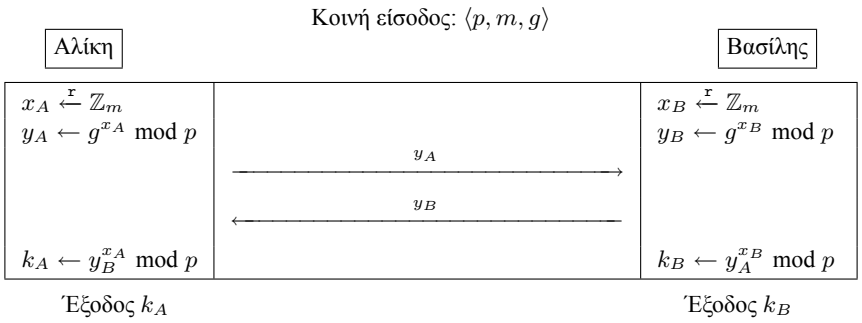
1 Diffie-Hellman Key Exchange Protocol

Το 1976, οι Whitefield Diffie και Martin Hellman δημοσίευσαν το άρθρο *New Directions in Cryptography*, φέρνοντας επανάσταση στην οποία οφείλεται η λεγόμενη "μοντέρνα κρυπτογραφια". Πριν από αυτή την δημοσίευση, κάθε ουσιώδης κρυπτογραφική τεχνική βασιζόταν σε κάποιο προ-συμφωνημένο κλειδί. Στο άρθρο τους όμως, οι Diffie και Hellman πρότειναν ένα πρωτόκολλο που επέτρεπε σε δύο μεριές, δίχως προηγούμενη επικοινωνία, να καταλήξουν σε κάποιο μυστικό κλειδί μέσω ενός μη ασφαλούς καναλιού. Στην συνέχεια θα εισάγουμε το βασικό πρωτόκολλο ανταλλαγής κλειδιού των Diffie-Hellman και θα μελετήσουμε την ασφάλειά του παρουσία παθητικών και ενεργητικών αντιπάλων.

1.1 Το πρωτόκολλο Diffie-Hellman

Η εικόνα 1 αναπαριστά το απλό πρωτόκολλο Diffie-Hellman ανταλλαγής κλειδιού. Αρχικά, οι δύο πλευρές, η Αλίκη και ο Βασίλης, διαλέγουν τις τιμές x_A και x_B αντίστοιχα. Καμία μεριά δεν αποκαλύπτει την τιμή της στην άλλη.



Σχήμα 1: Το πρωτόκολλο Diffie-Hellman ανταλλαγής κλειδιού, όπου p είναι ένας μεγάλος πρώτος και g ένα στοιχείο της ομάδας $\mathbb{Z}_p^*$ τάξης m.

Ο συμβολισμός $x \xleftarrow{r} \mathbb{Z}_m$ σημαίνει πως το x δειγματοληπτείται σύμφωνα με την ομοιόμορφη κατανομή στο $\mathbb{Z}_m$. Παρατηρείστε πως $y_B^{x_A} = y_A^{x_B} \bmod p$, συνεπώς $k_A = k_B$ και οι δυο μεριές υπολογίζουν την ίδια τιμή στο $\mathbb{Z}_p^*$.

Στην ενότητα **??** αναφέραμε το ενδιαφέρον μας στους στόχους, σχεδιασμούς, αρχές, μοντέλα και αποδείξεις κρυπτογραφίας. Ο στόχος ενός πρωτοκόλλου ανταλλαγής κλειδιού είναι να συμφωνήσουν οι δύο πλευρές σε ένα κλειδί παρουσία κάποιου που "κρυφακούει" την συνομιλία. Ο σχεδιασμός που μας ενδιαφέρει είναι το πρωτόκολλο Diffie-Hellman, τα θεμέλια του οποίου βασίζονται στα πρωτόκολλα δειγματοληψίας τυχαίων στοιχείων. Στη συνέχεια θα θέλαμε να μάθουμε πως να μοντελοποιήσουμε την ασφάλεια του πρωτοκόλλου ανταλλαγής κλειδιού και να μελετήσουμε τις απαραίτητες υποθέσεις για να θεωρηθεί η ανταλλαγή κλειδιού Diffie-Hellman αποδείξιμα ασφαλής.

1.2 Σχετικά Αριθμο-Θεωρητικά Προβλήματα

Εδώ θα εισάγουμε διάφορα πιθανά δύσκολα προβλήματα της Θεωρίας αριθμών τα οποία θα χρησιμοποιήσουμε στην απόδειξη ασφάλειας του Diffie-Hellman μέσω αναγωγής. Στις επόμενες ενότητες εξετάζουμε τον κατάλληλο ορισμό ασφαλείας και ανάγουμε την επίλυση ενός κατάλληλου προβλήματος Θεωρίας Αριθμών στην παραβίαση της ασφαλείας του πρωτοκόλλου.

Definition 1.2.1. Για μία πολλαπλασιαστική ομάδα G έστω $g \in G$ τάξης m και $y \in \langle g \rangle$. Το πρόβλημα ***διακριτού λογαρίθμου (discrete logarithm problem)*** (ΔΛ (DL)) είναι να βρεθεί ένας ακέραιος $x \in \mathbb{Z}_m$

τέτοιος ώστε $g^x = y$. Το πρόβλημα είναι καλά ορισμένο αφού $\langle g \rangle = \{g^0, g^1, \ldots, g^{m-1}\}$.

