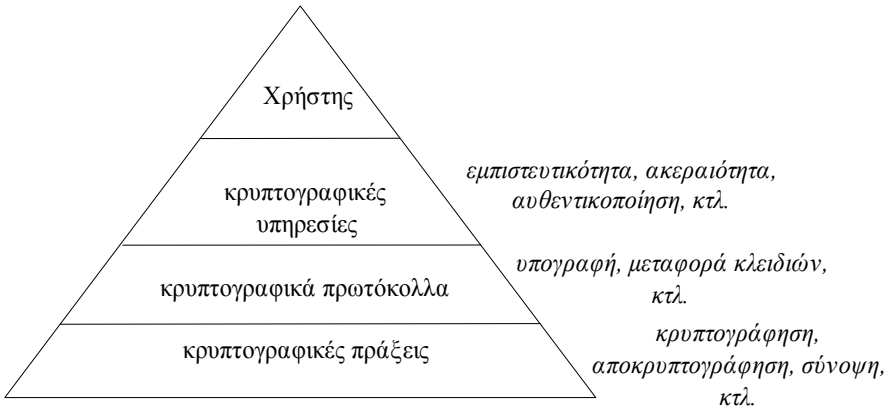
9 ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΠΡΩΤΟΚΟΛΛΑ

9.1. Εισαγωγή

Στο Κεφάλαιο 1, δώσαμε έναν ορισμό του πρωτοκόλλου. Είδαμε επίσης σε διάφορα σημεία του βιβλίου ότι προκειμένου να ολοκληρωθούν ορισμένες διαδικασίες, όπως η ανταλλαγή και εδραίωση κλειδιών, τα επικοινωνούντα μέλη ακολούθησαν κάποιο πρωτόκολλο. Στο κεφάλαιο αυτό θα ασχοληθούμε με κρυπτογραφικά πρωτόκολλα. Ένα κρυπτογραφικό πρωτόκολλο είναι ένα πρωτόκολλο το οποίο υλοποιείται με κρυπτογραφικούς μηχανισμούς.



Σχήμα 9.1 Κρυπτογραφικές πράξεις, πρωτόκολλα και υπηρεσίες.

Η ανάγκη χρησιμοποίησης κρυπτογραφικού πρωτοκόλλου φαίνεται στο Σχήμα 9.1. Ο χρήστης ενός συστήματος αντιλαμβάνεται την ασφάλεια με τη μορφή των κρυπτογραφικών υπηρεσιών (εμπιστευτικότητα, αυθεντικοποίηση, ακεραιότητα). Οι κρυπτογραφικές υπηρεσίες προσφέρονται με την υλοποίηση των κρυπτογραφικών πράξεων. Οι κρυπτογραφικές πράξεις όμως θα πρέπει να συνδυασθούν και να εκτελεσθούν με συγκεκριμένο τρόπο, προκειμένου να προσφέρουν τις επιθυμητές κρυπτογραφικές υπηρεσίες. Η περιγραφή με την οποία θα δράσουν οι κρυπτογρα-

φικές πράξεις βρίσκεται στο κρυπτογραφικό πρωτόκολλο. Επομένως, ένα κρυπτογραφικό πρωτόκολλο χαρακτηρίζεται από την αυστηρή περιγραφή του τρόπου λειτουργίας και δράσης των κρυπτογραφικών πράξεων, διότι όπως είδαμε σε πολλές περιπτώσεις, μια μικρή αλλαγή στη λειτουργία μιας κρυπτογραφικής πράξης μπορεί να έχει τεράστιες επιπτώσεις στην ασφάλεια.

Πολλές φορές ένα κρυπτογραφικό πρωτόκολλο παίρνει το όνομα της υπηρεσίας που παρέχει. Έτσι μπορούμε να έχουμε πρωτόκολλα αυθεντικοποίησης, ελέγχου ακεραιότητας, κοκ.

Ένα πρωτόκολλο έχει τα ακόλουθα χαρακτηριστικά (Pfleeger, 1989):

- Είναι καθορισμένο εκ των προτέρων. Δηλαδή ο σχεδιασμός ενός πρωτοκόλλου έχει ολοκληρωθεί προτού το πρωτόκολλο χρησιμοποιηθεί.
- Αμοιβαία συμφωνία. Όλα τα μέλη συμφωνούν να εκτελέσουν τα βήματα του πρωτοκόλλου με τη σειρά που υποδεικνύει το πρωτόκολλο.
- Σαφήνεια. Η εκτέλεση όλων των βημάτων του πρωτοκόλλου θα πρέπει να είναι σαφής, έτσι ώστε κανένα από τα μέλη να μην παρερμηνεύσει τα βήματα που του αναλογούν.
- Πληρότητα. Για οποιαδήποτε κατάσταση που μπορεί να βρεθεί οποιοδήποτε μέλος, θα πρέπει να υπάρχουν προκαθορισμένες ενέργειες.

9.2. Ο αντίπαλος

Εξετάζοντας την ασφάλεια ενός συστήματος στο επίπεδο των πρωτοκόλλων, ή έννοια του αντιπάλου είναι πιο διευρυμένη σε σχέση με τον αντίπαλο που επιτίθεται στις κρυπτογραφικές πράξεις. Το κρυπτογραφικό πρωτόκολλο παρέχει ένα σύνολο κανόνων με το οποίο θα γίνει ανταλλαγή και μετάδοση συγκεκριμένων πληροφοριών, ώστε να προστατευθεί το κάθε μέλος από τον αντίπαλο. Εκτός από τον αντίπαλο που συναντήσαμε συχνά να επιβλέπει ή να παρεμβαίνει στην επικοινωνία μεταξύ της Αλίκης και του Βύρωνα, υπάρχει και ο αντίπαλος που μπορεί να είναι η Αλίκη, ο Βύρων ή και οι δύο. Σε πολλές περιπτώσεις, η απειλή σε μια επικοινωνία είναι ένα ή περισσότερα από τα επικοινωνούντα μέλη. Ένα σύστημα επικοινωνίας δεν μπορεί να θεωρηθεί ασφαλές αν εμπιστεύεται όλα τα μέλη σε ανεξέλεγκτο βαθμό. Όταν η Αλίκη και ο Βύρων εκτελούν κάποια συναλλαγή από την οποία αναδεικνύεται σύγκρουση ενδιαφερόντων, τότε είναι σφάλμα το σύστημα συναλλαγής να εμπιστεύεται ότι η Αλίκη και ο Βύρων θα εκτελέσουν με συνέπεια τη συναλλαγή. Υπάρχει πληθώρα σεναρίων όπου η Αλίκη και ο Βύρων έρχονται σε διαφωνία και ο ένας προσπαθεί να εξαπατήσει τον άλλον. Μερικά παραδείγματα που παραθέσαμε στα προηγούμενα κεφάλαια είναι η πλαστογραφία της υπογραφής, η απάρνηση παραλαβής ενός μηνύματος και η απάρνηση αποστολής ενός μηνύματος.

ΟΡΙΣΜΟΣ 9.1 – Η κατάσταση όπου ένας αντίπαλος καταφέρνει, με κατάλληλο χειρισμό των μηχανισμών ενός πρωτοκόλλου, να καταστήσει το πρωτόκολλο αδύ-

ναμο στο να προσφέρει την κρυπτογραφική υπηρεσία, ονομάζεται ***αποτυχία πρωτοκόλλου*** (protocol failure).

Ο χειρισμός των μηχανισμών ενός πρωτοκόλλου αναφέρεται στην αυθαίρετη αλλαγή των μηνυμάτων που ανταλλάσσονται μεταξύ των μελών κατά τα διάφορα βήματα εκτέλεσης του πρωτοκόλλου. Συνεπώς, τα κρυπτογραφικά πρωτόκολλα εφαρμόζονται τόσο για την προστασία των επικοινωνούντων μελών από «εξωτερικούς» αντιπάλους, όσο και για την προστασία ενός μέλους, όταν τα άλλα μέλη δεν είναι έντιμα.

9.2.1. Ανάλυση των κρυπτογραφικών πρωτοκόλλων

Η ανάλυση των κρυπτογραφικών πρωτοκόλλων έχει στόχο τη διαπίστωση ότι το πρωτόκολλο έχει τη δυνατότητα να προσφέρει την υπηρεσία για την οποία είναι σχεδιασμένο να προσφέρει. Στη βιβλιογραφία υπάρχουν διάφορες τεχνικές ανάλυσης των κρυπτογραφικών πρωτοκόλλων, αλλά φυσικά η ανάλυση δεν περιορίζεται στις τεχνικές αυτές. Γενικά οι τεχνικές ανάλυσης συσχετίζουν το πρωτόκολλο με τους πόρους που απαιτείται να έχει ο αντίπαλος, προκειμένου να καταστήσει το πρωτόκολλο αδύναμο να προσφέρει την επιθυμητή υπηρεσία. Οι κυριότερες τεχνικές ανάλυσης πρωτοκόλλων είναι οι εξής (προσαρμογή από Menezes *et al.*):

- ανάλυση με βάση τη θεωρία της πληροφορίας. Η ανάλυση επικεντρώνεται στην πληροφορία που περιέχουν τα μηνύματα που ανταλλάσσουν τα μέλη που εκτελούν το πρωτόκολλο, τόσο μεταξύ τους, όσο και σε τρίτους. Ο αντίπαλος θεωρείται ότι έχει άπειρη υπολογιστική ισχύ, οπότε ένα πρωτόκολλο το οποίο αποδεικνύεται ασφαλές από πλευράς θεωρίας της πληροφορίας, δεχόμαστε ότι είναι ασφαλές άνευ όρων (unconditionally secure).
- ανάλυση με βάση τη θεωρία πολυπλοκότητας. Σύμφωνα με την ανάλυση αυτή, ο αντίπαλος αναλύεται ως προς την υπολογιστική ισχύ και το χρόνο που απαιτείται για να καταρρίψει ένα πρωτόκολλο. Έτσι ένα πρωτόκολλο θεωρείται υπολογιστικά ασφαλές, αν ο αντίπαλος δεν μπορεί να αντεπεξέλθει στους πόρους που απαιτούνται (ισχύς, χρόνος) για να καταρρίψει το πρωτόκολλο.
- αναγωγή σε «δύσκολα» προβλήματα. Η ανάλυση αυτή σχετίζεται με την αναγωγή ασφάλειας του πρωτοκόλλου σε ισοδύναμα δύσκολα προβλήματα. Με την τεχνική ανάλυσης με αναγωγή, ένα πρωτόκολλο θεωρείται αποδείξιμα ασφαλές (provably secure).
- τυπική ανάλυση. Η τυπική ανάλυση των πρωτοκόλλων περιλαμβάνει εργαλεία ανάλυσης τα οποία είναι κατασκευασμένα ειδικά για τη συγκεκριμένη εργασία. Τα εργαλεία ανάλυσης αποτελούνται από μια γλώσσα ανάλυσης των πρωτοκόλλων και από ένα λογικό μοντέλο. Το πρωτόκολλο μοντελοποιείται και περιγράφεται με τη γλώσσα ανάλυσης και στη συνέχεια εξετάζονται με μια σειρά λογικών κανόνων αν το πρωτόκολλο δύναται να προσφέρει την επιθυμητή υπηρεσία και σε ποιο βαθμό. Ένα από τα

πιο επιτυχημένα λογικά μοντέλα ανάλυσης είναι το μοντέλο των Burrows, Abadi και Needham, το οποίο ονομάζεται **λογική BAN**, από τα αρχικά των δημιουργών του. Η λογική BAN αναλύει το πρωτόκολλο με βάση την πίστη και τη γνώση των μελών για κάποια κατάσταση.

9.3. Κατηγορίες πρωτοκόλλων

Τα πρωτόκολλα χωρίζονται σε τρεις κατηγορίες με βάση την ικανότητα προσφοράς της υπηρεσίας, σε σχέση με την απαίτηση συμμετοχής τρίτης οντότητας. Οι κατηγορίες αυτές είναι ονομαστικά:

- Αυτοεπιβαλλόμενα πρωτόκολλα (self enforcing protocols).
- Πρωτόκολλα με δικαστή (adjudicated protocols).
- Πρωτόκολλα με διαιτητή (arbitrated protocols).

Από τις τρεις κατηγορίες πρωτοκόλλων, τα αυτοεπιβαλλόμενα πρωτόκολλα δεν απαιτούν τρίτη οντότητα, σε αντίθεση με τα άλλα δύο τα οποία βασίζονται στη συμμετοχή μιας τρίτης οντότητας.

Τα αυτοεπιβαλλόμενα πρωτόκολλα είναι τα πιο επιθυμητά από τα τρία, καθότι εκτελούνται μεταξύ των επικοινωνούντων μελών και δε βασίζονται στην εμπιστοσύνη τρίτων, χαρακτηρίζονται δε από μεγάλη ταχύτητα εκτέλεσης. Τα αυτοεπιβαλλόμενα πρωτόκολλα έχουν έμφυτους μηχανισμούς οι οποίοι εγγυώνται αμεροληψία, δίνοντας τη δυνατότητα στα επικοινωνούντα μέλη να ανιχνεύσουν αν κάποιο από αυτά επιχειρήσει απάτη.

