Δημήτριος Κυριακίδης
el17077

Κρυπτογραφία
3º Φυλλάδιο Ασκήσεων

Άσκηση 1:

Με τον τρόπο λειτουργίας Cipher Block Chaining - CBC, αλλοίωση bit του κρυπτοτμήματος y_i προκαλεί αλλοίωση του αποτελέσματος x_{i+1} στην ίδια θέση, γιατί το κρυπτογράφημα του προηγούμενου τμήματος κρυπτοκειμένου γίνεται XOR με το τρέχον τμήμα αρχικού κειμένου πριν αυτό κρυπτογραφηθεί. Θεωρώντας ότι η αλλοίωση αυτή συμβαίνει μεταξύ φάσης encryption και decryption, και συνεπώς τα υπόλοιπα τμήματα κρυπτοκειμένου είναι σωστά, το μόνο άλλο τμήμα που επηρεάζει αυτή η αλλαγή είναι το plaintext x_i, σε πολλά σημεία.

Άρα, η επικόλληση ενός ακόμα block στο τέλος του μηνύματος δεν εξασφαλίζει την ακεραιότητα, καθώς αλλαγή (ή μη) σε αυτό οδηγεί σε συμπέρασμα μόνο για το αμέσως προηγούμενο τμήμα.

(Όπως προκύπτει από το σχήμα του CBC, στην κρυπτογράφηση το τελευταιο q_l εξαρτάται από όλα τα προηγούμενα q και p, ενώ στην αποκρυπτογράφηση κάθε q_i επηρεάζει μόνο p_i και p_{i+1}. Η μέθοδος αυτή θα ανιχνεύσει λάθος μόνο αν το λάθος προήλθε από τα δύο τελευταία q. Αν για έλεγχο ακεραιότητας χρησιμοποιείτο το τελευταίο κρυπτογραφημένο block και όχι plaintext τότε πράγματι θα ήταν καλός έλεγχος ακεραιότητας).

Άσκηση 2:

Η συνάρτηση *h* έχει την ιδιότητα δυσκολίας εύρεσης συγκρούσεων (collision resistance), δηλαδή είναι υπολογιστικώς δύσκολο να βρεθούν $x, x' \in X$ τέτοια, ώστε $h(x) = h(x')$.

Πρώτα θα δειχθεί ότι, αν μπορούσε να βρεθεί σύγκρουση για την h_2, τότε θα βρισκόταν και για την *h*: έστω ότι είναι υπολογιστικώς εύκολο να βρεθούν συμβολοσειρές μήκους *n*, x_1, x_2, x_3, x_4 και x_1', x_2', x_3', x_4', τέτοιες, ώστε $x_1 \parallel x_2 \parallel x_3 \parallel x_4 \neq x_1' \parallel x_2' \parallel x_3' \parallel x_4'$ (άρα τουλάχιστον ένα ζεύγος x_i, x_i' είναι διαφορετικό) και $h_2(x_1 \parallel x_2 \parallel x_3 \parallel x_4) = h_2(x_1' \parallel x_2' \parallel x_3' \parallel x_4')$.
Τότε $h\big(h(x_1 \parallel x_2) \parallel h(x_3 \parallel x_4)\big) = h\big(h(x_1' \parallel x_2') \parallel h(x_3' \parallel x_4')\big)$ και θέτοντας $h(x_i \parallel x_j) = y_{ij}$:
$h(y_{12} \parallel y_{34}) = h(y_{12}' \parallel y_{34}')$. Αν $y_{12} \parallel y_{34} = y_{12}' \parallel y_{34}'$ τότε $y_{12} = y_{12}'$ και $y_{34} = y_{34}' \Leftrightarrow$
$\Leftrightarrow h(x_1 \parallel x_2) = h(x_1' \parallel x_2')$ και $h(x_3 \parallel x_4) = h(x_3' \parallel x_4')$, οπότε έχει βρεθεί τουλάχιστον μία σύγκρουση, εφόσον όπως εξηγήθηκε υπάρχει ζεύγος $x_i \neq x_i'$. Αν $y_{12} \parallel y_{34} \neq y_{12}' \parallel y_{34}'$ τότε προφανώς έχει βρεθεί σύγκρουση. Σε κάθε περίπτωση, επομένως, εύρεση σύγκρουσης για την h_2 συνεπάγεται το ίδιο και για την *h*, επομένως αυτή δεν είναι υπολογιστικώς εύκολη.