Δεν έχουμε απόδειξη πως αυτό το πρόβλημα είναι δύσκολο. Με βάση τις γνώσεις που έχουμε ως τώρα όμως, ο αριθμός απαραίτητων βημάτων για εύρεση λύσης σε αυτό το πρόβλημα είναι υπερ-πολυωνυμικός (super-polynomial) στο μέγεθος του στοιχείου της ομάδας, αν η ομάδα έχει επιλεγεί κατάλληλα.

Definition 1.2.2. Δεδομένης μιας κυκλικής ομάδας $\langle g \rangle$ τάξης m, g^a και g^b όπου $a, b \xleftarrow{\text{r}} \mathbb{Z}_m$, το ***υπολογιστικό Diffie-Hellman πρόβλημα (computational Diffie-Hellman problem)*** (YDH (CDH)) είναι να υπολογιστεί το g^{ab}.

Αξίζει να παρατηρηθεί ότι ένας αντίπαλος που επιτίθεται στο Diffie-Hellman πρωτόκολλο δεν ενδιαφέρεται για τον διακριτό λογάριθμο. Ο στόχος του είναι να λύσει το YDH. Είναι όμως ξεκάθαρο πως αν ένας αντίπαλος μπορεί να λύσει το ΔΛ έτσι ώστε να βρει το x από το g^x, τότε θα μπορούσε να λύσει και το YDH μέσω μιας απλής ύψωσης σε δύναμη. Με άλλα λόγια το υπολογιστικό πρόβλημα Diffie-Hellman ανάγεται στο διακριτό λογάριθμο: YDH $\leq$ ΔΛ.

Lemma 1.2.1. *Το υπολογιστικό πρόβλημα Diffie-Hellman problem δεν είναι πιο δύσκολο από τον πρόβλημα διακριτού λογαρίθμου.*

Είναι άγνωστο αν το ανάποδο ισχύει.

Definition 1.2.3. Το ***πρόβλημα απόφασης Diffie-Hellman (decisional Diffie-Hellman problem)*** (ADH) είναι το εξής: δεδομένης μιας ομάδας $G = \langle g \rangle$ τάξης m και g^a, g^b, g^c, όπου $a, b, c \xleftarrow{\text{r}} \mathbb{Z}_m$, αποφάσισε αν $c = ab$ ή $c \xleftarrow{\text{r}} \mathbb{Z}_m$.

Το παραπάνω είναι ένα πολύ ασθενές πρόβλημα αφού ρωτά τον αντίπαλο να αποφανθεί αν το c είναι επιλεγμένο τυχαία. Αν κάποιος μπορούσε να λύσει το YDH, θα μπορούσε να λύσει το ADH υπολογίζοντας το g^{ab} και συγκρίνοντας το με το g^c; συνεπώς, ADH $\leq$ YDH.

Lemma 1.2.2. *Το πρόβλημα απόφασης Diffie-Hellman δεν είναι δυσκολότερο από το υπολογιστικό πρόβλημα Diffie-Hellman.*

Επιπλέον, το τελευταίο πρόβλημα δεν είναι δυσκολότερο από το πρόβλημα διακριτού λογαρίθμου.

Στη συνέχεια της διάλεξης θα δείξουμε ότι το πρωτόκολλο του Diffie-Hellman είναι ασφάλες βάσει μιας υπόθεσης που σχετίζεται με το πρόβλημα ADH.

Μέχρι στιγμής δεν έχουμε προσδιορίσει πως επιλέξαμε την ομάδα. Στην πραγματικότητα έχουμε επιλέξει τις παραμέτρους μας με τέτοιο τρόπο έτσι ώστε να εξασφαλίσουμε πως τα προβλήματα που προκύπτουν είναι πραγματικά δύσκολα. Το επόμενο παράδειγμα δείχνει πως το πρόβλημα του διακριτού λογαρίθμου λύνεται σε πολυωνυμικό χρόνο αν δεν διαλέξουμε προσεκτικά την ομάδα.

Example. Θεωρήστε την ομάδα $\mathbb{Z}_p^*$ για κάποιον μεγάλο πρώτο p. Από ένα θεώρημα του Euler, το $\mathbb{Z}_p^*$ έχει τάξη $p-1$. Για το παράδειγμα αυτό θεωρείστε την περίπτωση που το $p-1$ παραγοντοποιείται σε μικρούς πρώτους q_i: $p - 1 = q_1 q_2 \cdots q_s$. Υπάρχει μια υπο-ομάδα G_i τάξης q_i.[1] Όρισε τον ομομορφισμό ομάδας $f_i \colon \mathbb{Z}_p^* \longrightarrow G_i$ ως $x \mapsto x^{p-1/q_i}$ και έστω $g_i = g^{p-1/q_i}$ για κάποιον φιξαρισμένο γεννήτορα g του $\mathbb{Z}_p^*$. Παρατηρείστε πως το g_i έχει τάξη q_i.

Διαλέγουμε κάποιο $y = g^x \bmod p$. Υψώνοντας και τις δύο μεριές στην δύναμη $(p-1)/q_i$, έχουμε $y^{p-1/q_i} \equiv (g^{p-1/q_i})^x \equiv g_i^{x \bmod q_i} \bmod p$ όπου $1 \leq i \leq s$. Επειδή το q_i είναι ένας μικρός πρώτος, μπορούμε να χρησιμοποιήσουμε ***εξαντλητική αναζήτηση (brute force)*** για να λύσουμε το πρόβλημα διακριτού λογαρίθμου, δηλαδή να βρούμε το σύνολο των αναλογιών $x_i \equiv x \bmod q_i$. Έτσι μπορούμε να υπολογίσουμε το x με βάση το κινέζικο θεώρημα υπολοίπων.

