ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΛΕΤΗ ΠΡΩΤΟΚΟΛΛΩΝ ΣΥΜΦΩΝΙΑΣ ΚΛΕΙΔΙΟΥ ΒΑΣΙΣΜΕΝΑ ΣΕ ΖΕΥΓΙΣΜΟΥΣ

Διπλωματική Εργασία

της

Τσιμούρα Παυλίνας

Θεσσαλονίκη, Οκτώβριος 2022

ΜΕΛΕΤΗ ΠΡΩΤΟΚΟΛΛΩΝ ΣΥΜΦΩΝΙΑΣ ΚΛΕΙΔΙΟΥ ΒΑΣΙΣΜΕΝΑ ΣΕ ΖΕΥΓΙΣΜΟΥΣ

Τσιμούρα Παυλίνα

Πτυχίο Μαθηματικών, ΑΠΘ, 2020

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

Επιβλέπουσα Καθηγήτρια

Πετρίδου Σοφία

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την

Πετρίδου Σοφία	Μαμάτας Ελευθέριος	Ψάννης Κωνσταντίνος
……	……	……

Τσιμούρα Παυλίνα

……

Περίληψη

Η διασφάλιση του απορρήτου των επικοινωνιών καθορίζεται από τα πρωτόκολλα κλειδιών ασφαλείας, τα οποία συντάσσονται, επιλέγονται και εφαρμόζονται για αυτό το σκοπό. Ως εκ τούτου η ασφάλεια των πρωτοκόλλων σημειώνεται ως εξαιρετικά σημαντική για την ακεραιότητα και το απόρρητο όλων των επικοινωνιών, καθ' όλη τη διάρκεια της χρήσης τους. Συγκεκριμένα, στην περίπτωση που τα πρωτόκολλα ανταλλαγής κλειδιών περιέχουν αδυναμίες ως προς την ασφάλειά τους, δίνεται η δυνατότητα σε κακόβουλους επιτιθέμενους να υποκλέπτουν το κλειδί και να αποκρυπτογραφούν και κρυπτογραφούν μηνύματα που ανταλλάσσουν οι χρήστες του πρωτοκόλλου. Με αυτόν τον τρόπο, ο επιτιθέμενος έχει την δυνατότητα να μαθαίνει όλες τις πληροφορίες που θέλουν να ανταλλάξουν οι χρήστες μεταξύ τους, χωρίς να γίνεται αντιληπτός. Αυτή ακριβώς η αδυναμία της ασφάλειας των επικοινωνιών αποτελεί την προβληματική της παρούσας διπλωματικής. Μέσω της βιβλιογραφικής ανασκόπησης μελετάται η εξέλιξη των πρωτοκόλλων συμφωνίας κλειδιού βασισμένα σε ζευγισμούς. Σε πρώτο επίπεδο περιγράφεται και εξετάζεται η εξέλιξή τους, ιστορικά, με σκοπό τη λεπτομερή μελέτη τους. Σε δεύτερο επίπεδο, γίνεται σύγκριση μεταξύ πρωτοκόλλων ανταλλαγής κλειδιών σε ελλειπτικές καμπύλες με μερικά από τα πρωτόκολλα ανταλλαγής κλειδιών που βασίζονται σε ζευγισμούς. Στόχος της εργασίας είναι ο εντοπισμός των αδυναμιών των επιλεγμένων πρωτοκόλλων έναντι των ενδεχομένων επιθέσεων.

Λέξεις κλειδιά: Ελλειπτικές καμπύλες, Ζευγισμοί, Πρωτόκολλα ανταλλαγής κλειδιών, Εσωτερική επίθεση, Παραβίαση κλειδιού, Joux, Shim, ABTKA, Man in the middle

Abstract

Key agreement protocols are essential to ensuring that confidentiality and data integrity are achieved during communications. They are designed, chosen and implemented to fulfill the purpose of insuring communications security. Therefore, key agreement protocols security is considered as vital for the privacy and integrity of all communications throughout their use. For instance, if key agreement protocols have security weaknesses, they can be vulnerable to certain attacks and malicious participants, which can intercept, encrypt and decrypt messages exchanged between users of the protocol. As a result, malicious participants are able to acquire confidential information from the users, without being noticed. According to the aforementioned information, security weaknesses of key agreement protocols is the problematic of this thesis. Through an extensive literature review, pairing based key agreement protocols are presented and examined. On a first level, this Master's thesis examines and analyses the evolution of key agreement protocols over the years. On a second level, a comparative analysis is implemented between pairing-based key agreement protocols with key agreement protocols based on elliptic curves. The aim of this thesis is to identify and exhibit security weaknesses of specific protocols against possible attacks.

Keywords: Elliptic curves, Pairings, Key agreement protocols, Inside attack, Key compromise impersonation, Joux, Shim, ABTKA, Man in the middle.

Ευχαριστίες

Για την εκπόνηση αυτής της διπλωματικής εργασίας θα ήθελα να ευχαριστήσω την καθηγήτρια μου για την πολύτιμη καθοδήγηση της, αλλά και την οικογένεια μου και ιδιαίτερα τις αδερφές μου Μαρία και Αλεξία για την υποστήριξή τους.

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Εικόνων

Κεφάλαιο 1

Εισαγωγή

1.1 Ιστορικά Στοιχεία

Η ανάπτυξη του ανθρωπίνου πολιτισμού για την επίτευξη της συνοχής των ανθρώπων σε κοινωνίες δημιούργησε την ανάγκη της επικοινωνίας, η οποία αποτελεί ακρογωνιαίο λίθο στην ομαλή συμβίωση των λαών, κοινωνιών, εθνών, κρατών. Η ανάγκη και η ζήτηση όμως της ασφαλούς επικοινωνίας, που κατέστη απαραίτητη σε εμπόλεμες συνθήκες ώστε να δομήσουν οι λαοί την πολιτική και στρατηγική τους ενάντια στον αντίπαλο, οδήγησε τους ανθρώπους να εφεύρουν κώδικες επικοινωνίας. Το γεγονός αυτό θεωρείται η απαρχή της κρυπτογραφίας. Η ιστορία της κρυπτογραφίας χρονολογείται πολλούς αιώνες πριν, υπογραμμίζοντας την ανάγκη των ανθρώπων να κρυπτογραφούν κώδικες. Η κρυπτογραφία προέρχεται ετυμολογικά από τις αρχαίες ελληνικές λέξεις «κρυπτός και γραφείν» και θεωρείται πως δημιουργήθηκε ταυτόχρονα με τη γραφή, καταδεικνύοντας τη σημασία της για την κοινωνία του τότε. Η ανακάλυψη αρχαιολογικών ευρημάτων αποδεικνύει ότι η κρυπτογραφία είναι μέρος πολλών αρχαίων πολιτισμών, όπως του αιγυπτιακού και του ελληνικού. Συγκεκριμένα, έχει βρεθεί στην Περσία ένα βιβλίο που περιγράφει κρυπτοκωδικούς, που αντιστοιχίζουν αριθμούς με σφηνοειδή σύμβολα (Deavours et al., 1990). Ευρήματα λοιπόν και ιστορικές πηγές αναφέρονται στη σημασία της κρυπτογραφίας, η οποία συμβάλει στην ομαλή και ασφαλή επικοινωνία μεταξύ των ανθρώπων. Η εξέλιξή της ανά τους αιώνες σημειώνει παράλληλα και την ανάπτυξη των κρυπτοσυστημάτων.

Μια από τις σημαντικότερες εποχές στην εξέλιξη της κρυπτογραφίας αποτελεί ο 20ος αιώνας, λόγω της ταραχώδους παγκόσμιας πολιτικής σκηνής με την ύπαρξη δύο παγκόσμιων πόλεμων, οι οποίοι συνέβαλαν στην ανάπτυξη κρυπτοσυστημάτων. Σημειώνεται πως η κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων ανάμεσα στους συμμάχους (στον Α' Παγκόσμιο) ήταν το πιο σύνηθες και το πιο ασφαλές μέσο επικοινωνίας έως τότε. Στην περίπτωση όμως που κάποιος από τους αντιπάλους έβρισκε τρόπο να αποκρυπτογραφήσει ένα μήνυμα είχε αυτόματα πρόσβαση σε κάθε πληροφορία που είχε ανταλλάξει η άλλη πλευρά. Την αδυναμία αυτή της κρυπτογράφησης επιλύσανε οι Γερμανοί κατά τη διάρκεια του Β΄ παγκοσμίου πολέμου. Η Enigma, μηχανή κρυπτογράφησης χρησιμοποιήθηκε από τους Γερμανούς στο Β' παγκόσμιο πόλεμο, με την οποία διασφάλισαν την επικοινωνία και τους κώδικες που χρησιμοποιούσαν (Trappe and Washington, 2006). Η επιτυχία της μηχανής έγκειται στο

γεγονός ότι η αποκρυπτογράφηση των μηνυμάτων της Enigma απαιτούσε πάρα πολύ χρόνο διότι το κλειδί της κρυπτογράφησης άλλαζε κάθε μέρα και έκανε την Enigma πολύ ισχυρή (Trappe and Washington, 2006). Η Enigma έχασε την παντοδυναμία της όμως από μια ανακάλυψη του Alan Turin, ενός έγκριτου μαθηματικού. Ο Turin εφηύρε μια μηχανή που μπορούσε να αποκρυπτογραφεί τα κρυπτοκείμενα της Enigma σε αρκετά μικρό χρονικό διάστημα, γεγονός που συνέβαλλε στη λήξη του πολέμου (Trappe and Washington, 2006). Το παράδειγμα αυτό, το οποίο καταδεικνύει τη σημασία των δύο μηχανών στην έκβαση ενός παγκοσμίου πολέμου, αποδεικνύει περίτρανα την ανάγκη ασφάλειας των επικοινωνιών, της ενίσχυσης των πρωτοκόλλων και τη δύναμη των κλειδιών στη διασφάλιση του απορρήτου και το ρόλο που μπορούν να διαδραματίσουν σε παγκόσμια κλίμακα.

Κατά τις επόμενες δεκαετίες παράλληλα με την ανάπτυξη της τεχνολογίας, ο κλάδος της κρυπτογραφίας επεκτείνεται και ολοένα και περισσότεροι επιστήμονες μελετούν με ποιο τρόπο θα επιτύχουν το ζητούμενο της ασφαλούς επικοινωνίας. Σημαντικό ρόλο στην ασφάλεια καταλαμβάνουν στοιχεία της μαθηματικής επιστήμης, όπως ο κλάδος της Άλγεβρας και πιο συγκεκριμένα της Θεωρίας Αριθμών. Στοιχεία όπως οι ομάδες, οι ελλειπτικές καμπύλες και οι ζευγισμοί χρησιμοποιήθηκαν για να δημιουργηθούν κρυπτοσυστήματα που θα πετύχουν ασφαλέστερη επικοινωνία. Τα παραπάνω στοιχεία και η ανάλυση της αξίας και συμβολής τους παρατίθενται εκτενέστερα στο Κεφάλαιο 2.

Τα πρώτα κρυπτογραφικά μοντέλα λοιπόν χρησιμοποιούσαν τη μέθοδο της κρυπτογράφησης συμμετρικού κλειδιού. Η μέθοδος κρυπτογράφησης συμμετρικού κλειδιού έχει μόνο ένα μυστικό κλειδί, το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση των πληροφοριών. Το γεγονός της μοναδικότητας του κλειδιού επίφερε αδυναμία στη χρήση του. Συγκεκριμένα κατά την πορεία της εφαρμογής και χρήσης της μεθόδου, εντοπίστηκαν αρκετές αδυναμίες οπότε και δημιουργήθηκε η ανάγκη εύρεσης μιας νέας μεθόδου, της ασύμμετρης κρυπτογράφησης. Σ' αυτή τη μέθοδο χρησιμοποιείται ένας ζεύγος κλειδιών από κάθε οντότητα, ένα δημόσιο κι ένα ιδιωτικό, όπου χρησιμοποιούνται στις διαδικασίες της κρυπτογράφησης και της αποκρυπτογράφησης. Με βάση τη μέθοδο της ασύμμετρης κρυπτογράφησης αναπτύχθηκε η χρήση των ελλειπτικών καμπυλών στα κρυπτοσυστήματα, η οποία αποτέλεσε τεράστια καινοτομία. Οι ελλειπτικές καμπύλες αποτέλεσαν καινοτομία στην κρυπτογραφία, καθώς για συγκεκριμένο μήκους κλειδιού προσδίδεται μεγαλύτερη ασφάλεια στο κρυπτοσύστημα. Μετά την διάδοση των ελλειπτικών καμπυλών στην κρυπτογράφηση άρχισαν να χρησιμοποιούνται και οι ζευγισμοί ελλειπτικών καμπυλών στα κρυπτοσυστήματα, με αποτέλεσμα να δημιουργηθούν νέα καινοτόμα

πρωτόκολλα ανταλλαγής κλειδιών όπως είναι το Joux, το Shim και αρκετά χρόνια μετά το ΑΒΤΚΑ, τρία τριμερή πρωτόκολλα ανταλλαγής κλειδιών στα οποία θα αναφερθούμε πιο αναλυτικά στα κεφάλαια 3 και 5.

1.2 Σημασία έρευνας-Προβληματική Εργασίας

Μέσω της μελέτης των προαναφερθέντων πρωτοκόλλων επιδιώκεται αφενός να διερευνηθούν οι αδυναμίες των πρωτοκόλλων σχετικά με την ασφάλεια και αφετέρου να εξεταστεί κατά πόσο τα πρωτόκολλα ανταλλαγής κλειδιών, τα οποία βασίζονται σε ζευγισμούς προσφέρουν μεγαλύτερη ασφάλεια από τα ελλειπτικά πρωτόκολλα χωρίς ζευγισμούς. Μέσω της απάντησης των παραπάνω ερευνητικών ερωτημάτων επιδιώκεται να προκύψουν συμπεράσματα για τα σημεία που χρήζουν βελτίωση και πιθανόν νέα προσαρμογή στα διαρκώς εξελισσόμενα δεδομένα της πληροφορικής και της τεχνολογίας. Επιδιώκεται να κατανοηθούν οι μέθοδοι επίθεσης των πρωτοκόλλων ανταλλαγής κλειδιών, οι πληροφορίες για το σχεδιασμό τους και το κατά πόσο είναι ασφαλή η χρήση τους.

Η σημασία της έρευνας εκτιμάται να είναι προσθετική στην ήδη υπάρχουσα έρευνα του πεδίου των πρωτοκόλλων ασφαλείας. Ο τομέας της Πληροφορικής άλλωστε είναι ένας τομέας που αλλάζει ραγδαία. Λαμβάνοντας υπόψη το γεγονός ότι η Πληροφορική αποκτά συνεχώς μεγαλύτερο μέρος της ζωής μας, η ασφάλεια αποτελεί όλο και πιο σημαντικό παράγοντα στη χρήση της. Για την επίτευξη της ασφάλειας πολλά πρωτόκολλα ανταλλαγής κλειδιών έχουν προταθεί, χωρίς παρόλα αυτά να διαθέτουν όλα κάποια απόδειξη ασφαλείας. Σημειώνεται εδώ και η περίπτωση κατά την οποία το πρωτόκολλο που χρησιμοποιείται να παρέχει απόδειξη ασφαλείας αλλά να έχει αδυναμίες, τις οποίες εκμεταλλεύεται ο εξωγενής παράγοντας μιας νέας επίθεσης. Στο σημείο αυτό αντιλαμβάνεται κανείς την αναγκαιότητα της συνεχούς ανάλυσης των πρωτοκόλλων για την επιβεβαίωση της ασφάλειας την οποία προσφέρουν στην επικοινωνία. Άλλωστε τα πρωτόκολλα ανταλλαγής κλειδιών θεωρούνται από τα πιο δύσκολα πρωτόκολλα στο σχεδιασμό και αποτελούν μέρος από τα πιο σημαντικά στοιχεία ενός συστήματος όσον αφορά την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Για τους παραπάνω λόγους σημειώνονται συνεχώς νέες προτάσεις για πρωτόκολλα συμφωνίας κλειδιού. Το πρόβλημα σχετικά με την ασφάλεια αυτών των πρωτοκόλλων είναι ότι δεν έχουν απόδειξη ασφαλείας και δεν έχει γίνει διεξοδική μελέτη ώστε να αποκτηθεί επαρκής γνώση σχετικά με τις μεθόδους επίθεσης στα πρωτόκολλα ανταλλαγής κλειδιών. Πάνω σε αυτά τα στοιχεία βασίστηκε η μελέτη και έρευνα αυτής της εργασίας.

Η εργασία αυτής της διπλωματικής εργασίας μπορεί να χωριστεί σε δύο μέρη:

- Μελέτη και περιγραφή διαφόρων πρωτοκόλλων ανταλλαγής κλειδιών
- Μια περίληψη των διαφορετικών τρόπων επίθεσης στα πρωτόκολλα ανταλλαγής κλειδιών

1.3 Μεθοδολογία

Η μέθοδος που θα χρησιμοποιηθεί για την εύρεση απαντήσεων στα παραπάνω ερευνητικά ερωτήματα είναι η βιβλιογραφική ανασκόπηση. Αρχικά θα παρουσιαστεί το μαθηματικό υπόβαθρο της Θεωρίας Αριθμών και θα ερμηνευτούν οι έννοιες οι οποίες είναι άμεσα συνυφασμένες με τα πρωτόκολλα ανταλλαγής κλειδιών. Οι έννοιες αυτές είναι η θεωρία και η λειτουργία των ελλειπτικών καμπυλών και η θεωρία των ζευγισμών ελλειπτικών καμπυλών, που κάνουν χρήση τα τριμερή πρωτόκολλα ανταλλαγής κλειδιών. Στη συνέχεια, θα περιγραφούν πρωτόκολλα ανταλλαγής κλειδιών βασισμένα στις ελλειπτικές καμπύλες καθώς και τριμερή πρωτόκολλα συμφωνία κλειδιών βασισμένα σε ζευγισμούς ελλειπτικών καμπυλών. Η παραπάνω περιγραφή των πρωτοκόλλων αυτών θα διευκολύνει την μελέτη των επιθέσεων τους.

