Εθνικο Μετσοβιο Πολυτεχνειο

Σχολη Ηλεκτρολογων Μηχανικων & Μηχανικων Υπολογιστων

Σημειώσεις Διαλέξεων

Στοιχεία Θεωρίας Αριθμών

&

Εφαρμογές στην Κρυπτογραφία

Επιμέλεια σημειώσεων:
Ελένη Μπακαλη
Άρης Παγουρτζης

Διδάσκοντες:
Στάθης Ζαχος
Άρης Παγουρτζης

14 Νοεμβρίου 2011

1 Κρυπτοσυστήματα ρέυματος / ροής (stream ciphers)

Παράγουμε μία ακολουθία κλειδιών με βάση κάποιο αρχικό κλειδί, και το plaintext. Το κρυπτοσύστημα μπορεί να είναι synchronous (δηλ. το κλειδί να μην εξαρτάται από το plaintext), ή asynchronous, και periodic ($\forall i : z_{i+d} = z_i$, όπου d η περίοδος), ή aperiodic. Π.χ. το Vigenère είναι synchronous και periodic.
Plaintext: $x_0, x_1, \ldots, x_{n-1}$
Αρχικό κλειδί:k
Συναρτήσεις:f_i
Key stream: $z_i = f_i(k, x_0, \ldots, x_{i-1})$
Ciphertext: $y_i = e_{z_i}(x_i)$

Η e_k είναι η συνάρτηση κρυπτογράφησης, και d_k η συνάρτηση αποκρυπτογράφησης. Π.χ. για δυαδικές ακολουθίες:

$$e_z(x) = x \oplus z = x + z \bmod 2$$

$$d_z(y) = y \oplus z = y + z \bmod 2$$

Linear Recurrence Keystream

Έχουμε ένα αρχικό διάνυσμα κλειδιών $(z_0, z_1, \ldots, z_{m-1})$. Τα υπόλοιπα κλειδιά υπολογίζονται ως εξής.

$$z_{m+i} = \sum_{j=0}^{m-1} c_j zi + j \bmod 2$$

όπου οι συντελεστές c_j είναι 0 ή 1. Εάν το πολυώνυμο $c_0 + c_1 x + c_2 x^2 + \ldots + c_{m-1} x^{m-1}$ που ορίζουν αυτοί οι συντελεστές είναι primitive, τότε το κρυπτοσύστημα είναι περιοδικό με περίοδο $d \leq 2^m - 1$.
Π.χ. $c_0 = c_1 = 1, c_2 = c_3 = 0$ ορίζουν το πολυώνυμο $x + 1$, και με δεδομένα τα αρχικά $z_0, \ldots, z_4$ έχουμε $z_{4+i} = z_i + z_{i+1} \bmod 2$. Παρατηρούμε ότι το κρυπτοσύστημα έχει περίοδο 15.

2 Τύποι κρυπταναλυτικών επιθέσεων

1. Κρυπτοκείμενο μόνο (ciphertext only). Ο κρυπταναλυτής διαθέτει μόνο το κρυπτοκείμενο.

2. Γνωστό αρχικό κείμενο (known plaintext attack – KPA). Ο κρυπταναλυτής διαθέτει ζεύγη αρχικού κειμένου–κρυπτοκειμένου.

3. Επιλεγμένο αρχικό κείμενο (chosen plaintext attack – CPA). Ο κρυπταναλυτής διαθέτει ζεύγη αρχικού κειμένου–κρυπτοκειμένου, αλλά με αρχικά κείμενα της επιλογής του.

4. Επιλεγμένο κρυπτοκείμενο (chosen ciphertext attack – CCA). Ο κρυπταναλυτής διαθέτει ζεύγη αρχικού κειμένου–κρυπτοκειμένου για ορισμένα κρυπτοκείμενα της επιλογής του (ισοδύναμα, μπορεί να αποκρυπτογραφήσει ορισμένα κρυπτοκείμενα της επιλογής του).

Π.χ. στο προγούμενο κρυπτοσύστημα παρατηρούμε ότι $y_i = x_i \oplus z_i \Rightarrow x_i \oplus y_i = z_i$. Άρα με KPA πρώτα βρίσκουμε τα $z_0, \ldots, z_{m-1}$ και με μήκος κειμένου πάνω από $2m$ μπορούμε να βρούμε τα c_i λύνοντας ένα σύστημα m εξισώσεων με m αγνώστους (για m που το μαντεύουμε με διαδοχικές δοκιμές).

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

'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 $x_1, x_2 \in \{0, \ldots, 25\}$.

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.

Κρυπτοσυστήματα Γινομένου (Product Cryptosystems)

Προκύπτουν από σύνθεση των συναρτήσεων κρυπτογράφησης δύο ή περισσοτέρων κρυπτοσυστημάτων:

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

4 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 $\mathcal{M}, \mathcal{K}, \mathcal{C}$.

Ορισμός τέλειας μυστικότητας

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

Δηλαδή, δεν μπορούμε από το κρυπτοκείμενο να ανακτήσουμε καμμία πληροφορία για το αρχικό κείμενο, που να μην την γνωρίζουμε εξ αρχής.

Ο Shannon απέδειξε ότι δεν είναι δυνατόν να έχουμε perfect secrecy, παρά μόνο αν το κλειδί είναι ίδιου μήκους με το αρχικό κείμενο.

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

Θεωρούμε το shift cipher ($C = M + K \bmod 26$), με κατανομή του K την ομοιόμορφη στο $\{0, \ldots, 25\}$. Δηλ. $\forall i \Pr[K = i] = \frac{1}{26}$.

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

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

Επίσης παρατηρούμε και ότι

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

Οπότε από το θεώρημα του Bayes έχουμε:

$$\Pr[M = x, C = y] = \Pr[M = x | C = y] \Pr[C = y] = \Pr[C = y | M = x] \Pr[M = x] \Rightarrow$$

$$\Pr[M = x | C = y] = \frac{\Pr[C = y | M = x] \Pr[M = x]}{\Pr[C = y]} = \frac{\frac{1}{26} \Pr[M = x]}{\frac{1}{26}} = \Pr[M = x].$$

Από τα παραπάνω προκύπτει και ότι ισοδύναμη συνθήκη για τέλεια μυστικότητα είναι και η:

$$\Pr[C = y] = \Pr[C = y | M = x]$$

που εκφράζει ότι η πιθανότητα εμφάνισης οποιουδήποτε κρυπτοκειμένου είναι ίδια ανεξαρτήτως αρχικού κειμένου, με άλλα λόγια το κρυπτοκείμενο και το αρχικό κείμενο είναι ανεξάρτητες τυχαίες μεταβλητές.

Χρησιμοποιώντας αυτή τη μορφή μπορεί να δείξει κανείς ότι αναγκαία συνθήκη για τέλεια μυστικότητα είναι ο χώρος των κλειδιών να είναι ισοπληθικός με τον χώρο των αρχικών κειμένων (και με αυτόν των κρυπτοκειμένων).