Για να αποφύγουμε αυτού του είδους την επίθεση, μπορούμε να διαλέξουμε το Z_p^* έτσι ώστε να περιέχει μια μεγάλη υπο-ομάδα. Για παράδειγμα αν $p = 2q+1$ και ο q είναι πρώτος, υπάρχει μια υπο-ομάδα μεγέθους q που μπορούμε να χρησιμομοποιήσουμε για να τρέξουμε το πρωτόκολλο Diffie-Hellman.

Η μεγαλύτερη ομάδα μέσα στο Z_p^* που υπάρχει περίπτωση ο διακριτός λογάριθμος να είναι γενικά δύσκολος είναι τα τετραγωνικά υπόλοιπα του $\mathbb{Z}_p^*$.

[1] Η ύπαρξη μιας τέτοιας υπο-ομάδας είναι εγγυημένη από το θεώρημα Cauchy.

Definition 1.2.4. Το ***τετραγωνικό υπόλοιπο (quadratic residue)*** του G είναι η υπο-ομάδα που αποτελείται από όλα τα $y \in G$ τέτοια ώστε υπάρχει $x \in G$ με $x^2 = y$.

Όταν $G = \mathbb{Z}_n^*$, γράφουμε το τετραγωνικό υπόλοιπο ως $QR(n)$. Στην συγκεκριμένη περίπτωση $G = \mathbb{Z}_p^*$ για κάποιον πρώτο p, $QR(p) = \langle g^2 \rangle$ ενός γεννήτορα g του G. Η ομάδα $QR(p)$ έχει ακριβώς τα μισά στοιχεία της ομάδας G. Είναι το μεγαλύτερη γνήσια υπο-ομάδα του $\mathbb{Z}_p^*$.

Η απεικόνιση $x \mapsto x^{\frac{p-1}{2}}$ είναι ιδιαίτερα χρήσιμη στην συγεκριμένη περίπτωση. Είναι εύκολο να δει κανείς πως η εικόνα της απεικόνισης είναι $\{1, -1\}$.

Αποδεικνύουμε το επόμενο χρήσιμο αποτέλεσμα σχετικά με τα τετραγωνικά υπόλοιπα.

Lemma 1.2.3. *Θεωρείστε κάποιο $a \in \mathbb{Z}$ και $p \equiv 3 \bmod 4$. Ισχύει πως $a^{\frac{p-1}{2}} = 1 \bmod p$ αν και μόνο αν $a \in QR(p)$.*

Απόδειξη. Για την ευθεία κατεύθυνση, υποθέστε πως υπάρχει κάποιο $a^{\frac{p-1}{2}} = 1 \bmod p$. Έστω $y = a^{\frac{p+1}{4}} \bmod p$. Τότε έχουμε πως

$$y^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a = a \bmod p$$

Δεδομένου ότι $y^2 = a \bmod p$ παίρνουμε $a \in QR(p)$.

Για την ανάποδη κατεύθυνση, αν $a \in QR(p)$, δηλαδή $y^2 = a \bmod p$ έχουμε πως $a^{\frac{p-1}{2}} = y^{p-1} = 1 \bmod p$. ∎

Παρατηρείστε πως η απόδειξη του λήμματος είναι κατασκευαστική, δηλαδή μας δίνει και έναν τρόπο να κατασκευάσουμε τις ρίζες ενός τετραγωνικού υπολοίπου του p. Πράγματι, δεδομένου ενός a και δύο ρίζες του a υπόλοιπο p υπολογίζονται ως $\pm a^{\frac{p+1}{4}} \bmod p$.

1.3 Γεννήτορες ομάδας

Definition 1.3.1. Ένας ***γεννήτορας ομάδας (group generator)*** GGen είναι ένας πιθανοτικός αλγόριθμος που παράγει μια περιγραφή μιας πεπερασμένης ομάδας G δεδομένου ενός μήκους λ. Το λιγότερο, η περιγραφή περιέχει ένα στοιχείο της ομάδας, μια πράξη στην ομάδα και έναν τρόπο (αλγόριθμο) ελέγχου ενός στοιχείου αν είναι μέλος της ομάδας.

Example. Διαλέγουμε το $\mathbb{Z}_p$ να είναι η ομάδα μας για κάποιο πρώτο p μήκους λ. Ο GGen επιστρέφει ένα στοιχείο g τάξης m, όπου m είναι μια συνάρτηση των λ και p. Η πράξη της ομάδας είναι ο πολλαπλασιασμός υπόλοιπό p και αν ένας ακέραιος είναι μεταξύ 0 και $p-1$, θεωρείτε μέλος της ομάδας.

Για παράδειγμα, ο αλγόριθμος GGen με είσοδο 1^λ μπορεί να υπολογίσει ένα τυχαίο αριθμό p της μορφής $3k+4$ που έχει λ bits, μετά να ελέγξει άν p είναι πρώτος. Αν όχι, διαλέγει άλλο p, αλλιώς ελεγχει άν $(p-1)/2$ είναι πρώτος, αν όχι διαλέγει άλλο p. Όταν βρεθεί το κατάλληλο p, διαλέγει ένα αριθμό $a \in \{2, \ldots, p-2\}$ στην τύχη και υπολογίζει το $a^{(p-1)/2} \bmod p$. Αν αυτή η τιμή είναι 1 τότε διαλέγει άλλο a. Αλλιώς θέτει $g = a^2 \bmod p$. Η έξοδος του αλγόριθμου GGen είναι οι τιμές $(p, g, m = (p-1)/2)$.

1.4 Η υπόθεση προβλήματος απόφασης Diffie-Hellman

Διαισθητικά, το ADH υποθέτει πως είναι δύσκολο να διακρίνει κανείς πλειάδες της μορφής $\langle G, m, g, g^a, g^b, g^{ab} \rangle$ και $\langle G, m, g, g^a, g^b, g^c \rangle$, όπου το g ανήκει σε κάποιο πολλαπλασιαστική ομάδα και τα a, b και c είναι τυχαία επιλεγμένες δυνάμεις.

