Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)

3η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 27/1/2022

Άσκηση 1. Κάποιος σκέφτηκε να χρησιμοποιήσει ένα ασφαλές κρυπτοσύστημα τμήματος (π.χ. AES) για ταυτόχρονη κρυπτογράφηση και έλεγχο ακεραιότητας χρησιμοποιώντας τον τρόπο λειτουργίας CBC ως εξής: ο αποστολέας προσθέτει ένα επιπλέον block, αποτελούμενο από '0' μόνο, στο τέλος του απλού κειμένου και κρυπτογραφεί με CBC mode. Αν ο παραλήπτης κατά την αποκρυπτογράφηση πάρει το ίδιο block (όλο '0') στο τέλος του αποκρυπτογραφημένου κειμένου, θεωρεί ότι το μήνυμα μεταδόθηκε σωστά. Εξασφαλίζει αυτή η μέθοδος την ακεραιότητα του μηνύματος;

Άσκηση 2. 'Εστω 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 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. $h_2(x_1||x_2||x_3||x_4) = h(h(x_1||x_2)||h(x_3||x_4))$
2. $h_3(x_1||x_2||x_3||x_4) = h(x_1||x_2) \oplus h(x_3||x_4)$

(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. Θεωρήστε την γεννήτρια ψευδοτυχαίων bit BBS με Blum integer $n = pq$.
(α) Να προσδιορίσετε επακριβώς την περίοδο της γεννήτριας. Εξηγήστε γιατί πρέπει να είναι μικρό το $\gcd(p-1, q-1)$.
(β) Οι "safe primes" είναι ειδικοί πρώτοι αριθμοί της μορφής $p = 2p' + 1$ όπου p' είναι επίσης πρώτος. Ονομάζουμε "SafeSafe primes" τους ειδικούς εκείνους πρώτους p για τους οποίους ισχύει ότι αν p'' είναι πρώτος με $p'' \equiv 1 \pmod 4$, τότε $2p''+1$: πρώτος και $p = 2(2p''+1)+1$. Ποια είναι η **μέγιστη** περίοδος της γεννήτριας στην περίπτωση που τόσο ο p όσο και ο q είναι "SafeSafe" πρώτοι; Να αποδείξετε τον ισχυρισμό σας.

Άσκηση 4. 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;

Άσκηση 5. ☠

(α) Σας δίνεται ένα κρυπτοσύστημα RSA με τα παρακάτω δημόσια κλειδιά, σε δεκαεξαδική αναπαράσταση:

```
n = 0xb844986fc061a2c0baf528a960e208832625f725fa09bfe1ac4c15bccad6031d09f8f37bf
00520bb59480070e59441ed34b7e3d118db67a035ac4b46a055a4963df4af0baa4dfab3f98566f2
c09f7c83ffec458b63931ce311241c98614659172cfe9f21ecc7d7241aea1ae1e88f796568f49a6
45ffce12c87629e8783462e5dbeb52a85c95
e = 0x369d89b820f2450462f21b02d91bcec9de528805bb22123d843fcd776ad57025980f1c335
9d45d65c9a9e363a0a51eaf8873b3dc2ffab45787c5e86bacbf2a6bbca5106828eec95cb2ea534f
a2e64d672a2c69e21589f84daa54a164db28ade473e8009972279cd89c5afaf1b312914256dac66
6e7f824db23f33a9867616898686a1fe63c5
```

Σας δίνεται ότι το ιδιωτικό κλειδί d είναι αρκούντως μικρό, ώστε να επιτρέπεται επίθεση μικρού ιδιωτικού εκθέτη. Να κατασκευάσετε έναν αλγόριθμο και το αντίστοιχο κομψό και αποδοτικό πρόγραμμα σε γλώσσα προγραμματισμού Python ή C (πιθανόν να σας φανεί χρήσιμη η βιβλιοθήκη χειρισμού πολύ μεγάλων αριθμών GMP, που έχει μεταξύ άλλων και ένα φιλικό interface σε Python) που να σας επιτρέπει να σπάσετε το παραπάνω κρυπτοσύστημα. Ποιο είναι το ιδιωτικό κλειδί d; Ποια είναι η υπολογιστική πολυπλοκότητα του αλγορίθμου σας;

(β) Να κατασκευάσετε ένα κομψό και αποδοτικό πρόγραμμα σε γλώσσα Python ή C που να σας επιτρέψει να παραγοντοποιήσετε το παραπάνω n. Ποιοι είναι οι πρώτοι του παράγοντες, p και q;

Άσκηση 6.

Σταθερό σημείο ενός κρυπτοσυστήματος ονομάζουμε ένα μήνυμα που το κρυπτοκείμενό του είναι το ίδιο το μήνυμα, δηλαδή $enc(m) = m$. 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 7. Έστω πρώτος $p = 4^m + 1, m \in \mathbb{Z}$. Διατυπώστε αποδοτικό αλγόριθμο για την εύρεση διακριτού λογαρίθμου στην ομάδα $\mathbb{Z}_p^*$.

Άσκηση 8.

΄Εστω το παρακάτω σχήμα υπογραφών όπου για τις παραμέτρους ισχύει ό,τι και στο σχήμα υπογραφών ElGamal. Κάθε χρήστης έχει ιδιωτικό κλειδί x και δημόσιο $y = g^x \bmod p$. Η υπογραφή λειτουργεί ως εξής:

i. Ο υπογράφων αρχικά επιλέγει $h \in \{0, \ldots, p-2\}$ ώστε: $\mathcal{H}(m) + x + h \equiv 0 \pmod{p-1}$, όπου $\mathcal{H}$ collision resistant συνάρτηση σύνοψης.

ii. Η υπογραφή είναι η τριάδα: $sign(x, m) = (m, (x + h) \bmod p - 1, g^h \bmod p)$.

iii. Για την επαλήθευση ότι μια τριάδα (m, a, b) είναι έγκυρη υπογραφή ελέγχεται εάν:

- $yb \equiv g^a \pmod{p}$ και
- $g^{\mathcal{H}(m)} yb \equiv 1 \pmod{p}$.

Να δείξετε ότι το σχήμα αυτό δεν προστατεύει από επίθεση καθολικής πλαστογράφησης.

☠: bonus ερώτημα.

Σύντομες οδηγίες: (α) προσπαθήστε μόνοι σας, (β) συζητήστε με συμφοιτητές 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*.