Εργασία 2

Κωσταντίνος Σαΐτας - Ζαρκιάς - 2406
Οδυσσεύς Κρυσταλάκος - 2362

27 Μαΐου 2016

Θέμα 1

(i)

Το πρωτόκολλο Diffie - Hellman είναι μια μέθοδος ανταλλαγής κλειδιού που βασίζεται σε μια αμφίδρομη μέθοδο δημιουργίας ενός κλειδιού μεταξύ 2 ατόμων.

Η μέθοδος μπορεί να αναλυθεί στα εξής παρακάτω βήματα:

1 - Εύρεση 2 πρώτων αριθμών p και g από την μία πλευρά και μετάδοση τους στο άλλο άκρο.

2 - Η μια πλευρά επιλέγει έναν μυστικό αριθμό a, υπολογίζει την παράσταση $A = g^a mod p$ και αποστέλλει στην άλλη πλευρά μόνο το αποτέλεσμα A. Αντίστοιχα, η άλλη πλευρά κάνει την ίδια διαδικασία με έναν μυστικό αριθμό b και αποστέλλει το αποτέλεσμα B.

3 - Υπολογισμός της παράστασης $K1 = B^a mod p$ από την μια πλευρά και της παράστασης $K2 = A^b mod p$ από την άλλη.

4 - Παρατηρούμε όμως ότι K1 = K2 καθώς $(g^a mod p)^b mod p = (g^b mod p)^a mod p$ και συνεπώς και οι 2 πλευρές έχουν το κλειδί.

Η μέθοδος αυτή βασίζεται στο πρόβλημα του διακριτού λογάριθμου που είναι υποεκθετικού χρόνου και πολύ δύσκολο στην επίλυσή του αν οι αριθμοί που επιλεχθούν είναι κατάλληλα μεγάλοι.

(ii)

Ένα σύστημα επικοινωνίας στο οποίο δημοσιεύεται ένα δημόσιο κλειδί σε μη-ασφαλή δίαυλο και μέσω αυτού οι 2 πλευρές δημιουργούν ένα κοινό μυστικό κλειδί ονομάζεται κρυπτοσύστημα δημοσίου κλειδιού (ασυμμετρική κρυπτογράφηση) και εφευρέθηκε από τους Diffie και Hellman. Με αυτήν την μέθοδο δεν γίνεται ποτέ ανταλλαγή των ίδιων των μυστικών κλειδιών μέσω του διαύλου επικοινωνίας και συνεπώς δεν υπάρχει ο φόβος υποκλοπής του μυστικού κλειδιού .

(iii)

Μια συνάρτηση f ονομάζεται λτ τραπδοορ φυνςτιον αν είναι εύκολο να υπολογίσουμε το $y = f(x)$ αλλά δύσκολο την $x = f^{-}1(y)$ χωρίς κάποια επιπλέον πληροφορία k. Με απλά λόγια, μια trapdoor function είναι μια είδους συνάρτηση η οποία είναι πολύ εύκολο να υπολογιστεί από την μια φορά αλλά πολύ δύσκολο να υπολογιστεί από την αντίθετη αν δεν υπάρχει καμία επιπλέον πληροφορία.

(iv)

Το πρωτόκολλο ανταλλαγής κλειδιού Diffie - Hellman από μόνο του δεν προσφέρει αυθεντικοποίηση των χρηστών και συνεπώς είναι ευάλωτο σε επιθέσεις Man-In-The-Middle. Μια λύση για το πρόβλημα αυτό είναι η χρήση ψηφιακών πιστοποιητικών (Digital Certificates) τα οποία εξασφαλίζουν στον δέκτη ότι ο πομπός ήταν όντως αυτός που υποστηρίζει ότι είναι μέσω ενός έμπιστου τρίτου προσώπου. Συνεπώς, ο Bob και η Alice χρησιμοποιώντας ο καθένας την δικιά του ψηφιακή υπογραφή μπορούν να εξασφαλίσουν ότι το κλείδι που αντάλλαξαν προήλθε πραγματικά από τους ίδιους χωρίς την εμπλοκή της Eve.

