ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ
ΣΗΜΕΙΩΣΕΙΣ #3

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

1. Το πρωτοκολλο των Diffie-Hellman

Μέχρι τώρα έχουμε δει ότι αν δύο άτομα, η Αλίκη και ο Βασίλης, έχουν ένα κοινό κλειδί, τότε μπορούν να επικοινωνήσουν μυστικά χρησιμοποιώντας ένα τμηματικό κώδικα. Το πρόβλημα που υπάρχει είναι πώς μπορούν η Αλίκη και ο Βασίλης να δημιουργήσουν αυτό το *κοινό* και *κρυφό* κειδί. Η γενική εντύπωση ήταν ότι η Αλίκη και ο Βασίλης δεν είναι δυνατό να δημιουργήσουν ένα τέτοιο κλειδί επικοινωνώντας φανερά: δεν μπορείς να δημιουργήσεις ένα κοινό μυστικό από το τίποτα.

Το 1976, σε μια ιστορική δημοσίευση, οι Diffie και Hellman πρότειναν το παρακάτω πρωτόκολλο.

Η Αλίκη και ο Βασίλης συμφωνούν σε ένα «μεγάλο» πρώτο p και ένα γεννήτορα g της ομάδας $(\mathbb{Z}/p\mathbb{Z})^\times$. Τα p και g είναι γνωστά σε όλους.

(1) Η Αλίκη επιλέγει τυχαίο $a \in [1, p-1]$ και υπολογίζει το $A = g^a \mod p$. Στέλνει το A στον Βασίλη.
(2) Ο Βασίλης επιλέγει τυχαίο $b \in [1, p-1]$ και υπολογίζει το $B = g^b \mod p$. Στέλνει το B στην Αλίκη.
(3) Η Αλίκη υπολογίζει $K = B^a$. Ο Βασίλης υπολογίζει $K = A^b$.

Οι Diffie και Hellman ισχυρίστηκαν ότι το K είναι το κοινό κρυφό κλειδί. Το ότι η Αλίκη και ο Βασίλης υπολογίζουν την ίδια τιμή είναι φανερό. Ότι η τιμή αυτή δεν μπορεί να υπολογίστει από κανένα άλλο δεν είναι καθόλου φανερό.

Κατ' αρχάς μπορούμε να δούμε ότι το πρωτόκολλο Diffie-Hellman μπορεί να περιγραφεί γενικώτερα για οποιαδήποτε πεπερασμένη αβελιανή ομάδα G.

Η Αλίκη και ο Βασίλης συμφωνούν σε μια ομάδα G και ένα $g \in G$. Ας είναι $|\langle g \rangle| = n$. Δηλαδή το g παράγει μια κυκλική υποομάδα τάξης n. Τα G, g και n είναι γνωστά σε όλους.

(1) Η Αλίκη επιλέγει τυχαίο $a \in [1, n]$ και υπολογίζει το $A = g^a$. Στέλνει το A στον Βασίλη.
(2) Ο Βασίλης επιλέγει τυχαίο $b \in [1, n]$ και υπολογίζει το $B = g^b$. Στέλνει το B στην Αλίκη.
(3) Η Αλίκη υπολογίζει $K = B^a$. Ο Βασίλης υπολογίζει $K = A^b$.

