ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΚΡΥΠΤΟΓΡΑΦΙΑ

(2021 – 2022)

3η Σειρά Ασκήσεων

Ονοματεπώνυμο:

- Χρήστος Τσούφης

Αριθμός Μητρώου:

- 031 17 176

Στοιχεία Επικοινωνίας:

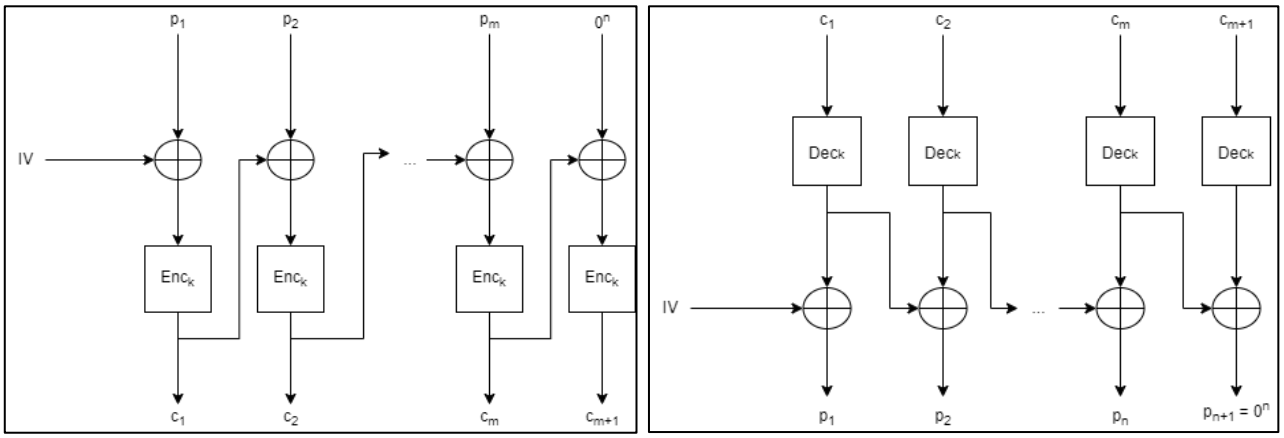
- el17176@mail.ntua.gr
- chris99ts@gmail.com

1η Άσκηση

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;

Λύση:

Η μέθοδος που περιγράφεται χρησιμοποιεί το κρυπτοσύστημα AES με τρόπο λειτουργίας CBC για ταυτόχρονη κρυπτογράφηση και έλεγχο ακεραιότητας. Συγκεκριμένα, ο αποστολέας προσθέτει ένα block, αποτελούμενο από '0' μόνο, στο τέλος του απλού κειμένου και κρυπτογραφεί με CBC mode (αριστερή εικόνα). Επιπλέον, αν ο παραλήπτης κατά την αποκρυπτογράφηση πάρει το ίδιο block (όλο '0') στο τέλος του αποκρυπτογραφημένου κειμένου, θεωρεί ότι το μήνυμα μεταδόθηκε σωστά (δεξιά εικόνα).



Με την παραπάνω μέθοδο δεν εξασφαλίζεται η ακεραιότητα του μηνύματος.

Κατά την κρυπτογράφηση με CBC mode η πληροφορία από κάθε plaintext μεταφέρεται στο επόμενο στάδιο. Συνεπώς, το τελευταίο ciphertext ενσωματώνει όλο το αρχικό κείμενο. Έτσι, ο έλεγχος για το εάν το τελευταίο block είναι όλο '0' μπορεί να πραγματοποιηθεί από την εκ νέου κρυπτογράφηση με βάση τα p_i που παραλήφθηκαν και να γίνει σύγκριση ομοιότητας μεταξύ των τελευταίων block.

Κατά την αποκρυπτογράφηση με CBC mode έχει την ιδιότητα να πραγματοποιεί self-recovery, δηλαδή όταν προκύπτει ένα λάθος σε κάποιο q_i τα κείμενα που επηρεάζονται είναι τα p_i, p_{i+1}. Συνεπώς, το τελευταίο block μπορεί να είναι όλο '0' όμως κάποια αρχικά μηνύματα να είναι λανθασμένα.