(v)

Η εντροπία κατα Shannon αφόρα την αναμενόμενη τιμή ενός μηνύματος σε ένα σύστημα. Συγκεκριμένα, πόση πληροφορία προσφέρει ένα σύστημα με την έξοδό του αναλόγως την πιθανότητα εύρεσης της αναμενόμενης τιμής των πιθανών μηνυμάτων. Στο παράδειγμα της ρίψης ενός νομίσματος που το αποτέλεσμα είναι 50/50 η πληροφορία που εξάγεται από την έξοδο του συστήματος είναι μικρή, δηλαδή 1 shannon που προκύπτει από τον αριθμό των bits που χρειάζονται για να αναπαραστίσουν τις πιθανές εξόδους του συστήματος όταν η πιθανότητα αποτελέσματος για όλες τις εξόδους είναι ίδια για όλες.

(vi)

Υπάρχουν 4 τύποι επιθέσεων στις ψηφιακές υπογραφές:

- Existential forgery: Ο επιτιθέμενος μπορεί να παράξει υπογραφεί για κάποιο μήνυμα m στο οποίο δεν έχει καμία επιρροή. Αυτό σημαίνει ότι ο επιτηθέμενος δεν διαλέγει το m και το μήνυμα δεν είναι απαραίτητο να έχει κάποιο νόημα.
- Selective forgery: Ο επιτηθέμενος επιλέγει ένα μήνυμα m και στην συνέχεια μπορεί να παράξει υπογραφή για αυτό το συγκεκριμένο m.
- Universal forgery: Ο επιτηθέμενος μπορεί να παράξει ψηφιακή υπογραφή για οποιοδήποτε μήνμυμα m
- Total break: Ο επιτηθέμενος αποκτά πρόσβαση στο ιδιωτικό κλειδί.

(vii)

Με p και q γνωστά μπορούμε να υπολογίσουμε το N και $f(N)$.

$$N = p \cdot q = 463 \cdot 547 = 253261$$

$$\phi(N) = (p-1) \cdot (q-1) = 462 \cdot 546 = 252252$$

επομένως το d υπολογίζεται:

$$ed \equiv 1(\mathrm{mod}\phi(N)) \Leftrightarrow d = 27473$$

Τελικά για την αποκρυπτογράφηση του ς αρκεί να υπολογισθεί

$$c^d(\mathrm{mod}N) = 12584$$

(vii)

Ο λόγος που χρησιμοποιείται μία συνάρτηση κατακερματισμού πριν την υπογραφή του μηνύματος είναι η αποφυγή existential forgergeries. Για παραδειγμα, έστω το δημόσιο κλειδί (y, N). Κάποιος θα μπορούσε να παράξει μία τυχαία υπογραφή, έστω s. Αυτή η υπογραφή αντιστοιχεί στο μήνυμα $m = s^y$ και περνά τον έλεγχο. Επομένως ο επιτηθέμενος κατάφερε να υπογράψει ένα τυχαίο μήνυμα m δηλαδή κατάφερε existential forgery. Για να αποφευχθεί αυτό το πρόβλημα, το μηνύματα περνούν από μία hash H. Έτσι είναι δύσκολο να επιλεχθεί s ώστε $H(m) = s^y$.

(ix)

Έστω ότι έχουμε σύστημα ψηφιακής υπογραφής με τα εξής στοιχεία:
H: Συνάρτηση κατακερματισμού
p: Μεγάλος πρώτος ακέραιος
g: Τυχαίος generator στην κυκλική ομάδα Z_p^*
x: Μυστικό κλειδί $< p$
y: Δημόσιο κλειδί με $y = g^x \mathrm{mod} p$

Έστω πώς η Alice θέλει να υπογράψει ένα μήνυμα m και να το στείλει στον Bob. Κατά τη διαδικασία της υπογραφής, επιλέγεται ένα τυχαίο k έτσι ώστε $1 < k < p-1$. Επίσης υπολογίζονται:

$$r \equiv g^k \pmod{p}$$

$$s \equiv k^{-1}(H(m) - xr) \pmod{p-1}$$

Έτσι στον Bob αποστέλονται τα (m, r, s). Φυσικά αυτά μπορεί να τα λάβει και οποιοσδήποτε άλλος παρακολουθεί το κανάλι επικοινωνίας.

Έστω ότι η Alice χρησιμοποιεί δύο φορές το ίδιο k. Τότε για δύο διαφορετικά μηνύματα m_1 και m_2 ισχύει:

$$s_1 \equiv k^{-1}(H(m_1) - xr) \pmod{p-1}$$

$$s_2 \equiv k^{-1}(H(m_2) - xr) \pmod{p-1}$$

εκ των οποίων προκύπτει:

$$k(s_2 - s_1) = H(m_2) - H(m_1)$$

Από αυτή την εξίσωση μπορούν να βρεθούν μία σειρά από k τα οποία αν αντικατασταθούν στην σχέση:

$$r \equiv g^k \pmod{p}$$

μπορεί να βρεθεί η μοναδική σωστή τιμή του k. Με αντικατάσταση στις παραπάνω σχέσεις, μπορεί να βρεθεί το ιδιωτικό κλειδί.