Σε πολλές περιπτώσεις τα αυτοεπιβαλλόμενα πρωτόκολλα δεν μπορούν να εφαρμοστούν στην πράξη και έτσι απαιτείται τρίτη οντότητα προκειμένου να λυθεί η διαμάχη. Τα πρωτόκολλα με δικαστή έχουν το χαρακτηριστικό να παρέχουν αρκετά στοιχεία ώστε μια τρίτη οντότητα που παίζει το ρόλο του δικαστή να μπορεί να αποφασίσει πιο από τα μέλη διέπραξε την απάτη. Στα πρωτόκολλα με δικαστή δε συμμετέχει η τρίτη οντότητα κατά την εκτέλεσή τους. Η τρίτη οντότητα καλείται να συμμετάσχει μόνον όταν υπάρξει διαφωνία μεταξύ των επικοινωνούντων μελών. Τα πρωτόκολλα με δικαστή θα πρέπει να έχουν τη δυνατότητα τα στοιχεία τα οποία παρουσιάζονται στο δικαστή να μην μπορούν να τροποποιηθούν χωρίς αυτό να γίνει αντιληπτό. Τα στοιχεία θα πρέπει να δίνουν τη δυνατότητα στο δικαστή να διακρίνει όχι μόνον αν διαπράχθηκε απάτη, αλλά και να αναγνωρίσει το μέλος το οποίο διέπραξε την απάτη.

Τέλος, τα πρωτόκολλα με διαιτητή είναι αυτά στα οποία η τρίτη οντότητα συμμετέχει κατά τη διάρκεια εκτέλεσης του πρωτοκόλλου. Η συμμετοχή τρίτου κατά τη διάρκεια εκτέλεσης του πρωτοκόλλου έχει σαν αποτέλεσμα τη χαμηλή ταχύτητα εκτέλεσης του πρωτοκόλλου, που είναι και το βασικό μειονέκτημα της κατηγορίας αυτής. Σε δίκτυα υπολογιστών όπου χρησιμοποιείται κάποιος server ως διαιτητής, μπορεί να υπάρξει αισθητή μείωση στην απόδοση, αν η υπηρεσία του διαιτητή χρησιμοποιείται με μεγάλη συχνότητα.

9.4. Παραδείγματα κρυπτογραφικών πρωτοκόλλων

Στη βιβλιογραφία υπάρχει μεγάλος αριθμός κρυπτογραφικών πρωτοκόλλων. Ουσιαστικά κάθε πρόβλημα που απαιτεί συμφωνία ή δέσμευση δύο ή περισσοτέρων μελών μπορεί να εκφρασθεί με κάποιο πρωτόκολλο. Στη συνέχεια θα εξετάσουμε τα πιο δημοφιλή από αυτά.

9.4.1. «Νοερό πόκερ»

Το πρωτόκολλο του νοερού πόκερ μπορεί να χρησιμοποιηθεί όταν απαιτείται να σταλεί ένα μήνυμα κρυπτογραφημένο, χωρίς να προηγηθεί στάδιο εδραίωσης κλειδιού. Μάλιστα με το πρωτόκολλο του νοερού πόκερ δεν υπάρχει καμία μεταφορά κλειδιών από το ένα μέλος στο άλλο. Το όνομα του πρωτοκόλλου καθιερώθηκε από τον τίτλο της δημοσίευσης της μεθόδου ("Mental Poker") από τους Shamir, Rivest και Adleman.

Η αρχή του νοερού πόκερ είναι απλή. Το πρωτόκολλο απαιτεί τη χρήση ενός κρυπταλγόριθμου όπου η ισχύει η μεταβατική ιδιότητα για την κρυπτογράφηση και αποκρυπτογράφηση. Έστω ότι η Αλίκη επιθυμεί να διαβιβάσει εμπιστευτικά ένα μήνυμα στον Βύρωνα. Αρχικά, κρυπτογραφεί το μήνυμα με το δικό της κλειδί. Στη συνέχεια στέλνει το κρυπτογραφημένο μήνυμα στον Βύρωνα. Ο Βύρων κρυπτογραφεί το κρυπτοκείμενο που έλαβε με το δικό του κλειδί και στέλνει το αποτέλεσμα στην Αλίκη. Η Αλίκη απομακρύνει το κλειδί της από το κρυπτοκείμενο που παρέλαβε. Λόγω της μεταβατικής ιδιότητας, το αποτέλεσμα που προκύπτει θα είναι το αρχικό μήνυμα της Αλίκης κρυπτογραφημένο με το κλειδί του Βύρωνα. Η Αλίκη στέλνει το κρυπτοκείμενο στον Βύρωνα, ο οποίος το αποκρυπτογραφεί, ανακτώντας έτσι το μήνυμα της Αλίκης σε μορφή απλού κειμένου.

Η αρχή που περιγράψαμε μπορεί να εφαρμοσθεί για να μοιρασθούν ψηφιακά φύλλα τράπουλας μεταξύ της Αλίκης και του Βύρωνα μέσω ενός καναλιού επικοινωνίας, καθώς δεν βρίσκονται στην ίδια φυσική τοποθεσία. Το πρωτόκολλο έχει ως εξής:

1. Η Αλίκη και ο Βύρων επιλέγουν την ψηφιακή τράπουλα. Το κάθε φύλλο αντιστοιχεί σε κάποιο μήνυμα. Η τράπουλα είναι ένα σύνολο $\boldsymbol{T} = \{x_1, x_2, \ldots, x_{52}\}$, με μια συνάρτηση o: $\boldsymbol{O} \rightarrow \boldsymbol{T}$, η οποία είναι 1 – 1, με $\boldsymbol{O}$ ={"♠Α", "♠2", "♠3", …, "♦Q", "♦K"} και φυσικά $|\boldsymbol{O}| = |\boldsymbol{T}| = 52$.
2. Η Αλίκη κρυπτογραφεί όλα τα μηνύματα και «ανακατεύει» την τράπουλα. Το ανακάτεμα γίνεται επιλέγοντας μια αναδιάταξη των στοιχείων του συνόλου $\boldsymbol{T}$. Έστω $\boldsymbol{U_{ka}}$ η αναδιάταξη των στοιχείων του $\boldsymbol{T}$, κρυπτογραφημένα με το κλειδί της Αλίκης *ka*.

   Αλίκη → Βύρων: $\boldsymbol{U_{ka}}$

3. Ο Βύρων επιλέγει τυχαία 10 φύλλα από το σύνολο των κρυπτογραφημένων φύλλων $\boldsymbol{U_{ka}}$. Στη συνέχεια κρυπτογραφεί 5 από αυτά με το δικό του κλειδί *kb*. Έτσι προκύπτουν δύο σύνολα, ένα υποσύνολο του $\boldsymbol{U_{ka}}$ και ένα

σύνολο όπου 5 στοιχεία του $\boldsymbol{U_{ka}}$ τα οποία είναι κρυπτογραφημένα διπλά. Έστω $\boldsymbol{V_{ka}}$ το υποσύνολο του $\boldsymbol{U_{ka}}$ και $\boldsymbol{W_{ka.kb}}$ το σύνολο των 5 στοιχείων του $\boldsymbol{U_{ka}}$ που έχουν κρυπτογραφηθεί με το κλειδί του Βύρωνα.

Βύρων → Αλίκη: $\boldsymbol{U_{ka}}$, $\boldsymbol{W_{ka.kb}}$

4. Η Αλίκη αποκαλύπτει τα φύλλα της στον εαυτό της αποκρυπτογραφώντας τα στοιχεία του $\boldsymbol{U_{ka}}$ και εξακριβώνει ότι ο Βύρων δεν έκανε κρυπτογραφικές αλλαγές στο περιεχόμενό του. Στη συνέχεια αποκρυπτογραφεί τα στοιχεία του $\boldsymbol{W_{ka.kb}}$, αφαιρώντας με αυτόν τον τρόπο το κλειδί της, *ka*. Έστω το $\boldsymbol{W_{kb}}$ σύνολο που προκύπτει.

Αλίκη → Βύρων: $\boldsymbol{W_{kb}}$

5. Ο Βύρων αποκαλύπτει τα φύλλα του στον εαυτό του αποκρυπτογραφώντας τα στοιχεία του $\boldsymbol{W_{kb}}$ και εξακριβώνει ότι η Αλίκη δεν έκανε κρυπτογραφικές αλλαγές στο περιεχόμενό του. Η εξακρίβωση επιτυγχάνεται εφαρμόζοντας την αντίστροφη o^{-1}: $\boldsymbol{T} \rightarrow \boldsymbol{O}$, η οποία ορίζεται μόνον αν ακολουθήθηκαν οι κρυπτογραφήσεις όπως ορίζει το πρωτόκολλο.

Η δυνατότητα ανίχνευσης από τη συνάρτηση αντιστοίχισης $o(\ )$, προϋποθέτει ότι το κρυπτοσύστημα επιτρέπει μεγάλη περίσσεια έτσι ώστε οποιαδήποτε αυθαίρετη αλλαγή ενός μηνύματος-φύλλου να έχει σαν αποτέλεσμα η τελική αποκρυπτογράφηση να δώσει μήνυμα το οποίο να είναι εκτός του συνόλου $\boldsymbol{T}$.

Υλοποίηση με ασύμμετρη κρυπτογραφία

Το πρωτόκολλο του νοερού πόκερ μπορεί να υλοποιηθεί με μια τροποποίηση του κρυπτοσυστήματος RSA. Η Αλίκη και ο Βύρων συμφωνούν σε έναν πρώτο αριθμό p ο οποίος θα είναι το κοινό modulus. Στη συνέχεια το κάθε μέλος υπολογίζει τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης. Αναλυτικότερα, η Αλίκη επιλέγει έναν ακέραιο e και στη συνέχεια υπολογίζει τον d έτσι ώστε $ed \equiv 1 \bmod (p - 1)$. Παρόμοια, ο Βύρων επιλέγει έναν ακέραιο u και στη συνέχεια υπολογίζει τον v έτσι ώστε $uv \equiv 1 \bmod (p - 1)$.

Θα περιγράψουμε το πρωτόκολλο για ένα μήνυμα, καθώς η διαδικασία μπορεί να επαναληφθεί για οποιονδήποτε αριθμό μηνυμάτων. Έστω ότι το μήνυμα που θα σταλεί στον Βύρωνα είναι το m *όπου* $1 < m < p$. Το πρωτόκολλο έχει ως εξής:

Αλίκη → Βύρων: $m^e \bmod p$
Βύρων → Αλίκη: $(m^e)^u \bmod p$
Αλίκη → Βύρων: $(m^{eu})^{\mathrm{d}} \equiv \mathrm{m}^{\mathrm{u}} \pmod p$
Βύρων: $(m^u)^v \equiv m \pmod p$

Η διαφορά με το κρυπτοσύστημα RSA είναι ότι το modulo δε χρειάζεται να είναι γινόμενο δύο πρώτων αριθμών, επειδή κανένας από τους δύο δε δημοσιεύει τα

κλειδιά του. Φυσικά, στην περίπτωση που κάποιο από τα κλειδιά e, d, u, v πέσει στα χέρια του αντιπάλου, ο αντίπαλος θα μπορέσει να υπολογίσει το αντίστοιχο αντίστροφο κλειδί αφού ο p είναι γνωστός, οπότε είναι και ο $p - 1$.

9.4.2. Bit πρωτόκολλα δέσμευσης

Τα bit πρωτόκολλα δέσμευσης (bit commitment protocols) χρησιμοποιούνται για να δεσμεύσουν κάποιο μέλος που έχει πάρει κάποια απόφαση, με τη δυνατότητα αποκάλυψης της πληροφορίας στο μέλλον. Για παράδειγμα, η Αλίκη μπορεί να δώσει μια δεσμευτική τιμή στον Βύρωνα για κάποια αγορά, χωρίς όμως να θέλει να αποκαλύψει πρόωρα την τιμή στον Βύρωνα.

Η αρχή του πρωτοκόλλου δέσμευσης είναι η εξής. Η Αλίκη κατασκευάζει ένα ψηφιακό χρηματοκιβώτιο στο οποίο εσωκλείει το μήνυμα δέσμευσης. Στη συνέχεια, στέλνει το χρηματοκιβώτιο στον Βύρωνα, χωρίς όμως να αποκαλύψει το κλειδί. Τη στιγμή της αποδέσμευσης στέλνει το κλειδί στον Βύρωνα ο οποίος μπορεί να ανοίξει το χρηματοκιβώτιο και να επαληθεύσει το μήνυμα της Αλίκης. Είναι προφανές ότι μια κρυπτογραφική πράξη από μόνη της δε μπορεί να εκτελέσει δέσμευση, διότι για κάθε κλειδί το αποτέλεσμα που προκύπτει θα είναι διαφορετικό. Για αυτόν το λόγο χρησιμοποιήθηκε ο όρος «χρηματοκιβώτιο», το οποίο προστατεύει τόσο την Αλίκη, όσο και τον Βύρωνα, από την αυθαίρετη παρέμβαση της Αλίκης. Ένα χρηματοκιβώτιο ανοίγει με ένα και μόνο κλειδί (θεωρητικά), ενώ οποιοδήποτε άλλο κλειδί είναι άχρηστο. Έτσι και στα πρωτόκολλα δέσμευσης η Αλίκη είναι υποχρεωμένη να αποκαλύψει το σωστό κλειδί.

Υλοποίηση με συμμετρική κρυπτογραφία

Το πρωτόκολλο δέσμευσης μπορεί να υλοποιηθεί με συμμετρικό κρυπταλγόριθμο ως εξής. Έστω b το bit δέσμευσης της Αλίκης. Αρχικά ο Βύρων επιλέγει ένα τυχαίο μήνυμα m και το στέλνει στην Αλίκη:

Βύρων $\rightarrow$ Αλίκη: m

Στη συνέχεια η Αλίκη επιλέγει ένα μυστικό κλειδί k και με το συμμετρικό κρυπταλγόριθμο κρυπτογραφεί το μήνυμα του Βύρωνα μαζί με το bit δέσμευσης. Το αποτέλεσμα στέλνεται στον Βύρωνα:

Αλίκη $\rightarrow$ Βύρων: $c = e_k(m \,||\, b)$

Κατά το στάδιο αποκάλυψης της δέσμευσης, η Αλίκη στέλνει το κλειδί k στον Βύρωνα, ο οποίος μπορεί πλέον να αποκρυπτογραφήσει το κρυπτοκείμενο c που περιέχει τη δέσμευση:

Βύρων: $d_k(c) = m \,||\, b$

Αν το πρώτο τμήμα του απλού κειμένου είναι ίσο με το μήνυμα του Βύρωνα που έστειλε στην Αλίκη κατά την έναρξη του πρωτοκόλλου, τότε ο Βύρων μπορεί να εμπιστευθεί ότι η δέσμευση της Αλίκης είναι το *b*.

