Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Ελένη Μπακάλη
Άρης Παγουρτζής

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

15 Νοεμβρίου 2012

1 Άλλα κλασικά κρυπτοσυστήματα

Affine Cipher

Key: (a, k) τ.ω. $gcd(a, 26) = 1$
$Enc(x) = ax + k \bmod 26$
$Dec(y) = a^{-1}(y - k) \bmod 26$.

Ορθότητα αποκρυπτογράφησης: $y = ax + k \bmod 26 \Rightarrow y - k \equiv ax \pmod{26} \Rightarrow a^{-1}(y - k) \equiv x \pmod{26}$.

Σημείωση: δύο ακέραιοι a, b λέγονται *ισότιμοι modulo* n, και γράφουμε $a \equiv b \pmod{n}$ ανν $a \bmod n = b \bmod n$.

Ο πολλαπλασιαστικός αντίστροφος του a modulo 26 (συμβολίζεται με a^{-1}) είναι ο *ακέραιος* από το σύνολο $\mathbb{Z}_{26} = \{0, \cdots, 25\}$ για τον οποίο ισχύει

$$a \cdot a^{-1} \bmod 26 = 1$$

Είναι γνωστό (θα το αποδείξουμε αργότερα) ότι αντίστροφος του a modulo n υπάρχει ανν $gcd(a, n) = 1$. Αν υπάρχει είναι μοναδικός. Αυτόν τον ρόλο παίζει η απαίτηση $gcd(a, 26) = 1$.

'1-1' κρυπτογράφηση: πράγματι, $ax_1 + k \equiv ax_2 + k \pmod{26} \Rightarrow ax_1 = ax_2 \Rightarrow a(x_1 - x_2) \equiv 0 \pmod{26} \Rightarrow 26 \mid a(x_1 - x_2)$ αλλά αφού $(26, a) = 1$ έχουμε $26 \mid x_1 - x_2 \Rightarrow x_1 = x_2$, αφού $x_1, x_2 \in \{0, \ldots, 25\}$.

Είναι μονοαλφαβητικό σύστημα, εύκολη κρυπτανάλυση (στατιστική) αν το αρχικό κείμενο είναι σε κάποια φυσική γλώσσα. Πολυαλφαβητικό αν χρησιμοποιείται ένα σύνολο κλειδιών, π.χ. με περιοδικό τρόπο. Στην τελευταία περίπτωση κρυπτανάλυση με Kasiski test, Index of Coincidence, κ.λπ.

Permutation Cipher

Το κλειδί είναι μία μετάθεση (permutation) του $\{1, \ldots, m\}$. Χωρίζουμε το αρχικό κείμενο σε μπλοκ μεγέθους m και σε κάθε μπλοκ εφαρμόζουμε την μετάθεση.

Σημαντική ιδιότητα: το κρυπτοκείμενο περιέχει τους ίδιους χαρακτήρες με το αρχικό κείμενο.

Άσκηση: ποιες ιδέες από τα προηγούμενα θα μπορούσαμε να χρησιμοποιήσουμε για κρυπτανάλυση του συστήματος αυτού;

Κρυπτοσυστήματα Γινομένου (Product Cryptosystems)

Προκύπτουν από σύνθεση των συναρτήσεων κρυπτογράφησης δύο ή περισσοτέρων κρυπτοσυστημάτων:

$$e_k(x) = e_{k_1}(e_{k_2}(x))$$

Idempotent λέγονται τα κρυπτοσυστήματα που το γινόμενο με τον εαυτό τους δίνει το ίδιο κρυπτοσύστημα, π.χ. το Shift Cipher.

Άσκηση: δείξτε ότι το Affine Cipher είναι idempotent.

2 One-time pad

Είναι απόλυτα ασφαλές κρυπτοσύστημα, προτάθηκε από τον Vernam το 1917.

Plaintext: $x = (x_0, x_1, \ldots, x_{n-1}), \quad x_i \in \{0, 1\}$
Key: $k = (k_0, k_1, \ldots, k_{n-1}), \quad k_i \in \{0, 1\}$
Ciphertext: $y = (y_0, y_1, \ldots, y_{n-1}), \quad y_i \in \{0, 1\}$

Δηλαδή, αρχικό κείμενο, κρυπτοκείμενο και κλειδί είναι όλα δυαδικές ακολουθίες του ίδιου μήκους. Το κλειδί επιλέγεται τυχαία με ομοιόμορφο τρόπο.

Κρυπτογράφηση: $y_i = x_i \oplus k_i = x_i + k_i \bmod 2$

Αποκρυπτογράφηση: $x_i = y_i \oplus k_i$

Η απόλυτη ασφάλεια του συστήματος στηρίζεται στο γεγονός ότι οποιοδήποτε κρυπτοκείμενο y μπορεί να έχει παραχθεί από οποιοδήποτε αρχικό κείμενο x, με κλειδί $k = x \oplus y$ (bitwise XOR). Η αυστηρή απόδειξη θα δοθεί στην παρακάτω ενότητα.