Τελικά, ο Bob ή οποιοσδήποτε άλλος παρακολουθεί το κανάλι μπορεί να υπογράφει με την υπογραφή της Alice.

(x)

Ισχύει

$$\phi(n) = (p-1)(q-1) = pq - p - q + 1 = pq - (p+q) + 1$$

και επειδή $N = pq$

$$\phi(n) = N - (p+q) + 1$$

Θέμα 2

(i)

Υλοποιώντας και χρησιμοποιώντας τον εκτεταμένο αλγόριθμο του Ευκλείδη για την εύρεση του GCD, βρέθηκε:

$$GCD(126048, 5050) = 202$$

$$-1 \cdot 126048 + 25 \cdot 5050 = 202$$

(ii)

Για τον υπολογισμό του αντίστροφου, υπολογίσθηκαν όλα τα γινόμενα $809 * i$ όπου i παίρνει τιμές από 1 έως 1000. Βρέθηκε πως ο αντίστροφος είναι το 464.

(iii)

Καθώς το 2^{100} είναι δύσκολο να αποθηκευτεί και να χρησιμοποιηθεί σε πράξεις με ακρίβεια, χρησιμοποιήθηκε μία διαφορετική τεχνική. Υπολογίσθηκε το 2 modulo 101 και το αποτέλεσμα πολλαπλασιάστηκε(modulo 101) με το 2. Αυτό έγινε επαναληπτικά 100 φορές και το αποτέλεσμα είναι 464.

(iv)

Ο αλγόριθμος υλοποιήθηκε στο αρχείο fast.py. Τα αποτελέσματα είναι:

$$2^{1234567} \text{mod} 12345 = 8648$$

$$130^{7654321} \text{mod} 567 = 319$$

Θέμα 3

(i)

Ισχύει $ed \equiv 1 \pmod 1$. Δοκιμάζοντας κάθε πιθανό d για $1 < d < \phi(n)$ βρέθηκε $d = 2532979$.

(ii)

Για την εύρεση των p,q γνωρίζουμε δύο σχέσεις:

$$N = pq \tag{1}$$

$$N + 1 - \phi(N) = p + q \tag{2}$$

Για την επίλυση του συστήματος:

$$\frac{(1) \Rightarrow p = N}{q} \tag{3}$$

$$(2),(3) \Rightarrow N + 1 - \phi(N) = \tfrac{N}{q} + q \Rightarrow qN + q - q\phi(N) = N + q^2$$

$$\Rightarrow q^2 - (N + 1 - \phi(N))q + N = 0$$

Λύνοντας την δευτεροβάθμια, προκύπτει ότι το q πάιρνει τις τιμές 1999 και 2003.

Επομένως $p = 1999$ και $q = 2003$ ή το αντίστροφο.

Θέμα 4

Για την επίλυση των παρακάτω γραμμικών ισοδυναμιών εκτελέστηκε η εξής μέθοδος που βασίζεται στο Κινέζικο Θεώρημα Υπολοίπων.

$x = 9(mod17)$ $x = 9(mod12)$ $x = 13(mod19)$

Έστω $m1 = 17, m2 = 12, m3 = 19$ και $n1 = 9, n2 = 9, n3 = 13$.

1. Έλεγχος αν οι μεταβλητές m1,m2,m3 είναι πρώτοι μεταξύ τους χρησιμοποιώντας τον αλγόριθμο του ευκλείδη, δηλαδή να έχουν μέγιστο κοινό διαιρέτη το 1. Εφόσον περάσουν τον έλεγχο υπολογίζεται η λύση του συστήματος με το Κινέζικο Θεώρημα Υπολοίπων.

2. Έστω $M = m1 * m2 * m3$ και $M_i = M/m_i$ για $i = 1, 2, 3$ αντίστοιχα.

3. Υπολογισμός των αντίστροφων στοιχείων u_i των εξισώσεων $u_i * M_i = 1(modm_i)$ με την συνάρτηση modular inverse.