Υλοποίηση με ασύμμετρη κρυπτογραφία

Χρησιμοποιώντας ασύμμετρη κρυπτογραφία, ένα πρωτόκολλο δέσμευσης μπορεί να υλοποιηθεί με τετραγωνικά κατάλοιπα ή να βασιστεί στο πρόβλημα του διακριτού λογάριθμου.

Στην περίπτωση υλοποίησης με τετραγωνικά κατάλοιπα, έστω το σύνολο $\boldsymbol{Z}_n^*$, όπου *n* μεγάλος ακέραιος. Η Αλίκη και ο Βύρων συμφωνούν σε ένα στοιχείο $y \in \boldsymbol{Z}_n^*$, το οποίο δεν είναι τετραγωνικό κατάλοιπο. Στη συνέχεια η Αλίκη επιλέγει ένα στοιχείο $x \in \boldsymbol{Z}_n^*$ και υπολογίζει το τετραγωνικό κατάλοιπο $x^2 \bmod n$ και στέλνει το στοιχείο *g* στον Βύρωνα, όπου:

$$g = \begin{cases} x^2 \bmod n, & \text{δέσμευση σε } \mathbf{0} \\ yx^2 \bmod n, & \text{δέσμευση σε } \mathbf{1} \end{cases},$$

δηλαδή το στοιχείο το οποίο είναι τετραγωνικό κατάλοιπο υποδηλώνει **0**, ενώ στο στοιχείο το οποίο δεν είναι τετραγωνικό κατάλοιπο υποδηλώνει **1**. Ο Βύρων δεν είναι σε θέση να διακρίνει τη δομή του *g*. Κατά το στάδιο της αποκάλυψης, η Αλίκη γνωστοποιεί το *x* στον Βύρωνα.

Στην περίπτωση υλοποίησης με βάση το διακριτό λογάριθμο, η Αλίκη και ο Βύρων αρχικά συμφωνούν σε έναν πρώτο αριθμό *p*, σε έναν ακέραιο $a \in \boldsymbol{Z}_p^*$, ο οποίος είναι γεννήτορας του πεπερασμένου πεδίου, και ένα στοιχείο $s \in \boldsymbol{Z}_p^*$, του οποίου ο διακριτός λογάριθμος δεν είναι γνωστός. Η δέσμευση της Αλίκης εκφράζεται από το:

$$g = \begin{cases} a^x \bmod n, & \text{δέσμευση σε } \mathbf{0} \\ sa^x \bmod n, & \text{δέσμευση σε } \mathbf{1} \end{cases}$$

Ο Βύρων δεν είναι σε θέση να διακρίνει τη μορφή του *g*. Κατά το στάδιο της αποκάλυψης, η Αλίκη γνωστοποιεί το *x* στον Βύρωνα, ο οποίος μπορεί να ελέγξει με υπολογιστική ευκολία αν $g = a^x$ ή $g = sa^x$.

Υλοποίηση με μονόδρομες συναρτήσεις

Τέλος, η υλοποίηση του πρωτοκόλλου δέσμευσης γίνεται με κρυπτογραφικές μονόδρομες συναρτήσεις. Η συγκεκριμένη υλοποίηση δεν απαιτεί κανέναν αρχικό υπολογισμό, παρά μόνο φυσικά την επιλογή της μονόδρομης συνάρτησης που θα υποστηρίξει το πρωτόκολλο.

Έστω ότι η Αλίκη θέλει να δεσμευτεί με την τιμή *x*. Χρησιμοποιώντας την κρυπτογραφική μονόδρομη *h*( ), υπολογίζει τη σύνοψη της δέσμευσης:

$y = h(x)$.

Στη συνέχεια, στέλνει στον Βύρωνα την ποσότητα y. Κατά το στάδιο της αποκάλυψης η Αλίκη στέλνει το x, οπότε και ο Βύρων μπορεί να υπολογίσει το $h(x)$. Είναι σημαντικό η κρυπτογραφική μονόδρομη να παρουσιάζει ανθεκτικότητα σε συγκρούσεις. Θα πρέπει δηλαδή να είναι υπολογιστικά αδύνατο η Αλίκη να ανακαλύψει τιμή $x' \neq x$, τέτοια ώστε $h(x') = h(x)$.

9.4.3. Ρίψη κέρματος

Η ρίψη κέρματος είναι μια ενέργεια γνωστή σε όλους μας. Το χαρακτηριστικό της είναι ότι οι εμπλεκόμενοι σε μια ρίψη κέρματος θα πρέπει να είναι φυσικά παρόντες στο χώρο όπου πραγματοποιείται η ρίψη, αλλιώς υπάρχει κίνδυνος μεροληψίας.

Στην περίπτωση που οι εμπλεκόμενοι δεν είναι δυνατό να είναι παρόντες, η ρίψη μπορεί να γίνει μέσω τηλεφώνου, ηλεκτρονικού ταχυδρομείου, ή οποιουδήποτε καναλιού επικοινωνίας και η αμεροληψία μπορεί να υποστηριχθεί με κρυπτογραφία.

Η ρίψη κέρματος είναι μια ειδική περίπτωση δέσμευσης bit. Η Αλίκη πραγματοποιεί τη ρίψη του κέρματος και στη συνέχεια ο Βύρων μαντεύει το αποτέλεσμα. Το πρωτόκολλο δεσμεύει τη ρίψη της Αλίκης έτσι ώστε μετά την απάντηση του Βύρωνα, να μην μπορεί η Αλίκη να αλλάξει την επιλογή προκειμένου να επιτύχει ευνοϊκό αποτέλεσμα για τον εαυτό της.

Υλοποίηση με μονόδρομες συναρτήσεις

Η ρίψη κέρματος πραγματοποιείται με μονόδρομες συναρτήσεις ως εξής. Αρχικά, η Αλίκη και ο Βύρων συμφωνούν στην αντιστοιχία του λιγότερου σημαντικού bit των μηνυμάτων με την πλευρά του νομίσματος. Έστω ότι όλα τα μηνύματα τα οποία είναι περιττοί αριθμοί αντιστοιχούν στην «κορώνα» του νομίσματος. Όπως είναι γνωστό, στους περιττούς αριθμούς το λιγότερο σημαντικό bit της δυαδικής τους απεικόνισης είναι ίσο με **1**. Αντίστοιχα, ο άρτιοι αριθμοί έχουν το λιγότερο σημαντικό bit ίσο με **0** και παριστάνουν τα «γράμματα» του νομίσματος.

Μετά από τη συμφωνία αναπαράστασης, η Αλίκη επιλέγει τυχαία έναν αριθμό x και υπολογίζει τη σύνοψη αυτού, $y = h(x)$. Στη συνέχεια στέλνει τη σύνοψη στον Βύρωνα.

Ο Βύρων, μόλις παραλάβει τη σύνοψη, προχωράει στην επιλογή της πλευράς του νομίσματος, την οποία ανακοινώνει στην Αλίκη. Μόλις η Αλίκη λάβει την επιλογή του Βύρωνα, του αποκαλύπτει τον αριθμό x.

Υλοποίηση με θεωρία αριθμών

Η υλοποίηση της ρίψης κέρματος με μονόδρομες συναρτήσεις βασίζεται στο γεγονός ότι η Αλίκη γνωρίζει μια μερική λύση στην αντιστροφή της μονόδρομης συνάρτησης, η οποία δεν είναι γνωστή στον Βύρωνα. Δηλαδή, η αντιστροφή μιας

μονόδρομης συνάρτησης είναι «δύσκολο» πρόβλημα. Ασφαλώς η Αλίκη δεν αντιμετωπίζει δυσκολία στο να αντιστρέψει το $h(x)$, *αν* επιλέξει πρώτα το x. Για αυτόν το λόγο θεωρούμε ότι η αντιστροφή μιας μονόδρομης συνάρτησης είναι «δύσκολο» πρόβλημα για την πλειοψηφία των τιμών της συνάρτησης.

Με βάση την παραπάνω αρχή μπορούμε να εκμεταλλευτούμε τα δύσκολα προβλήματα της θεωρίας αριθμών. Ένα από τα πιο δημοφιλή δύσκολα προβλήματα είναι η παραγοντοποίηση μεγάλων σύνθετων ακεραίων. Η ρίψη κέρματος με βάση το πρόβλημα αυτό μπορεί να υλοποιηθεί ως εξής.

Για να δεσμευτεί η Αλίκη στο δυαδικό **0**, επιλέγει δύο μεγάλους πρώτους αριθμούς p και q, με τα ακόλουθα χαρακτηριστικά:

- $p < q$,
- $p \equiv 1 \pmod 4$,
- $q \equiv 3 \pmod 4$.

Για να δεσμευτεί η Αλίκη στο δυαδικό **1**, οι πρώτοι αριθμοί που επιλέγει θα πρέπει να έχουν τα ακόλουθα χαρακτηριστικά:

- $p < q$,
- $p \equiv 3 \pmod 4$,
- $q \equiv 1 \pmod 4$.

Στη συνέχεια υπολογίζει το γινόμενό τους $n = pq$, το οποίο στέλνει στον Βύρωνα.

Στη συνέχεια ο Βύρων επιλέγει την πλευρά του κέρματος (**1** ή **0**) και ανακοινώνει την επιλογή του στην Αλίκη, η οποία με τη σειρά της αποκαλύπτει τους παράγοντες του n στον Βύρωνα. Ο Βύρων μπορεί να εξακριβώσει με ευκολία αν οι παράγοντες που ανακοίνωσε η Αλίκη είναι του n, καθώς και να ελέγξει ποιος από τους δύο είναι ισότιμος με 1 (mod 4) και ποιος είναι ισότιμος με 3 (mod 4).

Η διαφορά της υλοποίησης με θεωρία αριθμών από την υλοποίηση με κρυπτογραφικές μονόδρομες hash είναι ότι στην περίπτωση της θεωρίας αριθμών το σύστημα είναι οριακά υπέρ του Βύρωνα, ενώ στην περίπτωση της μονόδρομης hash το σύστημα είναι οριακά υπέρ της Αλίκης. Χρησιμοποιούμε τον όρο «οριακά» γιατί ο σκοπός του πρωτοκόλλου είναι να προσφέρει αμεροληψία στη ρίψη του κέρματος. Ωστόσο, στην περίπτωση της μονόδρομης hash, η Αλίκη έχει θεωρητικά τη δυνατότητα να επιχειρήσει να ανακαλύψει συγκρούσεις οι οποίες να συνοψίζουν έναν άρτιο και έναν περιττό αριθμό στην ίδια τιμή. Στην περίπτωση της υλοποίησης με βάση το πρόβλημα της παραγοντοποίησης, από τη στιγμή που η Αλίκη στείλει το γινόμενο n στον Βύρωνα, δεν έχει τη δυνατότητα να αλλάξει το αποτέλεσμα, έστω και αν διαθέτει άπειρη υπολογιστική ισχύ.

9.4.4. Μεταφορά εν αγνοία

Τα πρωτόκολλα ρίψης κέρματος που παρουσιάσαμε παραπάνω έχουν το χαρακτηριστικό ότι ο νικητής της ρίψης δεν αποκαλύπτεται ταυτόχρονα στα δύο μέλη. Σε όλα τα πρωτόκολλα η Αλίκη ανακαλύπτει πρώτη ποιος είναι ο νικητής της ρίψης

και στη συνέχεια είναι υπεύθυνη να ενημερώσει τον Βύρων για το αποτέλεσμα. Αυτό στη βιβλιογραφία αναφέρεται ως *ρίψη κέρματος σε πηγάδι*, όπου η Αλίκη βρίσκεται κοντά σε ένα πηγάδι και ρίχνει το κέρμα μέσα σε αυτό, ενώ ο Βύρων δεν έχει οπτική επαφή με το πηγάδι. Έτσι η Αλίκη θα πρέπει να αναγγείλει στον Βύρωνα το αποτέλεσμα της ρίψης. Η χρήση του πηγαδιού αποτρέπει την Αλίκη να αλλάξει το αποτέλεσμα, ενώ δίνει την ευκαιρία στον Βύρωνα να εξακριβώσει το αποτέλεσμα.

Τα πρωτόκολλα μεταφοράς εν αγνοία (oblivious transfer) έχουν το χαρακτηριστικό ότι ο αποστολέας στέλνει ένα μήνυμα με τέτοιον τρόπο, ώστε αφενός το μήνυμα έχει πιθανότητα 0.5 να φθάσει στον παραλήπτη, αφετέρου ο αποστολέας δεν γνωρίζει αν το μήνυμα έχει φθάσει στον παραλήπτη, παρά μόνον κάποια στιγμή στο μέλλον. Αυτό στην περίπτωση της ρίψης κέρματος ερμηνεύεται ως εξής. Η Αλίκη ρίχνει ένα κέρμα και γράφει το αποτέλεσμα σε ένα κομμάτι χαρτί. Ταυτόχρονα ο Βύρων γράφει τη δική του επιλογή σε ένα κομμάτι χαρτί. Η Αλίκη και ο Βύρων κάποια στιγμή συναντιούνται και ανταλλάσσουν τα χαρτιά. Αν τα δύο χαρτιά έχουν το ίδιο αποτέλεσμα, κερδίζει ο Βύρων, ενώ αν τα χαρτιά δε συμφωνούν κερδίζει η Αλίκη.

