Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ, ΜΠ)

2η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 18 Δεκεμβρίου 2023

Άσκηση 1. Έστω Blum integer $n = pq$ και $y \in QR(n)$. Αποδείξτε ότι η κύρια (principal) τετραγωνική ρίζα του $y \pmod n$ (δηλαδή, η ρίζα του y που είναι επίσης τετραγωνικό υπόλοιπο) δίνεται από τον τύπο $x = y^{((p-1)(q-1)+4)/8} \bmod n$.

Άσκηση 2. Θεωρήστε την παραλλαγή του DES-X, με 2 κλειδιά k_1, k_2, όπου η κρυπτογράφηση ενός απλού κειμένου M γίνεται ως εξής :

$$Enc_{k_1,k_2}(M) = E_{k_1}(M \oplus k_2),$$

όπου E η συνάρτηση κρυπτογράφησης του DES.
Έχουμε περισσότερη ασφάλεια από τον κλασσικό DES στο παραπάνω σύστημα; Θεωρήστε ότι ο αντίπαλος έχει δυνατότητα KPA (διαθέτει αρκετά ζεύγη απλού κειμένου - κρυπτοκειμένου).

Άσκηση 3.

1. Ένα DES κλειδί k είναι ασθενές αν DES_k είναι ενέλιξη (involution). Βρείτε 4 ασθενή κλειδιά του DES.

   Παρατήρηση: Για ένα πεπερασμένο σύνολο S, μια 1-1 και επί συνάρτηση $f : S \to S$ είναι ενέλιξη αν $f(f(x)) = x, \forall x \in S$.

2. Ένα DES κλειδί k είναι ημιασθενές αν δεν είναι ασθενές και υπάρχει κλειδί k' ώστε:

   $$\mathsf{DES}_k^{-1} = \mathsf{DES}_{k'}$$

   Βρείτε 4 ημιασθενή κλειδιά DES.

Άσκηση 4. Έστω η κρυπτογράφηση ενός μηνύματος n blocks: $x = x_1||\ldots||x_n$ από ένα κρυπτοσύστημα E σε λειτουργία CBC και $y = y_1||\ldots||y_n$ το αντίστοιχο κρυπτοκείμενο.

1. Δείξτε ότι μπορούμε να εξάγουμε πληροφορία σε περίπτωση σύγκρουσης (δηλ. $y_i = y_j$ για $i \neq j$).
2. Ποια η πιθανότητα σύγκρουσης για block μεγέθους 64 bits;
3. Για ποια τιμή του n η επίθεση είναι χρήσιμη;

Άσκηση 5.

Δίνεται ένα oracle AES_k που μπορεί να δέχεται ως μηνύματα συμβολοσειρές ASCII και να παράγει κρυπτογραφήσεις με βάση το κρυπτοσύστημα AES χρησιμοποιώντας το μυστικό κλειδί k. Πριν την κρυπτογράφηση τοποθετεί σε κάθε μήνυμα μία μυστική συμβολοσειρά ASCII s ως επίθεμα (σαν salt με τη διαφορά ότι η s είναι η πάντοτε η ίδια). Δηλαδή $c = \text{AES}_k(m||s)$.

1. Να περιγράψετε αλγόριθμο με τον οποίο μπορείτε να βρείτε το μέγεθος block που χρησιμοποιεί το oracle.
2. Να περιγράψετε αλγόριθμο με τον οποίο μπορείτε να διαπιστώσετε αν το oracle χρησιμοποιεί ECB mode.
3. Να περιγράψετε αλγόριθμο με τον οποίο μπορείτε να βρείτε την μυστική συμβολοσειρά s που χρησιμοποιεί το oracle. Για τον σκοπό αυτό θεωρήστε ότι έχετε δυνατότητα CPA, δηλαδή ότι μπορείτε να χρησιμοποιήσετε το AES_k για να παράγετε κρυπτογραφήσεις μηνυμάτων της επιλογής σας. Υπόδειξη: εκμεταλλευτείτε το ότι μπορείτε να μάθετε το μέγεθος του block.

Άσκηση 6. Εξετάστε τη γεννήτρια ψευδοτυχαιότητας RC4. Αποδείξτε ότι το δεύτερο byte (κλειδί) εξόδου είναι ίσο με 0 με πιθανότητα περίπου ίση με 2^{-7}. Ξεκινήστε δείχνοντας ότι αν μετά τη φάση δημιουργίας κλειδιών (KSA) ισχύει για την μετάθεση P ότι $P[2] = 0$ και $P[1] \neq 2$ τότε το δεύτερο byte εξόδου είναι ίσο με 0 με πιθανότητα 1.

Άσκηση 7. Έστω $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ ψευδοτυχαία συνάρτηση. Εξετάστε τις παρακάτω συναρτήσεις ως προς την ψευδοτυχαιότητα τους:

1. $F_1(k,x) = F(k,x)||0$
2. $F_2(k,x) = F(k,x) \oplus x$
3. $F_3(k,x) = F(k, x \oplus 1^n)$
4. $F_4(k,x) = F(k,x)||F(k,F(k,x))$

Άσκηση 8. Θεωρήστε την γεννήτρια ψευδοτυχαίων bit BBS με Blum integer $n = pq$.