Σημαντικό μειονέκτημα είναι το μήκος του κλειδιού που είναι απαγορευτικό για πρακτικές εφαρμογές (αλλά απαραίτητο όπως θα δούμε για να έχουμε απόλυτη ασφάλεια), καθώς και η απαίτηση για χρήση μόνο μία φορά (εξ ού και το όνομα).

Άσκηση: Ποιό πρόβλημα ασφάλειας εμφανίζεται αν χρησιμοποιήσουμε το κλειδί και δεύτερη φορά;

3 Τέλεια Μυστικότητα (Perfect Secrecy)

Ας θεωρήσουμε το αρχικό κείμενο M, το κλειδί K και το κρυπτοκείμενο C σαν τυχαίες μεταβλητές που παίρνουν τιμές αντίστοιχα από τα σύνολα $\mathcal{M}, \mathcal{K}, \mathcal{C}$.

Ορισμός τέλειας μυστικότητας (Shannon, 1949)

Ο ορισμός που δόθηκε από τον Shannon ([Sha49]) είναι ο εξής:

$\forall x \in \mathcal{M}, y \in \mathcal{C}: \quad \Pr[M = x \mid C = y] = \Pr[M = x]$

Δηλαδή, έχουμε τέλεια μυστικότητα εάν δεν μπορούμε να ανακτήσουμε από οποιοδήποτε κρυπτοκείμενο καμμία πληροφορία για το αρχικό κείμενο, που δεν την γνωρίζουμε εξ αρχής (η *a posteriori* πληροφορία είναι ίδια με την *a priori*).

Παράδειγμα. Θεωρούμε το εξής κρυπτοσύστημα, που θα ονομάσουμε Random Shift Cipher:

$\mathcal{M} = \mathcal{C} = \{'\mathcal{A}', \ldots, '\mathcal{Z}'\}$ ή πιο απλά $\mathcal{M} = \mathcal{C} = \{0, \ldots, 25\}$ με κατανομή τις στατιστικές συχνότητες των γραμμάτων στην αγγλική γλώσσα. Φυσικά ισχύει $\sum_{i=0}^{25} \Pr[M = i] = 1$.

Κρυπτογράφηση: $C = enc_K(M) = M + K \bmod 26$

με κατανομή του K την ομοιόμορφη στο $\{0, \ldots, 25\}$. Δηλ. $\forall i \Pr[K = i] = \frac{1}{26}$.

Αποκρυπτογράφηση: $M = dec_K(C) = C - K \bmod 26$

Παρατηρούμε τώρα ότι για κάθε γράμμα j ισχύει $\Pr[C = j] = \frac{1}{26}$. Αυτό γιατί π.χ. για $i =' D' = 3$ έχουμε

$$\Pr[C =' D'] = \sum_{i=0}^{25} \Pr[M = i] \cdot \Pr[K = 3 - i \bmod 26] = \frac{1}{26} \sum_{i=0}^{25} \Pr[M = i] = \frac{1}{26}.$$

Γενικότερα ισχύει:

$$\forall x \in \mathcal{M}, y \in \mathcal{C}: \quad \Pr[C = y \mid M = x] = \Pr[K = y - x \bmod 26] = \frac{1}{26},$$

και επομένως

$$\forall y \in \mathcal{C}: \quad \Pr[C = y] = \sum_{x \in \mathcal{M}} \Pr[M = x] \cdot \Pr[K = y - x \bmod 26] = \frac{1}{26} \sum_{x \in \mathcal{M}} \Pr[M = x] = \frac{1}{26}.$$

Από θεώρημα Bayes έχουμε:

$$\Pr[M = x \mid C = y] = \frac{\Pr[C = y \mid M = x] \Pr[M = x]}{\Pr[C = y]}$$

και από τα παραπάνω τελικά προκύπτει:

$$\forall x \in \mathcal{M}, y \in \mathcal{C}: \Pr[M = x \mid C = y] = \frac{\frac{1}{26} \Pr[M = x]}{\frac{1}{26}} = \Pr[M = x].$$

επομένως το Random Shift Cipher διαθέτει την ιδιότητα της τέλειας μυστικότητας.

Από τα παραπάνω προκύπτουν και οι εξής *Ισοδύναμες Συνθήκες Τέλειας Μυστικότητας*:

1. $\forall x \in \mathcal{M}, y \in \mathcal{C}: \quad \Pr[C = y] = \Pr[C = y \mid M = x]$

   που εκφράζει ότι η πιθανότητα εμφάνισης ενός κρυπτοκειμένου είναι ίδια για κάθε αρχικό κείμενο, με άλλα λόγια το κρυπτοκείμενο και το αρχικό κείμενο είναι ανεξάρτητες τυχαίες μεταβλητές.

2. $\forall x_1, x_2 \in \mathcal{M}, y \in \mathcal{C}: \quad \Pr[C = y \mid M = x_1] = \Pr[C = y \mid M = x_2]$

   δηλαδή, για δοσμένο αρχικό κείμενο, τα κρυπτοκείμενα είναι ισοπίθανα.