Με ένα πρωτόκολλο μεταφοράς εν αγνοία, η Αλίκη στέλνει ένα μήνυμα στον Βύρωνα με πιθανότητα 0.5. Η Αλίκη δεν γνωρίζει αρχικά αν το μήνυμα στάλθηκε στον Βύρωνα. Το μήνυμα μπορεί να είναι «Βύρων, κέρδισες». Αν τελικά φθάσει στον Βύρωνα, τότε μπορεί ο Βύρων να ανακοινώσει το μήνυμα στην Αλίκη. Αν το μήνυμα δεν φθάσει, τότε ο Βύρων θα έχει στα χέρια του ένα μήνυμα από το οποίο δεν θα μπορεί να βγάλει νόημα, για παράδειγμα «ηΒγδευθσσζτ». Η πιθανότητα και για τα δύο μηνύματα είναι 0.5, ισοδύναμη με μια ρίψη κέρματος.

Υλοποίηση με ασύμμετρη κρυπτογραφία

Ένα πρωτόκολλο μεταφοράς εν αγνοία υλοποιημένο με ασύμμετρη κρυπτογραφία είναι το πρωτόκολλο του Rabin, το οποίο αποτελείται από τα εξής βήματα:

1. Η Αλίκη αναπτύσσει ένα κρυπτοσύστημα τύπου RSA. Με άλλα λόγια επιλέγει δύο μεγάλους πρώτους αριθμούς p, q και στη συνέχεια υπολογίζει το γινόμενό τους $n = pq$. Στη συνέχεια επιλέγει ένα μήνυμα m και το κρυπτογραφεί με κρυπτογραφική πράξη η οποία εκτελείται σε mod n και έχει την ιδιότητα η αποκρυπτογράφησή του να είναι δυνατή αν και μόνον αν είναι γνωστοί οι παράγοντες του n. Έστω c το κρυπτοκείμενο που προκύπτει.

   $$\text{Αλίκη} \rightarrow \text{Βύρων: } c, n$$

2. Ο Βύρων επιλέγει ένα τυχαίο στοιχείο $u \in \boldsymbol{Z}_n^*$ και στέλνει το τετράγωνο αυτού στην Αλίκη:

   $$\text{Αλίκη} \rightarrow \text{Βύρων: } v \equiv u^2 \pmod{n}$$

3. Η Αλίκη υπολογίζει τις τέσσερις τετραγωνικές ρίζες του *ν*, έστω *x*, *y*, *-x*, *-y* και στέλνει μια από αυτές, έστω $y \in \{ x,y,-x,-y \}$ στον Βύρωνα:
4. Από τις τετραγωνικές ρίζες, οι δύο από αυτές αντιστοιχούν στο ± *u*, οι οποίες γνωστές στον Βύρωνα από το βήμα (2). Στην περίπτωση που η απάντηση *y* της Αλίκης δεν είναι ± *u*, τότε ο Βύρων μπορεί να παραγοντοποιήσει το *n* και να αποκρυπτογραφήσει το *c*.

Επειδή η Αλίκη δε γνωρίζει την προέλευση του *ν* προτού τετραγωνιστεί από τον Βύρωνα, έχει πιθανότητα 0.5 να επιλέξει τους αριθμούς ± *u* που γνωρίζει ο Βύρων. Σε αυτήν την περίπτωση ο Βύρων δεν κερδίζει, αλλά ούτε και η Αλίκη δεν είναι σε θέση να γνωρίζει την κατάσταση του Βύρωνα.

9.4.5. Υπογραφή συμβολαίου

Το πρωτόκολλο μεταφοράς εν αγνοία μπορεί να χρησιμοποιηθεί ως δομικό συστατικό προκειμένου να χτισθούν πιο πολύπλοκα πρωτόκολλα, όπως αυτό για την ταυτόχρονη υπογραφή συμβολαίων. Πολλές φορές συναντάται το πρόβλημα όπου δεν υπάρχει αρκετή εμπιστοσύνη μεταξύ δύο μελών, με αποτέλεσμα να απαιτείται να υπογραφεί ταυτόχρονα ένα συμβόλαιο και από τα δύο μέλη.

Η χρήση μιας έμπιστης οντότητας μπορεί να απλοποιήσει σημαντικά το πρόβλημα. Η Αλίκη και ο Βύρων εκδηλώνουν την πρόθεσή τους να υπογράψουν το συμβόλαιο, υπογράφοντας ο καθένας τους ένα κείμενο το οποίο το στέλνουν στην τρίτη οντότητα. Το περιεχόμενο των υπογεγραμμένων κειμένων είναι οι προθέσεις των δύο μελών. Μόλις η έμπιστη οντότητα λάβει τις προθέσεις της Αλίκης και του Βύρωνα υπογεγραμμένες, ανακοινώνει στα μέλη ότι μπορούν να υπογράψουν το συμβόλαιο. Έτσι η Αλίκη υπογράφει το συμβόλαιο και το στέλνει στον Βύρωνα, και αντίστροφα.

Το πρωτόκολλο υπογραφής συμβολαίου των Even, Goldreich και Lempel που θα παρουσιάσουμε στη συνέχεια, χρησιμοποιεί μια ειδική εφαρμογή πρωτοκόλλου μεταφοράς εν αγνοία, όπου ο αποστολέας στέλνει ένα από δύο μηνύματα, χωρίς να είναι σε θέση να γνωρίζει ποιο από τα μηνύματα έχει σταλεί, ενώ η πιθανότητα αποστολής για το κάθε μήνυμα είναι 0.5.

1. Η Αλίκη και ο Βύρων συμφωνούν σε ένα αρχικό μήνυμα, *m*. Το περιεχόμενο του μηνύματος δεν έχει ιδιαίτερη σημασία, χρησιμοποιείται απλά για έλεγχο, όπως θα δούμε παρακάτω. Επίσης συμφωνούν να χρησιμοποιήσουν κάποιο συμμετρικό κρυπτοσύστημα.
2. Η Αλίκη επιλέγει τυχαία 2*n* συμμετρικά κλειδιά:

$$a_1, a_2, ..., a_{2n}$$

3. Για κάθε κλειδί, κρυπτογραφεί το προσυμφωνημένο μήνυμα και στέλνει τα κρυπτοκείμενα στον Βύρωνα:

$$\text{Αλίκη} \rightarrow \text{Βύρων: } e_{a_i}(m), \text{ για } 1 \le i \le 2n .$$

4. Ο Βύρων αντίστοιχα επιλέγει τυχαία $2n$ συμμετρικά κλειδιά:

$$b_1, b_2, ..., b_{2n}$$

5. Για κάθε κλειδί, κρυπτογραφεί το προσυμφωνημένο μήνυμα και στέλνει τα κρυπτοκείμενα στην Αλίκη:

$$\text{Βύρων} \rightarrow \text{Αλίκη: } e_{b_i}(m), \text{ για } 1 \le i \le 2n.$$

6. Καθώς τα κλειδιά είναι διατεταγμένα, η Αλίκη δηλώνει ότι δεσμεύεται από το συμβόλαιο αν ο Βύρων βρεθεί στη θέση να παρουσιάσει ένα ζεύγος κλειδιών της Αλίκης (a_i, a_{n+i}) για οποιοδήποτε i. Αντίστοιχα ο Βύρων δηλώνει ότι δεσμεύεται από το συμβόλαιο αν η Αλίκη είναι σε θέση να παρουσιάσει ένα ζεύγος κλειδιών του Βύρωνα (b_i, b_{n+i}) για οποιοδήποτε i.
7. Χρησιμοποιώντας πρωτόκολλο μεταφοράς εν αγνοία, η Αλίκη στέλνει τα ζεύγη (a_i, a_{n+i}) στον Βύρωνα, για $1 \le i \le n$. Έτσι το πρωτόκολλο εκτελείται n φορές, όπου σε κάθε εκτέλεση στέλνεται ένα κλειδί από τα a_i και a_{n+i}. Η Αλίκη δεν γνωρίζει ποιο κλειδί έχει σταλεί, αλλά γνωρίζει ότι κατά την ολοκλήρωση όλων των πρωτοκόλλων ο Βύρων έχει τα μισά της κλειδιά. Κάθε φορά που ολοκληρώνεται το πρωτόκολλο, ο Βύρων μπορεί να επιβεβαιώσει ότι η Αλίκη έχει στείλει το σωστό κλειδί, εφαρμόζοντάς το στην πράξη αποκρυπτογράφησης επάνω στα κρυπτοκείμενα που έλαβε. Έτσι μπορεί να διακρίνει αν έλαβε το a_i ή το a_{n+i}.
8. Αντίστοιχα ο Βύρων εκτελεί με τη σειρά του το πρωτόκολλο μεταφοράς εν αγνοία, για να στείλει τα ζεύγη των κλειδιών του (b_i, b_{n+i}) στην Αλίκη, για $1 \le i \le n$. Στο τέλος του σταδίου, η Αλίκη έχει στην κατοχή της τα μισά κλειδιά του Βύρωνα.
9. Η Αλίκη στέλνει το πρώτο bit όλων των κλειδιών της στον Βύρωνα. Επειδή δεν γνωρίζει ποια κλειδιά έχει ο Βύρων, είναι αναγκασμένη να στείλει τις πραγματικές τιμές, διότι η πιθανότητα να στείλει λάθος bit και να μην ανιχνευτεί από τον Βύρωνα είναι μικρή.
10. Αντίστοιχα ο Βύρων στέλνει το πρώτο bit όλων των κλειδιών του στην Αλίκη. Τα βήματα (9) και (10) επαναλαμβάνονται μέχρι να σταλούν όλα τα bits των κλειδιών.

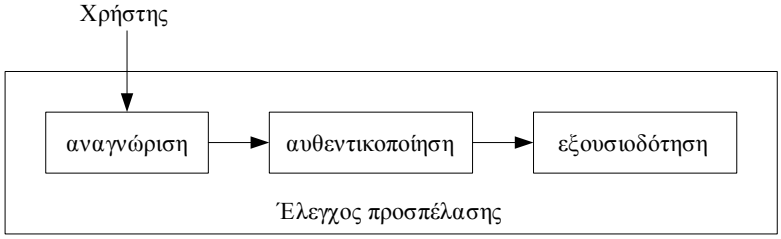
Επειδή η Αλίκη στέλνει πρώτη τα bits των κλειδιών στον Βύρωνα, ο Βύρων έχει ένα μικρό πλεονέκτημα. Γενικά κάθε φορά που στέλνεται μια σειρά από bits, ο χρόνος εξαντλητικής αναζήτησης μειώνεται στο μισό. Αν κάποια στιγμή ο Βύρων πάρει μια σειρά από bits των κλειδιών της Αλίκης και δεν απαντήσει με τη δική του σειρά, θεωρώντας ότι έχει αρκετό υλικό ώστε να πραγματοποιήσει με επιτυχία εξαντλητική αναζήτηση, το ίδιο μπορεί να κάνει και η Αλίκη με τη διαφορά ότι θα χρειασθεί διπλάσιο χρόνο για να ανακαλύψει κάποιο από τα κλειδιά του Βύρωνα (υποθέτοντας ότι η Αλίκη και ο Βύρων έχουν την ίδια υπολογιστική ισχύ). Ο παράγοντας 2. της προσπάθειας εξαντλητικής αναζήτησης της Αλίκης

έναντι της προσπάθειας του Βύρωνα δεν θεωρείται σημαντικός και δεν εμποδίζει την Αλίκη να ανακαλύψει το κλειδί του Βύρωνα με λίγο μεγαλύτερη καθυστέρηση.

9.5. Πρωτόκολλα αυθεντικοποίησης ταυτότητας

Στον ηλεκτρονικό κόσμο, όταν αναφερόμαστε σε κρυπτογραφικά πρωτόκολλα συνήθως εννοούμε τα πρωτόκολλα που έχουν στόχο την αυθεντικοποίηση της ταυτότητας ενός χρήστη, συστατικού του δικτύου, ή ενός μηνύματος. Επειδή στα δίκτυα υπολογιστών δεν υπάρχει άμεση σύνδεση μεταξύ δύο οντοτήτων αλλά παρεμβάλλονται τρίτοι, η επιβεβαίωση της ταυτότητας με την οντότητα που ανταλλάσσουμε μηνύματα είναι από τις υψηλότερες προτεραιότητες. Έτσι, το πρώτο στάδιο επικοινωνίας περιλαμβάνει διαδικασίες αναγνώρισης των επικοινωνούντων μελών, το οποίο υλοποιείται με πρωτόκολλα αυθεντικοποίησης ταυτότητας.

Η αυθεντικοποίηση ταυτότητας είναι ένα τμήμα της διαδικασίας ελέγχου προσπέλασης σε ένα σύστημα. Ο έλεγχος προσπέλασης είναι ακρογωνιαίος λίθος στην ασφάλεια των πληροφοριακών συστημάτων και αποτελείται από τη διαδικασία αναγνώρισης, αυθεντικοποίησης και εξουσιοδότησης, όπως φαίνεται στο Σχήμα 9.2.



Σχήμα 9.2 Στάδια του ελέγχου προσπέλασης

Από τις τρεις διαδικασίες του ελέγχου προσπέλασης, το βιβλίο αυτό επικεντρώνεται στη διαδικασία αυθεντικοποίησης, καθώς αυτή συγκεντρώνει τον κύριο όγκο των κρυπτογραφικών μηχανισμών. Ωστόσο, θα παρουσιάσουμε συνοπτικά τα χαρακτηριστικά της αναγνώρισης και της εξουσιοδότησης προκειμένου να δικαιολογήσουμε τις απαιτήσεις της διαδικασίας αυθεντικοποίησης.

