρχικοποίηση του συστήματος, η οποία είναι υπεύθυνη για την δημιουργία του κύριου κρυφού κλειδιού (Master Secret Key-msk) και του δημόσιου κλειδιού (Public Key).

Η 2η διαδικασία είναι υπεύθυνη για τη δημιουργία ενός μέρους του συστήματος, το οποίο είναι μείζονος σημασίας, εφόσον εντός του οποίου πραγματοποιείται η δημιουργία των χαρακτηριστικών των χρηστών. Στο σύστημα μας τα χαρακτηριστικά είναι ψηφιακά πιστοποιητικά τύπου X.509. Η δημιουργία πιστοποιητικών της 3ης μορφής έκδοσης υλοποιείται από μια έμπιστη Αρχή Πιστοποιητικών (Certification Authority). Το πιστοποιητικό αυτό περιέχει όλα τα πεδία της έκδοσης, η οποία έχει ήδη προαναφερθεί και σε προηγούμενο υποκεφάλαιο. Για τη δημιουργία των ψηφιακών πιστοποιητικών τύπου X.509 ακολουθούμε τα ακόλουθα βήματα:

1ο.Δημιουργία ζεύγους κλειδιών το οποίο ταυτίζεται με το πιστοποιητικό.

2ο.Δημιουργία δομής του νέου πιστοποιητικού.

3ο.«Φόρτωση» του κρυφού κλειδιού της αρχής πιστοποίησης και το πιστοποιητικό.

4ο. Υπογραφή πιστοποιητικού.

5ο. Αποθήκευση πιστοποιητικού σαν φάκελος

Σημαντικό μέρος της διαδικασίας παραγωγής είναι το 5ο βήμα όπου αναφέρεται η αποθήκευση του πιστοποιητικού αυτού για τη χρήση αυτού από άλλες εφαρμογές.

Ως συνέχεια της παραπάνω διαδικασίας προκύπτει η 3η διαδικασία, αυτή της δημιουργίας του μοναδικού κρυφού κλειδιού (Secret Key-skey). Η διαδικασία αυτή γίνεται με τον συνδυασμό του κύριου κρυφού κλειδιού και το σύνολο των χαρακτηριστικών, τα οποία κατέχει ο κάθε χρήστης.

Η 4η διαδικασία, η οποία ακολουθεί, είναι αυτή της κρυπτογράφησης. Πρόκειται για την διαδικασία που είναι αρμόδια για την κρυπτογράφησης δεδομένων με βάση την Boolean πολιτική, η οποία είναι απαραίτητή να εφαρμοστεί. Η κρυπτογράφηση εκτελείται με την

χρήση ενός κρυπταγλόριθμου στα δεδομένα. Το αποτέλεσμα της διαδικασίας είναι η δημιουργία του κρυπτογραφημένου κειμένου/αρχείου (Ciphertext-cpt).

Η 5η διαδικασία είναι εκείνη της αποκρυπτογράφησης των δεδομένων. Για την υλοποίηση της, ένας αλγόριθμος αποκρυπτογράφησης δέχεται τα αποτελέσματα των δύο τελευταίων διαδικασιών, δηλαδή του κρυπτογραφημένου κειμένου/αρχείου και το μοναδικό κρυφό κλειδί αλλά και το δημόσιο κλειδί. Μετά την αποκρυπτογράφηση δημιουργείται ένα αποκρυπτογραφημένο κειμένου (decrypted).