Κατ' αρχάς λίγα σχόλια για την ομάδα G. Για τις ανάγκες του πρωτοκόλλου, η G πρέπει να είναι πεπερασμένη και αβελιανή. Επιπλέον όμως θα πρέπει να μπορεί κανείς να κάνει τις πράξεις που απαιτούνται. Θα πρέπει δηλαδή οι πράξεις στην ομάδα να μπορούν να γίνουν αποτελεσματικά. Εφόσον εχουμε να αναπαραστήσουμε $|G|$ στοιχεία, χρειαζόμαστε $\log|G|+1$ ψηφία ή έστω $O(\log n)$ ψηφία (αν ο τρόπος που τα αναπαριστούμε δεν είναι ο πιο οικονομικός). Έτσι για να κάνουμε την πράξη $\alpha\cdot\beta$ στην ομάδα (εδώ $\alpha,\beta\in G$) το μήκος της εισόδου είναι περιπου $2\log n = O(\log n)$. Για να είναι η πράξη πολυωνυμικού χρόνου (στο μήκος της εισόδου) η πράξη πρέπει να μπορεί να γίνει σε χρόνο $O((\log n)^d)$ για κάποιο σταθερό d. Έχουμε δει ότι στην ομάδα $(\mathbb{Z}/p\mathbb{Z})^\times$ η πράξη γίνεται σε χρόνο $O((\log p)^2)$ που είναι πράγματι πολυωνυμικός στο μήκος της εισόδου, που είναι περίπου $2\log p$. Σημειώνουμε ακόμη ότι το πρωτόκολλο είναι πολυωνυμικού χρόνου καθώς η ύψωση σε δύναμη (π.χ. το g^a) μπορεί να υπολογιστεί κάνοντας $O(\log a)$ πράξεις την ομάδα. Αυτό γίνεται με διαδοχικούς τετραγωνισμούς και κατάλληλους πολλαπλασιασμούς ενδιάμεσων αποτελεσμάτων (πώς;)

Παράδειγμα 1.1. Ας δούμε ένα παράδειγμα. Έστω ότι η Αλίκη και ο Βασίλης επιλέγουν τις ακόλουθες παραμέτρους. Η ομάδα είναι η $(\mathbb{Z}/p\mathbb{Z})^\times$ με $p=29$ και η βάση είναι το $g=2$ που μπορεί κανείς να δει ότι έχει τάξη 28, δηλαδή γεννά την ομάδα. Προχωρούμε σε μία εφαρμογή του πρωτοκόλλου. Η Αλίκη επιλέγει ακέραιο $a\in[1,28]$, ας πούμε $a=13$ και στέλνει το $2^{13} \mod 29 = 14$ στο Βασίλη. Ο Βασίλης επιλέγει ακέραιο $b\in[1,28]$, ας πούμε $b=25$ και στέλνει το $2^{25} \mod 29 = 11$ στην Αλίκη. Η Αλίκη υπολογίζει το κλειδί ως $11^{13} \mod 29 = 21$ και ο Βασίλης υπολογίζει το κλειδί ως $14^{25} \mod 29 = 21$.

Ας δούμε τι δεδομένα έχει ένας παθητικός παρατηρητής της συνομιλίας, η Γεωργία. Γνώριζει τα G, g και n (αφού αυτές είναι παράμετροι του συστήματος γνώστες σε όλους), και έχει δει και τα g^a και g^b, αλλά *όχι* τα a και b. Το πρόβλημα που αντιμετωπίζει είναι αυτό του υπολογισμού του g^{ab}. Αυτό ακριβώς είναι το υπολογιστικό πρόβλημα των Diffie και Hellman.

Υπολογιστικό πρόβλημα Diffie-Hellman (CDH). Δεδομένης μιας πεπερασμένης αβελιανής ομάδας G, ενός $g\in G$ και των g^a, g^b, υπολόγισε το g^{ab}.

Ένα σχετικό πρόβλημα είναι αυτό του διακριτού λογάριθμου στην G.

Πρόβλημα του διακριτού λογάριθμου (DL). Δεδομένης μιας πεπερασμένης αβελιανής ομάδας G, ενός $g\in G$ και ενός $y\in\langle g\rangle$, υπολόγισε το $a\in[1,|\langle g\rangle|]$ τέτοιο ώστε $y=g^a$.

Είναι φανερό ότι όποιος μπορεί να λύσει το πρόβλημα DL, μπορεί να λύσει και το CDH (πώς;) Με άλλα λόγια το πρόβλημα CDH δεν είναι υπολογιστικά δυσκολότερο από το DL. Αυτό το γράφουμε $\mathrm{CDH}\leq\mathrm{DL}$. Ισχύει το αντίστροφο; Αν δηλαδή κάποιος μπορεί να λύσει το CDH μπορεί να λύσει και το DL; Αυτό δεν είναι γενικά γνωστό. Κάτω από κάποιες υποθέσεις (που δε μπορούμε να

αποδείξουμε) η απάντηση είναι ναι. Δηλαδή τα προβήματα αυτά *μάλλον* είναι ισοδύναμα.