9.5.1. Κατηγορίες αναγνώρισης

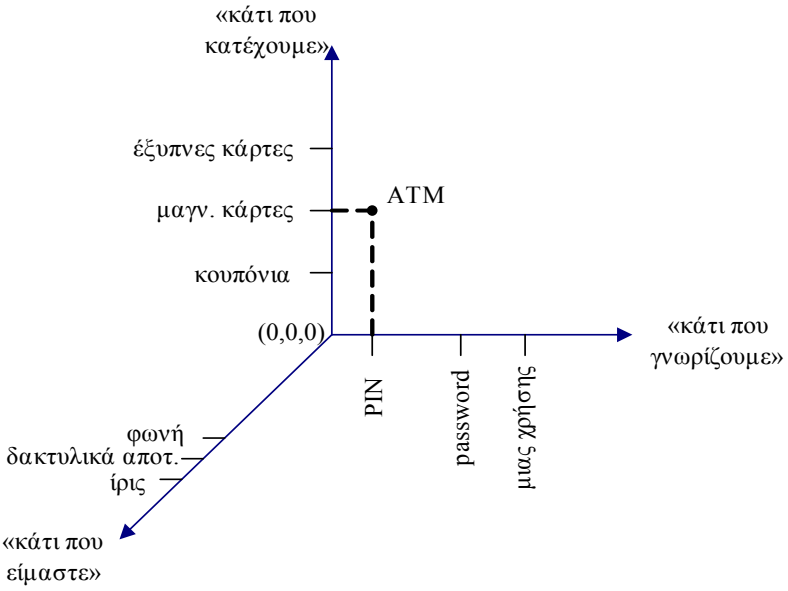
Κατά την αναγνώριση ενός χρήστη συλλέγονται τα πρωτογενή στοιχεία τα οποία περικλείουν πληροφορίες για την ταυτότητα του χρήστη. Τα στοιχεία αυτά αναλύονται σε τρεις διαστάσεις:

- «Κάτι που γνωρίζει ο χρήστης». Τα πρωτογενή στοιχεία της διάστασης αυτής περιλαμβάνουν κωδικούς πρόσβασης, κλειδιά, PIN και γενικά, δεδομένα τα οποία γνωρίζει ο χρήστης και τα οποία παρουσιάζει στο σύστη-

μα είτε με πρωτόκολλο μιας φοράς, είτε με πρωτόκολλο πρόκλησης-απόκρισης.

- «Κάτι που κατέχει ο χρήστης». Τα στοιχεία αυτά περιλαμβάνουν φυσικά αντικείμενα όπως κουπόνια, μαγνητικές κάρτες, ή έξυπνες κάρτες.
- «Κάτι που είναι ο χρήστης». Τα στοιχεία αυτά αποτελούνται από τα προσωπικά χαρακτηριστικά, όπως φωνή, δακτυλικά αποτυπώματα, χαρακτηριστικά προσώπου, κτλ.

Γενικά όσες διαστάσεις αναγνώρισης χρησιμοποιούνται, τόσο ισχυρότερη είναι η αναγνώριση και τόσο μικρότερη είναι η πιθανότητα εσφαλμένης αναγνώρισης. Στο Σχήμα 9.3 φαίνονται οι τρεις διαστάσεις αναγνώρισης, ταξινομημένες κατά αύξουσα διάταξη. Στο σημείο (0, 0, 0) η αβεβαιότητα αναγνώρισης είναι μέγιστη (δηλαδή δε γνωρίζουμε τίποτε για την ταυτότητα του χρήστη), ενώ όσο μεγαλώνει η απόσταση από το σημείο αυτό, τόσο μικραίνει η αβεβαιότητα.



Σχήμα 9.3 Οι τρεις διαστάσεις της αναγνώρισης

Η επιλογή του συνδυασμού των στοιχείων αναγνώρισης εξαρτάται από το ρίσκο που είμαστε διατεθειμένοι να δεχθούμε. Για παράδειγμα, στο σημείο (ATM) του σχήματος λειτουργεί η αναγνώριση των πελατών μιας τράπεζας κατά τη συναλλαγή με ATM. Οι τράπεζες δέχονται ότι το ρίσκο για αναγνώριση με μαγνητική κάρτα και PIN είναι αρκετά μικρό, ώστε να μπορούν να πραγματοποιηθούν συναλλαγές. Η ενδεχόμενη χρήση βιομετρικών τεχνικών (π.χ. αναγνώριση δακτυλικού αποτυπώματος) μειώνει το ρίσκο από τη μια, αλλά από την άλλη αυξάνει την πολυπλοκότητα και τις απαιτήσεις σε τέτοιο βαθμό ώστε το σύστημα θα γινό-

ταν δύσχρηστο. Έτσι το σημείο ισορροπίας βρίσκεται στο σημείο (ATM), το οποίο δέχονται όλες οι τράπεζες. Το PIN έχει μικρό χώρο αναζήτησης. Για παράδειγμα, για ένα τυπικό PIN τεσσάρων ψηφίων, ο χώρος είναι μόνο 10000 κλειδιά. Αυτό η τράπεζα το αντισταθμίζει εφαρμόζοντας την πολιτική ασφάλειας του «μεγίστου αριθμού προσπαθειών». Έτσι ο χρήστης για παράδειγμα, έχει τη δυνατότητα να δώσει στο σύστημα λάθος PIN μέχρι τρεις φορές. Αν υπερβεί τον αριθμό εσφαλμένων απαντήσεων, τότε το σύστημα θεωρεί ότι επιχειρείται επίθεση και εκτελεί «διαδικασία χειρισμού περιστατικού ασφάλειας», όπου διακόπτει τη συναλλαγή και δεσμεύει την κάρτα.

9.5.2. Εξουσιοδότηση

Κατά το στάδιο της εξουσιοδότησης, το σύστημα έχει γνώση της ταυτότητας του χρήστη (θεωρούμε ότι τα πρωτόκολλα αυθεντικοποίησης έχουν εκτελέσει με επιτυχία τα καθήκοντά τους), οπότε με βάση κανόνων πρόσβασης ελέγχει αν επιτρέπεται στο χρήστη να έχει πρόσβαση σε κάποιον πόρο του συστήματος και σε ποιο βαθμό. Το ποιο γνωστό μοντέλο εξουσιοδότησης είναι το μοντέλο των ***ρόλων*** (role based), όπου μόλις ολοκληρωθεί με επιτυχία η αυθεντικοποίηση της ταυτότητας του χρήστη, το σύστημα του αναθέτει κάποιο ρόλο. Ο ρόλος καθορίζει τους πόρους στους οποίους ο χρήστης έχει πρόσβαση, καθώς και το είδος της προσπέλασης (ανάγνωση, τροποποίηση, διαγραφή, κτλ.).

9.5.3. Αυθεντικοποίηση με κωδικούς πρόσβασης

Η συντριπτική πλειοψηφία των υπολογιστικών συστημάτων χρησιμοποιούν αυθεντικοποίηση της ταυτότητας όπου η αναγνώριση γίνεται με κωδικούς πρόσβασης. Αν και το ρίσκο είναι αρκετά μεγάλο, παραμένει εντός ανεκτών ορίων για πολλές εφαρμογές.

Ένα απλό πρωτόκολλο αυθεντικοποίησης μεταξύ ενός χρήστη και ενός συστήματος είναι το εξής (θεωρούμε ότι η αυθεντικοποίηση γίνεται από κάποιον server αυθεντικοποίησης):

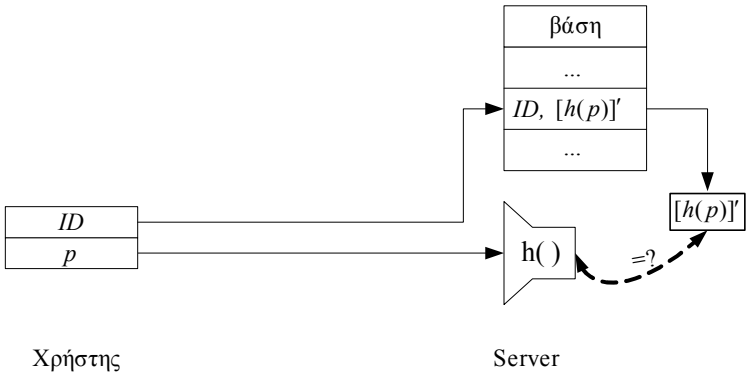
Χρήστης $\rightarrow$ Server: *ID*, *p*

όπου *ID*, η ταυτότητα (π.χ. όνομα) του χρήστη και *p*, ο κωδικός πρόσβασης για το χρήστη. Ο server στη συνέχεια ελέγχει τον κωδικό που έλαβε από το χρήστη με αυτόν που έχει αποθηκευμένο στη βάση των κωδικών των χρηστών. Το πρωτόκολλο αυτό έχει μεγάλα μειονεκτήματα. Αρχικά, η μεταφορά του κωδικού από το χρήστη στο server απαιτεί κανάλι εμπιστευτικότητας, διότι ένας υποκλοπέας μπορεί να καταγράψει τον κωδικό του χρήστη και στη συνέχεια να τον χρησιμοποιήσει για να κερδίσει πρόσβαση στο σύστημα. Δεύτερον, προκειμένου να μπορεί ο server να ελέγξει την ορθότητα του κωδικού θα πρέπει να έχει έναν χώρο αποθήκευσης (βάση) των κωδικών πρόσβασης όλων των χρηστών. Αυτό δημιουργεί μεγάλες απαιτήσεις ασφάλειας στη φύλαξη των κωδικών. Στην περίπτωση που ο

αντίπαλος καταφέρει να έχει πρόσβαση στη βάση αυτή, θα καταρρεύσει η υπηρεσία αυθεντικοποίησης του συστήματος. Μια βελτίωση θα ήταν να κρυπτογραφούνταν οι κωδικοί πρόσβασης με κάποιο κύριο κλειδί, οπότε η φύλαξη ενός κλειδιού είναι πρακτικότερη από τη φύλαξη όλης της βάσης.

Ωστόσο, η χρήση ενός κρυπτοσυστήματος για την προστασία της βάσης των κωδικών πρόσβασης επιτρέπει την απόπειρα κρυπτανάλυσης, σε περίπτωση που ο αντίπαλος καταφέρει να αποκομίσει ένα αντίγραφο της βάσης. Στην περίπτωση που ο αντίπαλος ανακαλύψει το κύριο κλειδί, θα έχει αυτόματα πρόσβαση σε όλους τους κωδικούς. Θα ήταν επομένως προτιμότερο σε περίπτωση που ο αντίπαλος έχει στην κατοχή του τη βάση, η απόπειρα κρυπτανάλυσης να του επιφέρει λιγότερο κέρδος. Λιγότερο κέρδος σημαίνει ότι σε μια απόπειρα κρυπτανάλυσης θα ανακαλύψει λίγα ή μόνον ένα από τους κωδικούς πρόσβασης και για κάθε επιπλέον κωδικό θα είναι αναγκασμένος να επαναλάβει την επίθεση από την αρχή.

Η απαίτηση που μόλις περιγράψαμε μπορεί να υλοποιηθεί με τη χρήση μονόδρομης συνάρτησης (Σχήμα 9.4) στη θέση του κρυπτοσυστήματος.



Σχήμα 9.4 Αυθεντικοποίηση με τη χρήση μονόδρομης συνάρτησης

Ο server στη βάση έχει αποθηκευμένες την ταυτότητα του χρήστη και τη σύνοψη του κωδικού πρόσβασης. Το πρωτόκολλο περιλαμβάνει ανταλλαγή των εξής μηνυμάτων:

Χρήστης → Server: *ID*, *p*
Server: *h*(*p*) = ? [*h*(*p*)]′

Ο server δέχεται τον κωδικό πρόσβασης μαζί με την ταυτότητα του χρήστη και στη συνέχεια υπολογίζει τη σύνοψη του κωδικού. Ο έλεγχος γίνεται με βάση τη σύνοψη που υπολογίζει και τη σύνοψη που είναι αποθηκευμένη στη βάση του. Αν οι δύο συνόψεις είναι ίσες, τότε συμπεραίνεται ότι και τα αρχικά μηνύματα (κωδικοί πρόσβασης) είναι ίσα.

Το πλεονέκτημα της χρήσης της μονόδρομης hash έναντι ενός κρυπτοσυστήματος (συμμετρικού ή ασύμμετρου) είναι ότι δεν απαιτούνται καθόλου κλειδιά για τη φύλαξη της βάσης. Ωστόσο, αν και ο αντίπαλος με μια επίθεση δεν έχει άμεσα όλους τους κωδικούς πρόσβασης, μπορεί με μια πλήρη επίθεση εξαντλητικής αναζήτησης να ανακαλύψει τους κωδικούς σταδιακά. Επιπλέον, αν ο αντίπαλος έχει μεγάλη αποθηκευτική ικανότητα, τότε μπορεί να δημιουργήσει λίστες μηνυμάτων με τη σύνοψή τους ως βάση αναφοράς για να επιταχύνει την ανακάλυψη των κωδικών. Αυτό μπορεί να γίνει επειδή οι κωδικοί πρόσβασης προέρχονται από ένα σχετικά μικρό σύνολο μηνυμάτων, αφού χρησιμοποιούνται οι χαρακτήρες πληκτρολογίου.

Προκειμένου να αποφευχθεί η δυνατότητα ανακάλυψης των κωδικών με μία και μόνο εξαντλητική αναζήτηση, εισάγεται μια επιπλέον πληροφορία η οποία εκφράζεται με τη χρήση δεδομένων ***αλατισμού*** (salting). Αλατισμός είναι η διαδικασία όπου η σύνοψη του κωδικού πρόσβασης παράγεται από τον κωδικό πρόσβασης και έναν τυχαίο αριθμό, ο οποίος είναι διαφορετικός για κάθε χρήστη. Έτσι, ο αντίπαλος είναι αναγκασμένος να δημιουργήσει διαφορετικές λίστες – επομένως και διαφορετική αναζήτηση – για κάθε κωδικό πρόσβασης. Ο τυχαίος αριθμός αποθηκεύεται μαζί με τα υπόλοιπα στοιχεία του χρήστη στη βάση και ο server πραγματοποιεί τον ακόλουθο έλεγχο:

Server: $h(s||p) = ?\ [h(s \,||\, p)]'$,

όπου s το «αλάτι» του κωδικού του χρήστη.