Definition 1.4.1. Ένας γεννήτορας GGen λέμε πως ικανοποιεί την ***υπόθεση απόφασης Diffie-Hellman (decisional Diffie-Hellman assumption)*** αν τα σύνολα πιθανοτήτων $\{\mathcal{D}_\lambda\}_{\lambda \in \mathbb{N}}$ και $\{\mathcal{R}_\lambda\}_{\lambda \in \mathbb{N}}$ είναι υπολογιστικά αδιακρίτα.

$$\mathcal{D}_\lambda := \left\{ \langle G, m, g \rangle \leftarrow \mathsf{GGen}(1^\lambda);\ a, b \xleftarrow{\mathrm{r}} \mathbb{Z}_m : (G, m, g^a, g^b, g^{ab}) \right\}$$
$$\mathcal{R}_\lambda := \left\{ \langle G, m, g \rangle \leftarrow \mathsf{GGen}(1^\lambda);\ a, b, c \xleftarrow{\mathrm{r}} \mathbb{Z}_m : (G, m, g^a, g^b, g^c) \right\}$$

όπου $m = \mathsf{ord}(g)$.

Αντίστοιχα, αν $\mathcal{A}$ είναι ένα στατιστικό τεστ που η υπολογιστική του ισχύς φράσσεται από πολυωνυμικό χρόνο με δυνατότητα χρήσης πιθανοτήτων (probabilistic polynomial-time (PPT)) ισχύει πως

$$\mathsf{Adv}^{\mathcal{A}}(\lambda) = \left| \underset{\gamma \leftarrow \mathcal{D}_\lambda}{\mathsf{Prob}} [\mathcal{A}(\gamma) = 1] - \underset{\gamma \leftarrow \mathcal{R}_\lambda}{\mathsf{Prob}} [\mathcal{A}(\gamma) = 1] \right|$$

είναι αμελητέο στο λ. Το $\mathsf{Adv}^{\mathcal{A}}$ ονομάζετε το ***πλεονέκτημα (advantage)*** of $\mathcal{A}$.

1.5 Μοντελοποίηση της Ασφάλειας έναντι Παθητικών Αντιπάλων

Όταν ορίζουμε την ασφάλεια, είναι σημαντικό να λαμβάνουμε υπ' όψη τον αναμενόμενο αντίπαλο. Στην ενότητα αυτή εστιάζουμε στου παθητικούς αντιπάλους. Ένας τέτοιος αντίπαλος "κρυφακούει" το κανάλι επικοινωνίας και προσπαθεί να εξάγει πληροφορία για το κλειδί χωρίς να παρεμβαίνει. Πριν μελετήσουμε τους ορισμούς ασφαλείας, καθιερώνουμε κάποιους κοινούς συμβολισμούς.

Έστω $\mathtt{trans}_{A,B}(1^\lambda)$ η κατανομή των καταγραφών των αλληλεπιδράσεων μεταξύ δύο παικτών A και B. Στο πρωτόκολλο Diffie-Hellman, η καταγραφή συμπεριλαμβάνει την κοινή είσοδο και κάθε ανταλλαγή πληροφορίας. Το κοινό κλειδί που παράγεται στο τέλος της καταγραφής τ συμβολίζεται ως $key(\tau)$. Τέλος, το κατηγόρημα V είναι ένας αλγόριθμος που η έξοδοι του είναι 1 και 0 (`True` και `False`).

Μοντέλο Ασφάλειας 1

Το πιο προφανές μοντέλο ασφαλείας για κάθε ανταλλαγή κλειδιού ορίζει πως το πρωτόκολλο για να είναι ασφαλές πρέπει ο αντίπαλος να μην μπορεί να λάβει μέρος του κλειδιού. Πιο συγκεκριμένα, για κάθε PPT αντιπάλους [2] $\mathcal{A}$,

$$\underset{\tau \leftarrow \mathtt{trans}_{A,B}(1^\lambda)}{\mathsf{Prob}} [\mathcal{A}(\tau) = key(\tau)]$$

είναι αμελητέα συνάρτηση στο λ. Σε αυτό το μοντέλο, είναι εύκολο ένας αντίπαλος να εξάγει πληροφορία για ένα μικρό μέρος του κλειδιού. Γι' αυτό το λόγο το μοντέλο είναι ανεπαρκές. Ο αριθμός των bits που προστατεύονται σε αυτό το μοντέλο μπορεί να είναι μόνο $\log^2(\lambda)$.

Μοντέλο Ασφάλειας 2

Για κάθε PPT αντίπαλο $\mathcal{A}$ και κατηγορήματα V, ορίζουμε πως μια ανταλλαγή κλειδιού είναι ασφαλής αν

$$\underset{\tau \leftarrow \mathtt{trans}_{A,B}(1^\lambda)}{\mathsf{Prob}} [\mathcal{A}(\tau) = V(key(\tau))] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

για κάποια αμελητέα συνάρτηση $\mathsf{negl}(\lambda)$. Αυτό το μοντέλο είναι ιδανικό, διότι αν το πρωτόκολλό μας είναι ασφαλές, ένας αντίπαλος δεν μπορεί να ανακαλύψει καμία πληροφορία για το κλειδί. Δυστυχώς, το παραπάνω μοντέλο δεν είναι ρεαλιστικό. Θα δούμε γιατί παρακάτω προσπαθώντας να αποδείξουμε ότι το DH πρωτόκολλο είναι ασφαλές.