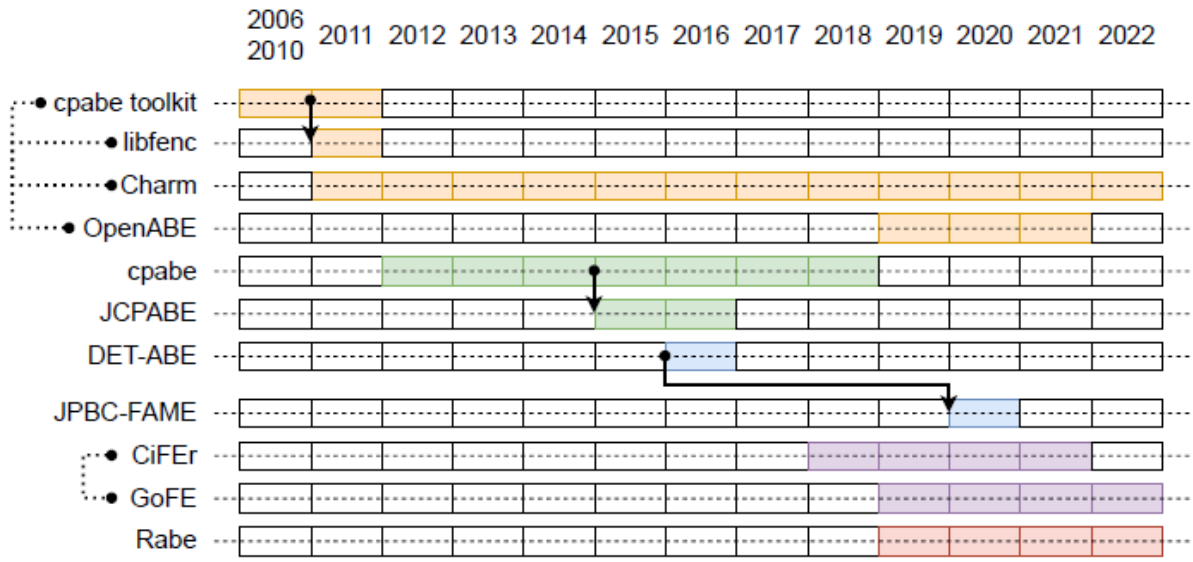
Η 6η και τελευταία διαδικασία είναι αυτή του ελέγχου-της επιβεβαίωσης της κρυπτογράφησης. Σε αυτή διεκπεραιώνεται η σύγκριση των αρχικών δεδομένων και του αποκρυπτογραφημένου κειμένου. Τα πιθανά αποτελέσματα είναι δύο. Στην 1η περίπτωση υπάρχει η ταύτιση των δύο συγκεκριμένων δεδομένων και έτσι το σύστημα μας ενημερώνει για την επιτυχία της αποκρυπτογράφησης. Στην 2η περίπτωση υπάρχει η μη ταύτιση των δύο δεδομένων και η αντίστοιχη ενημέρωση για το «Error» που έχει δημιουργηθεί.

(Υποκεφάλαιο 3.3) Τεχνολογίες συστήματος

Παρά την ύπαρξη πολλών διαφορετικών παραλλαγών σχημάτων-συστημάτων της Κρυπτογραφίας Βάσει Χαρακτηριστικών, δεν υπάρχει κάποια συγκεκριμένη βιβλιοθήκη η οποία να χρησιμοποιείται από το ευρύ κοινό. Έτσι οι προγραμματιστές έχουν να αντιμετωπίσουν το «πρόβλημα» της επιλογής της κατάλληλης βιβλιοθήκης που θα χρησιμοποιήσουν στα έργα τους με σκοπό αυτό να είναι αποδοτικό και ταυτόχρονα ισάξια ασφαλές.

Με τη δημοσίευση του κρυπτογραφικού σχήματος CP-ABE από τον Bethencourt το 2006 έγινε μαζί και η πρώτη παρουσίαση της βιβλιοθήκης cpabe, η οποία ήταν η μοναδική βιβλιοθήκη ABE για πέντε χρόνια περίπου. Το 2011 έχουμε την δημιουργία δύο καινούργιων βιβλιοθηκών: της libfenc από τους M. D. Green, J. A. Akinyele, M. A. Rushanan, η οποία χρησιμοποιεί μέρη της cpabe για την υλοποίηση της και της πρώτης έκδοσης της Charm, η οποία και αναπτύχθηκε και διατηρήθηκε από μερικούς από τους προγραμματιστές της libfenc μεταξύ των υπόλοιπων προγραμματιστών. Τον Οκτώβριο του 2015 από τους M. Morales-Sandoval, A. Diaz-Perez γίνεται η δημοσίευση της βιβλιοθήκης DET-ABE, η οποία αργότερα, τον Ιανουάριο του 2020 εξελίχθηκε από τον C.Chow, από τον οποίο δημιουργήθηκε και παρουσιάστηκε η Java Pairing Based Cryptography-Fast Attribute Based