Για την h_3, επειδή η πράξη XOR είναι αντιμεταθετική, αληθεύει
$h(x_1 \parallel x_2) \oplus h(x_3 \parallel x_4) = h(x_3 \parallel x_4) \oplus h(x_1 \parallel x_2)$ και συνεπώς

$h_3(x_1 \parallel x_2 \parallel x_3 \parallel x_4) = h_3(x_3 \parallel x_4 \parallel x_1 \parallel x_2)$ για οποιαδήποτε x_1, x_2, x_3, x_4, άρα η h_3 δεν έχει την επιθυμητή ιδιότητα.

Άσκηση 7:

Το πρόβλημα του Διακριτού Λογαρίθμου (DLP) εκφράζεται ως εξής:

«Δίνεται κυκλική ομάδα $\mathbb{G} = \langle g \rangle$ τάξης q και τυχαίο στοιχείο $y \in \mathbb{G}$. Να υπολογισθεί $x \in \mathbb{Z}_q$ ώστε $g^x = y$, δηλαδή ο $\log_g y \in \mathbb{Z}_q$».

Έστω ότι $q - 1 = \prod_{i=1}^{k} p_i^{n_i}$, με p_i πρώτο για κάθε i. Ο αλγόριθμος των Pohlig-Hellman απλοποιεί το πρόβλημα εύρεσης του διακριτού λογαρίθμου $x = \log_g y$, ανάγοντάς το σε k υποπροβλήματα, ούτως ώστε η συνολική πολυπλοκότητα επίλυσης του προβλήματος να μην είναι $O(q^{1/2})$, αλλά $O(p_{max}^{1/2})$, όπου p_{max} είναι ο μεγαλύτερος συντελεστής. Ο αλγόριθμος, δηλαδή, βρίσκει τα $x_i \equiv x \ mod\ p_i^{n_i}$, και στην συνέχεια χρησιμοποιεί το CRT για να βρεί το ζητούμενο x από τα x_i. Για κάθε υποπρόβλημα i χρειάζεται να λυθούν n_i προβλήματα διακριτού λογαρίθμου σε υποσύνολα της τάξης p_i.

Στην συγκεκριμένη περίπτωση, η τάξη της ομάδας $\mathbb{Z}_p^*$ είναι δύναμη πρώτου: $p - 1 = 2^{2m}$ και συνεπώς μπορεί να χρησιμοποιηθεί η εξής παραλλαγή του αλγορίθμου:

Input: A cyclic group G of order $n = p^e$ with generator g and an element $h \in G$.

Output: The unique integer $x \in \{0, \ldots, n-1\}$, such that $g^x = h$.

1. Initialize $x_0 = 0$.
2. Compute $\gamma = g^{p^{e-1}}$. By Lagrange's theorem, this element has order p.
3. For all $k \in \{0, \ldots, e-1\}$, do:
   a. Compute $h_k = (g^{-x_k} h)^{p^{e-1-k}}$. By construction, the order of this element must divide p, hence $h_k \in \langle \gamma \rangle$.
   b. Using the Baby-Step Giant-Step, compute $d_k \in \{0, \ldots, p-1\}$ such that $\gamma^{d_k} = h_k$. It takes time $O(\sqrt{p})$.
   c. Set $x_{\{k+1\}} = x_k + p^k d_k$.
4. Return x_e.

Assuming e is much smaller than p, the algorithm computes discrete logarithms in time complexity $O(e\sqrt{p})$, far better than BS-GS' $O(\sqrt{p^e})$.

Άσκηση 8:

Η επίθεση καθολικής πλαστογραφίας στο σύστημα υπογραφών El Gamal πραγματοποιείται ως εξής:

Κατασκευή r, s, m ταυτοχρόνως: επιλέγω i, j με $0 \leq i, j \leq p-2$ και $(j, p - 1) = 1$ και θέτω

$$r = g^i \cdot (g^X)^j \; mod \; p$$

$$s = -r \cdot j^{-1} \; mod \; p - 1$$

$$m = -r \cdot i \cdot j^{-1} \; mod \; p - 1$$

Τα (r, s) επαληθεύουν την υπογραφή. Το σενάριο αυτό είναι εφικτό και δίνει υπογραφή για τυχαίο m. Επομένως, στην προκείμενη περίπτωση, θέτοντας $a = -\mathcal{H}(m) \; mod \; p - 1$, θέλουμε να ισχύει $b = g^a y^{-1} \; mod \; p$, και οι δύο έλεγχοι είναι ισοδύναμοι. Επομένως πράγματι δεν υπάρχει προστασία στο συγκεκριμένο σύστημα από την επίθεση αυτήν.