Υποθέστε πως το μοντέλο αυτό ορίζει την ασφάλεια και υπάρχει ένα PPT αντίπαλος $\mathcal{A}$ ικανός να σπάσει το πρωτόκολλο ανταλλαγής κλειδιού. Τότε υπάρχει ένα κατηγόρημα V τέτοιο ώστε

$$\underset{\tau \leftarrow \mathtt{trans}_{A,B}(1^\lambda)}{\mathsf{Prob}} [\mathcal{A}(\tau) = V(key(\tau))] \geq \frac{1}{2} + \alpha,$$

όπου α μη αμελητέο. Έστω $\mathcal{B}$ ένα στατιστικό τεστ ADH τέτοιο ώστε, δεδομένου $\gamma = \langle G, m, g, a, b, c \rangle$, $\mathcal{B}$ χρησιμοποιεί γ για να κατασκευάσει μια καταγραφή $\tau_\gamma = \langle G, m, g, a, b \rangle$. $\mathcal{B}$ και προσομοιώνει τον $\mathcal{A}$ στο τ_γ για να λάβει το αποτέλεσμά του S. Ο $\mathcal{B}$ θα επιστρέψει 1 αν $V(c) = S$ και 0 αν $V(c) \neq S$. Όταν το c είναι ένα τυχαίο στοιχείο της κυκλικής ομάδας G, έστω $\mathsf{Prob}[V(c) = 1] = \delta$.

[2] Θα λέμε αντίπαλο εννοώντας οποιονδήποτε PPT αλγόριθμο.

1. Αν $\gamma \leftarrow \mathcal{D}_\lambda$, τότε $c = key(\tau_\gamma)$ και $\underset{\gamma \leftarrow \mathcal{D}_\lambda}{\mathsf{Prob}}[\mathcal{B}(\gamma) = 1] \geq \frac{1}{2} + \alpha$.

2. Αν $\gamma \leftarrow \mathcal{R}_\lambda$, τότε $c \xleftarrow{\mathtt{r}} G$ και

$$\begin{aligned}\underset{\gamma \leftarrow \mathcal{R}_\lambda}{\mathsf{Prob}}[\mathcal{B}(\gamma) = 1] &= \underset{\langle G,m,g,a,b,c\rangle \leftarrow \mathcal{R}_\lambda}{\mathsf{Prob}}[\mathcal{A}(G, m, g, a, b) = V(c)] \\ &= \mathsf{Prob}[\mathcal{A}(\tau_\gamma) = V(c)] \\ &= \mathsf{Prob}[\mathcal{A}(\tau_\gamma) = V(c) \mid V(c) = 1] \cdot \mathsf{Prob}[V(c) = 1] + \ldots \\ &\quad \ldots + \mathsf{Prob}[\mathcal{A}(\tau_\gamma) = V(c) \mid V(c) = 0] \cdot \mathsf{Prob}[V(c) = 0] \\ &= \mathsf{Prob}[\mathcal{A}(\tau_\gamma) = 1] \cdot \mathsf{Prob}[V(c) = 1] + \mathsf{Prob}[\mathcal{A}(\tau_\gamma) = 0] \cdot \mathsf{Prob}[V(c) = 0]\end{aligned}$$

Στην ειδική περίπτωση όπου $\delta = 1/2$, έχουμε πως

$$\underset{\gamma \leftarrow \mathcal{R}_\lambda}{\mathsf{Prob}}[\mathcal{B}(\gamma) = 1] = (\mathsf{Prob}[\mathcal{A}(\tau_\gamma) = 1] + \mathsf{Prob}[\mathcal{A}(\tau_\gamma) = 0])\frac{1}{2} = \frac{1}{2}.$$

Βλέποντας την υπόθεση DDH,

$$\mathsf{Adv}^{\mathcal{B}} \geq \left(\frac{1}{2} + \alpha\right) - \frac{1}{2} = \alpha.$$

Επειδή το α είναι μη αμελητέο, ο $\mathcal{B}$ παραβιάζει την υπόθεση ADH δοθέντος του $\mathcal{A}$ και ισχύει $\delta = 1/2$. Όταν όμως $\delta \neq 1/2$, είναι εύκολο να βρούμε V που ο αντίπαλος μπορεί να μαντέψει με πιθανότητα καλύτερη από $1/2$ (π.χ., V μπορεί να είναι το ``ή'' των δύο πρώτων bits του c). Ως αποτέλεσμα, όλα τα σχήματα αποτυγχάνουν στο αφύσικα ισχυρό μοντέλο.

Μοντέλο Ασφάλειας 3

Το παραπάνω παράδειγμα μας έδειξε οτι οι απαιτήσεις που είχαμε στο μοντέλο ασφάλειας ήταν μη ρεαλιστικές. Εδώ μελετούμε το μοντέλο στο οποίο η ασφάλεια του πρωτοκόλλου ανταλλαγής κλειδιού μπορεί να αποδειχθεί. Αυτό ορίζει την παθητική ασφάλεια.

