ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ
ΣΗΜΕΙΩΣΕΙΣ $\#4$

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

1. Συστηματα δημοσιου κλειδιου

Το πρωτόκολλο Diffie-Hellman μας λύνει ένα βασικό πρόβλημα – αυτό της δημιουργίας κοινού κρυφού κλειδιού. 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 $c = E_{P_B}(m)$. Ο Βασίλης υπολογίζει το $D_{S_B}(C) = m$.

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.

2. Το συστημα κρυπτογραφησης ElGamal

Το 1985, ο ElGamal δημοσίευσε ένα σύστημα κρυπτογράφησης δημόσιου κλειδιού, του οποίου η ασφάλεια βασίζεται στη δυσκολία επίλυσης του προβλήματος του διακριτού λογάριθμου σε κάποια πεπερασμένη αβελιανή ομάδα G. Στην ίδια δημοσίευση περιέγραψε και ένα σύστημα ψηφιακής υπογραφής, που θα δούμε αργότερα στο μάθημα.

Θα περιγράψουμε το σύστημα του ElGamal για μια πεπερασμένη αβελιανή ομάδα G (ο ίδιος το είχε περιγράψει για την πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος). Επίσης θεωρούμε ότι έχουμε κάποιο τρόπο να αντιστοιχούμε τα στοιχεία της ομάδας G σε ακολουθίες γραμμάτων. Με άλλα λόγια μπορούμε να κόψουμε το μήνυμα που θέλουμε να κρυπτογραφήσουμε σε κομμάτια, και κάθε κομμάτι να αντιστοιχεί (κατά μοναδικό τρόπο) σε ένα στοιχείο της ομάδας G. Κρυπτογραφούμε κάθε κομμάτι χωριστά. Από εδώ και στο εξής, θα θεωρούμε ότι το μήνυμα είναι ένα στοιχείο της ομάδας G.

Έστω, λοιπόν, πεπερασμένη αβελιανή ομάδα G, και $g \in G$, με $|\langle g \rangle| = n$. Τα G, g και n είναι παράμετροι του συστήματος κοινές για όλα τα μέλη.

Κάθε μέλος του συστήματος, ας πούμε η Αλίκη, δημιουργεί το ζευγάρι των κλειδιών του ως εξής: Επιλέγει τυχαία $a \in \{1, \dots, n\}$ και υπολογίζει το $y = g^a$. Το κρυφό κλειδί είναι το a και το δημόσιο το y.

Για να κρυπτογραφήσει ο Βασίλης το μήνυμα m που έχει προορισμό την Αλίκη, κάνει τα εξής βήματα:

(1) Επιλέγει τυχαίο $k \in \{1, \dots, n\}$ και υπολογίζει το $r = g^k$.
(2) Υπολογίζει το $c = m \cdot y^k$.
(3) Στέλνει το ζεύγος (r, c).

Η Αλίκη, παίρνοντας το κρυπτογράφημα (r, c), αποκρυπτογραφεί εύκολα:

$$m = \frac{c}{y^k} = \frac{c}{g^{ak}} = \frac{c}{r^a}.$$

Η τελευταία ποσότητα μπορεί να υπολογιστεί από την Αλίκη, η οποία γνωρίζει το κρυφό κλειδί a.

Το ότι το σύστημα είναι λειτουργικό – δηλαδή ότι η Αλίκη μπορεί μπορεί να αποκρυπτογραφήσει – είναι αναμενόμενο. Το σύστημα του ElGamal είναι ένας συνδυασμός του πρωτοκόλλου Diffie-Hellman και του One-time-pad. Πραγματικά, ο Βασίλης υπολογίζει το δικό του «μερίδιο του κλειδιού» Diffie-Hellman, δηλαδή το $r = g^k$, και το στέλνει στην Αλίκη ως μέρος του κρυπτογραφήματος. Το μερίδιο της Αλίκης είναι γνωστό σε όλους : είναι το δημόσιο κλειδί της $y = g^a$. Άρα ο Βασίλης μπορεί να υπολογίσει το κλειδί Diffie-Hellman που είναι το $g^{ak} = y^k$. Στη συνέχεια κρυπτογραφεί το μήνυμα m χρησιμοποιώντας One-time-pad με κλειδί το y^k. Υπολογίζει δηλαδή το $m \cdot y^k$. Η Αλίκη, για να αποκρυπτογραφήσει, πρέπει να γνωρίζει το κλειδί που χρησιμοποίησε ο Βασίλης για το One-time-pad. Για το λόγο αυτό ο Βασίλης έχει συμπεριλάβει το $r = g^k$ ως μέρος του κρυπτογραφήματος. Η Αλίκη μπορεί να υπολογίσει το κλειδί Diffie-Hellman, $g^{ak} = r^a$, και να αποκρυπτογραφήσει.

3. Ασφαλεια του συστηματος ElGamal

Κατ' αρχάς είναι φανερό ότι το σύστημα δεν μπορεί να είναι ασφαλές αν το πρόβλημα του DL δεν είναι δύσκολο. Όποιος μπορεί να λύσει το DL στην ομάδα G, δεδομένων των g και $y = g^a$ μπορεί να υπολογίσει το κρυφό κλειδί της Αλίκης, και αποκρυπτογραφεί οτιδήποτε.