2η Άσκηση

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 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. $h_2(x_1 \parallel x_2 \parallel x_3 \parallel x_4) = h\big(h(x_1 \parallel x_2) \parallel h(x_3 \parallel x_4)\big)$

2. $h_3(x_1 \parallel x_2 \parallel x_3 \parallel x_4) = h(x_1 \parallel x_2) \oplus h(x_3 \parallel x_4)$

(Με "⊕" 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*.*

Λύση:

Έστω h μια συνάρτηση σύνοψης $\{0,1\}^{2n} \to \{0,1\}^n$ με την ιδιότητα της δυσκολίας εύρεσης συγκρούσεων (collision free).

1. Έστω ότι υπάρχει collision για $y = x_1 \parallel x_2 \parallel x_3 \parallel x_4$ και $z = x_1' \parallel x_2' \parallel x_3' \parallel x_4'$ με $y \neq z$. Αφού η h είναι collision free, δεν υπάρχει τρόπος να βρεθούν 2 διαφορετικά ορίσματα που να δίνουν το ίδιο αποτέλεσμα. Συνεπώς, ο μόνος τρόπος να προκύψει το ίδιο αποτέλεσμα είναι να έχουν το ίδιο όρισμα. Έτσι:

$$h\big(h(x_1 \parallel x_2) \parallel h(x_3 \parallel x_4)\big) = h\big(h(x_1' \parallel x_2') \parallel h(x_3' \parallel x_4')\big) \Rightarrow$$

$$\Rightarrow h(x_1 \parallel x_2) \parallel h(x_3 \parallel x_4) = h(x_1' \parallel x_2') \parallel h(x_3' \parallel x_4') \Rightarrow$$

$$\Rightarrow h(x_1 \parallel x_2) = h(x_1' \parallel x_2') \;\&\&\; h(x_3 \parallel x_4) = h(x_3' \parallel x_4') \Rightarrow$$

$$\Rightarrow x_1 \parallel x_2 = x_1' \parallel x_2' \;\&\&\; x_3 \parallel x_4 = x_3' \parallel x_4' \Rightarrow$$

$$\Rightarrow x_1 = x_1' \;\&\&\; x_2 = x_2' \;\&\&\; x_3 = x_3' \;\&\&\; x_4 = x_4'$$

Δηλαδή, δεν μπορούν να βρεθούν 2 διαφορετικά κείμενα με την ίδια τιμή.

Οπότε, είναι collision free.

2. Ισχύει ότι για $z_1 = x_1 \parallel x_2 \parallel x_3 \parallel x_4$ και $z_2 = x_3 \parallel x_4 \parallel x_1 \parallel x_2$ προκύπτει ότι $h_3(z_1) = h_3(z_2)$, αφού:

$$h_3(z_1) = h(x_1 \parallel x_2) \oplus h(x_3 \parallel x_4) \;\;\&\;\; h_3(z_2) = h(x_3 \parallel x_4) \oplus h(x_1 \parallel x_2)$$

Οπότε, η h_3 δεν είναι collision free.

Εναλλακτικά, ισχύει ότι: $h_3(a \parallel b \parallel a \parallel b) = h(a \parallel b) \oplus h(a \parallel b) = 0$

Οπότε, δεν είναι collision free καθώς η σχέση ισχύει Va, b.

3η Άσκηση

Θεωρήστε την γεννήτρια ψευδοτυχαίων bit BBS με Blum integer n = p·q.

(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″ ≡ 1 (mod 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.*

Λύση:

(α) *1ος Τρόπος Επίλυσης*:

Έστω μια γεννήτρια ψευδοτυχαίων bit BBS με Blum integer n = p·q: p ≡ q ≡ 3 (mod 4).

Για την αρχικοποίηση της γεννήτριας επιλέγεται ένα $s \in \mathcal{U}(\mathbb{Z}_n)$.

Σε κάθε επανάληψη υπολογίζεται το $x_i = x_{i-1}^2 \ mod \ n$ και ως έξοδος δίνεται $z_i = x_i \ mod \ 2, \ i \geq 1$.