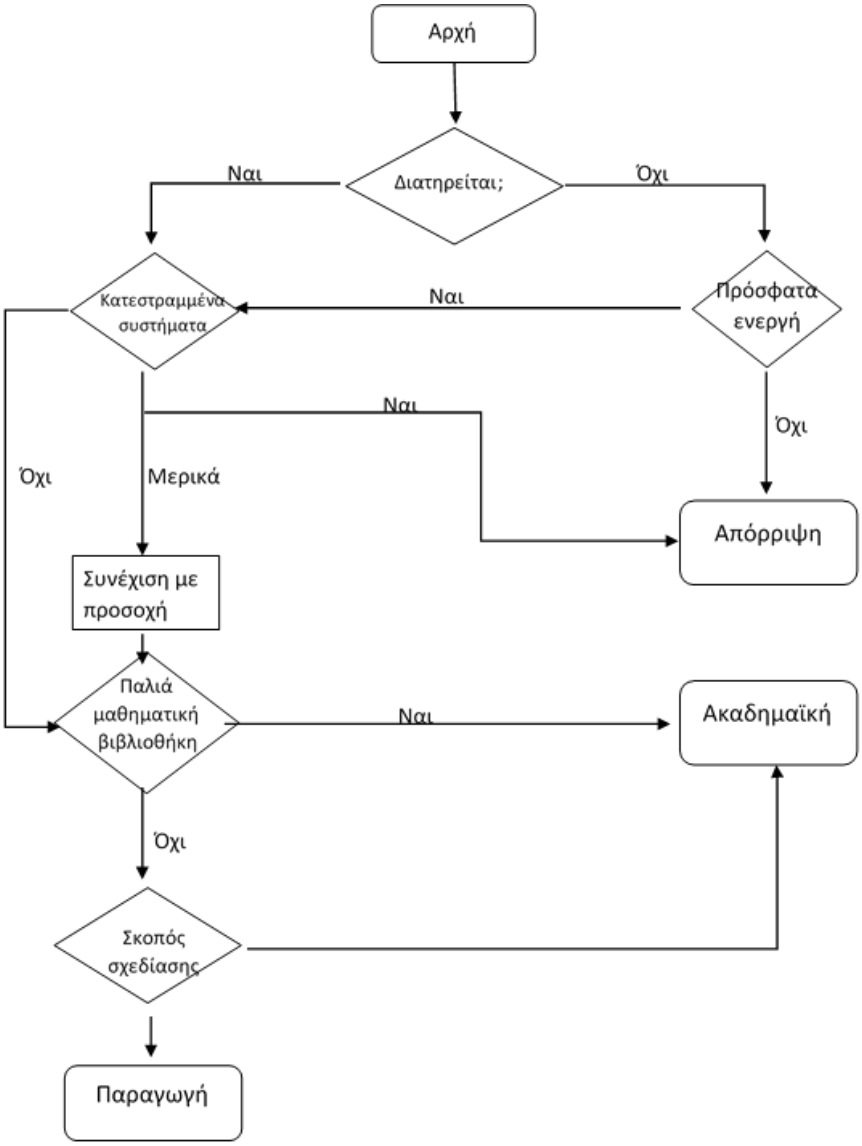
Encryption Message Encryption (jPBC-FAME). Στο παρακάτω σχήμα παρουσιάζονται οι βιβλιοθήκες που έχουν δημιουργηθεί, το πότε το πώς και εάν σχετίζονται μεταξύ τους .



Σχήμα 3.3.1: Χρονολογική αναπαράσταση βιβλιοθηκών ABE [Mosteiro-Sanchez et al., 2022]

Λόγω πλέον της μεγάλης ύπαρξης βιβλιοθηκών σχημάτων ABE, έχει δημιουργηθεί ένα διάγραμμα, το οποίο βοηθάει τους προγραμματιστές να αποφασίσουν ποια βιβλιοθήκη θα χρησιμοποιήσουν, με βάσει αυτό που θέλουν να κάνουν αλλά και τις συγκεκριμένες ιδιότητες που κατέχουν.

