Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ, ΜΠ)

2η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 21 Δεκεμβρίου 2025

Άσκηση 1.
(α) Αποδείξτε ότι για κάθε κλειδί k του DES και για κάθε μήνυμα m: $\text{DES}_{\overline{k}}(\overline{m}) = \overline{\text{DES}_k(m)}$, όπου $\overline{x}$ το συμπλήρωμα του x.
(β) Με δύο ζεύγη κειμένου-κρυπτοκειμένου (m_1, c_1) και (m_2, c_2), όπου τα m_1 και m_2 τα επιλέγετε εσείς, θέλετε να βρείτε k τέτοιο που τα c_1, c_2 να αποκρυπτογραφούνται στα m_1, m_2 αντίστοιχα. Υποθέστε ότι για καθένα από τα c_1, c_2 αυτό το k είναι μοναδικό. Εξηγείστε πώς μπορείτε να το κατορθώσετε αυτό με το πολύ 2^{55} κρυπτογραφήσεις (έναντι των 2^{56} που απαιτεί η εξαντλητική αναζήτηση).

Άσκηση 2. Έστω h συνάρτηση σύνοψης, η οποία συμπιέζει ακολουθίες μήκους $2n$ σε ακολουθίες μήκους n και έχει την ιδιότητα δυσκολίας εύρεσης συγκρούσεων (collision free). Θέλουμε να φτιάξουμε μία νέα συνάρτηση σύνοψης που να συμπιέζει ακολουθίες μήκους $4n$ σε ακολουθίες μήκους n, η οποία να έχει επίσης την ιδιότητα δυσκολίας εύρεσης συγκρούσεων. Έχουμε τις εξής υποψήφιες:

1. $h_1(x_1||x_2||x_3||x_4) = h((x_1 \oplus h(x_2||x_2))||(h(x_3||x_3) \oplus x_4))$
2. $h_2(x_1||x_2||x_3||x_4) = h(h(x_1||x_2)||h(x_3||x_4))$
3. $h_3(x_1||x_2||x_3||x_4) = h(x_1||x_2) \oplus h(x_3||x_4)$
4. $h_4(x_1||x_2||x_3||x_4) = h(h(h(x_1||x_2)||x_3)||x_4)$

(Με "$\oplus$" συμβολίζουμε το XOR, με "||" την παράθεση και $|x_i| = n$.)
Για κάθε i εξετάστε αν η h_i έχει την ιδιότητα δυσκολίας εύρεσης συγκρούσεων ή όχι. Για να δείξετε ότι την έχει, δείξτε ότι αν μπορούσαμε να βρούμε συγκρούσεις για την h_i, τότε θα μπορούσαμε να βρούμε συγκρούσεις και για την h. Για να δείξετε το αντίθετο βρείτε μία ή περισσότερες συγκρούσεις για την h_i.

Άσκηση 3. Δείξτε ότι η λειτουργία CTR δεν διαθέτει CCA ασφάλεια για οποιαδήποτε F.

Άσκηση 4. Έστω μια κυκλική ομάδα $\mathbb{G}$ με τάξη πρώτο q και γεννήτορα g.

1. Ορίζουμε το Τετραγωνικό πρόβλημα Diffie - Hellman (SDH) ως εξής:
   Δίνονται $g, g^x \in \mathbb{G}$. Να υπολογιστεί το g^{x^2}.

2. Ορίζουμε το πρόβλημα Diffie - Hellman Αντιστρόφου (IDH) ως εξής:
   Δίνονται $g, g^x \in \mathbb{G}$. Να υπολογιστεί το $g^{x^{-1}}$.

Να αποδείξετε ότι τα παραπάνω προβλήματα είναι ισοδύναμα τόσο μεταξύ τους, όσο και με το υπολογιστικό πρόβλημα Diffie - Hellman (CDH).

Άσκηση 5.
Σταθερό σημείο ενός κρυπτοσυστήματος ονομάζουμε ένα μήνυμα που το κρυπτοκείμενό του είναι το ίδιο το μήνυμα, δηλαδή $\mathsf{Enc}(m) = m$. Επομένως, στην περίπτωση του RSA, αν το δημόσιο κλειδί είναι το (n, e), τότε για ένα σταθερό σημείο ισχύει $m^e \equiv m \pmod{n}$. Αποδείξτε ότι το πλήθος των σταθερών σημείων στο RSA είναι $[\gcd(e-1, p-1) + 1][\gcd(e-1, q-1) + 1]$.