Αυτή η σχέση για τα x_i μπορεί να γραφτεί και ως εξής:

$$x_i = x_0^{2^i} \ mod \ n$$

Για τον υπολογισμό της περιόδου της γεννήτριας αρκεί να βρεθεί το ελάχιστο π για το οποίο ισχύει:

$$x_0^{2^\pi} \equiv x_0 (mod \ n)$$

Εξ ορισμού, το x_0 είναι το τετραγωνικό υπόλοιπο mod n. Οπότε, το x_0 είναι σχετικά πρώτο με το n και για αυτό το λόγο η σχέση μπορεί να γραφτεί και ως εξής:

$$x_0^{2^\pi - 1} \equiv 1 (mod \ n)$$

Έτσι, αρκεί να βρεθεί η τάξη του στοιχείου $x_0^k \equiv 1 (mod \ n)$ διότι $k | 2^\pi - 1 \Rightarrow 2^\pi \equiv 1 (mod \ k)$.

Ισχύει ότι το k διαιρεί το $\lambda(n)$, οπότε δοκιμάζοντας όλους τους διαιρέτες του $\lambda(n)$ μπορεί να βρεθεί.

Έπειτα, για την εύρεση του ελάχιστου π ισχύει $2^\pi \equiv 1 (mod \ k) \Leftrightarrow 2^\pi \equiv 1 (mod \ k')$, όπου το k' ορίζεται ως $k' = \frac{k}{gcd(2^\pi, k)}$ με $gcd(2^\pi, k) = i_{max}$ να είναι η μέγιστη δύναμη του 2 που διαιρεί το k, αφού $2^\pi \equiv 1 (mod \ k)$.

Έτσι, αφού δείχθηκε ότι είναι σχετικά πρώτοι μεταξύ τους, πάλι με δοκιμές μπορούν να βρεθούν όλοι οι διαιρέτες του $\lambda(k')$. Συνεπώς, η περίοδος δίνεται από την τάξη 2 στο $\mathbb{Z}_{k'}$.

Το $\gcd(p-1, q-1)$ πρέπει να είναι μικρό διότι το k και, κατά συνέπεια, η περίοδος εξαρτώνται από το $\lambda(n) = lcm(p-1, q-1) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}$.

2ος Τρόπος Επίλυσης:

Έστω ότι p, q είναι πρώτοι με 20 δυαδικά ψηφία ο καθένας.

Για τον υπολογισμό της περιόδου του BBS το i-οστό νούμερο εκφράζεται ως εξής:

$$x_i = x_0^{2^i} \, mod \, n \equiv x_0^{2^{i \, mod \, \lambda(n)}} \, mod \, n \equiv x_0^{2^{i \, mod \, \lambda(\lambda(n))} \, mod \, \lambda(n)} \, mod \, n$$

Όπου, λ η Carmichael function.

Συνεπώς, η περίοδος είναι:

$$\lambda\big(\lambda(n)\big) = \lambda\big(\lambda(p \cdot q)\big) = \lambda\big(lcm(p-1, q-1)\big) = \lambda\left(\frac{(p-1)(q-1)}{\gcd(p-1, q-1)}\right)$$

Οπότε, αναζητείται το $\gcd(p-1, q-1)$ να είναι μικρό ώστε να μειωθεί όσο το δυνατόν λιγότερο το lcm των πρώτων παραγόντων του $(p-1)(q-1)$.

Επομένως, για $p = 11, q = 17$, η περίοδος θα είναι:

$$\lambda\left(\frac{10 \cdot 16}{2}\right) = \lambda(80) = lcm\big(\lambda(5), \lambda(2^4)\big) = \frac{4 \cdot \frac{1}{2} \cdot 2^3}{4} = 4$$

Δηλαδή, θα πρέπει να έχουν μια περίοδο ίση με 4.

Αυτό το αποτέλεσμα επαληθεύεται και με την υλοποίηση σε Python που φαίνεται στο συνοδευόμενο Notebook.

(β) Οι "Safe primes" είναι ειδικοί πρώτοι αριθμοί της μορφής $p = 2p' + 1$, όπου p' είναι επίσης πρώτος.

Οι "SafeSafe primes" είναι εκείνοι οι ειδικοί πρώτοι p για τους οποίους ισχύει όταν αν p'' είναι πρώτος με $p'' \equiv 1(mod\ 4)$, τότε $2p'' + 1$: πρώτος και $p = 2(2p'' + 1) + 1$.