Στο παρακάτω σχεδιάγραμμα παρατίθεται το πώς γίνεται η διαδικασία επιλογής της βιβλιοθήκης:



Σχήμα 3.3.2 : Διαδικασία ανάλυσης επιλογής βιβλιοθήκης

Δεν θα αναλυθεί η παραπάνω διαδικασία που ακολουθείται για την εκάστοτε βιβλιοθήκη.

Για την παρούσα πτυχιακή εργασία ακολουθήσαμε την διαδικασία αυτή ώστε να γίνει η επιλογή της βιβλιοθήκης Java Pairing Based Cryptography-Fast Attribute Based Encryption Message Encryption (jPBC-FAME), η οποία όπως προαναφέρθηκε, δημιουργήθηκε το 2020 από τον C.Chow.

Στην υλοποίηση της πτυχιακή μας εκτός από την επιλογή της βιβλιοθήκης jPBC-FAME, γίνεται και η επιλογή της γλώσσας προγραμματισμού Java αλλά και η χρήση της βιβλιοθήκης Bouncycastle. Παρακάτω αναφέρουμε τους λόγους επιλογής αλλά και για καθεμία κάποιες πληροφορίες.

Java

Η Java είναι μια γλώσσα προγραμματισμού η οποία τα τελευταία χρόνια χρησιμοποιείται από πολλούς προγραμματιστές για την υλοποίηση εργασιών. Εξαιτίας αυτού του γεγονότος σημειώνεται η ύπαρξη αρκετών κρυπτογραφικών βιβλιοθηκών που την έχουν ως βάση τους. Η επιλογή της συγκεκριμένης γλώσσας έγινε λόγω της προσαρμοστικότητας (versatility) της, της φορητότητας (portability) της, της εξασφάλισης της ασφάλειας και της ανεξαρτησίας της από δυσνόητους αλγόριθμους ασφάλειας. Όλα τα παραπάνω επιτυγχάνονται διότι η Java παρέχει κρυπτογραφικά Application Programming Interface (API) τα οποία και συγκαταλέγονται στην Java Cryptography Extension (JCE). Ο JCE μηχανισμός επιτρέπει την εκτέλεση κρυπτογραφικών δραστηριοτήτων, οι οποίες έχουν ζωτικό χαρακτήρα για το σύστημα μας. Πιο συγκεκριμένα συμπεριλαμβάνονται οι εξής κρυπτογραφικές δραστηριότητες: Κρυπτογράφηση, Αποκρυπτογράφηση, Παραγωγή-διαχείριση κλειδιών, ψηφιακές υπογραφές και άλλα.

Για την καλύτερη κατανόηση της επιλεγόμενης βιβλιοθήκης θα αναλυθούν τα δύο μέρη της ξεχωριστά.

jPBC

Αρχικά,με την χρήση της βιβλιοθήκης Java Pairing Based Cryptography μας παρέχεται, αρχικά ένας τρόπος πρόσβασης της βιβλιοθήκης PBC, η οποία αναπτύχθηκε από τον Ben Lynn και εκτελεί μαθηματικές λειτουργίες, οι οποίες αποτελούν βάση για τα pairing-based κρυπτοσυστήματα. Επίσης, παρέχεται μια συνάρτηση περιτυλίγματος (wrapper function), η οποία χρησιμοποιείται, έτσι ώστε να αυξηθούν οι επιδόσεις του συστήματος. Η επιτυχία οφείλεται στην ανάθεση του pairing computation στη βιβλιοθήκη αυτή. Ένα ακόμα λόγος επιλογής της βιβλιοθήκης αυτής είναι το γεγονός ότι η jPBC προσφέρει στους προγραμματιστές ένα εύρος διεπαφών και κλάσεων, που έχουν σκοπό την ευκολότερη διαχείριση των διγραμμικών χαρτών κρυπτογράφησης. Τέλος υπάρχει και η εφαρμογή των πολυγραμμικών χαρτών (multinear map), των οποίων η χρήση προσφέρει την πολυδιάστατη ανάγνωση και αποθήκευση στην κεντρική μνήμη μέσω ενός αρχείου με αντιστοίχιση μνήμης (memory-mapped file).
Στη βιβλιοθήκη αυτή συγκαταλέγονται και τα «εργαλεία»: cpabe-setup, cpabe-keygen, cpabe-enc, cpabe-dec, τα οποία και χρησιμοποιούνται για την υλοποίηση του συστήματος της συγκεκριμένης εργασίας.