Οι Diffie και Hellman λοιπόν ισχυρίστηκαν ότι το πρόβλημα CDH (και συνεπώς το DL) είναι δύσκολα για την ομάδα $G = (\mathbb{Z}/p\mathbb{Z})^\times$.

Ορίζουμε και το πρόβλημα απόφαση των Diffie και Hellman.

Πρόβλημα απόφασης των Diffie-Hellman (DDH). Δεδομένης μιας πεπερασμένης αβελιανής ομάδας G και των $g, g^a, g^b, g^c \in G$ αποφάσισε αν $g^{ab} = g^c$.

Είναι φανερό ότι όποιος μπορεί να λύσει το CDH μπορεί να λύσει και το DDH (γιατι;) Άρα έχουμε

$$\mathrm{DDH} \leq \mathrm{CDH} \leq \mathrm{DL}.$$

Η δυσκολία υπολογιστικής επίλυσης των τριών παραπάνω προβλημάτων έχει άμεση σχέση με την ασφάλεια του πρωτοκόλλου Diffie-Hellman. Το ερώτημα που αντιμετωπίζουμε είναι: για ποιές ομάδες είναι τα παραπάνω προβλήματα δύσκολα; Για παράδειγμα για την προσθετική ομάδα $G = \mathbb{Z}/n\mathbb{Z}$ τα παραπάνω προβλήματα είναι εύκολα (γιατι;) Υπάρχουν ομάδες στις οποίες τα προβλήματα να είναι δύσκολα;

Μία ακόμη παρατήρηση: αν η Γεωργία δεν παρακολουθούσε παθητικά τη συνομιλία, αλλά παρενέβαινε σ' αυτή, τότε το πρωτόκολλο δεν είναι πια ασφαλές. Η Γεωργία μπορεί να «μπει ανάμεσα» στην Αλίκη και το Βασίλη, και να δημιουργήσει κοινό κλειδί και με τους δύο. Έτσι, η Αλίκη και ο Βασίλης θα συνομιλούν με τη Γεωργία νομίζοντας ότι μιλούν μεταξύ τους. Το πρόβλημα αυτό δε μπορεί να λυθεί με «μαθηματικό» τρόπο. Είναι φιλοσοφικό ζήτημα ταυτότητας και έχει σχέση και με την επόμενη ενότητα.

2. Κρυπτογραφια δημοσιου κλειδιου

Το πρωτόκολλο Diffie-Hellman μας λύνει ένα βασικό πρόβλημα. Είναι σημαντικότερο όμως ότι οδήγησε στην έννοια της κρυπτογραφίας δημόσιου κλειδιού. Σε ένα τέτοιο σύστημα, κάθε χρήστης, ας πούμε η Αλίκη και ο Βασίλης, έχουν ο καθένας από ένα *ζευγάρι* κλειδιών: το ιδιωτικό (που γνωρίζει μόνο ο χρήστης) και το δημόσιο (που είναι γνωστό σε όλους). Για να στείλει η Αλίκη ένα κρυπτογραφημένο μήνυμα στο Βασίλη, το κρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του Βασίλη (με ένα αλγόριθμο E). Ο Βασίλης για να αποκρυπτογραφήσει το μήνυμα, χρησιμοποιεί το δικό του ιδιωτικό κλειδί (με ένα αλγόριθμο D). Δηλαδή αν το ζευγάρι κλειδιών του Βασίλη είναι (S_B, P_B) η Αλίκη, για να κρυπτογραφήσει το μήνυμα m υπολογίζει $c = E_{P_A}(m)$. Ο Βασίλης υπολογίζει το $D_{S_A}(C) = m$.

Για κάθε σύστημα δημόσιου κλειδιού που θα περιγράψουμε πρέπει να πούμε πώς κατασκευάζονται τα κλειδιά (προφανώς το ιδιωτικό κλειδί έχει σχέση με το αντίστοιχο δημόσιο), και ποιοί είναι οι αλγόριθμοι E και D.