Αναζητείται η μέγιστη περίοδος π της γεννήτριας στην περίπτωση που τόσο ο p όσο και ο q είναι "SafeSafe" πρώτοι.

Έστω ένα τυχαία επιλεγμένο s σχετικά πρώτο με το n. Τότε,

$$x_0^{2^\pi} \equiv x_0 (mod\ n) \Rightarrow x_0^{2^\pi - 1} \equiv 1 (mod\ n)$$

Αφού το $n = p \cdot q$, θα ισχύει ότι:

$$x_0^{2^\pi - 1} \equiv 1 (mod\ p)$$

Εξ ορισμού, ισχύει ότι το x_0 είναι τετραγωνικό υπόλοιπο mod n, οπότε θα είναι και τετραγωνικό υπόλοιπο mod p (αντίστοιχα και mod q) που σημαίνει ότι γράφεται ως άρτια δύναμη κάποιου γεννήτορα του p: $x_0 \equiv g^{2a}$, για κάποιο $0 \leq \alpha < \frac{p-1}{2}$. Έτσι, θα ισχύει ότι:

$$x_0^{2^\pi - 1} \equiv g^{2a(2^\pi - 1)} \equiv 1 (mod\ p)$$

Το g είναι γεννήτορας τάξης $p-1$, οπότε:

$$(p-1)\left|2a(2^{\pi}-1)\xrightarrow{p=2(2p''+1)+1}\left(2(2p''+1)\right)\right|2a(2^{\pi}-1)\Rightarrow(2p''+1)|a(2^{\pi}-1)$$

Από τον ορισμό των "SafeSafe" πρώτων αριθμών, το $t=2p''+1$ είναι επίσης πρώτος.

Επιπλέον, ισχύει ότι $a<\frac{p-1}{2}=t$, οπότε για το α διακρίνονται οι εξής περιπτώσεις:

- Για $\alpha=0$ προκύπτει ότι $x_0=1$
- Για $0<a<t$ προκύπτει $t\left|a(2^{\pi}-1)\xrightarrow{t:prime,t>a}t\right|(2^{\pi}-1)\Rightarrow 2^{\pi}\equiv 1(mod\ t)$

Επομένως, η περίοδος της γεννήτριας θα είναι κάποιο πολλαπλάσιο της τάξης του 2 στο $\mathbb{Z}_t$.

Ομοίως, προκύπτει πως το π θα είναι πολλαπλάσιο της τάξης του 2 στο $\mathbb{Z}_{2q''+1}$.

Από το Chinese Theorem υπολοίπων είναι γνωστό ότι κάθε ζευγάρι στο $\mathbb{Z}_p\times\mathbb{Z}_q$ αντιστοιχεί μοναδικά σε ένα στοιχείο στο $\mathbb{Z}_{pq}$.

Συνεπώς, για κύκλους μεγέθους π_p στην $\mathbb{Z}_p$ και κύκλους μεγέθους π_q στην $\mathbb{Z}_q$, τότε στο $\mathbb{Z}_n$ οι κύκλοι θα είναι μεγέθους $lcm(\pi_p,\pi_q)$.

Άρα, για $\pi=lcm(\pi_p,\pi_q)$:

$$x_0^{2^{\pi}-1}\equiv 1(mod\ p)\ \&\&\ x_0^{2^{\pi}-1}\equiv 1(mod\ q)\Rightarrow x_0^{2^{\pi}-1}\equiv 1(mod\ p)$$

Τέλος, γίνεται ένας έλεγχος για το πως επηρεάζει το x_0 την περίοδο της γεννήτριας. Έστω ότι το x_0 έχει περίοδο k. Τότε, από το (α) θα ισχύει ότι:

$$k|\lambda(p)=p-1=2(2p''+1)$$

Συνεπώς, $k\in\{2,2p''+1,2(2p''+1)\}$.

Επίσης, ισχύει ότι $2^{\pi}-1=ck$.

Επομένως, είναι προτιμότερο να επιλεχθεί ένα x_0 που να έχει την μέγιστη τάξη.