FAME

Η Fast Attribute Based Encryption Message Encryption αναπτύχθηκε και παρουσιάστηκε το 2017 από τους Agrawal και Chase. Θεωρείται από τα πιο αποτελεσματικά σχέδια επίλυσης συστημάτων ABE, με βάση την πολυπλοκότητα των λειτουργιών. Αναλυτικότερα, η FAME επιτυγχάνει γρηγορότερη κρυπτογράφηση και παραγωγή κλειδιών [Agrawal and Chase, 2017], ενώ χρειάζεται μικρότερο αριθμό ζευγαρισμάτων (pairing) για την αποκρυπτογράφηση. Το σημαντικό πλεονέκτημα σε αυτήν την περίπτωση είναι πως δεν τίθενται περιορισμοί, όσον αφορά το μέγεθος των πολιτικών αλλά και το σύνολο των χαρακτηριστικών που εφαρμόζονται. Γι' αυτόν τον λόγο καθίσταται ιδανική για πολύπλοκες πολιτικές.

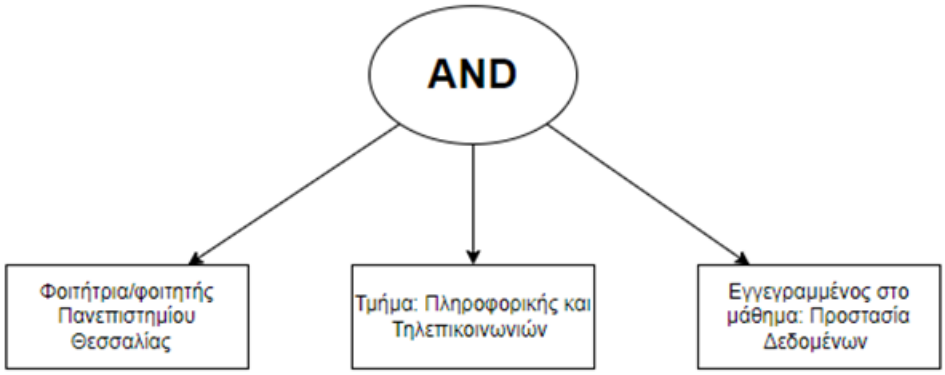
Bouncycastle

Για την δημιουργία του ψηφιακού πιστοποιητικού X.509 γίνεται χρήση της βιβλιοθήκης Bouncycastle. Η πρώτη δημοσίευση της βιβλιοθήκης αυτής έγινε το 2000 και σκοπός της είναι η εκτέλεση βασικών κρυπτογραφικών λειτουργιών. Η Bouncycastle είναι μια Java βιβλιοθήκη, που συμπληρώνει και παρέχεται στην JCE, ενώ ταυτόχρονα διαδραματίζει τον ρόλο ενός API, το οποίο χρησιμοποιείται στην κρυπτογραφία. Τα APIs της βιβλιοθήκης αυτής αποτελούν σημαντικό μέρος για την γεννήτρια εκδόσεων 1 και 3 ψηφιακών πιστοποιητικών τύπου X.509, για αυτό και επιλέχθηκε για την εργασία αυτή.

(Υποκεφάλαιο 3.4) Παράδειγμα χρήσης

Με βάση το σύστημα μας, παραθέτουμε το εξής απλό παράδειγμα χρήσης.

Στην πλατφόρμα e-class του πανεπιστημίου, ένας καθηγητής ανεβάζει διαφάνειες που αφορούν το μάθημα του, κάνοντας λήψη των αρχείων αυτών καταλαβαίνουμε ότι οι διαφάνειες είναι κρυπτογραφημένες με μια συγκεκριμένη πολιτική, δηλαδή ένα σύνολο χαρακτηριστικών που θα πρέπει να έχουν οι χρήστες για να έχουν πρόσβαση και είναι οι εξής: Πρώτον ο χρήστης να είναι φοιτητής/φοιτήτρια του Πανεπιστημίου Θεσσαλίας, δεύτερον να φοιτά στο τμήμα Πληροφορικής και Τηλεπικοινωνιών και τρίτον να είναι εγγεγραμμένος στο μάθημα «Προστασίας δεδομένων». Η πολιτική εμφανίζεται και σχηματικά παρακάτω.