S/Key

Το σύστημα αυθεντικοποίησης της ταυτότητας με αλατισμό της σύνοψης επιδιορθώνει τα προβλήματα προστασίας των κωδικών στη μεριά του server. Το πρόβλημα όμως της εμπιστευτικής μεταφοράς του κωδικού από το χρήστη στο server παραμένει. Το σύστημα S/Key είναι ένας αποτελεσματικός τρόπος αποστολής του κωδικού με τον οποίο δεν απαιτείται εμπιστευτικό κανάλι.

Το S/Key περιλαμβάνει ένα στάδιο αρχικοποίησης, όπου ο χρήστης επιλέγει ένα τυχαίο μήνυμα r και στη συνέχεια υπολογίζει αναδρομικά τη σύνοψη x_n, για κάποιο n:

Χρήστης: $x_n = h(x_{n-1})$,

όπου $h(\ )$ μια κρυπτογραφική μονόδρομη hash και $x_0 = r$. Μπορούμε να παρατηρήσουμε ότι λόγω της μονόδρομης συνάρτησης, μόνον ο χρήστης που γνωρίζει την αρχική τιμή x_0 έχει τη δυνατότητα να υπολογίσει το x_n, για οποιοδήποτε n. Αυτό όμως σημαίνει ότι αν ανακαλυφθεί ή γίνει γνωστό κάποιο από τα x_i για $i < n$, τότε μπορούν να υπολογισθούν με ευκολία όλα τα x_j, για $i \le j \le n$.

Το S/Key βασίζεται στις παραπάνω παρατηρήσεις. Έστω ότι $n = 100$. Κατά τη διαδικασία αρχικοποίησης, ο χρήστης υπολογίζει το x_{100} και το στέλνει στο server, ο οποίος το αποθηκεύει στη βάση. Επιπλέον, ο χρήστης θέτει έναν μετρητή i στην αρχική τιμή 99.

Κατά το στάδιο της αυθεντικοποίησης, εκτελείται το ακόλουθο πρωτόκολλο:

Χρήστης $\rightarrow$ Server: x_i
Χρήστης: $i \leftarrow i - 1$
Server: έλεγχος $x_i = ?\ h(x_{i-1})$. Αν ναι, τότε αποθηκεύει το x_{i-1} στη θέση του x_i και η αυθεντικοποίηση ολοκληρώνεται με επιτυχία.

Σε κάθε εκτέλεση του πρωτοκόλλου ο δείκτης i μειώνεται κατά ένα, υποδεικνύοντας το x_i που θα χρησιμοποιηθεί. Όταν ο δείκτης μηδενισθεί, απαιτείται νέα διαδικασία αρχικοποίησης.

Στο σύστημα S/Key, η υποκλοπή του x_i κατά την εκτέλεση του πρωτοκόλλου αυθεντικοποίησης δεν παρέχει ιδιαίτερο πλεονέκτημα στον αντίπαλο, καθώς η τιμή αυτή χρησιμοποιείται μόνον μια φορά. Επιπλέον, ο server που έχει αποθηκευμένο στη βάση το x_i, δε γνωρίζει το x_{i-1} παρά μόνον όταν σταλεί από το χρήστη. Έτσι μια πιθανή κλοπή της βάσης δε δίνει μεγάλη πληροφορία στον αντίπαλο. Η ασφάλεια του συστήματος στηρίζεται στην κρυπτογραφική ισχύ της μονόδρομης συνάρτησης, η οποία θα πρέπει να είναι ανθεκτική σε συγκρούσεις και το μέγεθος της σύνοψης να είναι αρκετά υψηλό. Μια ενδεικτική τιμή του μεγέθους της σύνοψης είναι 160 bits.

9.5.4. Αυθεντικοποίηση με ψηφιακές υπογραφές

Σε μια υποδομή δημόσιου κλειδιού, η αυθεντικοποίηση μπορεί να πραγματοποιηθεί με τη χρήση των ψηφιακών πιστοποιητικών. Η βάση του server σε αυτήν την περίπτωση θα έχει τα πιστοποιητικά όλων των χρηστών, από όπου ο server μπορεί να αναζητήσει το πιστοποιητικό του χρήστη.

Έστω ότι η Αλίκη επιθυμεί πρόσβαση στο σύστημα. Ο server γνωρίζει το δημόσιό της κλειδί, επομένως μπορεί να χρησιμοποιηθεί πρωτόκολλο πρόκλησης-απόκρισης, ώστε να εξακριβωθεί αν η Αλίκη κατέχει το ιδιωτικό κλειδί της. Αυτό μπορεί να πραγματοποιηθεί με το ακόλουθο πρωτόκολλο:

Αλίκη $\rightarrow$ Server: ID_A
Server $\rightarrow$ Αλίκη: c
Αλίκη $\rightarrow$ Server: $r = d_{kdA}(c)$
Server: $e_{keA}(r) = c?$

όπου:

ID_A	η ταυτότητα της Αλίκης,
c	το μήνυμα-πρόκληση του server,
r	το μήνυμα-απόκριση της Αλίκης,
$e(),d()$	Η πράξη κρυπτογράφησης και αποκρυπτογράφησης, αντίστοιχα,
kdA, keA	Το ιδιωτικό και το δημόσιο κλειδί της Αλίκης, αντίστοιχα.

Αν υποθέσουμε ότι μόνον η Αλίκη γνωρίζει το ιδιωτικό της κλειδί, τότε μόνον η Αλίκη έχει τη δυνατότητα να βρει ένα μήνυμα r τέτοιο ώστε η κρυπτογράφηση αυτού με το δημόσιο κλειδί της να δίνει το προεπιλεγμένο μήνυμα c.

Από πρακτική πλευρά, ένα σύστημα ψηφιακών υπογραφών χρησιμοποιεί την αναγνώριση του «κάτι που κατέχει» ο χρήστης. Όπως είδαμε στο Κεφάλαιο 6, η ασύμμετρη κρυπτογραφία απαιτεί πολύ μεγαλύτερα κλειδιά από αυτά που απαιτεί η συμμετρική κρυπτογραφία. Επιπλέον τα ασύμμετρα κλειδιά γεννιούνται από μαθηματικούς μετασχηματισμούς, με αποτέλεσμα τα κλειδιά αυτά να μην είναι φιλικά προς το χρήστη. Έτσι, από τη στιγμή που είναι δύσκολο να απομνημονευθούν τα ασύμμετρα κλειδιά, ο χρήστης υποχρεώνεται να τα φυλάξει σε αποθηκευτικές συσκευές. Ένα ιδιωτικό κλειδί μπορεί να αποθηκευθεί σε σκληρό ή αποσπώμενο δίσκο του υπολογιστή ως λογισμικό κουπόνι (software token), σε μαγνητική κάρτα ή σε έξυπνη κάρτα. Από τις εναλλακτικές αυτές, η ασφαλέστερη είναι η αποθήκευση σε έξυπνη κάρτα, διότι η έξυπνη κάρτα έχει τη δυνατότητα εκτέλεσης της κρυπτογραφικής πράξης με αποτέλεσμα να μην χρειάζεται το ιδιωτικό κλειδί να διατεθεί εκτός της κάρτας.

Αμοιβαία αυθεντικοποίηση

Έστω ότι η Αλίκη και ο Βύρων επιθυμούν να αυθεντικοποιήσουν ο ένας την ταυτότητα του άλλου με τη χρήση των ψηφιακών υπογραφών. Ένα μη ασφαλές πρωτόκολλο είναι το εξής:

Αλίκη $\rightarrow$ Βύρων: *keA*
Βύρων $\rightarrow$ Αλίκη: *keB,* c_B
Αλίκη $\rightarrow$ Βύρων: $r_B = d_{kdA}(c_B)$, c_A
Βύρων $\rightarrow$ Αλίκη: $r_A = d_{kdB}(c_A)$

όπου c_A, c_B η πρόκληση της Αλίκης και του Βύρωνα αντίστοιχα και r_A και r_B οι αποκρίσεις στις προκλήσεις. Το πρωτόκολλο ολοκληρώνεται με επιτυχία και από τις δύο πλευρές όταν επιβεβαιώσουν ότι οι αποκρίσεις ταιριάζουν κρυπτογραφικά στις προκλήσεις.

Το παραπάνω πρωτόκολλο της αμοιβαίας αυθεντικοποίησης δεν είναι ασφαλές διότι υποπίπτει σε επίθεση του ενδιάμεσου ατόμου. Ο αντίπαλος ο οποίος παρεμβάλλεται στο κανάλι επικοινωνίας της Αλίκης και του Βύρωνα, ελέγχει όλα τα μηνύματα που διακινούνται και συνεπώς μπορεί να αντικαταστήσει τα δημόσια

κλειδιά με το δικό του, πλαστογραφώντας με τον τρόπο αυτό την Αλίκη στον Βύρωνα και αντίστροφα.

Μια τροποποίηση του πρωτοκόλλου είναι η πρόκληση να είναι προκαθορισμένα μηνύματα, γνωστά στην Αλίκη και στον Βύρωνα. Έτσι τα c_A, c_B δεν στέλνονται σαν απλό κρυπτοκείμενο, αλλά κρυπτογραφημένα με το ιδιωτικό κλειδί του αντίστοιχου μέλους. Αν και το πρωτόκολλο αμοιβαίας αυθεντικοποίησης με προκαθορισμένα μυστικά είναι και αυτό ευάλωτο στην επίθεση του ενδιάμεσου ατόμου, μια μικρή τροποποίηση στη μετάδοση των μηνυμάτων μπορεί να αποτρέψει τη συγκεκριμένη επίθεση. Η τροποποίηση προτάθηκε από τους Rivest και Shamir και το πρωτόκολλο που προέκυψε το ονόμασαν ***πρωτόκολλο συναρμογής*** (interlock protocol) το οποίο έχει στόχο τη μείωση της πιθανότητας επιτυχίας επίθεσης του ενδιάμεσου ατόμου. Το πρωτόκολλο συναρμογής έχει ως εξής:

Αλίκη $\rightarrow$ Βύρων: keA
Βύρων $\rightarrow$ Αλίκη: keB
Αλίκη: $r_B = d_{kdA}(c_B) = r_B^L \,||\, r_B^L$
Αλίκη $\rightarrow$ Βύρων: r_B^L
Βύρων: $r_A = d_{kdB}(c_A) = r_A^L \,||\, r_A^R$
Βύρων $\rightarrow$ Αλίκη: r_A^L
Αλίκη $\rightarrow$ Βύρων: r_B^R
Βύρων $\rightarrow$ Αλίκη: r_A^R

Με άλλα λόγια, η Αλίκη και ο Βύρων υπογράφουν αντίστοιχα τα κοινά μυστικά c_A, c_B, αλλά στη συνέχεια χωρίζουν την υπογραφή σε δύο τμήματα και στέλνουν τα τμήματα χωριστά. Η Αλίκη στέλνει το αριστερό τμήμα της υπογραφής της, στη συνέχεια ο Βύρων στέλνει το αριστερό τμήμα της υπογραφής του και η διαδικασία επαναλαμβάνεται με τα δεξιά τμήματα. Ο παραλήπτης ο οποίος έχει μόνο ένα τμήμα της υπογραφής, δεν έχει τη δυνατότητα να εκτελέσει την απαιτούμενη κρυπτογραφική πράξη. Έτσι το ενδιάμεσο άτομο όταν θα έχει στην κατοχή του και τα δύο τμήματα, θα είναι πια αργά.

9.6. Πρωτόκολλα μηδενικής γνώσης

Μεγάλο ερευνητικό και πρακτικό ενδιαφέρον παρουσιάζουν τα πρωτόκολλα μηδενικής γνώσης (zero knowledge protocols). Τα πρωτόκολλα μηδενικής γνώσης κατατάσσονται στην κατηγορία πρωτοκόλλων ***απόδειξης με αλληλεπίδραση*** (Interactive Proof), που σημαίνει ότι τα συμμετέχοντα μέλη ανταλλάσσουν πλήθος μηνυμάτων τα οποία βασίζονται σε τυχαίους αριθμούς και σε οποιαδήποτε στιγμή μπορεί οποιοδήποτε από τα μέλη να τερματίσει το πρωτόκολλο. Τα πρωτόκολλα μηδενικής γνώσης αναφέρονται κυρίως σε πρωτόκολλα αυθεντικοποίησης ταυτότητας. Το κίνητρο της ανάπτυξης των πρωτοκόλλων μηδενικής γνώσης είναι το

γεγονός ότι στα «συμβατικά» πρωτόκολλα αυθεντικοποίησης, κατά την ολοκλήρωση της εκτέλεσής τους, το μέλος το οποίο επαληθεύει την ταυτότητα του ομότιμού του έχει στην κατοχή του μηνύματα και μυστικά τα οποία μπορεί να τα χρησιμοποιήσει για πλαστοπροσωπία. Στα πρωτόκολλα μηδενικής γνώσης, το μυστικό το οποίο χρησιμοποιείται για να αποδειχθεί η ταυτότητα ενός μέλους, εξαρτάται από συγκεκριμένη χρονική στιγμή, έτσι ώστε σε άλλη στιγμή να είναι άχρηστο. Με άλλα λόγια, η Αλίκη μπορεί να αποδείξει στον Βύρωνα ότι γνωρίζει κάποιο μυστικό, χωρίς να του αποκαλύψει καμία πληροφορία για το μυστικό αυτό.

Προκειμένου να κατανοήσουμε την έννοια του πρωτοκόλλου μηδενικής γνώσης είναι αναγκαίο να δώσουμε τον ορισμό από τον οποίο μπορούμε να χαρακτηρίσουμε ένα πρωτόκολλο ως πρωτόκολλο μηδενικής γνώσης. Ως ***μυστικό απόδειξης*** ορίζουμε το μυστικό το οποίο είναι γνωστό μόνο στο μέλος το οποίο προκαλούμε να μας αποδείξει ότι έχει στην κατοχή του το μυστικό αυτό.