4η Άσκηση

Ο διευθυντής μιας εταιρείας χρειάζεται να παίρνει συχνά κρυπτογραφημένα μηνύματα από τους υπαλλήλους του. Για τον σκοπό αυτό χρησιμοποιεί RSA, δηλαδή δίνει σε όλους το δημόσιο κλειδί του $\langle n, e \rangle$ *όπου* $n = p \cdot q$ *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* $c_p = m^e (mod\ p)$,
- *Υπολογίζει* $c_q = m^e (mod\ q)$, *και*
- *Συνδυάζει τις λύσεις με CRT ώστε να δώσει έξοδο τη μοναδική τιμή* $c \in \mathbb{Z}_n$ *τ.ω.* $c \equiv m^e (mod\ n)$.

Λόγω όμως εργοστασιακού λάθους, στο δεύτερο βήμα η συσκευή υπολογίζει $c'_p = m^e + 1 (mod\ q)$ *και δίνει στην έξοδο* $c' \in \mathbb{Z}_n$, *τέτοιο ώστε* $c' \equiv c_p (mod\ p)$ *και* $c' \equiv c'_q\ (mod\ q)$.

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;

Λύση:

Λόγω του εργοστασιακού λάθους, ο διευθυντής διαπιστώνει ότι τα μηνύματα που λαμβάνει δεν βγάζουν νόημα έπειτα από την αποκρυπτογράφησή τους. Συνεπώς, υποψιάζεται ότι κάτι δεν λειτουργεί σωστά με την συσκευή κρυπτογράφησης.

Η γραμματέας του κατορθώνει, πριν στείλει την συσκευή στο service, να βρει το ιδιωτικό κλειδί του διευθυντή. Αυτό το επιτυγχάνει δίνοντας ως είσοδο στην συσκευή το '0' διότι τότε θα ισχύει ότι:

$$c' \equiv 0 (mod\ p)\ \&\ c' \equiv 1 (mod\ q)$$

Συνεπώς, η c' είναι πολλαπλάσιο του p και όχι του q.

Ύστερα, από τον υπολογισμό του $\gcd(n, c')$ μπορεί να προκύψει ως έξοδος το p.

Έτσι, αφού $n = p \cdot q$ με p, q πρώτους, μπορεί να υπολογιστεί και το q.

5η Άσκηση

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

```
n=0xb844986fc061a2c0baf528a960e208832625f725fa09bfe1ac4c15bccad6031d09f8f
37bf00520bb59480070e59441ed34b7e3d118db67a035ac4b46a055a4963df4af0baa4dfa
b3f98566f2c09f7c83ffec458b63931ce311241c98614659172cfe9f21ecc7d7241aea1ae
1e88f796568f49a645ffce12c87629e8783462e5dbeb52a85c95
```

```
e=0x369d89b820f2450462f21b02d91bcec9de528805bb22123d843fcd776ad57025980f1
c3359d45d65c9a9e363a0a51eaf8873b3dc2ffab45787c5e86bacbf2a6bbca5106828eec9
5cb2ea534fa2e64d672a2c69e21589f84daa54a164db28ade473e8009972279cd89c5afaf
1b312914256dac666e7f824db23f33a9867616898686a1fe63c5
```

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;*

Λύση:

(α) Η υλοποίηση του αλγορίθμου φαίνεται στο συνοδευόμενο Notebook.

(β) Η υλοποίηση του αλγορίθμου φαίνεται στο συνοδευόμενο Notebook.

6η Άσκηση

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* $m^e = m(mod\ N)$. *Αποδείξτε ότι το πλήθος των σταθερών σημείων στο RSA είναι* $[gcd(e-1, p-1)+1][gcd(e-1, q-1)+1]$.