Η μελέτη επικεντρώθηκε στις επιθέσεις όπου τα πρωτόκολλα παρουσιάζουν αδυναμία ως προς την αντιμετώπιση των επιθέσεων αυτών. Η παραπάνω ανάλυση αποσκοπεί στην εισαγωγή συγκεκριμένων συμπερασμάτων συσχετιζόμενων με την φύση των ερευνητικών ερωτημάτων της εν λόγω εργασίας. Συγκεκριμένα, όσο αναφορά τις αδυναμίες των πρωτοκόλλων απέναντι σε κάποιες επιθέσεις και στην απάντηση του εάν οι ζευγισμοί ενισχύουν την ασφάλεια στα πρωτόκολλα ανταλλαγής κλειδιών.

Κεφάλαιο 2

Θεωρητικό Υπόβαθρο

Στο κεφάλαιο αυτό θα αναφερθούν κάποιες βασικές έννοιες των Μαθηματικών και της Κρυπτογραφίας, οι οποίες κρίνονται απαραίτητες για την κατανόηση των πρωτοκόλλων που θα μελετηθούν στο πλαίσιο της παρούσας διπλωματικής .

2.1 Θεωρία Αριθμών

Στον τομέα της Θεωρίας Αριθμών υπάρχουν αρκετές αλγεβρικές δομές που εφαρμόζονται στην Κρυπτογραφία, όμως η έννοια του αλγεβρικού σώματος είναι αυτή που εφαρμόζεται στα πρωτόκολλα που βασίζονται στους ζευγισμούς ελλειπτικών καμπυλών.

Ορισμός 2.1.1

Έστω G ένας δακτύλιος με μοναδιαίο στοιχείο. Ένα στοιχείο u του G λέγεται μονάδα του G αν έχει πολλαπλασιαστικό αντίστροφο στο G. Αν κάθε μη μηδενικό στοιχείο του δακτυλίου G είναι μονάδα, τότε ο G λέγεται δακτύλιος διαίρεσης (Fraleigh, 1967).

Ορισμός 2.1.2

Ένας αντιμεταθετικός δακτύλιος διαίρεσης $G \neq \{0\}$ καλείται σώμα (Πουλάκης, 1997).

Για παράδειγμα, ο δακτύλιος $\mathbb{Q}$ είναι σώμα ενώ οι δακτύλιοι $\mathbb{Z}$ και $\mathbb{Q}x\mathbb{Q}$ δεν είναι σώματα.

Θεωρείται γνωστό ότι η χαρακτηριστική ενός σώματος G (char (G)) είναι πάντοτε ή μηδέν ή ένας πρώτος αριθμός. Αν η χαρακτηριστική του G είναι ίση με μηδέν, τότε το σώμα G περιέχει ισόμορφα το άπειρο σώμα $\mathbb{Q}$ (Πουλάκης, 2015). Επομένως, αναγκαστικά είμαστε στην δεύτερη περίπτωση όπου η χαρακτηριστική είναι ένας πρώτος αριθμός p, διότι όπως θα περιγραφεί παρακάτω ενδιαφερόμαστε κυρίως για ελλειπτικές καμπύλες σε πεπερασμένα σώματα. Το ελάχιστο σώμα με χαρακτηριστική p είναι το $\mathbb{Z}_p$ και εμφυτεύεται σε κάθε σώμα με χαρακτηριστική p.

Πρόταση 2.1.1

Αν $\text{char}(G)=p$ τότε $|G|= p^n$, , όπου p πρώτος και n θετικός ακέραιος (Πουλάκης, 2015).

Πρόταση 2.1.2

Έστω ένα πολυώνυμο $q(x)$ με βαθμό $d-1$ πάνω από το $\mathbb{Z}_p$ και ένα σύνολο $S \subset Z_p$ με $|S| = d$. Έστω ότι η τιμή του πολυωνύμου $q(i)$ είναι δεδομένη για κάθε $i \epsilon S$. Σύμφωνα με την παρεμβολή του Lagrange το πολυώνυμο υπολογίζεται ως εξής:

$$q(x) = \sum_{i \epsilon S} q(i) \Delta_{i,S}(x)$$

Όπου το $\Delta_{i,S}(x)$ είναι ο συντελεστής Lagrange και υπολογίζεται ως εξής:

$$\Delta_{i,S}(x) = \prod_{j \epsilon S, j \neq i} \frac{x-j}{i-j}$$

για όλα τα $i \epsilon S$.

2.2 Ελλειπτικές Καμπύλες

Οι ελλειπτικές καμπύλες αποτελούν ένα αναπόσπαστο κομμάτι της κρυπτογραφίας από τη δεκαετία του ΄90 έως και σήμερα, διότι χρησιμοποιούνται από αρκετά πρωτόκολλα ανταλλαγής κλειδιών (π.χ. Diffie-Hellman). Απαραίτητη προϋπόθεση αποτελεί οι ελλειπτικές καμπύλες να βρίσκονται πάνω από πεπερασμένα σώματα. Δηλαδή οι μεταβλητές και οι συντελεστές των ελλειπτικών καμπυλών είναι στοιχεία ενός πεπερασμένου σώματος (Κάτος and Στεφανίδης, 2003). Πρέπει να σημειωθεί ότι το εύρος της ανάλυσης των ελλειπτικών καμπυλών σε αλγεβρικό και γεωμετρικό επίπεδο είναι μεγάλο και σ' αυτή την ενότητα θα γίνει μόνο μια μικρή περιγραφή.

Στις περισσότερες περιπτώσεις κρυπτογραφικών εφαρμογών χρησιμοποιούνται ελλειπτικές καμπύλες ορισμένες σε πεπερασμένο σώμα G, με char(G)=p όπου p>3 (Smart, 2016). Όταν η χαρακτηριστική του σώματος είναι ίση με 2 ή 3 τότε οι ελλειπτικές καμπύλες απαιτούν ξεχωριστή αντιμετώπιση (για περισσότερες πληροφορίες σχετικά με τις ελλειπτικές καμπύλες με χαρακτηριστική 2 ή 3 προτείνεται η ανάγνωση του) (Fotiadis, 2017). Ο περιορισμός στην χαρακτηριστική του πεπερασμένου σώματος είναι μόνο για τις καμπύλες στην κανονική μορφή Weierstrass, διότι οι αριθμοί 2 και 3 χρησιμοποιούνται στην προσθήκη σημείων της καμπύλης.

Ορισμός 2.2.1

Μια ελλειπτική καμπύλη είναι το σύνολο των σημείων που ικανοποιούν μια εξίσωση της μορφής

$E : y^2 = x^3 + \alpha x + \beta$ (2.1)

όπου τα α,β ϵ G και char (G) = p > 3. Έχει διακρίνουσα $\Delta = -16(4\alpha^3 + 27\beta^2)$ και αναλλοίωτο $j = 1728\frac{4a\hat{}3}{4a^3+27\beta^2}$.

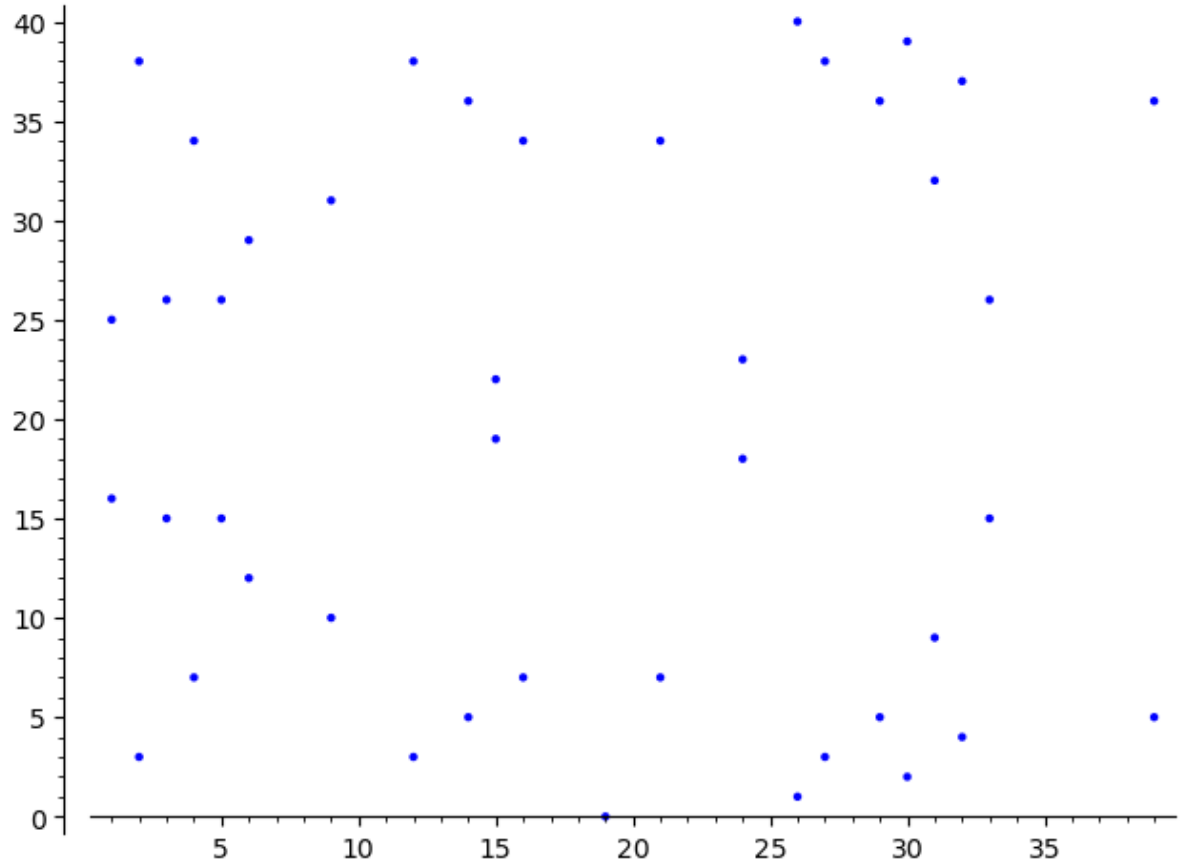
Αυτή η ελλειπτική καμπύλη ονομάζεται κανονική μορφή Weierstrass.

Έστω $P = (x_1, y_1)$ ένα σημείο της Ε τότε ισχύουν τα εξής:

- Αν $P = (x_1, y_1)$ τότε $-P = (x_1, -y_1)$
- Έστω $R = (x_3, y_3) = P + Q$ με $P = (x_1, y_1), Q = (x_2, y_2)\ \epsilon E$ τότε
  $x_3 = \lambda^2 - x_1 - x_2$ και $y_3 = (x_1 - x_3)\lambda - y_1$ όπου:
  1. Αν $x_1 \neq x_2$ έχουμε $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$
  2. Αν $x_1 = x_2, y_1 \neq 0$ τότε $\lambda = \frac{3x_1 + a}{2y_1}$

Παράδειγμα 2.2.1

Έστω μια ελλειπτική καμπύλη στο σώμα G ,με char(G)=41, και η εξίσωση που ικανοποιεί είναι η $E: y^2 = (x^3 - 8x + 17) mod 41$.



Εικόνα 1: Η γραφική αναπαράσταση της $E: y^2 = (x^3 - 8x + 17) mod 41$.

Θεώρημα 3.2.2 (Menezes, 2008)

Έστω μια ελλειπτική καμπύλη Ε πάνω στο G_p με τάξη $ord(G_p) = p$ και χαρακτηριστική $char(G_P) = q$. Τότε ο πληθικός αριθμός του συνόλου σημείων της καμπύλης

$$\#E(F_p) = p + 1 - t$$

το t καλείται ίχνος του Frobenius ή απλά ίχνος και ικανοποιεί την σχέση

$$|t| \leq 2\sqrt{p}$$

Μια ελλειπτική καμπύλη Ε πάνω στο G_p, με p πρώτο αριθμό, καλείται:

- Υπεριδιάζουσα (supersingular), αν $p|t$, όπου $t = p + 1 - \#E(Fp)$ το ίχνος.
- Μη υπεριδιάζουσα (non supersingular), αν $p \nmid t$.

2.3 Ζευγισμοί

Οι ζευγισμοί έκαναν την εμφάνιση τους στο τομέα της κρυπτογραφίας όταν εφαρμόστηκαν ως επίθεση στο πρόβλημα διακριτού λογαρίθμου με ελλειπτικές καμπύλες (Meffert, 2009). Έκτοτε, οι ζευγισμοί αποτελούν ένα από τα πιο χρήσιμα και ευέλικτα εργαλεία για την δημιουργία νέων κρυπτογραφικών πρωτοκόλλων. Οι πιο συνηθισμένοι ζευγισμοί στα πρωτόκολλα είναι οι Weil και οι Tate. Στο υπό κεφάλαιο αυτό θα γίνει η παρουσίαση μόνο τον Weil ζευγισμών.

Ορισμός 2.3.1

Έστω δύο κυκλικές ομάδες $G_1 = < p >$ και $G_2 = < q >$ με τάξη p, όπου p πρώτος. Θεωρούμε ότι η G_1 είναι η προσθετική υποομάδα της ομάδας των σημείων της ελλειπτικής καμπύλης πάνω σε ένα πεπερασμένο σώμα και η G_2 είναι υποομάδα την πολλαπλασιαστικής ομάδας του πεπερασμένου σώματος (Schmidt, 2012). Επομένως, ένα ζεύγος στο (G_1, G_2) ορίζεται με την εξής απεικόνιση

$$\hat{e}: G_1 \times G_1 \to G_2$$

η οποία ικανοποιεί κάποιες συνθήκες και ιδιότητες:

- $\forall\, R, S, T \in G_1$ ισχύει $\hat{e}(R + S, T) = \hat{e}(R, T)\hat{e}(S, T)$ και

$\hat{e}(R, S+T) = \hat{e}(R,S)\hat{e}(R,T)$, δηλαδή η απεικόνιση είναι διγραμμική.

- Το $\hat{e}(P,P)$ είναι γεννήτορας της G_2 δηλαδή $\hat{e}(P,P) \neq 1$, μη εκφυλισιμότητα.
- $\hat{e}(S,\infty) = 1 \; και \; \hat{e}(\infty, S) = 1.$
- $\hat{e}(S,-\mathrm{T}) = \hat{e}(-S,\mathrm{T}) = \hat{e}(S,T)^{-1}.$
- $\hat{e}(aS, bT) = \hat{e}(S,T)^{ab}, \forall a, b \in \mathbb{Z}.$
- $\hat{e}(S,T) = \hat{e}(T,S)$, συμμετρικότητα.
- Αν $\forall \; S \in \; G_1$ ισχύει $\hat{e}(S,R) = 1$ τότε το $R = \infty$ λόγω της δεύτερης συνθήκης

Για να μπορέσουμε να περιγράψουμε τους Weil ζευγισμούς πρέπει να αναφερθούμε στην έννοια του διαιρέτη στις ελλειπτικές καμπύλες.

Ορισμός 2.3.2

Η ομάδα των διαιρετών μια ελλειπτικής καμπύλης E είναι αβελιανή και παράγεται από τα σημεία που ανήκουν στην καμπύλη. Κάθε διαιρέτης D εκφράζεται από ένα άθροισμα σημείων με έναν ακέραιο συντελεστή $\mathrm{n_i}$ (Lauter and Naehrig, 2017).

$$D = \sum_i n_i(P_i)$$

όπου P_i είναι σημεία της καμπύλης E.

Ένας διαιρέτης έχει βαθμό μηδέν όταν συμβαίνει $\sum_i n_i = 0$.

Ορισμός 2.3.3

Ένας διαιρέτης λέγεται κύριος όταν είναι διαιρέτης μια συνάρτησης f της ελλειπτικής καμπύλης E (Koblitz and Menezes, 2005). Συγκεκριμένα μια τέτοια συνάρτηση f ορίζεται ως

$$D = div(f) = \sum_{P \in E} ord_P(f)(P)$$

Για να είναι ένας διαιρέτης με βαθμό μηδέν κύριος $D = \sum_i n_i(P_i)$ θα πρέπει να εκτιμήσουμε την τιμή του $\sum_i n_i(P_i)$. Αν το αποτέλεσμα είναι το σημείο στο άπειρο τότε ο D είναι κύριος διαιρέτης (Lauter and Naehrig, 2017).

Πρόταση 2.3.1

Έστω μια διγραμμική συνάρτηση $e_l: E[l] \times E[l] \rightarrow \; \mu_l$ όπου $E[l]$ ομάδα με πεπερασμένη τάξη ίση με l και μ_l πολλαπλασιαστική ομάδα επέκταση της G_p. Παίρνουμε δύο σημεία με

πεπερασμένη τάξη τα P και Q και υπολογίζουμε με την βοήθεια των συναρτήσεων f_P και f_Q τέτοιες ώστε $div(f_P) = l(P) - l(O), div(f_Q) = l(Q) - l(O)$.

$$e_l(P, Q) = {f_P(Q)}/{f_Q(P)}$$

Πρόταση 2.3.2

Έστω Ε ελλειπτική καμπύλη και $E[n] = \mathbb{Z}_n \times \mathbb{Z}_n$. Για $P, Q \in E[m], f_P, f_Q$ ρητές συναρτήσεις στην Ε τέτοιες ώστε $div(f_P) = m(P) - m(O), div(f_Q) = m(Q) - m(O)$ (Koblitz and Menezes, 2005). Τότε ο ζευγισμός Weil των σημείων αυτών ορίζεται ως

$$e_m(P, Q) = \frac{f_P(Q+S)}{f_p(S)} \Big/ \frac{f_Q(P-S)}{f_Q(-S)}$$

όπου $S \notin \{O, P, -Q, P-Q\}$.