ΟΡΙΣΜΟΣ 9.2 – Ένα πρωτόκολλο χαρακτηρίζεται ως πρωτόκολλο μηδενικής γνώσης, αν και μόνο αν υπάρχει αλγόριθμος ο οποίος λειτουργεί σε πολυωνυμικό χρόνο και έχει τη δυνατότητα να παράγει σύνολο μηνυμάτων του πρωτοκόλλου χωρίς τη γνώση του μυστικού απόδειξης, έτσι ώστε το σύνολο των μηνυμάτων να μην είναι δυνατό να διακριθεί από ένα σύνολο «πραγματικών» μηνυμάτων που προέρχονται από την εκτέλεση του πρωτοκόλλου με το μέλος που γνωρίζει το μυστικό απόδειξης.

Ισοδύναμα αυτό σημαίνει ότι όλα τα μηνύματα που ανταλλάσσονται σε ένα πρωτόκολλο μηδενικής γνώσης δε δίνουν καμία απολύτως πληροφορία για το μυστικό απόδειξης. Από τον παραπάνω ορισμό μπορούμε να κατανοήσουμε τη διαφορά ενός πρωτοκόλλου μηδενικής γνώσης από ένα πρωτόκολλο αυθεντικοποίησης πρόκλησης-απόκρισης με ψηφιακές υπογραφές. Αν και ο κάτοχος του ιδιωτικού κλειδιού δε φανερώνει ποτέ το κλειδί αυτό, είναι πολύ εύκολο να ελέγξουμε αν ένα μήνυμα είναι μέρος του πρωτοκόλλου. Για παράδειγμα, η ψηφιακή υπογραφή της Αλίκης επάνω στην πρόκληση του Βύρωνα, αποδεικνύει ότι η Αλίκη κατέχει το ιδιωτικό της κλειδί, αλλά το μήνυμα της ψηφιακής υπογραφής της Αλίκης δεν είναι δυνατό να δημιουργηθεί χωρίς τη συμμετοχή του ιδιωτικού κλειδιού (σε πολυωνυμικό χρόνο).

Αυτή η ειδοποιός διαφορά μεταξύ ενός πρωτοκόλλου μηδενικής γνώσης και ενός πρωτοκόλλου αυθεντικοποίησης με ψηφιακές υπογραφές, είναι ο λόγος όπου σε ένα πρωτόκολλο μηδενικής γνώσης δεν υπάρχει υποβάθμιση της ασφάλειας ως προς το χρόνο, καθώς δεν υπάρχει διαρροή της πληροφορίας του μυστικού απόδειξης. Αντίθετα, σε ένα πρωτόκολλο ψηφιακών υπογραφών, κάποιος αντίπαλος ο οποίος υποκλέπτει τα μηνύματα, μπορεί σε κάποια χρονική στιγμή να τα χρησιμοποιήσει για να επιτύχει πλαστοπροσωπία.

9.6.1. Δομή πρωτοκόλλων μηδενικής γνώσης

Θεωρούμε ότι η Αλίκη έχει ένα μυστικό και θέλει να το αποδείξει στον Βύρων με τη χρήση πρωτοκόλλου μηδενικής γνώσης. Ένας κύκλος ενός πρωτοκόλλου μηδενικής γνώσης αποτελείται από τρία στάδια:

1. στάδιο μαρτυρίας, όπου η Αλίκη στέλνει μήνυμα δέσμευσης στον Βύρωνα. Το στάδιο αυτό αρχικοποιεί το πρωτόκολλο εισάγοντας τυχαιότητα. Το στάδιο αυτό περιλαμβάνεται για δύο λόγους. Πρώτον, τα μηνύματα που θα επακολουθήσουν δεν θα μπορούν να χρησιμοποιηθούν στο μέλλον από τον αντίπαλο. Δεύτερον, η μαρτυρία είναι η δημοσίευση της δέσμευσης της Αλίκης, από την οποία ο Βύρων επιλέγει την πρόκληση στο επόμενο στάδιο.
2. στάδιο πρόκλησης, όπου ο Βύρων στέλνει την πρόκλησή του στην Αλίκη. Η πρόκληση επιλέγεται από το μήνυμα δέσμευσης της Αλίκης. Η Αλίκη δεν είναι σε θέση να γνωρίζει εκ των προτέρων ποια θα είναι η πρόκληση του Βύρωνα. Τα δύο στάδια παρομοιάζονται με την αρχή της «κοπής και επιλογής» (cut-and-choose), όπου ένας κόβει μια πίτα σε δύο κομμάτια, αλλά ο άλλος επιλέγει πρώτος το κομμάτι.
3. στάδιο απόκρισης, όπου η Αλίκη καλείται να υπολογίσει τη σωστή απάντηση της πρόκλησης του Βύρωνα σε πολυωνυμικό χρόνο και να ενημερώσει τον Βύρωνα για τη λύση.

Στη συνέχεια θα παρουσιάσουμε μερικά πρωτόκολλα μηδενικής γνώσης.

9.6.2. Πρωτόκολλο αυθεντικοποίησης των Fiat και Shamir

Το πρωτόκολλο αυθεντικοποίησης ταυτότητας των Fiat και Shamir είναι ένα πρωτόκολλο μηδενικής γνώσης που βασίζεται στο δύσκολο πρόβλημα υπολογισμού της τετραγωνικής ρίζας, modulo n, για μεγάλο n με άγνωστους πρώτους παράγοντες.

Το πρωτόκολλο περιλαμβάνει έμπιστη οντότητα η οποία υπολογίζει και ανακοινώνει το n και καταχωρεί τα δημόσια κλειδιά των μελών. Αρχικά, η έμπιστη οντότητα επιλέγει δύο μεγάλους πρώτους αριθμούς p, q και ανακοινώνει το $n = pq$. Η Αλίκη εγγράφεται στο σύστημα επιλέγοντας έναν μυστικό αριθμό s τέτοιον ώστε $0 < s < n - 1$. Στη συνέχεια υπολογίζει το τετράγωνο της μυστικής ποσότητας:

$$v \equiv s^2 \pmod{n}$$

το οποίο αντιπροσωπεύει το δημόσιο κλειδί της. Τέλος, στέλνει το δημόσιο κλειδί v στην έμπιστη οντότητα.

Κατά τη διαδικασία αυθεντικοποίησης στον Βύρωνα, εκτελούνται t κύκλοι του πρωτοκόλλου. Ο κάθε κύκλος του πρωτοκόλλου αποτελείται από τα ακόλουθα βήματα:

1. Η Αλίκη δεσμεύεται με έναν τυχαίο αριθμό r, όπου $0 < r < n$ και στη συνέχεια υπολογίζει το τετράγωνο αυτού, το οποίο και στέλνει στον Βύρωνα:

   Αλίκη $\rightarrow$ Βύρων: $x \equiv r^2 \pmod{n}$

2. Ο Βύρων επιλέγει τυχαία πρόκληση $b \in \{0, 1\}$, δηλαδή $b = 1$ ή $b = 0$ και τη στέλνει στην Αλίκη:

   Βύρων $\rightarrow$ Αλίκη: b

3. Η Αλίκη υπολογίζει την απόκριση y και τη στέλνει στον Βύρωνα:

   Αλίκη $\rightarrow$ Βύρων: y

   όπου:

   $$y = \begin{cases} r & \text{αν } b = 0 \\ rs \bmod n & \text{αν } b = 1 \end{cases}$$

4. Ο Βύρων ελέγχει αν ισχύει:

   $$y^2 \equiv xv^b \pmod{n}.$$

   Στην ειδική περίπτωση όπου $y = 0$, το πρωτόκολλο ακυρώνεται.

Ανάλυση του πρωτοκόλλου των Fiat και Shamir

Αρχικά παρατηρούμε ότι σε έναν κύκλο του πρωτοκόλλου η Αλίκη θα πρέπει να γνωρίζει και τις δύο προκλήσεις, για $b = 0$ και για $b = 1$. Για $b = 0$, η λύση είναι εύκολη για οποιονδήποτε που επιλέγει τυχαία r, επομένως εύλογα αναρωτιόμαστε ποιο είναι το κέρδος σε μια τέτοια δοκιμή. Η απάντηση είναι ότι στην περίπτωση όπου η Αλίκη καλείται να απαντήσει μόνο στην πρόκληση για $b = 1$, ο αντίπαλος μπορεί να προσποιηθεί την ταυτότητα της Αλίκης επιλέγοντας τυχαίο r και στέλνοντας την ποσότητα

$$x \equiv r^2 v^{-1} \pmod{n}$$

αντί του τετραγώνου του r. Έτσι θα ισχύει:

$$y^2 \equiv r^2 v v^{-1} \equiv r^2 \pmod{n}$$

Επειδή όμως ο Βύρων έχει την επιλογή να ζητήσει απόδειξη ότι η Αλίκη γνωρίζει την τετραγωνική ρίζα του x, ο αντίπαλος θα πρέπει να λύσει το δύσκολο πρόβλημα υπολογισμού της τετραγωνικής ρίζας του $r^2 v^{-1} \bmod n$.

Το πρωτόκολλο μπορεί να επαναληφθεί περισσότερες από μία φορές. Μάλιστα είναι επιθυμητό να επαναληφθεί περισσότερες από μία φορές, διότι λόγω των

παραπάνω, ο αντίπαλος έχει πιθανότητα 0.5 να επιτύχει πλαστοπροσωπία, με μία και μόνο εκτέλεση του πρωτοκόλλου. Αν το πρωτόκολλο επαναληφθεί t φορές, τότε η πιθανότητα επιτυχίας του αντιπάλου θα είναι ίση με 2^{-t}. Είναι ευνόητο πως αν υπάρξει έστω και μια εσφαλμένη απάντηση, ο Βύρων τερματίζει το πρωτόκολλο και απορρίπτει την απόπειρα απόδειξης.

Το πρωτόκολλο των Fiat και Shamir κατατάσσεται στην κατηγορία των πρωτοκόλλων μηδενικής γνώσης. Αυτό σημαίνει ότι μπορούμε να κατασκευάσουμε αλγόριθμο ο οποίος παράγει τα μηνύματα του πρωτοκόλλου χωρίς τη γνώση του μυστικού s και χωρίς να έχουμε τη δυνατότητα να διακρίνουμε ότι τα μηνύματα παράχθηκαν από τον αλγόριθμο και όχι από την εκτέλεση του πρωτοκόλλου μεταξύ της Αλίκης και του Βύρωνα. Όντως, ο παρακάτω αλγόριθμος έχει τη δυνατότητα παραγωγής των μηνυμάτων του πρωτοκόλλου, χωρίς τη γνώση του s:

1. Επιλογή τυχαίου y, τέτοιου ώστε $0 < y < n$.
2. Επιλογή τυχαίας πρόκλησης $b \in \{0, 1\}$.
3. – Αν $b = 0$ τότε:
   $$x \leftarrow y^2 \bmod n$$
   – Αν $b = 1$ τότε:
   $$x \leftarrow y^2 v^{-1} \bmod n$$

Ο παραπάνω αλγόριθμος παράγει τριάδες (x, b, y) οι οποίες ικανοποιούν τους ελέγχους του πρωτοκόλλου των Fiat και Shamir.

9.6.3. Πρωτόκολλο αυθεντικοποίησης των Guillou και Quisquater

Το πρωτόκολλο αυθεντικοποίησης μηδενικής γνώσης των Guillou και Quisquater (GQ) είναι επέκταση του πρωτοκόλλου των Fiat και Shamir που παρουσιάσαμε στην προηγούμενη ενότητα. Η ασφάλεια του πρωτοκόλλου GQ βασίζεται στη δυσκολία εύρεσης των πρώτων παραγόντων ενός σύνθετου αριθμού. Η βασική διαφορά των δύο πρωτοκόλλων είναι ότι στο πρωτόκολλο GQ ο χώρος της πρόκλησης αποτελείται από περισσότερα από 1 bits, με αποτέλεσμα να απαιτούνται λιγότερες επαναλήψεις του πρωτοκόλλου προκειμένου να επιτευχθεί μικρή πιθανότητα πλαστοπροσωπίας.

Το πρωτόκολλο περιλαμβάνει έμπιστη οντότητα η οποία καθορίζει τις δημόσιες παραμέτρους και απονέμει ταυτότητες στα μέλη. Οι δημόσιες παράμετροι προκύπτουν με βάση το κρυπτοσύστημα RSA. Η έμπιστη οντότητα επιλέγει δύο μεγάλους πρώτους αριθμούς p και q οι οποίοι καθορίζουν το δημόσιο modulus $n = pq$. Στη συνέχεια, επιλέγει ένα δημόσιο εκθέτη $e > 2$, με $\gcd(e, \phi(n)) = 1$ και υπολογίζει τον ιδιωτικό εκθέτη:

$$s = e^{-1} \bmod \phi(n).$$

Οι δημόσιες παράμετροι είναι οι (e, n).

Το επόμενο στάδιο είναι η διαδικασία εγγραφής του μέλους. Έστω ότι η Αλίκη επιθυμεί να εγγραφεί στο σύστημα αυθεντικοποίησης. Η έμπιστη οντότητα επιλέγει την ταυτότητα της Αλίκης, η οποία είναι ένας ακέραιος ID_A, έτσι ώστε $1 < ID_A < n$. Στη συνέχεια, η έμπιστη οντότητα υπολογίζει το μυστικό απόδειξης της Αλίκης:

$$s_A = (ID_A)^{-s} \bmod n$$

την οποία και παραδίδει εμπιστευτικά στην Αλίκη. Τέλος, η έμπιστη οντότητα δημοσιεύει την ταυτότητα της Αλίκης μαζί με τα στοιχεία της σε κάποιο δημόσιο ευρετήριο.