Λύση:

1ος Τρόπος Επίλυσης:

Για την εύρεση όλων των σταθερών σημείων πρέπει να λυθεί η εξίσωση $m^e = m(mod\ p)$. Είναι προφανές πως για $m|p$ θα ισχύει: $0 \equiv m^e \equiv m(mod\ p)$. Για $m \neq 0(mod\ p)$ ισχύει ότι $m \equiv a^z(mod\ p) \Rightarrow a^{ez} \equiv a^z(mod\ p)$. Από Euler, η εξίσωση μπορεί να γραφτεί ως: $z \cdot (e-1) \equiv 0\big(mod\ \varphi(p)\big)$. Είναι προφανές ότι υπάρχουν $\gcd(p-1, e-1)+1$ διαφορετικές λύσεις. Ομοίως, για το q, όπου $p \cdot q = N$, θα υπάρχουν $\gcd(q-1, e-1)+1$ διαφορετικές λύσεις. Οπότε, από το CRT θα υπάρχουν συνολικά:$[\gcd(p-1, e-1)+1] \cdot [\gcd(q-1, e-1)+1]$ λύσεις.

2ος Τρόπος Επίλυσης:

Ένα μήνυμα που το κρυπτοκείμενό του είναι ίδιο με το μήνυμα ονομάζεται σταθερό σημείο ενός κρυπτοσυστήματος. Για το RSA με δημόσιο κλειδί (n, e) σταθερά σημεία θεωρούνται τα σημεία στα οποία ισχύει ότι $m^e = m(mod\ n)$. Επίσης, είναι γνωστό ότι στο RSA το $n = p \cdot q$, με p, q πρώτους. Επομένως, ισχύει ότι $\mathbb{Z}_n \approx \mathbb{Z}_p \times \mathbb{Z}_q$. Συνεπώς, αναζητούνται οι λύσεις της εξίσωσης $x^e - x = 0(mod\ n)$ ή ισοδύναμα, οι λύσεις των εξισώσεων:

$$x_1^e - x_1 \equiv 0(mod\ p) \quad (1) \quad \& \quad x_2^e - x_2 \equiv 0(mod\ q) \quad (2)$$

Άρα, αρκεί να μελετηθεί η εξίσωση (2) αφού θα ισχύουν τα ίδια και για την (1).

Οπότε, υπάρχουν οι εξής περιπτώσεις:

- Για $x_1 = 0$ η (1) ικανοποιείται οπότε προκύπτει μια λύση.
- Για $x_1 \neq 0$ η εξίσωση (1) μπορεί να γραφεί ως εξής:
  $$x_1(x_1^e - 1) \equiv 0(mod\ p) \Rightarrow (x_1^e - 1) \equiv 0(mod\ p) \Rightarrow x_1^e \equiv 1(mod\ p)$$
  Κάθε τέτοιο x_1 μπορεί να γραφεί ως $x_1 = g^{y_1}(mod\ p)$, όπου g γεννήτορας της $\mathbb{Z}_p$.
  Άρα, $g^{y_1(e-1)} \equiv 1(mod\ p) \Rightarrow y_1(e-1) \equiv 0(mod\ p-1)$.
  Οπότε, το $y_1 = p-1$ είναι λύση.
  Επιπλέον, τα:
  $$y_1, y_1 + \frac{p-1}{gcd(e-1, p-1)}, y_1 + \frac{2(p-1)}{gcd(e-1, p-1)}, \dots, y_1 + \frac{(gcd(e-1, p-1)-1)(p-1)}{gcd(e-1, p-1)}$$
  είναι επίσης λύσεις.
  Συνολικά υπάρχουν $gcd(e-1, p-1)$ λύσεις.

Τελικά, προκύπτουν $gcd(e-1, p-1)+1$ λύσεις στο $\mathbb{Z}_p$ και $gcd(e-1, q-1)+1$ λύσεις στο $\mathbb{Z}_q$.

Οπότε, συνδυάζοντας τις λύσεις με το CRT προκύπτει ότι υπάρχουν $[\gcd(p-1, e-1)+1] \cdot [\gcd(q-1, e-1)+1]$ λύσεις στο $\mathbb{Z}_n$.

7η Άσκηση

Έστω πρώτος $p = 4^m + 1, m \in \mathbb{Z}$. *Διατυπώστε αποδοτικό αλγόριθμο για την εύρεση διακριτού λογαρίθμου στην ομάδα* $\mathbb{Z}_p^*$.

Λύση:

Έστω πρώτος $p = 4^m + 1, m \in \mathbb{Z}$.

Ο p θα είναι πρώτος μόνο αν ισχύει ότι πρώτος $p = 2^{2m} + 1 = 2^k + 1$ με $k = 2^n$, n ≥ 1 ($k = 2n$).