Κεφάλαιο 3

Πρωτόκολλα Ανταλλαγής Κλειδιών

3.1 Η έννοια του Πρωτοκόλλου

Η εφαρμογή των κρυπτογραφικών πρωτοκόλλων στη σύγχρονη εποχή ξεκίνησε περίπου 40 χρόνια πριν και έκτοτε υπάρχει συνεχής εξέλιξη και βελτίωση των πρωτοκόλλων για να διασφαλιστεί η ασφαλής ανταλλαγή και μεταφορά πληροφοριών μέσω του Διαδικτύου.

Τι ορίζεται όμως κρυπτογραφικό πρωτόκολλο;

Κρυπτογραφικό πρωτόκολλο ορίζεται μια σειρά από βήματα και μηνύματα πολλαπλών οντοτήτων προκειμένου να επιτευχθεί ένας συγκεκριμένος στόχος ασφαλείας (Wong, 2021). Ειδικότερα, ως πρωτόκολλο ασφαλείας αναφέρεται ένα κρυπτογραφικό πρωτόκολλο που εκτελεί διεργασίες που αφορούν στην ασφάλεια και χρησιμοποιεί κρυπτογραφικές μεθόδους (Meadows, 2003). Η απαρχή της εφαρμογής κρυπτογραφικών μεθόδων στα πρωτόκολλα γίνεται με την ανάλυση των πρωτοκόλλων διανομής κλειδιών με στόχο την επικοινωνία δύο οντοτήτων (Meadows, 2003). Δίνεται λοιπόν προς εξέταση ένα παράδειγμα. Έστω ότι οι οντότητες είναι η Αλίκη και Μπομπ και θέλουν να επικοινωνήσουν με ασφάλεια χρησιμοποιώντας ένα πρωτόκολλο. Χρειάζονται ένα κλειδί με το οποίο θα γίνεται η κρυπτογράφηση, επομένως θα πρέπει αυτό το κλειδί είτε να το δημιουργήσουν και να συμφωνήσουν οι ίδιοι, είτε να δημιουργηθεί από έναν διακομιστή κλειδιών. Αυτό το σημείο της επικοινωνίας τους είναι και το πιο δύσκολο διότι δεν είναι πάντα εφικτό να συμφωνήσουν σε ένα κλειδί χωρίς αυτό να υποκλαπεί από κάποιον εχθρικό εισβολέα (Meadows, 2003). Αυτό το σημείο, που ορίζεται ως το δυσκολότερο στην ασφάλεια της επικοινωνίας της Αλίκης και του Μπομπ, αποτελεί και το κυριότερο πρόβλημα του τομέα της κρυπτογραφίας. Συγκεκριμένα , το να συμφωνήσουν τα δύο μέρη της επικοινωνίας σε ένα κλειδί, για το οποίο πρέπει να διασφαλιστεί η ακεραιότητά του και η εμπιστευτικότητα των δεδομένων. Πρέπει λοιπόν το κλειδί να είναι τόσο δυνατό ώστε να μην μπορεί να υποκλαπεί ως στοιχείο από εξωγενή παράγοντα.

Όσον αφορά τα ονόματα των πρωτοκόλλων και τον τρόπο που αποδίδονται συνήθως προκύπτουν με βάση τις υπηρεσίες που παρέχουν. Συνεπώς υπάρχουν πρωτόκολλα ανταλλαγής κλειδιών, πρωτόκολλα αυθεντικοποίησης κ.τ.λ. Όλα όμως τα πρωτόκολλα έχουν κάποιες βασικές ιδιότητες που τα χαρακτηρίζουν (Pfleeger, 1989).

- **Είναι προκαθορισμένα τα βήματα από πριν.** Το πρωτόκολλο σχεδιάζεται εξ ολοκλήρου πριν χρησιμοποιηθεί.
- **Κοινή συμφωνία.** Όλες οι οντότητες συμφωνούν να εκτελέσουν τα βήματα του πρωτοκόλλου με τον τρόπο και την σειρά που υποδεικνύεται από το πρωτόκολλο.
- **Σαφήνεια.** Η διαδικασία της εκτέλεσης των βημάτων είναι απαραίτητο να διευκρινιστεί με τέτοιο τρόπο ώστε καμία οντότητα να μην κάνει κάποιο λάθος στην εκτέλεση των βημάτων του πρωτοκόλλου.
- **Ακεραιότητα.** Θα πρέπει να υπάρχουν προκαθορισμένες ενέργειες για κάθε πιθανή κατάσταση που επρόκειτο να αντιμετωπίσει κάποια από τις οντότητες.

Στην επόμενη ενότητα θα εξεταστούν τα πρωτόκολλα ανταλλαγής κλειδιών με ελλειπτικές καμπύλες.

3.2 Πρωτόκολλα ανταλλαγής κλειδιών με ελλειπτικές καμπύλες

Η πλειονότητα των πρωτοκόλλων που χρησιμοποιούν τις ελλειπτικές καμπύλες δημιουργούνται από παλαιότερα πρωτόκολλα τροποποιώντας τα βήματα τους κατάλληλα. Ένα από τα πρώτα πρωτόκολλα ανταλλαγής κλειδιών που τροποποιήθηκε σε πρωτόκολλο ανταλλαγής κλειδιών με ελλειπτικές καμπύλες ήταν το Diffie-Hellman το οποίο θα περιγραφεί παρακάτω.

3.2.1 Πρωτόκολλο ελλειπτικών καμπυλών Diffie - Hellman

Ένα από τα πιο γνωστά πρωτόκολλα ανταλλαγής κλειδιών είναι το πρωτόκολλο Diffie-Hellman που δημιουργήθηκε από τους Whitfield Diffie και Martin Hellman το 1976 και αποτελεί ένα σημαντικό κομμάτι της σύγχρονης κρυπτογραφίας (Diffie and Hellman, 1976). Το πρωτόκολλο ανταλλαγής κλειδιών Diffie - Hellman αποτέλεσε τη βάση για τη δημιουργία του πρωτοκόλλου ελλειπτικών καμπυλών Diffie - Hellman.

Το πρωτόκολλο Elliptic Curve Diffie - Hellman (ή ECDH) είναι ένα από τα πρωτόκολλα ανταλλαγής κλειδιών που χρησιμοποιούνται για την δημιουργία ενός κοινού κλειδιού μεταξύ δύο χρηστών (Kaabneh and Al-Bdour, 2005). Η αιτία δημιουργίας του πρωτοκόλλου ήταν η ασφαλής επικοινωνία δύο χρηστών σε έναν μη ασφαλή δίαυλο επικοινωνίας, έτσι ώστε τα μηνύματα που θέλουν να ανταλλάξουν οι δύο χρήστες να παραμένουν κρυφά από οποιονδήποτε κακόβουλο χρήστη θέλει να επιτεθεί. Το πρωτόκολλο ECDH χρησιμοποιεί και βασίζεται στην προσθετική ομάδα των ελλειπτικών καμπυλών.

Ας υποθέσουμε ότι οι δύο χρήστες, η Αλίκη και ο Μπομπ, χρειάζεται να συμφωνήσουν σε ένα κοινόχρηστο μυστικό κλειδί για να μπορέσουν να επικοινωνήσουν. Τα βήματα που ακολουθούν οι χρήστες είναι τα εξής (Kaabneh and Al-Bdour, 2005):

- Αρχικά μια αξιόπιστη πηγή διαλέγει έναν πολύ μεγάλο πρώτο αριθμό p, ένα πεπερασμένο σώμα G_p , μια ελλειπτική καμπύλη E πάνω στο πεπερασμένο σώμα και ένα σημείο $P \in E(G_p)$.
- Οι χρήστες επιλέγουν από έναν ακέραιο και υπολογίζουν αντίστοιχα το σημείο που θα στείλουν ο ένας στον άλλον. Η Αλίκη επιλέγει το ακέραιο αριθμό $k_A \in \{1,2, \dots, p-1\}$ ο οποίος θεωρείται το ιδιωτικό κλειδί και υπολογίζει $R_A = k_A * P$. Την ίδια διαδικασία θα ακολουθήσει και ο Μπομπ, επιλέγει έναν ακέραιο αριθμό $k_B \in \{1,2, \dots, p-1\}$ και εν συνεχεία υπολογίζει $R_B = k_B * P$.
- Η Αλίκη στέλνει στον Μπομπ το δημόσιο κλειδί R_A, αλλά κρατάει κρυφό το ιδιωτικό της κλειδί. Όμοια και ο Μπομπ στέλνει το δημόσιο κλειδί R_B στην Αλίκη και κρατάει κρυφό το μυστικό κλειδί του.
- Τέλος, η Αλίκη υπολογίζει το κοινόχρηστο κλειδί $k_A * R_B$, αντίστοιχα και ο Μπομπ υπολογίζει το κοινόχρηστο κλειδί $k_B * R_A$.

Πλέον και οι δύο χρήστες έχουν στη κατοχή τους ένα κοινό κλειδί το οποίο είναι ένα σημείο της ελλειπτικής καμπύλης E αφού ισχύει:

$$R_{AB} = k_B * R_A = k_B(k_A * P) = k_A(k_B * P) = k_A * R_B$$

Αλίκη	Κανάλι Επικοινωνίας	Μπομπ
Τυχαία επιλογή ακεραίου αριθμού $\mathrm{k}_A \in \{1,2,\dots,p-1\}$ ιδιωτικό κλειδί		Τυχαία επιλογή ακεραίου αριθμού $\mathrm{k}_B \in \{1,2,\dots,p-1\}$ ιδιωτικό κλειδί
Υπολογισμός $R_A = \mathrm{k}_A * P$		Υπολογισμός $R_B = \mathrm{k}_B * P$
Λαμβάνει το R_B	$R_B = \mathrm{k}_B * P$ ⟵ ⟶ $R_A = \mathrm{k}_A * P$	Λαμβάνει το R_A
Υπολογισμός $R_{AB} = \mathrm{k}_A * R_B$		Υπολογισμός $R_{AB} = \mathrm{k}_B * R_A$

Πίνακας 1. Πρωτόκολλο Diffie Hellman με ελλειπτικές καμπύλες (Kaabneh and Al-Bdour, 2005).

Παράδειγμα

Η Αλίκη και ο Μπομπ θέλουν να επικοινωνήσουν και αποφάσισαν να χρησιμοποιήσουν το πρωτόκολλο Diffie Hellman με ελλειπτικές καμπύλες. Επιλέγεται από μία έμπιστη γεννήτρια πρώτων αριθμών ο $p = 3533$ και έστω ότι επέλεξαν και την ελλειπτική καμπύλη $E: y^2 = x^3 + 426x + 1897$ και $P = (856, 942) \in E(G_{3533})$.

Η Αλίκη επιλέγει ως ιδιωτικό κλειδί τον ακέραιο $k_A = 864$ και Μπομπ επέλεξε $k_B = 1024$.

Υπολογίζουν και οι δύο το σημείο της καμπύλης που θα πρέπει να ανταλλάξουν:

Αλίκη: $R_A = \mathrm{k}_A * P = 864 * P = (1068, 1662) \in E(G_{3533})$

Μπομπ: $R_B = \mathrm{k}_B * P = 1024 * P = (2189, 1484) \in E(G_{3533})$

Ανταλλάσσουν τα σημεία της καμπύλης που υπολόγισαν και υπολογίζουν το κοινό μυστικό κλειδί:

Αλίκη: $\mathrm{k}_A * R_B = 864 * (2189, 1484) = (3122, 1237) \in E(G_{3533})$

Μπομπ: $\mathrm{k}_B * R_A = 1024 * (1068, 1662) = (3122, 1237) \in E(G_{3533})$

Παρατηρούμε ότι όντως κατέληξαν στο ίδιο κοινό μυστικό κλειδί (σημείο) το $(3122, 1237)$.

3.3 Τριμερή πρωτόκολλα ανταλλαγής κλειδιών

Στην ενότητα αυτή θα περιγράψουμε τρία τριμερή πρωτόκολλα ανταλλαγής κλειδιών το Joux, Shim και ABTKA. Το Joux αποτέλεσε το πρώτο τριμερές πρωτόκολλο (2000) και το Shim δημιουργήθηκε λίγα χρόνια αργότερα (2003) διότι το Joux δεν είναι ασφαλές απέναντι σε επιθέσεις Man in the Middle (βλ. Κεφάλαιο 4) (Sun and Hsieh, 2003). Το ABTKA είναι ένα πιο πρόσφατο πρωτόκολλο από τα προηγούμενα δύο το οποίο πρωτοεμφανίστηκε το 2013 και βάσει της βιβλιογραφίας που μελετήθηκε είναι ευάλωτο απέναντι σε θεωρητικές μαθηματικές επιθέσεις (Bayat and Reza Aref, 2015).

3.3.1 Πρωτόκολλο Joux

Τα τριμερή πρωτόκολλα ανταλλαγής κλειδιών έχουν ως στόχο τη δημιουργία ενός κλειδιού που θα μοιράζονται τρεις χρήστες μεταξύ τους (Schmidt, 2012). Το πρωτόκολλο του Joux βασίστηκε στο ελλειπτικό πρωτόκολλο Diffie Hellman όπως κι άλλα παρόμοια πρωτόκολλα, όμως χρειάζονταν περισσότερους από έναν γύρο για την δημιουργία των κλειδιών (Joux, 2004). Το Joux πρωτόκολλο ήταν το πρώτο ενός γύρου πρωτόκολλο εγκαθίδρυσης κλειδιού και χρησιμοποιεί ζευγισμούς ελλειπτικών καμπυλών (Schmidt, 2012). Για να καταστεί κατανοητό παρατίθεται το παρακάτω παράδειγμα.

Έστω λοιπόν οι τρεις χρήστες, η Αλίκη, ο Μπομπ και ο Κώστας κι ένα κανάλι επικοινωνίας με ένα πέρασμα. Με τον όρο ένα πέρασμα επικοινωνίας εννοείται ότι οι χρήστες μπορούν μόνο μια φορά να στείλουν τα δεδομένα τους στους άλλους δύο (Joux, 2004). Η διαδικασία του πρωτοκόλλου είναι παρόμοια με αυτή του Diffie Hellman και είναι η εξής (Joux, 2004):

- Μια αξιόπιστη πηγή επιλέγει έναν πρώτο αριθμό p μια ελλειπτική καμπύλη E και ένα σημείο $P \in E$.
- Η Αλίκη, ο Μπομπ και ο Κώστας επιλέγουν από έναν ακέραιο τυχαίο $a, b, c \in G_p^*$ αντίστοιχα.
- Έπειτα υπολογίζουν ο καθένας ξεχωριστά $P_A = \mathrm{a} * P$, $P_B = b * P$ και $P_C = c * P$ και τα αποστέλλουν στους άλλους δύο αντίστοιχα μέσω του διαύλου επικοινωνίας.
- Στη συνέχεια, οι χρήστες αφού έχω τα P_A, P_B και P_C με τη βοήθεια μια συνάρτησης F υπολογίζουν τα $F(a, P_B, P_C)$, $F(b, P_A, P_C)$ και $F(c, P_A, P_B)$ αντίστοιχα. Η συνάρτηση F έχει επιλεχθεί με τέτοιο τρόπο ώστε να εξασφαλίζεται ότι οι αριθμοί είναι ίσοι και ότι αυτή η κοινή τιμή K_{ABC} είναι πολύ δύσκολο να βρεθεί από κάποιον που θα ξέρει τα P_A, P_B και P_C.

Το μεγαλύτερο ζήτημα του παραπάνω πρωτοκόλλου ανάγεται στην εύρεση της συνάρτησης F. Με την χρήση των ζευγισμών Weil επιλέγεται η συνάρτηση με τύπο $F(x,P,Q) = \hat{e}(P,Q)^x$ (Al-Riyami and Paterson, 2003). Έτσι με τον ορισμό αυτό βγαίνει εύκολα το συμπέρασμα ότι $F(a,P_B,P_C) = F(b,P_A,P_C) = F(c,P_A,P_B) = F(1,P,P)^{abc}$ λόγω του ορισμού της $\hat{e}$ (βλ. Κεφάλαιο 2). Εν τούτοις, εξαιτίας των ιδιοτήτων των ζευγισμών Weil η συνάρτηση $\hat{e}$ δεν πετυχαίνει εξ ολοκλήρου τον σκοπό της αφού $\hat{e}(P,P) = 1$ άρα η κοινή τιμή των τριών χρηστών είναι πάντα $K_{ABC} = 1$ και επομένως είναι πολύ εύκολο να την βρει κάποιος κακόβουλος επιτιθέμενος (Joux, 2004). Ωστόσο, εκτός αυτού του προβλήματος που προκύπτει, η βασική ιδέα του πρωτοκόλλου του Joux είναι σωστή και είναι και υλοποιήσιμη εάν προσεγγιστεί διαφορετικά, το οποίο και εξηγείται παρακάτω.