Σχήμα 3.4.1 : Πολιτική παραδείγματος χρήσης

Για τη συνέχιση του παραδείγματος δεχόμαστε την ύπαρξη δυο διαφορετικών χρηστών. Και οι δύο χρήστες παρέχουν τα δύο πρώτα χαρακτηριστικά της συγκεκριμένης πολιτικής, δηλαδή είναι φοιτητές του Πανεπιστημίου Θεσσαλίας και πιο συγκεκριμένα του τμήματος Πληροφορικής και Τηλεπικοινωνιών. Η διαφοροποίηση των δύο αυτών χρηστών είναι στην ύπαρξη του τρίτου χαρακτηριστικού, όπου ο πρώτος χρήστης είναι εγγεγραμμένος στο μάθημά «Προστασίας δεδομένων» σε αντίθεση με τον δεύτερο όπου δεν είναι. Λόγω αυτής της διαφοροποίησης έχουμε την ύπαρξη 2 αποτελεσμάτων. Στο πρώτο αποτέλεσμα, ο πρώτος χρήστης επειδή ικανοποιεί και τα τρία χαρακτηριστικά της δοσμένης πολιτικής, θα μπορέσει να συνεχίσει στην διαδικασία της αποκρυπτογράφησης και την ανάγνωση των διαφανειών αυτών. Ενώ στο δεύτερο αποτέλεσμα, ο δεύτερος χρήστης παρόλο που καλύπτει τα δύο πρώτα χαρακτηριστικά δεν είναι εγγεγραμμένος στο συγκεκριμένο μάθημα που αναφέρεται η πολιτική, έτσι δεν καλύπτει το τρίτο χαρακτηριστικό, οπότε και δεν είναι σε θέση να αποκρυπτογραφήσει τις διαφάνειες.

ΚΕΦΑΛΑΙΟ 4 Συμπεράσματα

Η κρυπτογραφία Attribute Based Encryption, από την δημοσίευση του έως και τώρα, είναι μια πολλά υποσχόμενη τεχνολογία, η οποία συνεχώς αναπτύσσεται και περνάει από πολλά στάδια εξέλιξης . Είναι ένα εργαλείο το οποίο λόγο της δομής του παρέχει τον ασφαλή έλεγχο πρόσβασης στα κρυπτογραφημένα δεδομένα όπου υπάρχουν σε συστήματα διαφόρων τομέων. Το γεγονός ότι στο συγκεκριμένο σχέδιο κρυπτογράφησης, για την υλοποίηση του χρησιμοποιεί τον συνδυασμό των χαρακτηριστικών, μπορεί να λύσει και να αποτρέψει τα τυχόν ατυχήματα που προκύπτουν στην προστασία των ψηφιακών δεδομένων. Με τη χρήση των ψηφιακών πιστοποιητικών του τύπου X.509 ως χαρακτηριστικά, δίνεται λύση στην αυθεντικοποίηση και την αξιοπιστία των δεδομένων και των χρηστών. Επομένως το σχήμα Attribute Based Encryption παρέχει στους χρήστες του μεγαλύτερο έλεγχο και ασφάλεια των διαδικασιών από χρήστες τρίτους που δεν είναι εξουσιοδοτημένοι να έχουν πρόσβαση σε αυτές.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Agrawal, S. and Chase, M. (2017). FAME. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. doi:https://doi.org/10.1145/3133956.3134014.

Alex.Arnaut (2018). *What is a Digital Signature & How Do I Create One?* [online] DocuSign. Available at: https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq.

Amanda Tucker (2022). *What is an X.509 Digital Certificate?* [online] SecureW2. Available at: https://www.securew2.com/blog/what-is-an-x-509-certificate.

Appviewx (n.d.). *What is X.509 Standard? | x509 Certificates*. [online] AppViewX. Available at: https://www.appviewx.com/education-center/what-is-x-509-standard/.

Barker, E. (2006). *Recommendation for Obtaining Assurances for Digital Signature Applications Technology Administration*. [online] Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-89.pdf.