Άσκηση: αποδείξτε την ισοδυναμία των δύο παραπάνω συνθηκών με τη αρχική συνθήκη τέλειας μυστικότητας.

Ο Shannon απέδειξε ότι δεν είναι δυνατόν να έχουμε perfect secrecy, παρά μόνο αν το κλειδί είναι τουλάχιστον ίδιου μήκους με το αρχικό κείμενο (υποθέτοντας κωδικοποίηση με το ίδιο αλφάβητο).

Πράγματι, με χρήση των παραπάνω συνθηκών μπορεί να δείξει κανείς ότι αναγκαία συνθήκη για τέλεια μυστικότητα είναι ο χώρος των κλειδιών να είναι τουλάχιστον ισοπληθικός με τον χώρο των αρχικών κειμένων (και με αυτόν των κρυπτοκειμένων):

$$|\mathcal{M}| \leq |\mathcal{C}| \leq |\mathcal{K}| \tag{1}$$

Η πρώτη ανισότητα είναι απαραίτητη ώστε η συνάρτηση κρυπτογράφησης να είναι '1-1'. Η δεύτερη προκύπτει από την απαίτηση της τέλειας μυστικότητας: αν $|\mathcal{C}| > |\mathcal{K}|$, τότε, για οποιοδήποτε αρχικό κείμενο x θα υπάρχει κάποιο κρυπτοκείμενο y που δεν θα προκύπτει ως κρυπτογράφημα του x με κανένα κλειδί, δηλαδή $\Pr[C = y \mid M = x] = 0$. Επειδή όμως θα πρέπει να υπάρχει κάποιο x' που να κρυπτογραφείται σε y με μη μηδενική πιθανότητα (αφού $y \in \mathcal{C}$), παραβιάζεται η δεύτερη ισοδύναμη συνθήκη τέλειας μυστικότητας.

Ο Shannon έδειξε ακόμη ότι στην ειδική περίπτωση της σχέσης (1) όπου όλοι οι χώροι είναι ισοπληθικοί, έχουμε αναγκία και ικανή συνθήκη, συγκεκριμένα όλα τα κλειδιά να είναι ισοπίθανα και κάθε κρυπτοκείμενο να μπορεί να προκύψει από οποιοδήποτε αρχικό κείμενο με μη μηδανική πιθανότητα:

Θεώρημα. *Έστω κρυπτοσύστημα, τέτοιο ώστε $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$. Το σύστημα έχει τέλεια μυστικότητα ανν ισχύουν τα εξής: (1) για κάθε $x \in \mathcal{M}, y \in \mathcal{C}$, υπάρχει μοναδικό $k \in \mathcal{K}$, ώστε $enc_k(x) = y$, και (2) κάθε κλειδί επιλέγεται με την ίδια πιθανότητα, συγκεκριμένα $1/\mathcal{K}$.*

Απόδειξη (συνοπτική): Για την ορθή κατεύθυνση αποδεικνύουμε ότι η παραβίαση της (1) οδηγεί σε μηδενική δεσμευμένη πιθανότητα κάποιου y με δοσμένο x. Από την (1) προκύπτει ότι για κάθε $y \in \mathcal{C}$ και κάθε ζεύγος διαφορετικών κλειδιών $k_1, k_2 \in \mathcal{K}$ θα πρέπει να υπάρχουν διαφορετικά $x_1, x_2 \in$ τέτοια ώστε $enc_{k_1}(x_1) = y$ και $enc_{k_2}(x_2) = y$. Με χρήση της δεύτερης Ισοδύναμης Συνθήκης προκύπτει ότι τα k_1, k_2 επιλέγονται με την ίδια πιθανότητα.

Για το αντίστροφο, αρκεί να παρατηρήσει κανείς ότι για κάθε ζεύγος $x \in \mathcal{M}, y \in \mathcal{C}$ ισχύει $\Pr[C = y \mid M = x] = \frac{1}{|\mathcal{K}|}$. Επομένως:

$$\forall y \in \mathcal{C}: \quad \Pr[C = y] = \sum_{x \in \mathcal{M}} \Pr[M = x] \cdot \Pr[enc_K(x) = y] = \frac{1}{|\mathcal{K}|} \sum_{x \in \mathcal{M}} \Pr[M = x] = \frac{1}{|\mathcal{K}|}.$$

□

Με χρήση του θεωρήματος αυτού μπορούμε να δείξουμε ότι το One-Time Pad έχει την ιδιότητα της τέλειας μυστικότητας.

Άσκηση: Προκειμένου να έχουμε τέλεια μυστικότητα, είναι αναγκαία συνθήκη για οποιοδήποτε κρυπτοσύστημα τα κλειδιά να είναι ισοπίθανα;

Αναφορές

[Sha49] Shannon, Claude (1949). ”Communication Theory of Secrecy Systems”. Bell System Technical Journal 28 (4): 656–715.