Πράγματι η υλοποίηση του πρωτοκόλλου είναι δυνατό να συμβεί εάν χρησιμοποιηθούν δύο σημεία της ελλειπτικής καμπύλης αντί για ένα προκειμένου να λειτουργήσει σωστά το πρωτόκολλο. Επομένως κάνοντας χρήση των ζευγισμών Weil η διαδικασία του πρωτοκόλλου προκύπτει ως εξής (Joux, 2004):

- Επιλέγονται τα δύο σημεία της καμπύλης τυχαία (P $και$ Q) τα οποία είναι ανεξάρτητα και έχουν πεπερασμένη τάξη (π.χ. $ord(P) = l$).
- Έπειτα οι τρεις χρήστες θα υπολογίσουν και θα αποστείλουν στους υπόλοιπους δύο χρήστες αντίστοιχα τα $(P_A,Q_A) = (a*P, a*Q)$, $(P_B,Q_B) = (b*P, b*Q)$ και $(P_C,Q_C) = (c*P, c*Q)$.
- Επομένως, οι τρεις χρήστες υπολογίζουν

$$F(a,P_B,Q_C) = F(a,b*P,c*Q) = \hat{e}(bP,cQ)^a = \hat{e}(P,Q)^{abc} = \hat{e}(Q,P)^{abc}$$
$$= \hat{e}(bQ,cP)^a = F(a,Q_B,P_C)$$
$$F(b,P_A,Q_C) = F(b,a*P,c*Q) = \hat{e}(aP,cQ)^b = \hat{e}(P,Q)^{abc} = \hat{e}(Q,P)^{abc}$$
$$= \hat{e}(aQ,cP)^b = F(b,Q_A,P_C)\ και$$
$$F(c,P_A,Q_B) = F(c,a*P,b*Q) = \hat{e}(aP,bQ)^c = \hat{e}(P,Q)^{abc} = \hat{e}(Q,P)^{abc}$$
$$= \hat{e}(aQ,bP)^c = F(c,Q_A,P_B)$$

Παρατηρούμε λοιπόν ότι όλες οι τιμές είναι ίσες μεταξύ τους και επειδή τα σημεία P και Q είναι ανεξάρτητα δεν είναι σταθερές.

Αλίκη	Μπομπ	Κώστας
Επιλέγει a Υπολογίζει (P_A, Q_A)	Επιλέγει b Υπολογίζει (P_B, Q_B)	Επιλέγει c Υπολογίζει (P_C, Q_C)
	Μετάδοση των (P_A, Q_A) (P_B, Q_B) , (P_C, Q_C)	
Υπολογίζει το κοινό κλειδί $F(a, P_B, Q_C)$	Υπολογίζει το κοινό κλειδί $F(b, P_A, Q_C)$	Υπολογίζει το κοινό κλειδί $F(c, P_A, Q_B)$

Πίνακας 2. Τριμερές πρωτόκολλο ανταλλαγής κλειδιών Joux.

3.3.2 Πρωτόκολλο Shim

Λίγα χρόνια μετά την δημιουργία του πρωτοκόλλου του Joux ο Shim επισήμανε ότι το πρωτόκολλο ανταλλαγής κλειδιών του Joux δεν είναι ανθεκτικό απέναντι σε επιθέσεις man in the middle και πρότεινε ένα βελτιωμένο τριμερές πρωτόκολλο ανταλλαγής κλειδιών με αυθεντικοποίηση (Sun and Hsieh, 2003/ Lin and Lin, 2005).

Το τριμερές πρωτόκολλο που πρότεινε ο Shim είναι και αυτό ενός γύρου πρωτόκολλο, που επιτρέπει σε τρεις χρήστες να αποκτήσουν ένα κοινό κλειδί συνόδου σε μόνο ένα γύρο, αλλά παρέχει και την αυθεντικοποίηση των χρηστών. Η διαδικασία του πρωτοκόλλου είναι η εξής (Shim, 2003/Cheng et. al., 2004):

- Όπως και στα προηγούμενα πρωτόκολλα που παρουσιάστηκαν και σε αυτό το πρωτόκολλο μια έμπιστη πηγή επιλέγει και δημοσιοποιεί έναν μεγάλο πρώτο αριθμό p , μια ελλειπτική καμπύλη E κι ένα σημείο $P \epsilon E$.
- Έχουμε την Αλίκη, τον Μπομπ και τον Κώστα και επιλέγουν τυχαία έναν ακέραιο αριθμό για στατικό ιδιωτικό κλειδί a, b $και$ c αντίστοιχα και υπολογίζουν τα στατικά δημόσια κλειδιά τους $R_A = a * P$, $R_B = b * P$ και $R_C = c * P$.
- Έπειτα, οι τρεις χρήστες επιλέγουν από έναν τυχαίο αριθμό ως εφήμερο ιδιωτικό κλειδί x, y και z και υπολογίζουν τους εξής αριθμούς, τα εφήμερα δημόσια κλειδιά $T_A = x * R_A = x * (a * P)$, $T_B = y * R_B = y * (b * P)$ και $T_C = z * R_C = z * (c * P)$ αντίστοιχα.
- Μεταδίδουν μεταξύ τους τους αριθμούς αυτούς μαζί με τα πιστοποιητικά που αποδεικνύουν την ταυτότητα του κάθε χρήστη (τα πιστοποιητικά συμβολίζονται με $Cert_R$ όπου R ο χρήστης).

  Αλίκη: $T_A = x * R_A = x * (a * P), Cert_A$

Μπομπ: $T_B = y * R_B = y * (b * P), Cert_B$

Κώστας: $T_C = z * R_C = z * (c * P), Cert_C$

Το $Cert_R$ πιστοποιεί ότι το δημόσιο κλειδί που στέλνεται είναι του χρήστη R. Το πιστοποιητικό δίνει μοναδικές πληροφορίες που προσδιορίζουν τη ταυτότητα του R όπως όνομα διεύθυνση που υπογράφονται με το $Cert_R$.

- Στη συνέχεια υπολογίζουν το κοινόχρηστο κλειδί συνόδου:

$$K_A = \hat{e}(T_B, T_C)^{ax\hat{e}(R_B,R_C)^a} = \hat{e}(yR_B, zR_C)^{ax\hat{e}(bP,cP)^a}$$
$$= \hat{e}(bP, cP)^{axyz\hat{e}(P,P)^{abc}} = \hat{e}(P, P)^{abcxyz\hat{e}(P,P)^{abc}}$$
$$K_B = \hat{e}(T_A, T_C)^{by\hat{e}(R_a,R_C)^b} = \hat{e}(xR_A, zR_C)^{by\hat{e}(aP,cP)^b}$$
$$= \hat{e}(aP, cP)^{bxyz\hat{e}(P,P)^{abc}} = \hat{e}(P, P)^{abcxyz\hat{e}(P,P)^{abc}}$$
$$K_C = \hat{e}(T_A, T_B)^{cz\hat{e}(R_A,R_B)^c} = \hat{e}(xR_A, yR_B)^{cz\hat{e}(aP,bP)^c}$$
$$= \hat{e}(aP, bP)^{cxyz\hat{e}(P,P)^{abc}} = \hat{e}(P, P)^{abcxyz\hat{e}(P,P)^{abc}}$$

Το δημόσιο κλειδί είναι $K = kdf(K_A||A||B||C) = kdf(K_B||A||B||C) = kdf(K_C||A||B||C)$, όπου kdf είναι συνάρτηση εξαγωγής κλειδιών (Shim, 2003/ Lin and Lin 2005).

Αλίκη	Μπομπ	Κώστας
Επιλέγει a και υπολογίζει R_A Επιλέγει x και υπολογίζει T_A	Επιλέγει b και υπολογίζει R_B Επιλέγει y και υπολογίζει T_B	Επιλέγει c και υπολογίζει R_C Επιλέγει z και υπολογίζει T_C
Μετάδοση των $(T_A, Cert_A)$ $(T_B, Cert_B)$ και $(T_C, Cert_C)$		
Υπολογίζει το κοινό κλειδί K_A	Υπολογίζει το κοινό κλειδί K_B	Υπολογίζει το κοινό κλειδί K_C

Πίνακας 3. Τριμερές πρωτόκολλο ανταλλαγής κλειδιών Shim.

3.3.3 Πρωτόκολλο ABTKA

Ένα ακόμα τριμερές πρωτόκολλο συμφωνίας κλειδιού είναι το ABTKA (attribute tripartite-based key agreement) το οποίο σε αντίθεση με το πρωτόκολλο του Shim δεν έχει πιστοποίηση. Το συγκεκριμένο πρωτόκολλο βασίστηκε στο μοντέλο που παρουσίασαν οι Xiong, Chen και

Li (Xiong et. al., 2012). Το πρωτόκολλο ABTKA αποτελείται από τους εξής αλγορίθμους (Bayat and Reza Aref, 2015):

- Προετοιμασία: Αυτός ο αλγόριθμος λαμβάνει ως είσοδο την παράμετρο ασφαλείας 1^k. Μια γεννήτρια επιλέγει έναν μεγάλο πρώτο αριθμό p, ένα πεπερασμένο σώμα G_p, μια ελλειπτική καμπύλη E πάνω στο πεπερασμένο σώμα G_p, μια ομάδα A με τα σημεία της καμπύλης και γεννήτορα το σημείο P, μια συνάρτηση κατακερματισμού $H: \{0,1\}^* \rightarrow Z_p^*$ και ένα σύνολο U που εμπεριέχει όλα τα πιθανά χαρακτηριστικά και ταυτότητες των χρηστών. Έπειτα συσχετίζεται κάθε στοιχείο με έναν ακέραιο αριθμό του συνόλου Z_p^*. Η γεννήτρια ιδιωτικών κλειδιών επιλέγει έναν τυχαίο αριθμό $s \epsilon Z_p^*$ ως κύριο ιδιωτικό κλειδί και υπολογίζει το κύριο δημόσιο κλειδί $P_0 = s * P$. Επιπλέον, η γεννήτρια παράγει τυχαίους αριθμούς $t_i \epsilon Z_p^*$ και υπολογίζει $T_i = t_i * P$ για κάθε ένα από τα χαρακτηριστικά $i \epsilon U$. Αφού γίνουν όλες οι διαδικασίες ο αλγόριθμος δίνει όλες τις δημόσιες παραμέτρους $\{G_p, E, A, P, P_0, \{T_i\}_{i \epsilon U}, H, U\}$. Ως μυστικά κλειδιά ο αλγόριθμος έχει τα $\{t_i\}_{i \epsilon U}$ και s.
- Ορισμός μυστικής τιμής: Έστω ένας χρήστης U_X με αντίστοιχο σύνολο χαρακτηριστικών W_X, για κάθε χαρακτηριστικό του χρήστη $i \epsilon W_X$ ο αλγόριθμος παράγει μια τυχαία μυστική τιμή $\chi_{Xi} \epsilon Z_p^*$.
- Μερική εξαγωγή μυστικού κλειδιού: Η είσοδος αυτού του αλγορίθμου είναι το κύριο μυστικό κλειδί s και ένα σύνολο χαρακτηριστικών W_X και η έξοδος είναι ένα μερικό ιδιωτικό κλειδί s_i για κάθε ένα χαρακτηριστικό $i \epsilon W_X$. Η γεννήτρια επιλέγει ένα πολυώνυμο $q(x)$ τέτοια ώστε $q(0) = s$ και βαθμό πολυωνύμου $d - 1$. Η γεννήτρια επιλέγει τους τυχαίους αριθμούς $\{r_i \epsilon Z_p^*\}_{i \epsilon W_X}$ και υπολογίζει $R_i = r_i * T_i$ για κάθε $i \epsilon W_X$, και δημοσιοποιεί τα R_i. Το μερικώς ιδιωτικό κλειδί υπολογίζεται ως εξής:

  $$s_i = \frac{q(i)}{t_i} + r_i$$

  Ο χρήστης U_X μπορεί να επαληθεύσει το μερικώς ιδιωτικό κλειδί του ως:

  $$\sum_{i \epsilon \delta_X} T_i * s_i * \Delta_{i,\delta_X}(0) = P_0 + \sum_{i \epsilon \delta_X} R_i * \Delta_{i,\delta_X}(0)$$

  όπου δ_X είναι υποσύνολο του W_X με d στοιχεία.
- Ορισμός ιδιωτικού κλειδιού: Ο αλγόριθμος αυτός θέτει τα ιδιωτικά κλειδιά ως $sk_X = \{x_{Xi}, s_i\}$ για κάθε $i \epsilon W_X$.

- Ορισμός δημοσίου κλειδιού: Ο αλγόριθμος υπολογίζει $P_{Xi} = \chi_{Xi} * P$ και θέτει το $P_X = \{P_{Xi}\}_{i \epsilon W_X}$ το σύνολο των δημοσίων κλειδιών.
- Πρωτόκολλο ανταλλαγής κλειδιών: Έστω τρείς χρήστες U_A, U_B και U_C με σύνολα χαρακτηριστικών W_A, W_B και W_C, με μυστικά κλειδιά $sk_A = \{x_i, s_i\}_{i \epsilon W_A}$, $sk_B = \{x_i, s_i\}_{i \epsilon W_B}$ και $sk_C = \{x_i, s_i\}_{i \epsilon W_C}$, τα δημόσια κλειδιά $P_A = \{P_i\}_{i \epsilon W_A}$, $P_B = \{P_i\}_{i \epsilon W_B}$ και $P_C = \{P_i\}_{i \epsilon W_C}$ και οι δημόσιοι παράμετροι $\{R_i\}_{i \epsilon W_A}$, $\{R_i\}_{i \epsilon W_B}$ και $\{R_i\}_{i \epsilon W_C}$. Η διαδικασία του πρωτοκόλλου είναι η εξής:

  (1) Οι χρήστες U_A, U_B και U_C επιλέγουν τυχαίους αριθμούς $a, b, c \epsilon Z_p^*$ αντίστοιχα.

  (2) Ο χρήστης U_A υπολογίζει $T_{AB1} = a * P$, $T_{AB2} = \{T_{AB2i} = a * T_i\}_{i \epsilon W_B}$ και $T_{AB3} = \{T_{AB3i} = a * R_i\}_{i \epsilon W_B}$. Ο χρήστης U_A στέλνει στον U_B $\{T_{AB1}, T_{AB2}, T_{AB3}, P_A, W_A\}$.

  (3) Ο χρήστης U_A υπολογίζει $T_{AC1} = a * P$, $T_{AC2} = \{T_{AC2i} = a * T_i\}_{i \epsilon W_C}$ και $T_{AC3} = \{T_{AC3i} = a * R_i\}_{i \epsilon W_C}$. Ο χρήστης U_A στέλνει στον U_C $\{T_{AC1}, T_{AC2}, T_{AC3}, P_A, W_A\}$.

  (4) Ο χρήστης U_B υπολογίζει $T_{BA1} = b * P$, $T_{BA2} = \{T_{BA2i} = b * T_i\}_{i \epsilon W_A}$ και $T_{BA3} = \{T_{BA3i} = b * R_i\}_{i \epsilon W_A}$. Ο χρήστης U_B στέλνει στον U_A $\{T_{BA1}, T_{BA2}, T_{BA3}, P_B, W_B\}$.

  (5) Ο χρήστης U_B υπολογίζει $T_{BC1} = b * P$, $T_{BA2} = \{T_{BC2i} = b * T_i\}_{i \epsilon W_C}$ και $T_{BC3} = \{T_{BC3i} = b * R_i\}_{i \epsilon W_C}$. Ο χρήστης U_B στέλνει στον U_C $\{T_{BC1}, T_{BC2}, T_{BC3}, P_B, W_B\}$.

  (6) Ο χρήστης U_C υπολογίζει $T_{CA1} = c * P$, $T_{CA2} = \{T_{CA2i} = c * T_i\}_{i \epsilon W_A}$ και $T_{CA3} = \{T_{CA3i} = c * R_i\}_{i \epsilon W_A}$. Ο χρήστης U_C στέλνει στον U_A $\{T_{CA1}, T_{CA2}, T_{CA3}, P_C, W_C\}$.

  (7) Ο χρήστης U_C υπολογίζει $T_{CB1} = c * P$, $T_{CB2} = \{T_{CB2i} = c * T_i\}_{i \epsilon W_B}$ και $T_{CB3} = \{T_{CB3i} = c * R_i\}_{i \epsilon W_B}$. Ο χρήστης U_C στέλνει στον U_B $\{T_{CB1}, T_{CB2}, T_{CB3}, P_C, W_C\}$.