Bethencourt, J., Sahai, A. and Waters, B. (2007). *Ciphertext-Policy Attribute-Based Encryption*. [online] IEEE Xplore. doi:https://doi.org/10.1109/SP.2007.11.

Binance Academy (2019). *Τι είναι η ψηφιακή υπογραφή;* [online] Binance Academy. Available at: https://academy.binance.com/el/articles/what-is-a-digital-signature.

Brugger, T. (2015). *Difference Between Direct & Arbitrated Digital Signature | Techwalla*. [online] Techwalla. Available at: https://www.techwalla.com/articles/difference-between-direct-arbitrated-digital-signature.

Chase, M. and Chow, S.S.M. (2009). Improving privacy and security in multi-authority attribute-based encryption. *Proceedings of the 16th ACM conference on Computer and communications security - CCS '09*. doi:https://doi.org/10.1145/1653662.1653678.

Χρυσούλας, Χ. (2013). *Ψηφιακές Υπογραφές στην Κρυπτογραφία Διπλωματική εργασία της*. [online] Available at: https://dspace.lib.ntua.gr/xmlui/bitstream/handle/123456789/38783/chatzic_digital.pdf?seque

nce=1 .

CISA (2009). *Understanding Digital Signatures | CISA*. [online] www.cisa.gov. Available at: https://www.cisa.gov/uscert/ncas/tips/ST04-018.

Coron, J.-S. . (2006). What is cryptography? *IEEE Security & Privacy Magazine*, 4(1), pp.70–73. doi:https://doi.org/10.1109/msp.2006.29.

CSRC (n.d.). *encryption - Glossary | CSRC*. [online] csrc.nist.gov. Available at: https://csrc.nist.gov/glossary/term/encryption.

De Caro, A. and Iovino, V. (2011). jPBC: Java pairing based cryptography. *2011 IEEE Symposium on Computers and Communications (ISCC)*. doi:https://doi.org/10.1109/iscc.2011.5983948.

Easttom, W. (2021). *MODERN CRYPTOGRAPHY : applied mathematics for encryption and information security.* S.L.: Springer Nature.

gas.dia.unisa.it. (2013). *JPBC - Java Pairing-Based Cryptography Library : Introduction*. [online] Available at: http://gas.dia.unisa.it/projects/jpbc/#.Y9Kp1HZBzIU.

Geeksforgeeks (2020). *Difference between Direct and Arbitrated Digital Signature*. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/difference-between-direct-and-arbitrated-digital-signature/.

GeeksforGeeks. (2022). *X.509 Authentication Service*. [online] Available at: https://www.geeksforgeeks.org/x-509-authentication-service/.

Goyal, V., Pandey, O., Sahai, A. and Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM conference on Computer and communications security - CCS '06*. doi:https://doi.org/10.1145/1180405.1180418.

Gremban, K. (2022). *Tutorial - Understand Cryptography and X.509 certificates for Azure IoT Hub*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/azure/iot-hub/tutorial-x509-introduction.

JavaTpoint (n.d.). *Cybersecurity Digital Signature - javatpoint*. [online]

www.javatpoint.com. Available at: https://www.javatpoint.com/cyber-security-digital-signature.

Καρέτση, Φ. (2016). *Κρυπτογραφία: Όλα όσα χρειάζεται να ξέρεις για να μην είσαι πια αρχάριος!* [online] Frapress. Available at: https://frapress.gr/2016/12/kriptografia-ola-osa-chriazete-na-xeris-gia-na-min-ise-pia-archarios/.

Kaspersky (2021). *Cryptography Definition*. [online] Kaspersky. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cryptography.

Kessler, G. (2019). *An Overview of Cryptography*. [online] Garykessler.net. Available at: https://www.garykessler.net/library/crypto.html.

KOTHARI, J. (2019). *Cryptography and its Types - GeeksforGeeks*. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/cryptography-and-its-types/.

Lakshmi, R., Laavanya, R., Meenakshi, M. and Gana Dhas, Dr.C.Suresh. (2015). Analysis of Attribute Based Encryption Schemes. *International Journal of Computer Science and Engineering Communications*, [online] 3(3), pp.1076–1081. Available at: https://oaji.net/articles/2015/2028-1433398925.pdf.