4. Υπολογισμός του $x = \sum_{i=1}^{3} n_i * u_i * M_i$

5. Η απάντηση είναι $xmodM$ και πρέπει να είναι μεταξύ 0 και 1000.

   Συνεπώς, το αποτέλεσμα είναι το 621.

Θέμα 5

Για την αποκρυπτογράφηση του δοσμένου κρυπτογραφημένου μηνύματος με textbook RSA καθώς τα N και e είναι γνωστά έπρεπε πρώτα να βρεθεί το ιδιωτικό κλειδί και ύστερα εύρεση των τιμών ASCII δουλεύοντας block by block στο C.

Για την εύρεση του ιδιωτικού κλειδιού εκτελέστηκαν τα εξής βήματα:

1. Εύρεση των πρώτων παραγόντων p, q του N. Εύρεση του ενός πρώτου παράγοντα με brute force και ύστερα διαίρεση το N με τον αριθμό αυτό για την εύρεση του άλλου παράγοντα.

2. Εύρεση του φ(N) από τον τύπο: $\varphi(N) = (p-1) * (q-1)$

3. Εύρεση του μυστικού κλειδιού d από τον τύπο: $e * d = 1mod\ \varphi(N)$ με την συνάρτηση modular inverse

4. Αποκρυπτογράφηση του κάθε block ξεχωριστά με το d και το N με την συνάρτηση fast και μετατροπή της τιμής ASCII σε γράμμα.

Το αποκρυπτογραφημένο μήνυμα είναι: 'welcowe to real world'

Θέμα 6

(i)

$$\frac{123454}{546542} = 0 + \frac{1}{4 + \frac{52726}{123454}}$$

$$= 0 + \frac{1}{4 + \frac{1}{2 + \frac{18002}{52726}}} = 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{16722}{18002}}}} = 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1280}{16722}}}}}$$

$$= 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{82}{1280}}}}}} = 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{50}{82}}}}}}} = 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{1}{1 + \frac{32}{50}}}}}}}}$$

$$= 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{1}{1 + \frac{1}{1 + \frac{18}{32}}}}}}}}} = 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{1}{1 + \frac{1}{1 + \frac{14}{18}}}}}}}}}$$

$$= 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{4}{14}}}}}}}}}} = 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3 + \frac{2}{4}}}}}}}}}}}$$

$$= 0 + \frac{1}{4 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{13 + \frac{1}{15 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3 + \frac{1}{2 + 0}}}}}}}}}}}$$

(ii)

Εφαρμόστηκε η επίθεση του Wiener όπως περιγράφεται στις σημειώσεις και στον ψευδοκώδικα. Η μόνο αλλαγή που έγινε ήταν η χρήση ακέραιας διαίρεσης κατά την εύρεση του ϕ. Επίσης χρείαστηκε να υλοποιηθούν οι αλγόριθμοι για την εύρεση του συνεχούς κλάσματος. Τελικά, υπολογίσθηκαν δύο πιθανές τιμές για το d οι οποίες είναι 3 και 20881. Καθώς η τιμή 3 δεν οδηγεί σε αριθμούς εντός των ορίων του ASCII, απορρίπτεται. Η τιμή 20881 οδήγησε στο σωστό κείμενο που είναι:

Just because you are a character doesn't mean that you have character

Θέμα 7

Η εύρεση του μηνύματος που κρυπτογραφήθηκε με την εφαρμογή της trapdoor function του Rabin έγινε με την βοήθεια του Κινέζικου Θεωρήματος Υπολοίπων ως αναπαράσταση του προβλήματος σε σύστημα γραμμικών ισοδυναμιών. Καθώς, οι πρώτοι παράγοντες p, q είναι γνωστοί γίνεται να υπολογιστεί η αντίστροφη συνάρτηση $F^{-}1(sk, y)$ για την εύρεση του x.

1. Έστω $p = 5, q = 11, N = p * q, c = 14(= y)$. Από την συνάρτηση

$$F^{-}1(sk, y) : x^2 = y(modN) \Leftrightarrow x^2 = 14(mod55) \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} x^2 = 14(mod5) \Leftrightarrow x = 2 \\ x^2 = 14(mod11) \Leftrightarrow x = 5 \end{cases}$$

   βρέθηκαν τα $x = 2$ και $x = 5$ με την χρήση brute force.