  (8) Αφού λάβει ο U_A τα μηνύματα των άλλων δύο χρηστών υπολογίζει τα κοινά μυστικά ως εξής:

$$bsP = \sum_{i \epsilon \delta_A} (s_i * T_{BA2i} - T_{BA3i}) * \Delta_{i,\delta_A}(0) = b * P_0$$

$$csP = \sum_{i \epsilon \delta_A} (s_i * T_{CA2i} - T_{CA3i}) * \Delta_{i,\delta_A}(0) = c * P_0$$

$$K_{ABC}^1 = (a + b + c) * P_0$$

$$K_{ABC}^2 = \hat{e}(T_{BA1}, T_{CA1})^a = \hat{e}(P, P)^{abc}$$

$K_{ABC}^3 = \{K_{ABCi}^3 = \hat{e}(P_{Bi2}, P_{Ci3})^{x_{Ai1}} = \hat{e}(P, P)^{x_{Ai1} x_{Bi2} x_{Ci3}}\}$ για $i1 \epsilon W_A$, $i2 \epsilon W_B$ και $i3 \epsilon W_C$

(9) Αφού λάβει ο U_B τα μηνύματα των άλλων δύο χρηστών υπολογίζει τα κοινά μυστικά ως εξής:

$$asP = \sum_{i \epsilon \delta_A} (s_i * T_{AB2i} - T_{AB3i}) * \Delta_{i,\delta_B}(0) = a * P_0$$

$$csP = \sum_{i \epsilon \delta_A} (s_i * T_{CB2i} - T_{CB3i}) * \Delta_{i,\delta_B}(0) = c * P_0$$

$$K_{ABC}^1 = (a + b + c) * P_0$$

$$K_{ABC}^2 = \hat{e}(T_{AB1}, T_{CB1})^b = \hat{e}(P, P)^{abc}$$

$K_{ABC}^3 = \{K_{ABCi}^3 = \hat{e}(P_{Ai1}, P_{Ci3})^{x_{Bi2}} = \hat{e}(P, P)^{x_{Ai1} x_{Bi2} x_{Ci3}}\}$ για $i1 \epsilon\, W_A$, $i2 \epsilon\, W_B$ και $i3 \epsilon\, W_C$

(10) Αφού λάβει ο U_C τα μηνύματα των άλλων δύο χρηστών υπολογίζει τα κοινά μυστικά ως εξής:

$$asP = \sum_{i \epsilon \delta_A} (s_i * T_{AC2i} - T_{AC3i}) * \Delta_{i,\delta_C}(0) = a * P_0$$

$$bsP = \sum_{i \epsilon \delta_A} (s_i * T_{BC2i} - T_{BC3i}) * \Delta_{i,\delta_C}(0) = b * P_0$$

$$K_{ABC}^1 = (a + b + c) * P_0$$

$$K_{ABC}^2 = \hat{e}(T_{AC1}, T_{BC1})^c = \hat{e}(P, P)^{abc}$$

$K_{ABC}^3 = \{K_{ABCi}^3 = \hat{e}(P_{Ai1}, P_{Bi2})^{x_{Ci3}} = \hat{e}(P, P)^{x_{Ai1} x_{Bi2} x_{Ci3}}\}$ για $i1 \epsilon\, W_A$, $i2 \epsilon\, W_B$ και $i3 \epsilon\, W_C$

(11) Τέλος και οι τρείς χρήστες υπολογίζουν το κοινό κλειδί της συνόδου ως εξής:

$$SK = H\big(W_A, W_B, W_C, T_{AB1} = T_{AC1,}\, T_{BC1} = T_{BA1,}\, T_{CA1} = T_{CB1}, P_A, P_B, P_C, K_{ABC}^1, K_{ABC}^2, K_{ABC}^3\big)$$

Αν υποθέσουμε ότι ο U_A χρήστης είναι η Αλίκη, ο U_B χρήστης είναι ο Μπομπ και ο U_C χρήστης είναι ο Κώστας, τότε στον παρακάτω πίνακα περιγράφεται η διαδικασία του πρωτοκόλλου.

Αλίκη	Μπομπ	Κώστας
Η Αλίκη στέλνει στον Μπομπ: $\{T_{AB1}, T_{AB2}, T_{AB3}, P_A, W_A\}$ Η Αλίκη στέλνει στον Κώστα:$\{T_{AC1}, T_{AC2}, T_{AC3}, P_A, W_A\}$	Ο Μπομπ στέλνει στην Αλίκη:$\{T_{BA1}, T_{BA2}, T_{BA3}, P_B, W_B\}$ Ο Μπομπ στέλνει στον Κώστα:$\{T_{BC1}, T_{BC2}, T_{BC3}, P_B, W_B\}$	Ο Κώστας στέλνει στην Αλίκη: $\{T_{CA1}, T_{CA2}, T_{CA3}, P_C, W_C\}$. Ο Κώστας στέλνει στον Μπομπ: $\{T_{CB1}, T_{CB2}, T_{CB3}, P_C, W_C\}$.
Η Αλίκη υπολογίζει $K_{ABC}^1 = (a+b+c)P_0$ $K_{ABC}^2 = \hat{e}(P,P)^{abc}$ $K_{ABC}^3 = \hat{e}(P,P)^{x_{Ai1}x_{Bi2}x_{Ci3}}$	Ο Μπομπ υπολογίζει $K_{ABC}^1 = (a+b+c)P_0$ $K_{ABC}^2 = \hat{e}(P,P)^{abc}$ $K_{ABC}^3 = \hat{e}(P,P)^{x_{Ai1}x_{Bi2}x_{Ci3}}$	Ο Κώστας υπολογίζει $K_{ABC}^1 = (a+b+c)P_0$ $K_{ABC}^2 = \hat{e}(P,P)^{abc}$ $K_{ABC}^3 = \hat{e}(P,P)^{x_{Ai1}x_{Bi2}x_{Ci3}}$
Υπολογίζει το κλειδί της συνόδου SK	Υπολογίζει το κλειδί της συνόδου SK	Υπολογίζει το κλειδί της συνόδου SK

Πίνακας 4.Τριμερές πρωτόκολλο ανταλλαγής κλειδιών ΑΒΤΚΑ.

Κεφάλαιο 4

Επιθέσεις πρωτοκόλλων

4.1 Man in the Middle Attack

Στον τομέα της κρυπτογραφίας και της ασφάλειας στον κυβερνοχώρο ως man in the middle αναφέρεται η επίθεση όπου ένα τρίτο πρόσωπο (επιτιθέμενος) αναμεταδίδει και τροποποιεί κρυφά τα δεδομένα μιας επικοινωνίας μεταξύ δύο οντοτήτων που επιθυμούν να ανταλλάξουν μηνύματα μέσω ενός πρωτοκόλλου (Elakrat and Jung, 2018/ Rosenberg, 2017). Η επίθεση man in the middle είναι υποκλοπή πληροφοριών και μηνυμάτων που αποστέλλονται σε ένα πρωτόκολλο (Vesteras, 2006). Η υποκλοπή γίνεται καθ' όλη την διάρκεια της συνομιλίας των οντοτήτων με αποτέλεσμα ο επιτιθέμενος να «κρυφακούει» πληροφορίες που θα έπρεπε να γνωρίζουν μόνο οι χρήστες του πρωτοκόλλου (Vesteras, 2006). Η διαδικασία είναι απλή, ο επιτιθέμενος δημιουργεί ανεξάρτητες συνδέσεις με τους χρήστες και αναμεταδίδει μηνύματα μεταξύ τους ώστε να τους κάνει να πιστέψουν ότι συνομιλούν οι δυο τους μέσω ιδιωτικής σύνδεσης, ένα στην πραγματικότητα ολόκληρη η συνομιλία παρακολουθείται και ελέγχεται από τον επιτιθέμενο (Wang and Wyglinski, 2014/ Rosenberg, 2017).

Ο επιτιθέμενος θεωρείται απαραίτητο να είναι σε θέση να μπορεί να υποκλέπτει κάθε μήνυμα που αποστέλλουν οι δύο οντότητες και να εισάγει νέα. Η προϋπόθεση αυτή είναι απλή διότι αφού σε περίπτωση που ο επιτιθέμενος βρίσκεται εντός εμβέλειας λήψη ενός μη κρυπτογραφημένου Wi-Fi μπορεί πολύ εύκολα να εισέλθει ως man in the middle (Rosenberg, 2017). Ο έλεγχος ταυτότητας στα κρυπτογραφικά πρωτόκολλα έχει ενταχθεί σε αρκετά από αυτά για να αποφεύγεται η πιθανότητα των επιθέσεων Man in the middle, επειδή η επίθεση αυτή αποσκοπεί στην παράκαμψη της αυθεντικοποίησης των οντοτήτων για να μπορέσει ο επιτιθέμενος να υποδυθεί έναν από τους χρήστες. Η αυθεντικοποίηση συνήθως γίνεται από μία ανεξάρτητη έμπιστη αρχή που πιστοποιεί τους χρήστες, όπως γίνεται στο TLS πρωτόκολλο όπου γίνεται αυθεντικοποίηση ή του ενός ή και των δύο μερών του πρωτοκόλλου (Elakrat and Jung, 2018). ΄

Έστω ότι η Αλίκη και ο Μπομπ θέλουν να επικοινωνήσουν και χρησιμοποιούν ένα πρωτόκολλο ανταλλαγής κλειδιών. Ο Μάκης θέλει να μάθει τι θα στείλουν οι δύο χρήστες στον άλλον και ενδεχομένως να παραποιήσει τα μηνύματα τους (Rosenberg, 2017). Η Αλίκη ζητάει αρχικά το δημόσιο κλειδί του Μπομπ. Ο Μπομπ στέλνει το δημόσιο κλειδί του στην

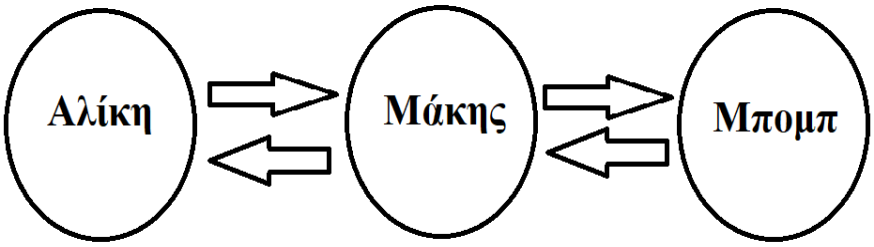
Αλίκη. Σε περίπτωση που ο Μάκης έχει την δυνατότητα να υποκλέψει το κλειδί του Μπομπ έχουμε μια man in the middle επίθεση. Έτσι ο Μάκης θα εξαπατήσει την Αλίκη στέλνοντας της το δικό του δημόσιο κλειδί αντί του Μπομπ. Έπειτα η Αλίκη αφού νομίζει ότι το κλειδί που έλαβε είναι του Μπομπ, κρυπτογραφεί το μήνυμα της με το κλειδί του Μάκη και στέλνει το κρυπτομήνυμα στο Μπομπ. Ο Μάκης υποκλέπτει το κρυπτομήνυμα της Αλίκης το αποκρυπτογραφεί και ενδεχομένως το τροποποιεί εάν θέλει, το κρυπτογραφεί εκ νέου με το κλειδί του και το στέλνει στον Μπομπ. Ο Μπομπ λαμβάνει το μήνυμα πιστεύοντας ότι είναι από την Αλίκη.

Παράδειγμα 4.1.1 (Rosenberg, 2017)

Η Αλίκη και ο Μπομπ θέλουν να επικοινωνήσουν μεταξύ τους. Ο Μάκης όμως θέλει να μάθει τι πληροφορίες θα ανταλλάξουν η Αλίκη και ο Μπομπ χωρίς να γίνει αντιληπτός. Στο παράδειγμα ως ψεύτικος Μπομπ και ψεύτικη Αλίκη αναφέρεται ο Μάκης. Η διαδικασία είναι η εξής:

- Η Αλίκη στέλνει ένα μήνυμα στον Μπομπ, το οποίο υποκλέπτει ο Μάκης.
  Αλίκη «Γειά σου Μπομπ, είμαι η Αλίκη στείλε μου το κλειδί σου» → ψεύτικος Μπομπ
- Ο Μάκης αναμεταδίδει το μήνυμα στον Μπομπ, όπου δεν γνωρίζει ότι δεν το έστειλε η Αλίκη το μήνυμα.
  Ψεύτικη Αλίκη «Γειά σου Μπομπ, είμαι η Αλίκη στείλε μου το κλειδί σου» → Μπομπ
- Ο Μπομπ στέλνει το κλειδί του.
  Ψεύτικη Αλίκη ← [κλειδί του Μπομπ] Μπομπ
- Ο Μάκης αντικαθιστά το κλειδί του με το δικό και το στέλνει στην Αλίκη.
  Αλίκη ← [κλειδί του Μάκη] Ψεύτικος Μπομπ
- Η Αλίκη κρυπτογραφεί το μήνυμα που θέλει να στείλει με το κλειδί του Μάκη πιστεύοντας ότι το κρυπτομήνυμα θα μπορεί να αποκρυπτογραφηθεί μόνο από τον Μπομπ.
  Αλίκη «Τα κλειδιά του σπιτιού είναι κάτω από το χαλάκι»[κρυπτογραφημένο με το κλειδί το Μάκη]→Ψεύτικος Μπομπ
- Ο Μάκης λαμβάνει το μήνυμα το αποκρυπτογραφεί το διαβάζει και μπορεί αν θέλει να το τροποποιήσει εάν επιθυμεί. Έπειτα το ξανακρυπτογραφεί με το κλειδί του Μπομπ και το αποστέλλει στον Μπομπ.

- Ψεύτικη Αλίκη «Τα κλειδιά του σπιτιού είναι μέσα στην γλάστρα»[κρυπτογραφημένο με το κλειδί του Μπομπ]→ Μπομπ



Εικόνα 2. Man in the middle επίθεση

Η Αλίκη και ο Μπομπ πιστεύουν ότι είχαν μια ασφαλή επικοινωνία, όμως όπως φαίνεται από το παράδειγμα αυτό δεν ισχύει. Δημιουργείται λοιπόν η ανάγκη να πιστοποιείται κάθε οντότητα που λαμβάνει μέρος σε μια συνεδρία επικοινωνίας.

Γενικότερα, δυστυχώς, δεν υπάρχει τρόπος αποτροπής της υποκλοπής κρυπτομηνυμάτων αλλά είναι δυνατή η προστασία του περιεχομένου. Αν ο επιτιθέμενος δεν γνωρίζει το κλειδί με το οποίο κρυπτογραφήθηκε το μήνυμα δεν μπορεί να διαβάσει το μήνυμα. Το γεγονός αυτό προϋποθέτει το κλειδί της κρυπτογράφησης να μείνει μυστικό και να είναι γνωστό μόνο στους χρήστες που θέλουν να επικοινωνήσουν. Ένας τρόπος αποφυγής των επιθέσεων man in the middle είναι η ένταξη των πιστοποιητικών ταυτότητας στα πρωτόκολλα ανταλλαγής κλειδιών. Μια αξιόπιστη αρχή θα εκδίδει τα πιστοποιητικά των χρηστών που θα αποδεικνύουν την ταυτότητα του εκάστοτε χρήστη.

4.2 Επίθεση πλαστοπροσωπίας με παραβίαση κλειδιού

Σχεδόν όλα τα πρωτόκολλα ανταλλαγής κλειδιών είναι ευάλωτα απέναντι σε επιθέσεις πλαστοπροσωπίας με παραβίαση κλειδιού. Αν ένας κακόβουλος θέλει να επιτεθεί με την επίθεση πλαστοπροσωπίας σε ένα πρωτόκολλο, αρχικά θα υποδυθεί μια διαφορετική οντότητα με σκοπό να εξαπατήσει έναν από τους χρήστες (π.χ. την Αλίκη) του πρωτοκόλλου και να εγκαθιδρύσει ένα έγκυρο κλειδί συνόδου με την Αλίκη. Με αυτόν τον τρόπο δεν χρειάζεται να υποκλαπεί κάποιο επιπλέον κλειδί διότι ο επιτιθέμενος (Μάκης) γνωρίζει το ιδιωτικό κλειδί της Αλίκης και μπορεί να ξεκινήσει μια νέα σύνοδο με την Αλίκη χρησιμοποιώντας ένα εφήμερο δημόσιο κλειδί προσποιούμενος ότι είναι ο Μπομπ. Ο Μάκης μπορεί να υπολογίσει το ίδιο κλειδί συνόδου με την Αλίκη, αφού γνωρίζει το δημόσιο κλειδί του Μπομπ και το ιδιωτικό κλειδί της Αλίκης, μπορεί να υπολογίσει το ίδιο κλειδί συνόδου με την Αλίκη η οποία νομίζει ότι μοιράζεται το κλειδί με τον Μπομπ. Η έλλειψη της ταυτοποίησης στα πρωτόκολλα είναι ο σημαντικότερος λόγος της επιτυχίας της επίθεσης πλαστοπροσωπίας με παραβίαση

κλειδιού. Ακόμα κι όταν υπάρχει η ταυτοποίηση και ο επιτιθέμενος έχει υποκλέψει το πιστοποιητικό ενός ή περισσοτέρων οντοτήτων από μια παλαιότερη συνεδρία, είναι εύκολο να τα επαναχρησιμοποιήσει για να υποδυθεί έναν εκ των χρηστών και να εξαπατήσει τους υπόλοιπους (Chalkias et. al., 2008).

Μια λύση στην επίθεση πλαστοπροσωπίας, αποτελεί η έγκυρη ταυτοποίηση των χρηστών. Ένας τρόπος για να γίνει αυτό είναι να αποστέλλουν οι χρήστες μαζί με το εφήμερο δημόσιο κλειδί μια ψηφιακή υπογραφή. Έπειτα ο παραλήπτης θα επαληθεύει την υπογραφή πριν αποδεχθεί το εφήμερο δημόσιο κλειδί για να βεβαιωθεί για τη ταυτότητα του αποστολέα. Η συγκεκριμένη λύση λειτουργεί μόνο αν η υπογραφή του χρήστη είναι διαφορετική σε κάθε συνεδρία αποφεύγοντας έτσι την περίπτωση επαναχρησιμοποίησης της από κάποιον κακόβουλο (Chalkias et. al., 2008).

4.3 Εσωτερική επίθεση

Εσωτερική επίθεση ορίζεται η επίθεση όπου ο κακόβουλος είναι ένας από τους χρήστες που επικοινωνούν. Οι χρήστες που πραγματοποιούν τέτοιες επιθέσεις έχουν μεγάλο πλεονέκτημα διότι είναι εξοικειωμένοι με το περιβάλλον στο οποίο πραγματοποιείται το εκάστοτε πρωτόκολλο ανταλλαγής κλειδιών (Rosenberg, 2017). Οι εσωτερικές επιθέσεις είναι αρκετά εύκολο να πραγματοποιηθούν από κάποιον χρήστη, αφού στα περισσότερα πρωτόκολλα δημιουργούνται μηχανισμοί κατά κύριο λόγω για προστασία από εξωτερικούς παράγοντες και όχι από εσωτερικούς.