(α) Να προσδιορίσετε την περίοδο της γεννήτριας σαν συνάρτηση του n και του s_0. 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 prime" έναν safe prime $p = 2p' + 1$ για τον οποίο ισχύει ότι p' είναι επίσης safe prime και $p'' \equiv 1 \pmod 4$, όπου $p'' = (p' - 1)/2$. Ποια είναι η **μέγιστη** περίοδος της γεννήτριας στην περίπτωση που τόσο ο p όσο και ο q είναι "SafeSafe" primes; Να αποδείξετε τον ισχυρισμό σας.

Άσκηση 9. (προγραμματιστική συνέχεια της προηγούμενης άσκησης)
Κατασκευάζοντας Blum integer $n = pq$ με "SafeSafe" primes p, q, 20 δυαδικών ψηφίων ο καθένας, όπως ορίζεται στο ερώτημα (β) της άσκησης 8, θα προσομοιώσουμε την γεννήτρια BBS, διαλέγοντας το s_0 έτσι ώστε αυτή να έχει **μέγιστη** περίοδο.
(α) Γράψτε ένα πρόγραμμα που να κατασκευάζει κατάλληλα την γεννήτρια (δηλαδή να βρίσκει "έξυπνα" κατάλληλο s_0) για συγκεκριμένα p, q που εσείς θα έχετε διαλέξει σύμφωνα με τις παραπάνω συνθήκες.
(β) Επεκτείνετε το παραπάνω πρόγραμμα για να προσομοιώσετε τη γεννήτρια και επαληθεύστε πειραματικά την θεωρητικά υπολογιζόμενη περίοδό της.

Άσκηση 10.

1. Έστω $\mathsf{H} : \{0,1\}^* \to \{0,1\}^n$ μια συνάρτηση σύνοψης, η οποία όταν δεχθεί είσοδο $m = x \oplus w$ δίνει έξοδο $\mathsf{H}(m) = \mathsf{H}(x) \oplus \mathsf{H}(w)$. Να εξετάσετε την H ως προς τη δυσκολία εύρεσης συγκρούσεων.
2. Έστω H μια συνάρτηση σύνοψης $\mathsf{H}(x) = \mathsf{H}_1(x)||\mathsf{H}_2(x)||\mathsf{H}_3(x)$ όπου μόνο μία εκ των $\mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3$ έχει δυσκολία εύρεσης συγκρούσεων. Έχει και η H ως προς τη δυσκολία εύρεσης συγκρούσεων;

Άσκηση 11. Δίνεται μια συνάρτηση σύνοψης $\mathsf{H}_1 : \{0,1\}^{2n} \to \{0,1\}^n$. Η συνάρτηση αυτή χρησιμοποιείται σε κάποιο δένδρο Merkle ύψους h με είσοδο μια δυαδική ακολουθία $x_0 x_1 \dots x_{2^h}$ όπου κάθε x_i είναι μια δυαδική ακολουθία μεγέθους n bits. Με διαδοχικές εφαρμογές της H_1, το δένδρο Merkle μπορεί να θεωρηθεί καθ' αυτό ως μια συνάρτηση σύνοψης H που συμπιέζει συμβολοσειρές μεγέθους $n2^h$ σε συμβολοσειρές μεγέθους n. Να δείξετε ότι αν η H_1 διαθέτει δυσκολία εύρεσης συγκρούσεων τότε και η H διαθέτει δυσκολία εύρεσης συγκρούσεων.

Άσκηση 12.

- Δίνεται ένα κρυπτοσύστημα $\mathcal{CS}$ και αντίπαλος $\mathcal{A}$ που μπορεί να ανακτήσει το κλειδί από κρυπτοκείμενο του $\mathcal{CS}$ με μη-αμελητέα πιθανότητα. Να αποδείξετε ότι το $\mathcal{CS}$ δεν παρέχει ασφάλεια CPA.
- Δίνεται ένα κρυπτοσύστημα $\mathcal{CS}$ το οποίο κρυπτογραφεί όλα τα μηνύματα χρησιμοποιώντας τη λειτουργία CBC. Όμως αντί να επιλέγεται κάθε φορά καινούριο IV, το $\mathcal{CS}$ αυξάνει το προηγούμενο IV κατά 1. Δηλαδή για το i-οστό μήνυμα: $IV_i \leftarrow IV_{i-1} + 1$. Να δείξετε πώς ένας αντίπαλος μπορεί να κερδίσει το παίγνιο CPA για το $\mathcal{CS}$ με μη-αμελητέα πιθανότητα.
- Δείξτε ότι η λειτουργία κρυπτογράφησης OFB δεν παρέχει ασφάλεια CCA.

Σε όλες τις ασκήσεις με "$\oplus$" συμβολίζουμε το XOR και με "||" την παράθεση.

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!