2. Συνεπώς, προκύπτουν τα εξής 4 συστήματα:
   $x = y_p(modp) = 2(mod5)$
   $x = -y_p(modp) = -2(mod5)$
   $x = y_q(modq) = 5(mod11)$
   $x = -y_q(modq) = -5(mod11)$

3. Για την επίλυση των συστημάτων χρησιμοποιήθηκε το CRT με τις αντίστοιχες μεταβλητές: $m1 = p, m2 = q, n1 = 2, n2 = 5, n3 = -2, n4 = -5$ δίνοντας τις εξής 4 λύσεις: [27, 38, 17, 28].

4. Κατα την εκφώνηση, η λύση που είναι μικρότερη του 20 είναι η σωστή, δηλαδή το 17.

Θέμα 8

Από την άσκηση αυτή φαίνεται ο λόγος για τον οποίο όταν χρησιμοποιείται η κρυπτογράφηση του RSA δεν πρέπει να γίνεται ποτέ μόνη της, χωρίς pad, και να μην χρησιμοποιείται ο ίδιος εκθέτης e. Στο συγκεκριμένο παράδειγμα, είναι γνωστό πως το μήνυμα m έχει κρυπτογραφηθεί 3 φορές με τον ίδιο εκθέτη $e = 3$ και τα αντίστοιχα $N[i] = 391, 55, 87$ και $c[i] = 208, 38, 32$. Καθώς, το e είναι γνωστό και επίσης είναι γνωστό ότι και στις 3 εξισώσεις το αποτέλεσμα (m) είναι κοινό αρκεί να λυθεί το εξής σύστημα: $m^3 = c[i] mod N[i], i = 1, 2, 3$, δηλαδή:

$$x = 208 \pmod{391}$$

$$x = 38 \pmod{55}$$

$$x = 32 \pmod{87}$$

Ένα τέτοιο σύστημα, όπως έχει υποθεί και προηγουμένος, λύνεται εύκολα με το Κινέζικο Θεώρημα Υπολοίπων. Συνεπώς, χρησιμοποιώντας την ήδη υλοποιημένη συνάρτηση CRT η λύση του συστήματος είναι $x = 103823$ και καθώς το μήνυμα έχει εκθέτη το 3, η απάντηση είναι η τρίτη ρίζα του x, δηλαδή το 47.

Θέμα 9

(α)

Εφαρμόστηκε το τεστ του Fermat με τις συνθήκες που αναφέρονται στην εκφώνηση. Αυτό που παρατηρείται είναι ότι, κατά προσέγγιση, οι μισοί αριθμοί που παράγονται από την $f(x)$ είναι πρώτοι ενώ οι υπόλοιποι μισοί όχι.

(β)

Τα μόνα πολυώνυμα του Z που, για κάθε ακέραια τιμή, δίνουν πρώτο αριθμό είναι τα σταθερά πολυώνυμα με τιμή κάποιον πρώτο αριθμό.

$$P(x) = p$$

όπου p πρώτος αριθμός

Αντιθέτως, δεν υπάρχει μή σταθερό πολυώνυμο για το οποίο να ισχύει η παραπάνω συνθήκη.

Απόδειξη

Έστω ένα μη σταθερό πολυώνυμο $P(x)$ που μας δίνει πρώτο αριθμό για κάθε τιμή του $x \in Z$

Τότε ισχύει

$$P(1) = p$$

όπου π πρώτος αριθμός.

Επομένως ισχύει και

$$P(1 + np) \equiv 0 \pmod{p}, n \in Z$$

γιατί η παραπάνω τιμή του P διαιρείται με το p. Επομένως, αφού η τιμή του $P(1 + np)$ διαιρείται με το p, δεν είναι πρώτος αριθμός. Άτοπο, άρα η αρχική υπόθεση είναι εσφαλμένη και δεν υπάρχει τέτοιο μη σταθερό πολυώνυμο.

Θέμα 10

(α)

Υλοποιήθηκε ο αλγόριθμος και ο πρώτος που παράγεται αποθηκεύεται στο αρχείο prime.txt.

(β)

Με τη χρήση του αλγορίθμου του Shanks βρέθηκε ότι ισχύουν τα εξής:

$$3^{27} = 2 \pmod{43}$$

$$3^{12} = 4 \pmod{43}$$
$$3^{25} = 5 \pmod{43}$$

Η μέθοδος Pollard-ρ δεν μπόρεσε να δώσει έγκυρο αποτέλεσμα για αυτά τα δεδομένα (καθώς είναι πιθανοκρατικός αλγόριθμος).