Η πιο συνηθισμένη περίπτωση εσωτερικού επιτιθέμενου προέρχεται από άτομα που έχουν την νόμιμη πρόσβαση στο κυβερνοσύστημα του οργανισμού και το εκμεταλλεύονται για κακόβουλους σκοπούς ή δημιουργούν άθελα τους ευπάθειες στο σύστημα. Με την πρόσβαση που έχουν στο σύστημα μπορούν να υποκλέπτουν και να τροποποιούν δεδομένα χωρίς να γίνονται αντιληπτοί από την ασφάλεια τους συστήματος διότι το σύστημα εστιάζει σε εξωτερικές απειλές που μπορεί να εισέλθουν στο σύστημα και όχι στο ποιος είναι ήδη μέσα (Rosenberg, 2017). Σύμφωνα με τον (Rosenberg, 2017) : «Πάνω από το 50% των οργανισμών αναφέρουν ότι κάθε χρόνο αντιμετωπίζουν μια κυβερνοεπίθεση εκ των έσω. Οι περιπτώσεις απειλών εκ των έσω αποτελούν περίπου το 23% όλων των περιστατικών εγκλήματος στον κυβερνοχώρο, ποσοστό που παραμένει σταθερό από χρόνο σε χρόνο. Σημειώνεται δυστυχώς ότι ο συνολικός αριθμός των επιθέσεων έχει αυξηθεί σημαντικά».

Οι εσωτερικές επιθέσεις δεν γίνονται τόσο εύκολα αντιληπτές από τα συστήματα και πλέον οι ζημιές και οι αρνητικές επιπτώσεις που προκαλούνται φαίνεται να είναι υψηλότερες από

εκείνες των περιστατικών που προκαλούνται από εξωτερικό παράγοντα ή άλλων εγκλημάτων στον κυβερνοχώρο. Αυτό έχει ως αποτέλεσμα αρκετές επιθέσεις πολλαπλών σταδίων να αρχίζουν να μοιάζουν με εσωτερικές επιθέσεις (Rosenberg, 2017).

Κεφάλαιο 5

Ασφάλεια πρωτοκόλλων

5.1 Ασφάλεια πρωτοκόλλων

Τα πρωτόκολλα ανταλλαγής κλειδιών είναι σχεδιασμένα με τέτοιον τρόπο ώστε να μπορούν να παρέχουν ασφαλή επικοινωνία μεταξύ δύο ή και περισσότερων χρηστών σε μη ασφαλείς διαύλου επικοινωνίας στον κυβερνοχώρο. Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο σκοπός των πρωτοκόλλων είναι να καθιερωθεί ένα κοινό μυστικό κλειδί ανάμεσα στους χρήστες που λαμβάνουν μέρος στο πρωτόκολλο. Υπάρχουν πολλές προϋποθέσεις που είναι απαραίτητες και πρέπει να ληφθούν υπόψη για την ασφάλεια πρωτοκόλλων ανταλλαγής κλειδιών (Wang et. al., 2009). Η σημαντικότερη προϋπόθεση είναι όταν ένας κακόβουλος επιτιθέμενος «παρακολουθεί» την ανταλλαγή πληροφοριών των χρηστών να μην μπορεί να υποκλέψει το κοινό μυστικό κλειδί. Για ένα πρωτόκολλο απαιτείται ο αντίπαλος να μη είναι σε θέση να μπορεί να διακρίνει από τις πληροφορίες που ανταλλάσσονται ποιο μπορεί να είναι το κοινό μυστικό κλειδί (Wang et. al., 2009). Γενικότερα είναι σημαντικό να αναμένεται ότι κακόβουλος επιτιθέμενος είναι ικανός να συλλέγει τα μηνύματα (συμβολοσειρές), να τα τροποποιεί, να τα διαγράφει ακόμα και να κατασκευάζει δικά του, γεγονός που δηλώνει ότι έχει το έλεγχο του δικτύου επικοινωνίας (Boyd et. al., 2003). Οι πιο σημαντικές προϋποθέσεις για την ασφάλεια των πρωτοκόλλων είναι οι εξής (Boyd et. al., 2003):

- **Ασφάλεια γνωστού κλειδιού**. Ένα πρωτόκολλο ανταλλαγής κλειδιών παρέχει ασφάλεια ακόμα και σε περίπτωση που κάποιος αντίπαλος έχει καταφέρει να μάθει ένα ή περισσότερα κλειδιά από προηγούμενες συνόδους. Αυτό θεωρείται μια τυπική απαίτηση για τα πρωτόκολλα ανταλλαγής κλειδιών.
- **Τέλεια μυστικότητα προς τα εμπρός**. Όταν το μακροπρόθεσμο κλειδί μιας οντότητας παραβιάζεται, ο αντίπαλος δύναται να μεταμφιεστεί ως η ίδια η οντότητα σε κάθε μελλοντική εκτέλεση πρωτοκόλλου. Ωστόσο, η κατάσταση θα είναι ακόμη χειρότερη εάν ο αντίπαλος μπορεί επίσης να χρησιμοποιήσει το παραβιασμένο μακροπρόθεσμο κλειδί για να αποκτήσει κλειδιά συνόδου που είχαν γίνει αποδεκτά πριν από την παραβίαση. Ένα πρωτόκολλο αντιστέκεται στην υποκλοπή κλειδιού όταν η απώλεια δεν επιτρέπει στον αντίπαλο να υποδυθεί κάποια από τις οντότητες και να αποκτήσει το κοινόχρηστο κλειδί της συνόδου. Δεδομένου ότι υπάρχει συνήθως υπολογιστικό

κόστος στην παροχή μυστικότητας προς τα εμπρός μερικές φορές θυσιάζεται προς όφελος της αποτελεσματικότητας.

- **Αυθεντικότητα στην υποκλοπή κλειδιού**. Ας υποθέσουμε ότι το μακροπρόθεσμο ιδιωτικό κλειδί αποκαλύπτεται. Τότε φυσικά ένας αντίπαλος μπορεί να υποδυθεί τον Α σε οποιοδήποτε πρωτόκολλο, στον οποίο ο Α αναγνωρίζεται από αυτό το κλειδί. Ένα πρωτόκολλο αντιστέκεται στην υποκλοπή κλειδιού όταν αυτή η απώλεια δεν επιτρέπει σε έναν αντίπαλο να υποδυθεί άλλες οντότητες και να αποκτήσει το μυστικό κλειδί.
- **Δεν υπάρχει άγνωστη κοινή χρήση κλειδιού**. Σε μια επίθεση άγνωστης κοινής χρήσης κλειδιού, ένας αντίπαλος πείθει μια ομάδα οντοτήτων ότι μοιράζονται ένα κλειδί με τον αντίπαλο, ενώ στην πραγματικότητα το κλειδί μοιράζεται μεταξύ της ομάδας και ενός άλλου μέρους. Αυτή η κατάσταση μπορεί να αξιοποιηθεί με διάφορους τρόπους από τον αντίπαλο, όταν το κλειδί χρησιμοποιείται στη συνέχεια για την παροχή κρυπτογράφησης.
- **Κανένας έλεγχος κλειδιού**. Δεν θα πρέπει να είναι δυνατό για οποιονδήποτε από τους συμμετέχοντες ή για έναν αντίπαλο να επιβάλει το κλειδί συνόδου σε μια προεπιλεγμένη τιμή ή να προβλέψει την τιμή του κλειδιού της συνόδου. Αυτό αποτρέπει οποιονδήποτε να επιβάλει τη χρήση ενός παλιού κλειδιού για κλειδί της συνόδου.

5.1.1 Το πρόβλημα του Διακριτού Λογαρίθμου

Ο κλασικός λογάριθμος είναι η αντίστροφη πράξη της εκθετοποίησης. Ο διακριτός λογάριθμος είναι η αντίστροφη πράξη της modulo εκθετοποίησης.

Έστω μια πεπερασμένη κυκλική ομάδα Z_p^* με τάξη $p-1$ και $g \epsilon Z_p^*$ ένας γεννήτορας της. Αν έχουμε $y = g^x$ και $g^x \equiv h \, mod \, p$ και $h \epsilon Z_p^*$, τότε ο διακριτός λογάριθμος είναι το $log_g y = x$. Το πρόβλημα του διακριτού λογαρίθμου είναι η δυσκολία προσδιορισμού του $x \epsilon Z_p^*$ (Allen, 2008).

Το παραπάνω αποτελεί έναν διακριτό λογάριθμο στην κυκλική ομάδα $< g >$ όπου μπορεί να είναι ή και όχι ίση με Z_p^*. Στην περίπτωση όπου το $|g| = n$ με n πολύ μεγάλο και έχει έναν πολύ μεγάλο πρώτο για παράγοντα τότε το πρόβλημα του διακριτού λογαρίθμου είναι πολύ δύσκολο (Allen, 2008).

Το πρόβλημα του διακριτού λογαρίθμου στις ελλειπτικές καμπύλες.

Έστω ότι έχουμε μια ελλειπτική καμπύλη E ένα σημείο $P\epsilon\ E$ κι έναν πρώτο αριθμό p. Οι χρήστες επιλέγουν το ιδιωτικό κλειδί k και υπολογίζουν το δημόσιο $Q = k * P$. Εφόσον το k είναι ιδιωτικό δεν θα πρέπει να είναι εφικτό σε κανέναν να βρει αυτή την τιμή. Σε αυτό το σημείο εκμεταλλεύονται τα πρωτόκολλα ελλειπτικών καμπυλών το πρόβλημα του διακριτού λογαρίθμου (RSA Laboratories, 2000). Η εκτέλεση της αντίστροφης πράξης και η εύρεση του k όταν είναι γνωστό το Q θεωρείται από δύσκολη έως και αδύνατη να γίνει. Ειδικά όταν βρισκόμαστε σε πεπερασμένο σώμα με το $modp$ μπορεί να υπάρχουν πάνω από ένα k που μπορούν να δώσουν αποτέλεσμα Q (RSA Laboratories, 2000).

5.1.2 Το Διωνυμικό πρόβλημα Diffie-Hellman

Διωνυμικό πρόβλημα Diffie-Hellman

Έστω ότι έχουμε μια αντιστοίχιση όπως έχει οριστεί στο κεφάλαιο 2

$$\hat{e}: G_1 \times G_1 \rightarrow G_2$$

είναι ένας διγραμμικός χάρτης. Έστω P ένας γεννήτορας του G_1. Το διωνυμικό πρόβλημα Diffie-Hellman (bilinear Diffie-Hellman problem (BDHP)) στο $< G_1, G_2, \hat{e} >$ έχει ως εξής: δεδομένου ότι $P, aP, bP, cP\ \epsilon\ G_1$, υπολογίζετε $\hat{e}(P,P)^{abc}\ \epsilon\ G_2$, όπου τα a, b, c τυχαία στοιχεία του Z_p^* (Duursma and Lee, 2005). Το BDHP είναι δύσκολο, διότι δεν υπάρχει πολυωνυμικός αλγόριθμος χρόνου τέτοιος ώστε να μπορεί να λύσει το BDHP με μη αμελητέα πιθανότητα (Duursma and Lee, 2005).

Υπολογιστικό Πρόβλημα Diffie-Hellman

Έστω P ένας γεννήτορας της κυκλικής ομάδας G, δίνονται δύο σημεία $aP, bP\ \epsilon\ Z_p^*$ με τυχαία $a, b\ \epsilon\ Z_p^*$. Το υπολογιστικό πρόβλημα Diffie-Hellman είναι ο υπολογισμός του $abP\ \epsilon\ G$.

5.1.3 Επίθεση Man in the Middle στο ελλειπτικό Diffie-Hellman

Όπως περιγράψαμε στο 3.2.1 στην ανταλλαγή κλειδιών στο ελλειπτικό Diffie-Hellman το κοινό μυστικό κλειδί δημιουργείται από το πολλαπλασιασμό του δημόσιου σημείου με το μυστικό κλειδί που παράγεται από την Αλίκη και τον Μπομπ. Ένας τρίτος, ο Μάκης, έχει ανταλλάξει κλειδιά με τον Μπομπ και την Αλίκη. Σε αυτή την περίπτωση υπάρχει ένα σημαντικό πρόβλημα, διότι τα κλειδιά που ανταλλάσσουν δεν είναι πιστοποιημένα (Kaabneh and Al-Bdour, 2005). Αυτό σημαίνει ότι η Αλίκη δεν μπορεί με κάποιον τρόπο να γνωρίζει αν το cP έχει προέλθει σίγουρα από τον Μπομπ. Πολύ εύκολα ο Μάκης θα μπορούσε να έχει

υποκλέψει την μετάδοση του Μπομπ και την αλλάξει με μια δική του cP. Με το ίδιο τρόπο ο Μάκης μπορεί να ανταλλάξει κλειδιά και με τον Μπομπ και οι Αλίκη και Μπομπ να νομίζουν ότι έχουν ανταλλάξει μεταξύ τους κλειδιά. Μετά από αυτή την διαδικασία ο Μάκης μπορεί να αποκρυπτογραφεί το μήνυμα του Μπομπ, να το επανακρυπτογραφεί με το κλειδί της Αλίκης και αντίστροφα. Έτσι θα παρακολουθεί την επικοινωνία των δύο χρηστών χωρίς να γίνεται αντιληπτός.

Αλίκη	Μάκης	Μπομπ
Επιλέγει τυχαία $a \in G_p$	Επιλέγει τυχαία $c \in G_p$	Επιλέγει τυχαία $b \in G_p$
Υπολογίζει aP	Υπολογίζει cP	Υπολογίζει bP
Λαμβάνει cP	Υποκλέπτει aP και bP από την Αλίκη και τον Μπομπ	Λαμβάνει cP
Υπολογίζει acP	Υπολογίζει acP και bc$P$	Υπολογίζει bc$P$

Πίνακας 5. Επίθεση Man in the Middle στον ελλειπτικό Diffie-Hellman.

5.2 Επιθέσεις στο Joux πρωτόκολλο

Για να είναι ασφαλές το τριμερές πρωτόκολλο Joux, που περιγράφεται στο κεφάλαιο 3, απαιτείται να είναι δύσκολοι, ο διακριτός λογάριθμος στην επιλεγμένη ελλειπτική καμπύλη και ο διακριτός λογάριθμος στο πεπερασμένο πεδίο G_p (Joux, 2004). Όμως το πρωτόκολλο αυτό όπως θα δούμε έχει μια πολύ σοβαρή αδυναμία απέναντι στην man in the middle επίθεση.

Ένας αντίπαλος ο Μάκης δημιουργεί εφήμερα ιδιωτικά κλειδιά a', b'και c'. Ο Μάκης αντικαθιστά τα (P_A, Q_A), (P_B, Q_B) και (P_C, Q_C), με $({P_A}', {Q_A}') = (a' * P, a' * Q)$, $({P_B}', {Q_B}') = (b' * P, b' * Q)$ και $({P_C}', {Q_C}') = (c' * P, c' * Q)$ αντίστοιχα. Τότε οι χρήστες υπολογίζουν το κλειδί συνόδου αντίστοιχα:

Αλίκη: $K_A = \hat{e}({P_B}', {Q_C}')^a = \hat{e}(P, Q)^{ab'c'}$

Μπομπ: $K_B = \hat{e}({P_A}', {Q_C}')^b = \hat{e}(P, Q)^{a'bc'}$

Κώστας: $K_C = \hat{e}({P_A}', {Q_B}')^c = \hat{e}(P, Q)^{a'b'c}$

Τότε ο Μάκης που γνωρίζει τις τιμές a', b'και c'είναι επίσης σε θέση να υπολογίσει αυτά τα κλειδιά συνόδου από τις γνωστές τιμές ως εξής:

$$K_A = \hat{e}(P_A, Q)^{b'c'} = \hat{e}(P, Q)^{ab'c'}$$

$$K_B = \hat{e}(P_B, Q)^{a'c'} = \hat{e}(P, Q)^{a'bc'}$$

$$K_C = \hat{e}(P_C, Q)^{a'b'} = \hat{e}(P, Q)^{a'b'c}$$

Όταν στη συνέχεια η Αλίκη στέλνει ένα μήνυμα στον Μπομπ και στο Κώστα κρυπτογραφημένο με κλειδί K_A, ο Μάκης το αποκρυπτογραφεί, το ξανακρυπτογραφεί με K_B και K_C και το προωθεί στο Μπομπ και στο Κώστα, αντίστοιχα. Ομοίως, ο Μάκης αποκρυπτογραφεί μηνύματα κρυπτογραφημένα από τον Μπομπ ή τον Κώστα με K_B ή K_C, και τα κρυπτογραφεί εκ νέου με K_A. Τότε η Αλίκη, ο Μπομπ και ο Κώστας πιστεύουν ότι επικοινωνούν με ασφάλεια, ενώ ο Μάκης διαβάζει όλα τα μηνύματα που ανταλλάσσουν. Η man in the middle επίθεση οφείλεται στο γεγονός ότι δεν υπάρχει πιστοποίηση του μηνύματος που αποστέλλεται. Αυτό το μειονέκτημα μπορεί να ξεπεραστεί με τη χρήση δημόσιων κλειδιών που έχουν υπογραφεί από τον αποστολέα.