Legion of the Bouncy Castle (n.d.). *bouncycastle*. [online] www.bouncycastle.org. Available at: https://www.bouncycastle.org/.

Marget, A. (2022). *Data Encryption: How It Works & Methods Used*. [online] Unitrends. Available at: https://www.unitrends.com/blog/data-encryption.

Mosteiro-Sanchez, A., Barcelo, M., Astorga, J. and Urbieta, A. (2022). Too Many Options: A Survey of ABE Libraries for Developers. *arXiv:2209.12742 [cs]*. [online] Available at: https://arxiv.org/abs/2209.12742.

Παπαϊωάννου, Ε. (n.d.). *Ψηφιακές Υπογραφές (Digital Signatures)*. [online] Available at: https://www.ceid.upatras.gr/webpages/faculty/papaioan/dchmnt/2018-19/ita-lectures/lec7.pdf.

Parker, M.G. (2009). *Cryptography and Coding*. Springer Science & Business Media.

Paterson, K.G. (2011). *Advances in Cryptology – EUROCRYPT 2011*. Springer.

Ranjith, G., Prathusha, B. and Sagarika, P. (2015). ARBITRATED DIGITAL SIGNATURE FOR E- AUTHENTICATION TECHNIQUE OF A DIGITAL MESSAGE. *International Journal of Advances in Engineering & Technology*, [online] 8(5), pp.753–761. Available at: https://www.ijaet.org/media/8I29-IJAET0829527-v8-iss5-753-761.pdf.

Rubinstein-Salzedo, S. (2018). *Cryptography*. Cham, Switzerland: Springer.

Sahai, A. and Waters, B. (2005). Fuzzy Identity-Based Encryption. *Lecture Notes in Computer Science*, pp.457–473. doi:https://doi.org/10.1007/11426639_27.

Search Encrypt (2017). *What is Encryption & How Does It Work?* [online] Medium. Available at: https://medium.com/searchencrypt/what-is-encryption-how-does-it-work-e8f20e340537.

Sectigo (2021). *What Is an X.509 Certificate & How Does It Work?* [online] sectigo.com. Available at: https://sectigo.com/resource-library/what-is-x509-certificate.

Soule, M. (2019). *Your Guide to X509 Certificates (For Mortals)*. [online] adamtheautomator.com. Available at: https://adamtheautomator.com/x509-certificates/.

SSL.com Support Team (2019). *What Is an X.509 Certificate?* [online] SSL.com. Available at: https://www.ssl.com/faqs/what-is-an-x-509-certificate/.

Stallings, W. (2006). *Cryptography and network security : principles and practice : William Stallings*. Upper Saddle River, N.J.: Pearson/Prentice Hall.

Stallings, W. and Brown, L. (2015). *Computer security : principles and practice*. 3rd ed. Boston: Pearson.

Tutorialspoint (n.d.). *Java Cryptography - Introduction - Tutorialspoint*. [online] www.tutorialspoint.com. Available at: https://www.tutorialspoint.com/java_cryptography/java_cryptography_introduction.htm.

Venema, M., Alpár, G. and Hoepman, J.-H. (2022). Systematizing core properties of pairing-based attribute-based encryption to uncover remaining challenges in enforcing access control in practice. *Designs, Codes and Cryptography*. doi:https://doi.org/10.1007/s10623-022-01093-5.

Veskoukis, V. (2015). *Στοιχεία Τεχνολογίας Λογισμικού*. *Kallipos.gr*. doi:https://doi.org/978-960-603-060-4.

Yin, H., Xiong, Y., Zhang, J., Ou, L., Liao, S. and Qin, Z. (2019). A Key-Policy Searchable Attribute-Based Encryption Scheme for Efficient Keyword Search and Fine-Grained Access Control over Encrypted Data. *Electronics*, 8(3), p.265. doi:https://doi.org/10.3390/electronics8030265.

Zickau, S., Thatmann, D., Butyrtschik, A., Denisow, I. and Kupper, A. (2016). Applied Attribute-based Encryption Schemes. In: *Innovations in Clouds, Internet and Networks*. 19th International ICIN Conference.