Κατά τη διαδικασία αυθεντικοποίησης στον Βύρωνα, εκτελούνται t κύκλοι του πρωτοκόλλου αυθεντικοποίησης. Ο κάθε κύκλος του πρωτοκόλλου αποτελείται από τα ακόλουθα βήματα:

1. Η Αλίκη δεσμεύεται με έναν τυχαίο αριθμό r, όπου $0 < r < n$. Στη συνέχεια υψώνει τον αριθμό αυτό στο δημόσιο εκθέτη, και στέλνει το αποτέλεσμα στον Βύρωνα:

   $$\text{Αλίκη} \rightarrow \text{Βύρων: } x \equiv r^e \pmod{n}$$

2. Ο Βύρων επιλέγει την πρόκληση b, όπου $1 \le b \le e$ την οποία στέλνει στην Αλίκη:

   $$\text{Βύρων} \rightarrow \text{Αλίκη: } b$$

3. Η Αλίκη υπολογίζει την απόκριση y και τη στέλνει στον Βύρωνα:

   $$\text{Αλίκη} \rightarrow \text{Βύρων: } y \equiv r s_A^e \pmod{n}$$

4. Ο Βύρων προμηθεύεται την ταυτότητα της Αλίκης από το ευρετήριο και ελέγχει αν ισχύει:

   $$x \equiv (ID_A)^b y^e \pmod{n},$$

   απορρίπτοντας την περίπτωση όπου $x \equiv 0 \pmod{n}$.

Η ανάλυση του πρωτοκόλλου GQ είναι παρόμοια με την ανάλυση του πρωτοκόλλου των Fiat και Shamir. Η πιθανότητα επιτυχούς πλαστοπροσωπίας από τον αντίπαλο για t γύρους είναι ίση με $(1/e)^{-t}$.

9.6.4. Πρωτόκολλο αυθεντικοποίησης του Schnorr

Το πρωτόκολλο των Fiat και Shamir καθώς και το πρωτόκολλο των Guillou και Quisquater που παρουσιάσαμε βασίζονται στο πρόβλημα της παραγοντοποίησης ενός σύνθετου ακεραίου σε γινόμενο πρώτων παραγόντων. Η ασφάλεια του πρωτοκόλλου του Schnorr που θα παρουσιάσουμε στη συνέχεια βασίζεται στο πρόβλημα του διακριτού λογάριθμου.

Σε αντίθεση με τα πρωτόκολλα μηδενικής γνώσης που παρουσιάσαμε, το πρωτόκολλο του Schnorr δεν απαιτεί επαναληπτική εκτέλεση του πρωτοκόλλου προκειμένου να μειωθεί η πιθανότητα πλαστοπροσωπίας. Η πιθανότητα καθορίζεται από την επιλογή μίας εκ των παραμέτρων, όπως θα δούμε παρακάτω.

Το πρωτόκολλο αυθεντικοποίησης απαιτεί τη συμμετοχή τρίτης έμπιστης οντότητας, προκειμένου να καθοριστούν οι δημόσιες παράμετροι. Επιπλέον, η έμπιστη οντότητα λειτουργεί και ως Αρχή Πιστοποίησης, εκδίδοντας ψηφιακά πιστοποιητικά στα μέλη της. Αρχικά, η έμπιστη οντότητα επιλέγει δύο πρώτους αριθμούς p και q τέτοιους ώστε ο q να είναι παράγοντας του $(p–1)$. Στη συνέχεια, επιλέγει u τέτοιο ώστε η πολλαπλασιαστική τάξη να είναι q και $0 < u < p$.

Η παραμετροποίηση του επιπέδου της ασφάλειας γίνεται με τον q. Αν θέσουμε

$$t=\lfloor \log_2(q) \rfloor,$$

τότε θα ισχύει και $2^t \le q$. Η παράμετρος t καθορίζει το επίπεδο ασφάλειας. Έτσι μπορούμε να εργασθούμε αντίστροφα, δηλαδή να ορίσουμε το t και στη συνέχεια να επιλέξουμε q τέτοιο ώστε $2^t < q$.

Οι δημόσιοι παράμετροι είναι η τριάδα (p, q, u) καθώς και το δημόσιο κλειδί της οντότητας το οποίο χρησιμοποιείται για την επαλήθευση των πιστοποιητικών των μελών.

Κατά την εγγραφή ενός μέλους, η έμπιστη οντότητα επιλέγει την ταυτότητα ID_A, ενώ το μέλος (για παράδειγμα η Αλίκη) επιλέγει έναν ακέραιο a τέτοιον ώστε $0 < a < q$. Στη συνέχεια η Αλίκη υπολογίζει το:

$$v = u^{-a} \bmod p\ ,$$

το οποίο στέλνει στην έμπιστη οντότητα. Τέλος, η έμπιστη οντότητα εκδίδει πιστοποιητικό για την Αλίκη το οποίο αποτελείται από τα στοιχεία ID_A και v, καθώς και την ψηφιακή υπογραφή της έμπιστης οντότητας στα στοιχεία αυτά. Έστω $cert_A$ το πιστοποιητικό που προκύπτει.

Κατά την εκτέλεση του πρωτοκόλλου αυθεντικοποίησης, η Αλίκη αποδεικνύει την ταυτότητά της στον Βύρων με τα ακόλουθα βήματα:

1. Η Αλίκη επιλέγει τυχαίο ακέραιο r με $0 < r < q$ τον οποίο χρησιμοποιεί ως εκθέτη στη δημόσια παράμετρο u και στέλνει το αποτέλεσμα στον Βύρωνα μαζί με το πιστοποιητικό της:

   Αλίκη $\rightarrow$ Βύρων: $cert_A,\ x \equiv u^r \pmod p$.

2. Ο Βύρων επιλέγει πρόκληση b, με $1 \le b \le 2^t$, την οποία στέλνει στην Αλίκη:

   Βύρων $\rightarrow$ Αλίκη: b.

3. Η Αλίκη υπολογίζει την απόκριση y την οποία στέλνει στον Βύρωνα:

$$\text{Αλίκη} \rightarrow \text{Βύρων: } y \equiv a \cdot b + r \pmod{q}$$

4. Ο Βύρων δέχεται την ταυτότητα της Αλίκης ελέγχοντας αν ισχύει η σχέση:
$$x \equiv u^y v^b \pmod{p}$$

Είναι φανερό ότι η επιτυχής εκτέλεση του πρωτοκόλλου απαιτεί τη γνώση του μυστικού απόδειξης a από το μέλος του οποίου αυθεντικοποιείται η ταυτότητα. Ο συνυπολογισμός της δέσμευσης r στα μηνύματα x και y έχει ως αποτέλεσμα την απόκρυψη του μυστικού απόδειξης, εφόσον ο r είναι τυχαίος και δεν είναι γνωστό σε κανέναν παρά μόνο στην Αλίκη. Επομένως, τα μηνύματα του πρωτοκόλλου δεν αποκαλύπτουν καμία μυστική παράμετρο.

Ωστόσο, για μεγάλη τιμή της πρόκλησης b, ο Βύρων στο τέλος του πρωτοκόλλου έχει τη λύση (x, y, b) της εξίσωσης

$$x \equiv u^y v^b \pmod{p}$$

που σημαίνει ότι μπορεί να αποδείξει ότι γνωρίζει τη λύση (την οποία δεν μπορούσε να υπολογίσει πριν ολοκληρωθεί το πρωτόκολλο),οπότε και το πρωτόκολλο χάνει την ιδιότητα της μηδενικής γνώσης.

Από πλευράς ασφάλειας, η πιθανότητα επιτυχίας του αντιπάλου είναι της τάξης του 2^{-t}. Αυτό αναλύεται με τον ακόλουθο αλγόριθμο επίθεσης του αντιπάλου (ο οποίος συμπίπτει και με την απόδειξη της ιδιότητας της μηδενικής γνώσης) :

1. Ο αντίπαλος επιλέγει μια πρόκληση b. Η πιθανότητα να επιλέξει τη σωστή πρόκληση είναι 2^{-t}.
2. Ο αντίπαλος επιλέγει τυχαία απόκριση y και υπολογίζει τη δέσμευση x όπως απαιτεί η προεπιλεγμένη απόκριση:
$$x \equiv u^y v^b \pmod{p}$$
3. Ο αντίπαλος έχει μια τριάδα (x, y, b) η οποία πληροί τις απαιτήσεις του πρωτοκόλλου αυθεντικοποίησης και μπορεί να εκτελέσει το πρωτόκολλο με τον Βύρωνα.

Ο αλγόριθμος του αντιπάλου ολοκληρώνεται σε πολυωνυμικό χρόνο, παράγοντας τα επιθυμητά μηνύματα του πρωτοκόλλου.

9.6.5. Πρωτόκολλα μηδενικής γνώσης βασισμένα στη θεωρία γράφων

Μια κατηγορία δύσκολων προβλημάτων ανήκει στην περιοχή της θεωρίας των γράφων. Το πρωτόκολλο που θα παρουσιάσουμε είναι των Goldreich, Michali και Wigderson, στο οποίο η Αλίκη αποδεικνύει στον Βύρωνα ότι γνωρίζει τον ισομορφισμό δύο γράφων G_1 και G_2.

Είναι γνωστό από τη θεωρία γράφων, ότι ο έλεγχος ισομορφισμού δύο γράφων, είναι ένα από τα δύσκολα προβλήματα, για μεγάλους γράφους. Ωστόσο από έναν γράφο G_1 μπορεί να προκύψει ισομορφικός γράφος G_2, από την αντιμετάθεση των στοιχείων του G_1. Αυτή είναι και η διαδικασία που ακολουθεί η Αλίκη προκειμένου να έχει στην κατοχή της δύο γράφους και επιπλέον να γνωρίζει τον ισομορφισμό αυτών.

Με το πρωτόκολλο αυθεντικοποίησης, η Αλίκη αποδεικνύει στον Βύρωνα ότι γνωρίζει τον ισομορφισμό των G_1 και G_2, χωρίς να αποκαλύψει τη λύση στον Βύρωνα. Αυτό επιτυγχάνεται με τα ακόλουθα βήματα:

1. Η Αλίκη δημιουργεί έναν γράφο H αντιμεταθέτοντας τα στοιχεία του G_1. Ο H θα είναι ισομορφικός με τον G_1 και κατ επέκταση και με τον G_2. Η Αλίκη γνωρίζοντας τον ισομορφισμό των G_1 και H και τον ισομορφισμό των G_1 και G_2, μπορεί να υπολογίσει και τον ισομορφισμό του H και G_2. Στη συνέχεια δεσμεύεται στέλνοντας τον H στον Βύρωνα:

   Αλίκη $\rightarrow$ Βύρων: H

2. Ο Βύρων επιλέγει τυχαία την πρόκληση $b \in \{1, 2\}$ την οποία στέλνει στην Αλίκη:

   Βύρων $\rightarrow$ Αλίκη: b

3. Η Αλίκη αποκαλύπτει τον ισομορφισμό μεταξύ των G_b και H στον Βύρωνα.
4. Ο Βύρων μπορεί να ελέγξει αν ο ισομορφισμός είναι σωστός.

Το πρωτόκολλο επαναλαμβάνεται t φορές. Η πιθανότητα επιτυχούς επίθεσης είναι ίση με 2^{-t}.

Ο Βύρων, έχοντας μόνον τη λύση του ισομορφισμού μεταξύ του H και ενός από τους G_i, δεν είναι σε θέση να υπολογίσει κανέναν άλλο ισομορφισμό μεταξύ των τριών γράφων.

Όροι-κλειδιά του κεφαλαίου
• κρυπτογραφικά πρωτόκολλα και κρυπτογραφικές υπηρεσίες
• αποτυχία πρωτοκόλλου
• αυτοεπιβαλλόμενο πρωτόκολλο
• πρωτόκολλο με δικαστή και διαιτητή
• bit δέσμευση
• νοερό πόκερ
• έλεγχος προσπέλασης
• εξουσιοδότηση
• πρωτόκολλα μηδενικής γνώσης

9.7. Ασκήσεις

1. Κατασκευάστε ένα πρωτόκολλο για το «πρόβλημα του ραντεβού», του Κεφαλαίου 1.
2. Δείξτε πως μπορεί να πραγματοποιηθεί ρίψη κέρματος μέσω τηλεφώνου, χρησιμοποιώντας έναν τηλεφωνικό κατάλογο (σημ. το πρωτόκολλο που θα κατασκευάστε να είναι αυτοεπιβαλλόμενο).
3. Έστω ένα σύστημα στο οποίο η πρόσβαση απαιτεί τη διαδοχική εισαγωγή δύο κωδικών πρόσβασης, PIN και PWD. Ο PIN αποτελείται από έναν τετραψήφιο αριθμό, ενώ ο PWD μπορεί να είναι αλφαριθμητικός κωδικός, μήκους 12 χαρακτήρων. Λόγω του μικρού μεγέθους του PIN, απαιτείται το «κλείδωμα» του χρήστη, στην περίπτωση που εισάγει λάθος PIN τρεις συνεχόμενες φορές. Θεωρούμε τις δύο εναλλακτικές ελέγχου πρόσβασης:

   Εναλλακτική 1:
   - Το σύστημα ζητάει τον κωδικό PWD.
   - Μόλις ο χρήστης δώσει το σωστό PWD, το σύστημα ζητάει τον κωδικό PIN.

   Εναλλακτική 2:
   - Το σύστημα ζητάει τον κωδικό PIN.
   - Μόλις ο χρήστης δώσει το σωστό PIN, το σύστημα ζητάει τον κωδικό PWD.

   Ποια από τις παραπάνω εναλλακτικές προτείνετε; Αιτιολογήστε την απάντησή σας.