Αλίκη	Μπομπ	Μάκης	Κώστας
Επιλέγει a	Επιλέγει b	Επιλέγει a', b', c'	Επιλέγει c
Υπολογίζει (P_A, Q_A)	Υπολογίζει (P_B, Q_B)	Υπολογίζει $(P_A{}', Q_A{}')$, $(P_B{}', Q_B{}')$ και $(P_C{}', Q_C{}')$	Υπολογίζει (P_C, Q_C)
Στέλνει στον Μπομπ και στο Κώστα (P_A, Q_A)	Στέλνει στην Αλίκη και στον Κώστα (P_B, Q_B)	Υποκλέπτει και αντικαθιστά τα (P_A, Q_A), (P_B, Q_B) και (P_C, Q_C) με τα $(P_A{}', Q_A{}')$, $(P_B{}', Q_B{}')$ και $(P_C{}', Q_C{}')$	Στέλνει στην Αλίκη και στον Μπομπ (P_C, Q_C)
Λαμβάνει $(P_B{}', Q_B{}')$ και $(P_C{}', Q_C{}')$	Λαμβάνει $(P_A{}', Q_A{}')$ και $(P_C{}', Q_C{}')$		Λαμβάνει $(P_A{}', Q_A{}')$ και $(P_B{}', Q_B{}')$
Υπολογίζει K_A	Υπολογίζει K_B	Υπολογίζει K_A, K_B, K_C	Υπολογίζει K_C

Πίνακας 6. Επίθεση man in the middle στο πρωτόκολλο Joux

5.3 Επιθέσεις στο Shim πρωτόκολλο

Σε αυτή την ενότητα θα δούμε πόσο ασφαλές είναι το πρωτόκολλο του Shim και ποιες είναι οι αδυναμίες του.

Επίθεση πλαστοπροσωπίας με παραβίαση κλειδιού

Η επίθεση πλαστοπροσωπίας με παραβίαση κλειδιού συμβαίνει όταν ο επιτιθέμενος, ο οποίος έχει παραβιάσει το ιδιωτικό κλειδί μιας οντότητας, μπορεί όχι μόνο να υποδυθεί την

παραβιασμένη οντότητα αλλά να υποδυθεί και τις άλλες οντότητες στην παραβιασμένη οντότητα (Lin and Lin, 2005/ Sun and Hsieh, 2003). Για παράδειγμα, ένας εξωτερικός επιτιθέμενος ο Μάκης, ο οποίος έχει παραβιάσει το ιδιωτικό κλειδί b του Μπομπ, μπορεί να υποδυθεί τις άλλες δύο οντότητες (Αλίκη και Κώστα) στον Μπομπ. Αναλυτικά (Lin and Lin, 2005):

- Η Αλίκη, ο Μπομπ και ο Κώστας είναι νόμιμες οντότητες που χρησιμοποιούν το πρωτόκολλο.
- Τα $Cert_A, Cert_B$ και $Cert_C$ είναι τα πιστοποιητικά της Αλίκης, του Μπομπ και του Κώστα αντίστοιχα που έχουν πιστοποιηθεί από μια έμπιστη αρχή.
- Ο Μάκης ως εξωτερικός επιτιθέμενος θέλει να υποδυθεί την Αλίκη και τον Κώστα και να επικοινωνήσει με τον Μπομπ. Υποκλέπτει ο Μάκης τα b, T_B και $Cert_B$ για να υποδυθεί τον Μπομπ και αποκτά τα $Cert_A, Cert_C$.
- Ο Μάκης αφού έχει ό,τι χρειάζεται υποδύεται ότι είναι η Αλίκη και ο Κώστας και ξεκινά ένα πρωτόκολλο ανταλλαγής κλειδιού με τον Μπομπ, ο οποίος πιστεύει ότι επικοινωνεί με την Αλίκη και τον Κώστα.

Ο αλγόριθμος που ακολουθείται από τον Μάκης είναι (Sun and Hsieh, 2003):

- Ο Μάκης επιλέγει δύο τυχαίου αριθμούς s και v, και υπολογίζει $T'_A = s * P$ και $T'_C = v * P$
- Ο Μάκης στέλνει στον Μπομπ τα $(T'_A, Cert_A)$, $(T'_C, Cert_C)$.
- Ο Μπομπ στέλνει στους υποτιθέμενους Αλίκη και Κώστα $(T_B, Cert_B)$.
- Η «Αλίκη», ο Μπομπ και ο «Κώστας» υπολογίζουν K'_A, K_B και K'_C αντίστοιχα και ισχύει ότι $K'_A = K_B = K'_C = \hat{e}(P,P)^{bysv\hat{e}(P,P)^{abc}}$.

Αλίκη	Κώστας	Μάκης	Μπομπ
Αποκτά από την έμπιστη αρχή το $Cert_A$	Αποκτά από την έμπιστη αρχή το $Cert_B$		Αποκτά από την έμπιστη αρχή το $Cert_C$

Επιλέγει a και υπολογίζει R_A Επιλέγει x και υπολογίζει T_A	Επιλέγει c και υπολογίζει R_C Επιλέγει z και υπολογίζει T_C		Επιλέγει b και υπολογίζει R_B Επιλέγει y και υπολογίζει T_B
Μετάδοση $(T_A, Cert_A)$ στους Μπομπ και Κώστας	Μετάδοση $(T_C, Cert_C)$ στους Μπομπ και Κώστας	Υποκλέπτει από τον Μπομπ τα $b, T_B, Cert_B, Cert_A$ και $Cert_C$	Μετάδοση $(T_B, Cert_B)$ στους Μπομπ και Κώστας
Τέλος συνεδρίας	Τέλος συνεδρίας	Τέλος συνεδρίας	Τέλος συνεδρίας
		Ξεκινά νέα συνεδρία υποδυόμενος στον Μπομπ ότι είναι η Αλίκη και ο Κώστας	
		Επιλέγει s και v και υπολογίζει T'_A και T'_C	Επιλέγει b και υπολογίζει R_B Επιλέγει y και υπολογίζει T_B
		Στέλνει $(T'_A, Cert_A)$, $(T'_C, Cert_C)$ στον Μπομπ	Στέλνει $(T_B, Cert_B)$ στους υποτιθέμενους Αλίκη και Κώστα
		Υπολογίζει τα K'_A, K'_C που είναι το κοινό κλειδί $K'_A = K'_C$	Υπολογίζει το κοινό κλειδί K_B

Πίνακας 7. Επίθεση πλαστοπροσωπίας με παραβίασει κλειδιού στο πρωτόκολλο Shim

Εσωτερική επίθεση:

Η εσωτερική επίθεση σε ένα τριμερές πρωτόκολλο ανταλλαγής κλειδιών σημαίνει ότι κάποια από τις οντότητες προσπαθεί να υποδυθεί οποιαδήποτε άλλη οντότητα (Lin and Lin, 2005). Για παράδειγμα, αν ο Μπομπ είναι ένας εσωτερικός επιτιθέμενος θα προσπαθήσει να υποδυθεί τον Κώστα (για να ξεγελάσει την Αλίκη) ότι αυτός και ο Κώστας ταυτόχρονα συμμετέχουν σε ένα πρωτόκολλο ανταλλαγής κλειδιών ενώ στην πραγματικότητα ο Κώστας δεν επικοινώνησε με κάποιον. Πιο αναλυτικά:

- Η Αλίκη, ο Μπομπ και ο Κώστας είναι νόμιμες οντότητες που χρησιμοποιούν το πρωτόκολλο.
- Τα $Cert_A, Cert_B$ και $Cert_C$ είναι τα πιστοποιητικά της Αλίκης, του Μπομπ και του Κώστα αντίστοιχα που έχουν πιστοποιηθεί από μια έμπιστη αρχή.
- Ο Μπομπ θέλει να υποδυθεί ότι είναι ο Κώστας στην Αλίκη το οποίο είναι εφικτό αφού έχει αποκτήσει το $Cert_C$.
- Ο Κώστας δεν γνωρίζει τίποτα γι' αυτό το γύρο επικοινωνίας.

Έτσι με αυτόν τον τρόπο ο Μπομπ μπορεί να ξεκινήσει το τριμερές πρωτόκολλο Shim και ταυτόχρονα να υποδύεται και τον Κώστα. Η Αλίκη φυσικά δεν μπορεί να αντιληφθεί ότι επικοινωνεί μόνο με τον Μπομπ και όχι με τον Μπομπ και τον Κώστα.

Ο αλγόριθμος που ακολουθεί ο Μπομπ είναι:

- Ο Μπομπ διαλέγει έναν τυχαίο αριθμό z' και υπολογίζει $T'_C = z' * R_C = z' * (c * P)$.
- Ο Μπομπ στέλνει στην Αλίκη και στον «Κώστα» $(T_B, Cert_B)$.
- Ο «Κώστας» στέλνει στην Αλίκη και στον Μπομπ $(T'_C, Cert_C)$.
- Η Αλίκη στέλνει στον Μπομπ και στον Κώστα $(T_A, Cert_A)$.
- Όλες οι οντότητες υπολογίζουν $K_A = K_B = K'_C = \hat{e}(P,P)^{abcxyz'\hat{e}(P,P)^{abc}}$.

Αλίκη	Μπομπ	«Κώστας»
	Κατέχει από προηγούμενη συνεδρία το πιστοποιητικό του Κώστα $Cert_C$	Είναι ο Μπομπ υποδυόμενος τον Κώστα
	Επιλέγει z' και υπολογίζει T_C'	
Στέλνει $(T_A, Cert_A)$ στον Μπομπ και στον «Κώστα»	Στέλνει $(T_B, Cert_B)$ στην Αλίκη και στον «Κώστα»	Στέλνει $(T_C', Cert_C)$ στην Αλίκη και στον Μπομπ
Υπολογίζει το κοινό κλειδί K_A	Υπολογίζει το κοινό κλειδί K_B	Υπολογίζει το κοινό κλειδί K_C'

Πίνακας 8. Εσωτερική επίθεση στο πρωτόκολλο Shim

5.4 Επιθέσεις στο πρωτόκολλο ABTKA

Στο ABTKA πρωτόκολλο παρατηρούνται μαθηματικές επιθέσεις. Υπάρχει ένας τύπος αντιπάλου που ενεργεί ως κακόβουλος χρήστης και μπορεί να αντικαταστήσει τα δημόσια κλειδιά οποιουδήποτε χρήστη με ένα δικό του επιθυμητό δημόσιο κλειδί. Ο αντίπαλος ελέγχει όλες τις επικοινωνίες μεταξύ των χρηστών και κάθε χρήστης απλώς απαντά στις ερωτήσεις του αντιπάλου και δεν μπορεί να στείλει ή να λάβει άμεσα ένα μήνυμα από τον άλλο χρήστη.

Ο αντίπαλος θέτει κάποια ερωτήματα στο προσομοιωτή S και η διαδικασία είναι η εξής:

- **Δημιουργία (U_X):** Ο αντίπαλος ζητά από τον προσομοιωτή S να δημιουργήσει έναν νέο χρήστη U_X με σύνολο χαρακτηριστικών W_X και το αντίστοιχο ιδιωτικό και δημόσιο κλειδί.
- **Δημόσιο Κλειδί (U_X):** Ο προσομοιωτής δημιουργεί το δημόσιο κλειδί P_X που αντιστοιχεί στο σύνολο χαρακτηριστικών W_X. Έστω το $P_X = \{P_i\}_{i \epsilon W_X}$ το δημόσιο κλειδί, το P_i είναι το αντίστοιχο δημόσιο κλειδί στο χαρακτηριστικό $i \epsilon W_X$.
- **Μερικό Ιδιωτικό Κλειδί (U_X):** Ο αντίπαλος λαμβάνει το μερικό ιδιωτικό κλειδί s_i για κάθε χαρακτηριστικό $i \epsilon W_X$.

- **Διαφθορά (U_X)**: Ο προσομοιωτής δίνει το ιδιωτικό κλειδί sk_i για κάθε χαρακτηριστικό $i \epsilon W_X$ στον αντίπαλο.
- **Αλλαγή Δημοσίου Κλειδιού (U_X, P'_X)**: Ο προσομοιωτής αντικαθιστά το δημόσιο κλειδί P_X με το P'_X για τον χρήστη U_X.
- **Αποστολή ($\Pi^n_{X,Y,Z}, M_1, M_2$)**: Ο αντίπαλος λαμβάνει την απάντηση για τα μηνύματα M_1, M_2.

Λήμμα 5.4.1 (Bayat and Reza Aref, 2015)

Έστω το πρωτόκολλο ABTKA. Εξαιτίας της δύσκολης λύσης του υπολογιστικού προβλήματος Diffie-Hellman στο πρωτόκολλο, το πλεονέκτημα του αντιπάλου είναι αμελητέο.

Απόδειξη

Υποθέτουμε ότι ο αντίπαλος μπορεί να σπάσει το πρωτόκολλο με μη αμελητέο πλεονέκτημα. Στη συνέχεια, δείχνουμε ότι μπορεί να κατασκευαστεί ένας προσομοιωτής S για την επίλυση του υπολογιστικού προβλήματος Diffie-Hellman. Έστω μια περίπτωση (lP, mP) του προβλήματος, και ο προσομοιωτής S θέλει να υπολογίσει το lmP. □

Ο προσομοιωτής S θέτει $P_0 = lP$ και ορίζει τις παραμέτρους του συστήματος $\{G_p,\ E,\ A,\ P,\ P_0, \{T_i\}_{i \epsilon U}, U\}$.. Έστω q_s ο μέγιστος αριθμός πιθανών συνόδων και q_c ο μέγιστος αριθμός χρηστών. Ο προσομοιωτής S επιλέγει τυχαία έναν χρήστη U_A με σύνολο χαρακτηριστικών W_A. Στη συνέχεια, ο S απαντά στα ερωτήματα του αντιπάλου ως εξής (Bayat and Reza Aref, 2015):

- **Δημιουργία (U_X):** Για να απαντήσει, ο S συντάσσει μια λίστα L_C που περιέχει $(U_X, \{R_i\}_{i \epsilon W_X}, s_X = \{s_i\}_{i \epsilon W_X}, \{\chi_{Xi}\}_{i \epsilon W_X}, P_X = \{P_{Xi}\}_{i \epsilon W_X})$.Οι συνιστώσες χ_{Xi} και P_{Xi}υπολογίζονται σύμφωνα με το πρωτόκολλο, αλλά ο υπολογισμός των s_i και R_i θα περιγραφεί παρακάτω.
- **Δημόσιο Κλειδί (U_X)**: Ο προσομοιωτής S αναζητά στη λίστα L_C και απαντά αυτό το ερώτημα.
- **Μερικό Ιδιωτικό Κλειδί (U_X)**: Εάν $|W_X \cap W_A| \geq d$, ο προσομοιωτής S σταματάει αλλιώς ορίζει τρία σύνολα $\Gamma = |W_X \cap W_A|$, ένα σύνολο $d-1$ στοιχείων θέτει Γ' τέτοιο ώστε $\Gamma \subseteq \Gamma' \subset W_X$ και $F = \Gamma' \cup \{0\}$. Τότε, ο S θέτει $q(i) = \lambda_i \epsilon Z_p^*$ για όλα τα χαρακτηριστικά $i \epsilon \Gamma'$. Σύμφωνα με αυτόν τον ορισμό, ο προσομοιωτής λαμβάνει στην πραγματικότητα $d-1$ σημεία του $q(x)$ και ένα σημείο είναι $q(0) = l$ τέτοιο ώστε $P_0 = lP$. Επομένως, ο S προσομοιώνει το μερικό ιδιωτικό κλειδί ως εξής:

- $i \epsilon \Gamma'$: Στην περίπτωση αυτή, ο S επιλέγει έναν τυχαίο αριθμό $r_i \epsilon Z_p^*$και προσομοιώνει το ακόλουθο μερικό ιδιωτικό κλειδί:

  $$s_i = \frac{\lambda_i}{r_i} + r_i$$

  ο S υπολογίζει $R_i = r_i T_i$
- $i \epsilon W_X \backslash \Gamma'$: Ο προσομοιωτής S επιλέγει ένα τυχαίο r_i' και υπολογίζει το μερικό ιδιωτικό κλειδί

  $s_i = \frac{\sum_{j \epsilon F \backslash \{0\}} \lambda_i \Delta_{j,F}(i)}{t_i} + r_i'$

  όπου

  $$r_i' = r_i + \frac{q(0)\Delta_{0,F}(i)}{t_i}$$

  Επομένως ο S εξάγει $R_i = r_i' t_i P + P_0 \Delta_{0,F}(i)$.

- **Διαφθορά (U_X)**: Εάν $|W_X \cap W_A| \geq d$, ο προσομοιωτής S σταματάει αλλιώς απαντά στο ερώτημα του αντιπάλου σύμφωνα με την λίστα L_C
- **Αλλαγή Δημοσίου Κλειδιού (U_X, P_X')**: Δεδομένης της λίστα L_C, ο προσομοιωτής S αντικαθιστά το $P_{Xi} \epsilon P_X$ με $P_{Xi}' \epsilon P_X'$ και θέτει όλα τα $\chi_{Xi} = null$ για κάθε $i \epsilon W_X$
- **Αποστολή ($\Pi_{X,Y,Z}^n, M_1, M_2$)**: Ο προσομοιωτής S ετοιμάζει μια λίστα L_S που περιέχει

  $$(\Pi_{X,Y,Z}^n, u_X^n, T_{XY1}^n, T_{XY2}^n, T_{XY3}^n, T_{XZ1}^n, T_{XZ2}^n, T_{XZ3}^n, P_X^n, P_Y^n, P_Z^n)$$

  Το P_X^nείναι το τρέχον δημόσιο κλειδί του χρήστη U_X και τα P_Y^n και P_Z^n είναι τα δημόσια κλειδιά των χρηστών U_Y και U_Z αντίστοιχα. Το u_X^n είναι ένας τυχαίος αριθμός που επέλεξε ο U_X σ αυτή την συνεδρία. Η απάντηση που θα δώσει ο S είναι η εξής:
  - Έστω $\Pi_{A,B,C}^T$ είναι μια δοκιμαστική συνεδρία. Αν $\Pi_{X,Y,Z}^T = \Pi_{A,B,C}^T$ τότε ο προσομοιωτής θέτει $u_X^n = null$, $T_{XY1}^n = mP$, $T_{XY2}^n = \{t_i mP\}_{i \epsilon W_B}$ και $T_{XY3}^n = \{r_i t_i mP\}_{i \epsilon W_B}$. Στο τέλος ο προσομοιωτής S ενημερώνει την λίστα L_S.
  - Αλλιώς, ο προσομοιωτής S επιλέγει ένα τυχαίο νούμερο $u_X^n \epsilon Z_n^*$ και εκτελεί το πρωτόκολλο με τον συνήθη τρόπο και στο τέλος ενημερώνει την λίστα L_S.