Άσκηση 6.
Να υλοποιήσετε σε γλώσσα προγραμματισμού της επιλογής σας την επίθεση αποκρυπτογράφησης ενός κρυπτοκειμένου c σε RSA που χρησιμοποιεί ένα oracle το οποίο μπορεί να αποφανθεί αν το μήνυμα που αντιστοιχεί στο κρυπτοκείμενο είναι στο 'πάνω' ή στο 'κάτω' μισό του $\mathbb{Z}_n$ (δηλ. συνάρτηση loc).

Συγκεκριμένα πρέπει να υλοποιήσετε 2 τμήματα κώδικα:
(1) Το πρώτο θα 'προσομοιώνει' το oracle, αποκρυπτογραφώντας (κανονικά με το ιδιωτικό κλειδί) το c και υπολογίζοντας την loc.
(2) Το δεύτερο θα υλοποιεί την επίθεση ρωτώντας επαναληπτικά το oracle κατάλληλες ερωτήσεις για την loc χρησιμοποιώντας την ιδιότητα του malleability που χαρακτηρίζει το RSA.

Για την επικοινωνία των προγραμμάτων μπορείτε να χρησιμοποιήσετε ένα κοινόχρηστα αρχείο ή απλούστερα εσωτερικά στο πρόγραμμα με κατάλληλη κλήση συνάρτησης. Η παραγωγή των κλειδιών και η αρχική κρυπτογράφηση μπορεί να γίνει από δικό σας κώδικα ή χρησιμοποιώντας ένα έτοιμο εργαλείο όπως το Openssl.

Άσκηση 7. Ο διευθυντής μιας εταιρείας χρειάζεται να παίρνει συχνά κρυπτογραφημένα μηνύματα από τους υπαλλήλους του. Για τον σκοπο αυτό χρησιμοποιεί RSA, δηλαδή δίνει σε όλους το δημόσιο κλειδί του $\langle n, e\rangle$ όπου $n = pq$ με p, q πρώτους. Φυσικά κρατάει κρυφούς τους πρώτους p, q.
Για ευκολία, δίνει επιπλέον στη γραμματέα του μία συσκευή με την οποία θα μπορούν οι υπάλληλοι που δεν διαθέτουν το πρόγραμμα κρυπτογράφησης να κρυπτογραφούν τα μηνύματά τους.
Η συσκευή υποτίθεται ότι λειτουργεί ως εξής για είσοδο m:

- Υπολογίζει $c_p = m^e \bmod p$,
- Υπολογίζει $c_q = m^e \bmod q$, και
- Συνδυάζει τις λύσεις με CRT ώστε να δώσει ως έξοδο τη μοναδική τιμή $c \in \mathbb{Z}_n$ τ.ω. $c \equiv m^e \pmod{n}$.

Λόγω όμως εργοστασιακού λάθους, στο δεύτερο βήμα η συσκευή υπολογίζει $c'_q = m^e + 1 \bmod q$ και δίνει στην έξοδο $c' \in \mathbb{Z}_n$, τ.ώ. $c' \equiv c_p \pmod{p}$ και $c' \equiv c'_q \pmod{q}$.

Όπως είναι φυσικό, ο διευθυντής σύντομα διαπιστώνει (με ποιον τρόπο;) ότι κάτι δεν πάει καλά, και ζητάει από την γραμματέα του να στείλει την συσκευή για επισκευή. Η γραμματέας όμως, που είναι ιδιαίτερα έξυπνη, κατορθώνει πριν στείλει την συσκευή στο service να βρει το ιδιωτικό κλειδί του διευθυντή. Πώς το κατάφερε αυτό;

Σύντομες οδηγίες: (α) προσπαθήστε μόνοι σας, (β) συζητήστε με συμφοιτητ(ρι)ές σας, (γ) αναζητήστε ιδέες στο διαδίκτυο – με αυτή τη σειρά και αφού αφιερώσετε αρκετό χρόνο σε κάθε στάδιο! Σε κάθε περίπτωση οι απαντήσεις πρέπει να είναι *αυστηρά ατομικές*. Ενδεχομένως σας ζητηθεί να παρουσιάσετε σύντομα κάποιες από τις λύσεις σας.

Καλή επιτυχία!