Τι γίνεται αν το CDH είναι εύκολο; Και πάλι το σύστημα είναι εντελώς ανασφαλές. Τώρα δεν είναι φανερό πως μπορεί κανείς να βρει το κρυφό κλειδί. Παρόλα αυτά, μπορεί να αποκρυπτογραφεί *κάθε* κρυπτογράφημα ως εξής : δεδομένων των $y = g^a$ και $r = g^k$, μπορεί να υπολογίσει (αφού μπορεί να λύνει το CDH στην G) το g^{ak}, και μετά να αποκρυπτογραφεί όπως η Αλίκη. Δηλαδή, να υπολογίζει το $c/g^{ak} = m$. Άρα για είναι το σύστημα ασφαλές πρέπει και το CDH να είναι δύσκολο στην G.

Το πόσο δύσκολα είναι τα παραπάνω προβλήματα είναι φανερά πολυ σημαντικό ζήτημα και θα ασχοληθούμε μ' αυτό σε επόμενα μαθήματα.

Ας υποθέσουμε τώρα ότι το CDH (άρα και το DL) είναι δύσκολο στην ομάδα G. Δηλαδη δεν υπάρχει αλγόριθμος που να κάνει πολυωνυμικό (στο $\log n$) αριθμό βημάτων και να λύνει το CDH στην G. Δεδομένου ότι η πράξη στην G γίνεται εύκολα (δηλαδή σε πολυωνυμικό αριθμό βημάτων), μπορούμε να μετράμε κάθε πράξη στην G σαν ένα βήμα. Μπορεί τότε κάποιος να βρει *όλο* το μήνυμα m; Η απάντηση είναι όχι. Μπορούμε να δείξουμε το παρακάτω θεώρημα.

Θεώρημα 3.1. *Εάν το πρόβλημα CDH σε μια ομάδα G δεν μπορεί να λυθεί σε πολυωνυμικό χρόνο, τότε το σύστημα ElGamal στην G είναι ασφαλές σύμφωνα με την παραπάνω έννοια.*

Απόδειξη. Θέλω να δείξω την πρόταση «Αν δεν υπάρχει πολυωνυμικός αλγόριθμος που να λύνει το CDH στην G τότε δεν υπάρχει πολυωνυμικός αλγόριθμος που να σπάει το σύστημα ElGamal.» Η πρόταση αυτή είναι ισοδύναμη με την πρόταση «Αν υπάρχει πολυωνυμικός αλγόριθμος $\mathcal{A}$ που να σπάει το σύστημα ElGamal τότε υπάρχει πολυωνυμικός αλγόριθμος που να λύνει το CDH στη G.» Θα αποδείξουμε τη δεύτερη πρόταση.

Υποθέτουμε, λοιπόν, ότι έχουμε ένα αλγόριθμο $\mathcal{A}$, ο οποίος δεδομένων της ομάδας G, ενός στοιχείου $g \in G$, ενός δημόσιου κλειδιού y και ενός κρυπτογραφήματος (r, c) μας υπολογίζει το μήνυμα σε πολυωνυμικό χρόνο. Θα κατασκευάσουμε ένα αλγόριθμο $\mathcal{B}$ ο οποίος λύνει το CDH στη G (και φυσικά χρησιμοποιεί τον $\mathcal{A}$).

Έστω ότι στον $\mathcal{B}$ δίνονται τα $g, A = g^a$ και $B = g^b$. Σκοπός του $\mathcal{B}$ είναι να υπολογίσει το g^{ab}. Ο $\mathcal{B}$ κάνει τα παρακάτω: Κατασκευάζει ένα σύστημα ElGamal με τις εξής παραμέτρους : Ομάδα G, και $g \in G$. Δημόσιο κλειδί $y = A$. Θέτει $r = B$ και c οποιοδήποτε στοιχείο της G. Δίνει στον $\mathcal{A}$ τις παραμέτρους (δηλαδή τα G, g, y) και το κρυπτογράφημα (r, c). Τώρα ο $\mathcal{A}$ έχουμε υποθέσει ότι μπορεί να αποκρυπτογραφήσει σε πολυωνυμικο χρόνο, δηλαδή να υπολογίσει το

$$m = \frac{c}{r^a} = \frac{c}{g^{ab}}.$$

Ο $\mathcal{A}$ επιστρέφει το m και τώρα ο $\mathcal{B}$ υπολογίζει το

$$g^{ab} = \frac{c}{m}$$

και έτσι λύνει το πρόβλημα CDH. □

Είμαστε σε θέση να διατυπώσουμε τον πρώτο ορισμό (ασθενούς) ασφάλειας.

Ορισμός 3.2. Ένα σύστημα κρυπτογράφησης θα ονομάζεται αντιστρέψιμο, αν υπάρχει πολυωνυμικού χρόνου αλγόριθμος ο οποίος δεδομένων επιτρεπτών δημόσιων παραμέτρων του συστήματος, ενός δημόσιου κλειδιού K και ενός κρυπτογραφήματος $c = E_K(m)$ υπολογίζει το m. Ένα σύστημα κρυπτογράφησης ονομάζεται μη αντιστρέψιμο αν δεν είναι αντιστρέψιμο.

Δείξαμε ότι το σύστημα του ElGamal είναι μη αντιστρέψιμο εφόσον το CDH είναι δύσκολο στην ίδια ομάδα. Με άλλα λόγια, σύμφωνα με τον παραπάνω ορισμό, η ασφάλεια του συστήματος κρυπτογράφησης ElGamal σε μια ομάδα G είναι ισοδύναμη με τη δυσκολία του προβλήματος CDH στην G.