Αν τελικά ο αντίπαλος καταφέρει να υπολογίσει το κλειδί συνόδου με πιθανότητα ε, τότε ο προσομοιωτής μπορεί να λύσει το υπολογιστικό πρόβλημα του Diffie-Hellman με πιθανότητα τουλάχιστον $\varepsilon \times \frac{1}{q_C^2 q_S (q_S - 1)}$. Επειδή η πιθανότητα της επιλογής της δοκιμαστικής συνεδρίας είναι $\frac{1}{q_S(q_S-1)}$, οι U_B και U_C επιλέγονται με πιθανότητα $\frac{1}{q_C^2}$. Τέλος,

$K^1_{A,B,C} - bP_0 - cP_0$ είναι η λύση του υπολογιστικού προβλήματος Diffie-Hellman , με b και c να είναι δύο τυχαίοι αριθμοί που επιλέχθηκαν από τον προσομοιωτή S για να υπολογίσει τα M_1 και M_2 (Bayat and Reza Aref, 2015).

Κεφάλαιο 6

Συμπεράσματα

Σκοπός αυτής της διπλωματικής εργασίας είναι να μελετήσει επιλεγμένα πρωτόκολλα ανταλλαγής κλειδιών βασισμένα σε ελλειπτικές καμπύλες και σε ζευγισμούς ελλειπτικών καμπυλών καθώς και να εντοπίσει τις αδυναμίες των πρωτοκόλλων. Αναλυτικά, εντοπίστηκαν οι αδυναμίες που παρουσιάζουν τα πρωτόκολλα ενάντια σε επιθέσεις όπως η man in the middle και η εσωτερική επίθεση. Σ' αυτό το τελευταίο κεφάλαιο θα διατυπωθούν ορισμένα συμπεράσματα σχετικά με τα ερευνητικά ερωτήματα που αναφέρθηκαν στην Εισαγωγή.

Αδυναμίες των πρωτοκόλλων σε διάφορες επιθέσεις

Στα πρωτόκολλα που μελετήθηκαν στα προηγούμενα κεφάλαια εντοπίστηκαν κυρίως αδυναμίες απέναντι σε παθητικές επιθέσεις. Παθητική ορίζεται μια επίθεση όπου τα μηνύματα συλλέγονται αλλά δεν τροποποιούνται από τον αντίπαλο. Σε αντίθεση με τις ενεργητικές επιθέσεις όπου γίνεται συλλογή και τροποποίηση των μηνυμάτων στην παθητική επίθεση ο κακόβουλος παράγοντας απλά συλλέγει μηνύματα.

- Στο πρωτόκολλο Diffie-Hellman με ελλειπτικές καμπύλες εντοπίστηκε αδυναμία στην επίθεση man in the middle. Σύντομα αναφέροντας όταν η Αλίκη και ο Μπομπ έχουν ξεκινήσει μια συνεδρία με το πρωτόκολλο Diffie-Hellman νομίζουν ότι αντάλλαξαν τα κλειδιά μεταξύ τους και ότι δημιούργησαν το μυστικό κλειδί της συνόδου ενώ στην πραγματικότητα έχουν ανταλλάξει κλειδιά με τον Μάκη (middle man). Μ' αυτόν τον τρόπο ο Μάκης (middle man) συλλέγει όλες τις πληροφορίες που ανταλλάσσουν η Αλίκη και ο Μπομπ (κύριες οντότητες) χωρίς να το γνωρίζει κανένας από τους δύο χρήστες. Το πρόβλημα αυτό εκτιμάται αρκετά σοβαρό και συμβαίνει γιατί το πρωτόκολλο δεν χρησιμοποιεί κανενός είδους πιστοποίηση των χρηστών ώστε να επαληθεύεται ότι πίσω από κάθε ανταλλαγή κλειδιών είναι το σωστό άτομο και όχι κάποιος επιτιθέμενος.
- Το τριμερές πρωτόκολλο Joux, το οποίο έχει βασιστεί στο Diffie-Hellman πρωτόκολλο, είναι και αυτό αδύναμο απέναντι σε επιθέσεις man in the middle. Η διαδικασία είναι η ίδια με αυτή του πρωτοκόλλου Diffie-Hellman. Ο Μάκης ανταλλάσσει κλειδιά με την Αλίκη και τον Μπομπ ενώ οι ίδιοι πιστεύουν ότι έχουν ανταλλάξει μεταξύ τους. Έπειτα ο Μάκης παρακολουθεί όλη την συνεδρία εν αγνοία

της Αλίκης και του Μπομπ. Η αδυναμία του πρωτοκόλλου οφείλεται και πάλι στο γεγονός ότι τα κλειδιά που ανταλλάσσονται δεν πιστοποιούνται από μια έμπιστη αρχή για αποδεικνύεται η ταυτότητα του χρήστη.

- Το τριμερές πρωτόκολλο ανταλλαγής κλειδιών Shim προτάθηκε λίγα χρόνια μετά το Joux. Σε αυτό το πρωτόκολλο εντοπίστηκαν αδυναμίες σε δύο επιθέσεις, την επίθεση πλαστοπροσωπίας με παραβίαση κλειδιού και την εσωτερική επίθεση.
  - Η πρώτη επίθεση γίνεται όταν ο επιτιθέμενος θέλει να υποδυθεί έναν ή και δυο χρήστες στο πρωτόκολλο. Αρχικά επικοινωνεί με μία από τις οντότητες (π.χ. Μπομπ) και αφού υποκλέψει τα στοιχεία του (ιδιωτικό, δημόσιο κλειδί και πιστοποιητικό) υποδύεται στις υπόλοιπες οντότητες ότι είναι ο Μπομπ. Αφότου έχει στην κατοχή του οτιδήποτε χρειάζεται, εξαπατά τον Μπομπ υποδυόμενος ότι είναι η Αλίκη και ο Κώστας.
  - Στην εσωτερική επίθεση δεν υπάρχει εξωτερική οντότητα που επιτίθεται στο πρωτόκολλο, αλλά ένας από τους χρήστες θέλει να παριστάνει μια από τις υπόλοιπες οντότητες. Έστω ότι ο Μπομπ διαπράττει εσωτερική επίθεση, έχοντας το πιστοποιητικό του Κώστα είναι πολύ εύκολο να υποδύεται τον Κώστα αλλά και τον εαυτό του ταυτόχρονα στη Αλίκη. Δηλαδή, ξεκινά μια συνεδρία με την Αλίκη, τον Μπομπ και τον «Κώστα» εξαπατώντας την Αλίκη η οποία πιστεύει ότι επικοινωνεί με τον Μπομπ και τον πραγματικό Κώστα. Οι επιθέσεις αυτές οφείλονται στο γεγονός ότι είναι εύκολο να υποκλαπούν τα πιστοποιητικά των χρηστών.
- Στο τριμερές πρωτόκολλο ABTKA που προτάθηκε από τους Bayat και Reza το 2015, παρατηρούνται θεωρητικές επιθέσεις. Υπάρχει ο αντίπαλος ο οποίος αντικαταστεί τα δημόσια κλειδιά των χρηστών με δικά του δημόσια κλειδιά. Με αυτόν τον τρόπο μπορεί να ελέγχει όλες τις επικοινωνίες που πραγματοποιούνται από τους χρήστες. Επιπλέον ο αντίπαλος μπορεί να επέμβει σε κάθε μήνυμα ή πληροφορία, που αποστέλλεται από τους χρήστες. Ο αντίπαλος καταφέρνει να επέμβει στην επικοινωνία με την βοήθεια ενός προσομοιωτή, που τον βοηθά να επιλύσει το υπολογιστικό πρόβλημα του Diffie-Hellman.

<u>Σύγκριση των δύο ειδών πρωτοκόλλων σχετικά με την ασφάλεια τους</u>

Όλα τα πρωτόκολλα ανταλλαγής κλειδιών που μελετήθηκαν στα προηγούμενα κεφάλαια εμπεριέχουν αδυναμίες. Το πρωτόκολλο Diffie-Hellman με ελλειπτικές καμπύλες είναι ευάλωτο απέναντι στην man in the middle επίθεση επειδή δεν υπάρχει κάποιο μέσο

πιστοποίησης των χρηστών. Από τη άλλη το ένα πρωτόκολλο ανταλλαγής κλειδιών με ζευγισμούς Joux έχει ακριβώς την ίδια αδυναμία με το Diffie-Hellman ενώ το Shim είναι ευάλωτο σε επιθέσεις πλαστοπροσωπίας και εσωτερικές επιθέσεις. Το πρωτόκολλο ABTKA είναι ευάλωτο σε θεωρητικές μαθηματικές επιθέσεις όπως έχει μελετηθεί. Ο παρακάτω πίνακας απεικονίζει σε ποιες επιθέσεις είναι ευάλωτα τα παραπάνω πρωτόκολλα.

	Man in the middle	Πλαστοπροσωπία με παραβίαση κλειδιού	Εσωτερική επίθεση	Θεωρητική – Μαθηματική επίθεση
Diffie-Hellman	NAI	–	–	–
Joux	NAI	–	–	–
Shim	–	NAI	NAI	–
ABTKA	–	–	–	NAI

Πίνακας 9. Σύγκριση πρωτοκόλλων σε σχέση σε ποιες επιθέσεις είναι ευάλωτα.

Παρατηρείται ότι, δεν είναι εφικτό να επιλεχθεί ένα είδος πρωτοκόλλων ως πιο ασφαλές διότι, σε κάθε πρωτόκολλο βρέθηκαν αδυναμίες απέναντι σε διαφορετικές επιθέσεις ανάλογα το πρωτόκολλο. Επομένως ο εκάστοτε χρήστης δεν μπορεί να βασιστεί σε κάποιο συγκεκριμένο πρωτόκολλο (το οποίο βασίζεται ή όχι στους ζευγισμούς) το οποίο θα διασφαλίσει οικουμενικά την προστασία του απέναντι σε πιθανές επιθέσεις. Ως εκ τούτου η επιλογή του πρωτοκόλλου που θα χρησιμοποιηθεί σε κάθε περίσταση θα πρέπει να βασίζεται στις εκάστοτε συνθήκες και χαρακτηριστικά του περιβάλλοντος μέσα στο οποίο θα γίνει η χρήση του. Συνεπώς, η επιλογή του κατάλληλου πρωτοκόλλου πρέπει να γίνει από ατομική μελέτη της εκάστοτε περίπτωσης. Προσιδιάζει λοιπόν η επιλογή του κατάλληλου πρωτοκόλλου σε custom made πρωτόκολλο ασφαλείας για το συγκεκριμένο σύστημα επικοινωνίας στο Διαδίκτυο μελετώντας όλους τους παράγοντες.

Βάσει του παραπάνω συμπεράσματος, εκτιμάται πως δεν υπάρχει μοναδικό πρωτόκολλο που θα παρέχει ασφάλεια έναντι όλων των διαφορετικών επιθέσεων. Προτείνεται η περαιτέρω μελέτη του τρόπου των επιθέσεων έναντι των πρωτοκόλλων. Η μελέτη και η ανάλυση του τρόπου προσβολής της ασφάλειας έχει ως σκοπό την εξακρίβωση ορισμένων κοινών βασικών χαρακτηριστικών των επιθέσεων, τα οποία μπορούν να ληφθούν υπόψη και να αξιοποιηθούν

στην κατασκευή ενός νέου ανθεκτικότερου πρωτοκόλλου. Στη μελέτη αυτή σημαντικό ρόλο θα διαδραματίσει και η μελέτη των χαρακτηριστικών και των αδυναμιών των πρωτοκόλλων, που τα καθιστούν ευάλωτα απέναντι σε πιθανές επιθέσεις.

Βιβλιογραφία

Ξενόγλωσση

Al-Riyami, S. and Paterson, K. (2003). Tripartite authenticated key agreement protocols from pairings. *Cryptography an Coding LNCS 2898*. pp 332-359.

Allen, B. (2008). *Implementing several attacks on plain ElGamal encryption*. Iowa State University. MSc.

Boyd, C. , Mathuria, A. and Stebila, D. (2003). *Protocols for Authentication and Key Establishment.* Springer Verlag.

Bayat, M. and Reza, Aref M. (2015). An attribute- based tripartite key agreement protocol. *International Journal of Communication Systems*. pp 1419-1431.

Chalkias, K., Baldimtsi, F., Hristu-Varsakelis, D. and Stephanides, G. (2008). Two Types of Key-Compromise Impersonation Attacks against One-Pass Key Establishment Protocols. *ICETE , pp. 227-238*.

Cheng, Z., Vasiu, L. and Comley, R. (2004). Pairing-based one-round tripartite key agreement protocols. *School of Computing Science, Middlesex University White Hart Lane, London*.

Deavours, C. and Kruh, L. (1990) David A. Kahn, *Cryptology: Machines, History & Methods*. Artech House Publishers.

Diffie, W. and Hellman, M. (1976). New Direction in Cryptography. *IEEE Transactions on Information Theory*. vol. 22, no. 6, pp 644-654.

Duursma, I., Lee, H. S. (2005). A group key agreement protocol from pairings. *Applied Mathematics and Computation* pp 1451-1456.

Elakrat, M. A. and Jung, J. C. (2018). Development of field programmable gate array-based encryption module to mitigate man in the middle attack for nuclear power plant data communication network. *Nuclear Engineering and Technology* vol. 50, pp. 780-787.

Fotiadis, G. (2017). *Constructing Suitable Parameters for pairing-based Cryptography.* Ph.D. dissertation, Dept. Information and Communication Systems Engineering, Univ. of Aegean, Samos.

Fraleigh, J. (1967). *A first course in abstract algebra*. Addison-Wesley Publishing Company Inc. .

Joux, A. (2004). A one round protocol for tripartite Diffie- Hellman. *Journal of Cryptology International Association for Cryptologic Research.* vol. 17. pp 263-276

Kaabneh, K. and Al-Bdour, H. (2005). Key Exchange Protocol in Elliptic Curve Cryptography with No Public Point. *American Journal of Applied Sciences.* 2(8), pp 1232-1235.

Koblitz, N. Menezes, A. (2005). Pairing-based cryptography at high security levels. *Proceedings of the Tenth IMA International Conference on Cryptography and Coding, Lecture Notes in Computer Science.*

Lauter, K., Naehrig, M. (2017). Cryptographic pairings. *Topics in Computational Number Theory inspired by Peter L. Montgomery*, Joppe W. Bos and Arjen K. Lenstra, Cambridge University Press.

Lin, C. H. and Lin, H. H. (2005). Secure one-round tripartite authenticated key agreement protocol from Weil pairing. *Proceedings of the 19th International Conference on Advanced Information Networking and Applications.*

Meadows, C. (2003). Formal Methods for Cryptographic Protocol Analysis: Emerging Issues and Trends. *IEEE Journal on selected areas in communications*, vol. 21, no. 1, pp 44-54.

Meffert, D. (2009). Bilinear Pairings in Cryptography. *Master Thesis, Dept. Computing Science, Radboud Universiteit Nijmegen.*

Menezes, A. (2008). An introduction to pairing-based cryptography. *Mathematic Subject Classification.*

Pfleeger, C. (1989). *Security in Computing.* Prentice -Hall.

Rosenberg, J. (2017). Embedded Security. In Vega, A., Bose, P. and Buyuktosunoglu, A. (Eds). *Rugged Embedded Systems.* Elsevier Inc. All rights reserved. pp. e1-e74.

RSA Laboratories, (2000). *RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version4.1.* RSA Security Inc.

Schmidt, B. (2012). Formal analysis of key exchange protocols and physical protocols. *Dept. of Computer Science*, Zurich.

Shim, K. (2003). Efficient one round tripartite authenticated key agreement protocol from Weil pairing. *Electronics Letters*. vol. 39, no. 2, pp 208-209.

Smart, N. (2016). *Cryptography Made Simple*. Springer.

Sun, H. and Hsieh, B. (2003). Security Analysis of Shim's Authenticated Key Agreement Protocols from Pairings. *Department of Computer Science, National Tsing Hua University, Hsinchu, Taiwan, Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan*.

Trappe, W., Washington, L. (2006). *Introduction to Cryptography with Coding Theory*. Prentice Hall.

Vesterås, B. (2006). *Analysis of Key Agreement Protocols*. Unpublished: Gjøvik University College. MSc.

Wang, S., Cao, Z., Choo, K. K. R and Wang, L. (2009). An improved identity-based key agreement protocol and its security proof. *Information Sciences*. vol. 179, pp 307-318.

Wang, L. and Wyglinski, M., A. (2014). Detection of man-in -the -middle attacks using physical layer wireless security techniques. *Wireless Communications and Mobile Computing*. vol. 66, pp. 408-426.

Wong, D. (2021). *Real-World Cryptography*. Manning Publications.

Xiong H, Chen Z, Li F. (2012). Provably secure and efficient certificateless authenticated tripartite key agreement protocol. *Mathematical and Computer Modelling* vol. 55, pp. 1213–1221.

Ελληνική

Κάτος, Β., Στεφανίδης, Γ. (2003). *Τεχνικές κρυπτογραφίας και κρυπτανάλυσης*. Εκδόσεις Ζυγός.

Πουλάκης, Δ. (2015). *Άλγεβρα*. ΖΗΤΗ.

Πουλάκης, Δ. (1997). *Θεωρία Αριθμών Μια σύγχρονη θεώρηση της κλασικής θεωρίας αριθμών*. ΖΗΤΗ.