Πρέπει να αναγνωρίσουμε ότι ο αντίπαλος να καταλάβει κάποια συνάρτηση ενός μέρος του κλειδιού με πιθανότητα καλύτερη από $1/2$, συνεπώς έστω

$$\underset{key \leftarrow \mathsf{Key}(1^\lambda)}{\mathsf{Prob}}[V(key) = 1] = \delta,$$

όπου $\mathsf{Key}(1^\lambda)$ είναι η πιθανοτική κατανομή του πεδίο ορισμού του κλειδιού για το πρωτόκολλο με παράμετρο 1^λ (δηλαδή η τυχαία μεταβλητή $key(\mathtt{trans}_{A,B}(1^\lambda))$. Μπορεί εύκολα να διαπιστώσει κανεις πως στη περίπτωση της ανταλλαγής κλειδιού Diffie Hellman ισχύει πως το $\mathsf{Key}(1^\lambda)$ ισούται με ένα ομοιόμορφα επιλεγμένο στοιχείο της ομάδας $\langle g \rangle$. Στη συνέχεια ορίζουμε πως το πρωτόκολλο είναι ασφαλές αν ισχύει πως

$$\underset{\tau \leftarrow \mathtt{trans}_{A,B}(1^\lambda)}{\mathsf{Prob}}[\mathcal{A}(\tau) = V(key(\tau))] \leq \max\{\delta, 1 - \delta\} + \mathsf{negl}(\lambda).$$

Υποθέτουμε ότι

$$\underset{\gamma \leftarrow \mathcal{D}_\lambda}{\mathsf{Prob}}[\mathcal{B}(\gamma) = 1] \geq \max\{\delta, 1 - \delta\} + \alpha$$

για μη αμελητεο α. Χρησιμοποιώντας αυτό δείχνουμε πως $\underset{\gamma \leftarrow \mathcal{R}_\lambda}{\mathsf{Prob}}[\mathcal{B}(\gamma) = 1] \leq \max\{\delta, 1 - \delta\}$:

$$\begin{aligned}\underset{\gamma\leftarrow\mathcal{R}_\lambda}{\mathsf{Prob}}[\mathcal{B}(\gamma)=1] &= \mathsf{Prob}[\mathcal{A}(\tau_\gamma)=1]\cdot\mathsf{Prob}[V(c)=1]+\mathsf{Prob}[\mathcal{A}(\tau_\gamma)=0]\cdot\mathsf{Prob}[V(c)=0]\\ &= \mathsf{Prob}[\mathcal{A}(\tau_\gamma)=1]\delta+\mathsf{Prob}[\mathcal{A}(\tau_\gamma)=0](1-\delta)\\ &\leq \mathsf{Prob}[\mathcal{A}(\tau_\gamma)=1](\max\{\delta,1-\delta\})+\mathsf{Prob}[\mathcal{A}(\tau_\gamma)=0](\max\{\delta,1-\delta\})\\ &= (\mathsf{Prob}[\mathcal{A}(\tau_\gamma)=1]+\mathsf{Prob}[\mathcal{A}(\tau_\gamma)=0])\max\{\delta,1-\delta\}\\ &= \max\{\delta,1-\delta\}.\end{aligned}$$

Βασιζόμενοι στο παραπάνω αποδεικνύουμε το παρακάτω θεώρημα.

Theorem 1.5.1. *Επειδή η υπόθεση ADH είναι αληθής, το πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman είναι ασφαλές έναντι παθητικών αντιπάλων στο μοντέλο Ασφαλείας 3.*

1.6 Κατάλληλοι γεννήτορες ομάδων για την υπόθεση ADH

Σε αυτή την ενότητα, εξετάζουμε την υπόθεση ADH σε δύο ομάδες.

Πρώτον θεωρείστε $\langle g\rangle = \mathbb{Z}_p^*$ για κάποιον μεγάλο πρώτο p. Αυτή η ομάδα είναι πιθανώς μια κακή επιλογή. Στην πραγματικότητα μπορούμε να κατασκευάσουμε έναν PPT αλγόριθμο $\mathcal{A}$ όπως στην εικόνα 2 που "σπάει" την υπόθεση ADH.

```
Αλγόριθμος A(p, m, g, a, b, c)
    Αν (a^{m/2} = 1 ∨ b^{m/2} = 1) ∧ (c^{m/2} = 1)
        τότε επέστρεψε 1
        διαφορετικά επέστρεψε 0
```

Σχήμα 2: Ένας PPT αλγόριθμος που "σπάει" την υπόθεση ADH όταν $\langle g\rangle = \mathbb{Z}_p^*$, $a, b, c \in \langle g\rangle$, και $m = \mathsf{ord}(g)$ είναι άρτιος.

Από το θεώρημα του Euler, το $\mathbb{Z}_p^*$ έχει τάξη $m = p-1$. Επειδή το p είναι περιττό για κάθε πρώτο μεγαλύτερο του 2, το m είναι περιττό για κάθε μη τετριμμένη ομάδα.

Έστω $\gamma = \langle p, m, g, a, b, c\rangle$ όπου $a = g^x, b = g^y$, and $c = g^{xy}$. Αν x είναι άρτιος, θέτουμε $x = 2k$ για κάποιο $k \in \mathbb{Z}$. Τότε

$a^{m/2} = (g^x)^{m/2} = g^{km} = 1$. Αν το x είναι περιττό, θέτουμε $x = 2j+1$ για κάποιο $j \in \mathbb{Z}$. Τότε $a^{m/2} = (g^{2j+1})^{m/2} = g^{m/2} = -1$.