Τότε, για την ομάδα $\mathbb{Z}_p^*$ ισχύει ότι έχει τάξη 2^n.

Έστω επίσης, γεννήτορας g της ομάδας $\mathbb{Z}_p^*$ και y ένα στοιχείο της ομάδας.

Για την εύρεση του διακριτού λογάριθμου x για τον οποίο θα ισχύει ότι $y = g^x$ ο αλγόριθμος είναι ο εξής:

- Θα πρέπει $x = c_0 \cdot 2^0 + c_1 \cdot 2^1 + \cdots + c_n \cdot 2^n$, αφού $x \in \mathbb{Z}_p^*$.
- Εύρεση του c_0 από τον υπολογισμό του $(g^x)^{2^n-1}$:
  - Αν το x είναι άρτιος, τότε $c_0 = 0$, αφού θα ισχύει $(g^x)^{2^n-1} \equiv 1(mod\ p)$.
  - Αν το x είναι περιττός, τότε $c_0 = 1$.
- Εύρεση του c_1 από τον υπολογισμό του $(g^{x-c_0})^{2^n-1}$
  - Αν το x είναι άρτιος, τότε $c_1 = 0$, αφού θα ισχύει ότι $(g^x)^{2^n-1} \equiv 1(mod\ p)$.
  - Αν το x είναι περιττός, τότε $c_1 = 1$.
- …
- Εύρεση του c_i: …

Τελικά ο αλγόριθμος επαναλαμβάνεται μέχρι τελικά να βρεθεί το x.

8η Άσκηση

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

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

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

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

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

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

Λύση:

1ος Τρόπος Επίλυσης:

Έστω μια υπογραφή (m, a, b) και αναζητείται για ένα m' μια έγκυρη υπογραφή (m', a', b').

Θέτοντας $a' = -\mathcal{H}(m')\ mod\ p - 1$ & $b' = \frac{g^{-\mathcal{H}(m')}}{y} = g^{-\mathcal{H}(m') - x}\ mod\ p$

Τότε, $y \cdot b \equiv g^x \cdot g^{-\mathcal{H}(m')-x} \equiv g^{-\mathcal{H}(m')} \equiv g^a\ mod\ p$. Οπότε αποδείχθηκε η πρώτη σχέση.

Επίσης, $g^{\mathcal{H}(m')} \cdot y \cdot b \equiv g^{\mathcal{H}(m')} \cdot g^x \cdot g^{-\mathcal{H}(m')-x} \equiv g^0 \equiv 1\ (mod\ p)$. Οπότε, αποδείχθηκε και η δεύτερη σχέση. Συνεπώς, με το ίδιο ιδιωτικό κλειδί είναι εφικτό να υπογραφτεί κάθε κείμενο που θα επιλέξει κανείς. Επομένως, το σχήμα δεν προστατεύει από επίθεση καθολικής πλαστογράφησης.

2ος Τρόπος Επίλυσης:

Αφού εξετάζεται η περίπτωση επίθεσης καθολικής πλαστογράφησης, θα πρέπει να ελεγχθεί αν ένας αντίπαλος μπορεί να υπογράψει οποιοδήποτε μήνυμα της επιλογής του.

Έστω m το μήνυμα που θέλει να υπογράψει και έστω ότι επιλέγεται το α και ότι αναζητείται το b που να ικανοποιεί την συνάρτηση επαλήθευσης. Τότε,

$$y \cdot b \equiv g^a (mod\ p) \Rightarrow b \equiv g^a g^{-x}$$

$$g^{\mathcal{H}(m)} \cdot y \cdot b \equiv 1 (mod\ p) \Rightarrow g^{\mathcal{H}(m)} g^x g^a g^{-x} \equiv 1 (mod\ p) \Rightarrow g^{\mathcal{H}(m)} g^a \equiv 1 (mod\ p)$$

Και αν τελικά επιλεχθεί $\alpha = -\mathcal{H}(m)$, τότε επαληθεύεται η υπογραφή χωρίς όμως την κατοχή του x.

Resources:

1. *Διαφάνειες Μαθήματος & Παλαιότερο Υλικό*