Το ίδιο αποτέλεσμα ισχύει για το g^y ανάλογα αν το y είναι άρτιο ή περιττό. Αν το xy είναι άρτιο ή περιττό εξαρτάται από τα x και y, συνεπώς $c^{m/2} = (g^{xy})^{m/2} = 1$ εφόσον ένα από τα δύο το x ή το y είναι άρτιο. Γι' αυτό ισχύει πως

$$\underset{\gamma\leftarrow\mathcal{D}}{\mathsf{Prob}}[\mathcal{A}(\gamma)=1] = \frac{3}{4}.$$

Αν διαφορετικά $\gamma \leftarrow \mathcal{R}$, συνεπώς $c = g^z$ για τυχαία επιλεγμένο z, υπάρχει ίση πιθανότητα το z να είναι άρτιο ή περιττό. Έτσι

$$\underset{\gamma\leftarrow\mathcal{R}}{\mathsf{Prob}}[\mathcal{A}(\gamma)=1] = \frac{3}{8}.$$

Βασιζόμενοι σε αυτήν την πληροφορία συμπεραίνουμε πως

$$\mathsf{Adv}^{\mathcal{A}} = \frac{3}{4} - \frac{3}{8} = \frac{3}{8}.$$

Σε μια ιδανική περίπτωση, και οι δυο πιθανότητες είναι κοντά στο $1/2$, συνεπώς η διαφορά του είναι αμελητέα. Επειδή το $\mathsf{Adv}^{\mathcal{A}} = 3/8$, ο $\mathcal{A}$ μπορεί να διαχωρίσει τις δύο πλειάδες. Συνεπώς είναι αναποτελεσματικό να εφαρμόσουμε ανταλλαγή κλειδιού στην ομάδα του $\mathbb{Z}_p^*$.

Μια ομάδα που μπορούμε να φτιάξουμε ανταλλαγή κλειδιού είναι τα τετραγωνικά υπόλοιπα $QR(p)$ του $\mathbb{Z}_p^*$. Για παράδειγμα, αν $p = 2q + 1$ για κάποιο πρώτο q, το $QR(p)$ έχει τάξη q. Με βάση τις υπάρχουσες γνώσεις, είναι μια επαρκής ομάδα. Θυμίζουμε πως το $QR(p) = \langle g^2 \rangle$ για κάποιον γεννήτορα g του $\mathbb{Z}_p^*$ είναι κυκλική ομάδα περιττής τάξης

1.7 Τροποποιημένο πρωτόκολλο Diffie-Hellman

Στην υπόθεση ADH, το κλειδί που παράγεται είναι ένα τυχαίο στοιχείο της ομάδας $\langle g \rangle$. Δυστυχώς δεν είναι ξεκάθαρο τι μπορεί κανεις να κάνει με ένα τυχαίο στοιχείο της ομάδας $\langle g \rangle$ (για να δείτε το πρόβλημα σκεφτείτε την εξής άσκηση: φτιάξτε ένα αλγόριθμο που παράγει ένα 10 τυχαία bits με μόνη τυχαιότητα την λειτουργία $y \xleftarrow{r} \langle g \rangle$). Αυτό είναι προβληματικό στην χρήση του κλειδιού σε κρυπτογραφικές εφαρμογές. Εδώ θα δούμε πως να εξάγουμε έναν τυχαίο ακέραιο από το τυχαίο στοιχείο της ομάδας. Αυτό μας βοηθάει αφού γνωρίζουμε την δομή των ακεραίων.

Μια προσέγγιση είναι να ορίσουμε ένα κατηγόρημα V τέτοιο ώστε $\mathsf{Prob}_{x \leftarrow \langle g \rangle}[V(x) = 1] = 1/2$. Το V τότε ορίζει ένα τυχαίο bit από την οπτική γωνία του αντιπάλου. Δεν είναι όμως ξεκάθαρο, πως να βρούμε ένα τέτοιο κατηγόρημα. Θα πρέπει κανείς να καταλάβει πλήρως τη δομή της ομάδας για να ξεχωρίσει πιο bit είναι τυχαίο.

Έστω τώρα:

$$H : \mathbb{Z}_m \longrightarrow QR(p)$$

με $x \mapsto (x+1)^2 \bmod p$. Αυτή η απεικόνιση είναι αμφιμονοσήμαντη (ένα-προς-ένα και επί). Για να δείξουμε πως είναι ένα-προς-ένα , υποθέτουμε πως $H(x) = H(y)$ για κάποια $x, y \in \mathbb{Z}_m$. Τότε

$$\begin{aligned}(x+1)^2 &\equiv (y+1)^2 \bmod p\\ (x+1)^2 - (y+1)^2 &\equiv 0 \bmod p\\ x^2 + 2x - 2y - y^2 &\equiv 0 \bmod p\\ (x-y)(x+y+2) &\equiv 0 \bmod p.\end{aligned}$$

Συνεπώς είτε $x - y \equiv 0 \bmod p$ ή $x + y + 2 \equiv 0 \bmod p$. Αφού $x, y \in \mathbb{Z}_m$, έχουμε πως $0 \leq x, y \leq m - 1$. Τότε

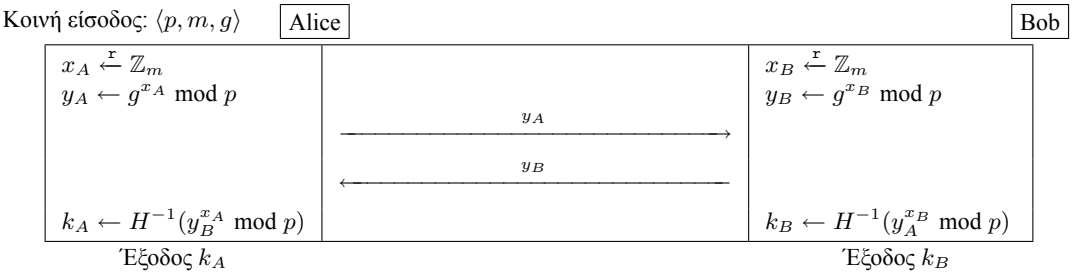
$$\begin{aligned}x + y + 2 &\leq 2(m-1) + 2 = 2m\\ &< 2m + 1 \equiv 0 \bmod p.\end{aligned}$$

Συνεπώς $x + y + 2 \not\equiv 0 \bmod p$, που σημαίνει πως $x - y \equiv 0 \bmod p$, ή αντίστοιχα $x \equiv y \bmod p$. Αφού $x, y \in \mathbb{Z}_m \subset \mathbb{Z}_p$, ισχύει πως $x = y$, δείχνοντας πως το H είναι ένα-προς-ένα. Η H είναι επί χρησιμοποιώντας αυτή την αντίστροφη απεικόνιση για κάθε $y \in QR(p)$,

$$H^{-1}(y) = \begin{cases} y^{p+1/4} \bmod p - 1, & \text{if } y^{p+1/4} \bmod p \in \{1, 2, \ldots, m\} \\ p - y^{p+1/4} \bmod p - 1, & \text{otherwise.} \end{cases}$$

Χρησιμοποιώντας αυτό μπορούμε να τροποποιήσουμε το πρωτόκολλο ανταλλαγής κλειδιού όπως φαίνεται στην εικόνα 3.

Στο τροποποιημένο πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman, μπορούμε να χρησιμοποιήσουμε την αμφιμονοσήμαντη απεικόνιση H για να μεταβούμε από ένα τυχαίο στοιχείο της ομάδας που δεν γνωρίζουμε την δομή της επακριβώς σε κάποιο τυχαίο ακέραιο υπόλοιπο m.



Σχήμα 3: Το τροποποιημένο πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman όπου ο p είναι ένας μεγάλος πρώτος, ο g είναι γεννήτορας της ομάδας $QR(p)$ τάξης m, και $H : \mathbb{Z}_m \longrightarrow QR(p)$ με $x \mapsto (x+1)^2 \bmod p$.

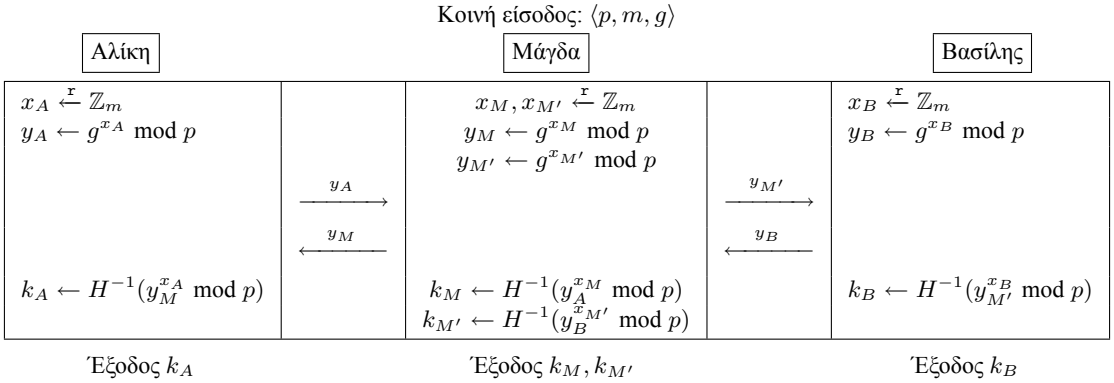
Άσκηση: Δείξαμε πως να βρούμε ένα τυχαίο στοιχείο στο $\mathbb{Z}_m$. Αυτό μας βοηθά στις κρυπτογραφικές εφαρμογές που χρειάζονται έναν ακέραιο υπόλοιπο m σαν κλειδί. Οι περισσότερες εφαρμογές όμως, απαιτούν πως το κλειδί είναι μια συμβολοσειρά από bit. Δείξτε πως μπορούμε να εξάγουμε τη μεγαλύτερη δυνατή bit συμβολοσειρά από έναν ακέραιο υπόλοιπο m.

Είναι ενδιαφέρον να αναφέρουμε πως σε ένα κλειδί με λ bits key, η πιθανότητα το λιγότερο σημαντικό bit (least significant bit) να είναι ένα είναι κοντά στο $1/2$, ενώ η πιθανότητα το περισσότερο σημαντικό bit (most significant bit) να είναι ένα μπορεί να απέχει αρκετά από το $1/2$.

1.8 Ισχυρότεροι Αντίπαλοι

Παρόλο που το πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman όπως δίνεται στην ενότητα 1.7, είναι ασφαλές έναντι ενός αντιπάλου που απλά "κρυφακούει", δεν παραμένει ασφαλές απέναντι σε πιο ενεργητικούς αντιπάλους. Στην εικόνα 3, δείχνουμε την ***man-in-the-middle attack*** στην οποία ο αντίπαλος, Μάγδα, συμμετέχει στην ανταλλαγή πληροφορίας της Αλίκης και του Βασίλη. Ο αντίπαλος τώρα είναι το ίδιο το επικοινωνιακό κανάλι. Η Μάγδα μπορεί να εμβάλει μηνύματα στην συζήτηση και να υποδυθεί την ταυτότητα μιας από της μεριές στην άλλη. Για να το καταφέρει η Μάγδα κατασκευάζει δύο κλειδιά, ένα για να μοιράζεται με την Αλίκη και ένα με τον Βασίλη.

Αυτή η επίθεση αιτιολογεί την ανάγκη για ταυτοποίηση και ελέγχου ταυτοποίησης σε κάθε ανταλλαγή. Στη συνέχεια θα εισάγουμε τις ψηφιακές υπογραφές, ένα σημαντικό κρυπτογραφικό σχήμα, που είναι απαραίτητο εργαλείο απέναντι σε τακτικές σαν την επίθεση man-in-the-middle.



Σχήμα 4: Η επίθεση ``man-in-the-middle" έναντι του πρωτοκόλλου ανταλλαγης κλειδιού Diffie-Hellman.

Επιμέλεια σημειώσεων Αγγλικά: S. Pehlivanoglu, J. Todd, & H.S. Zhou. Ελληνικά : Μ. Πουντουράκης.