Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)

3η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 30/11/2019

Άσκηση 1. 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 0 με πιθανότητα 1.

Άσκηση 2. Υλοποιήστε την γεννήτρια ψευδοτυχαίων bit BBS κατασκευάζοντας Blum integer $n = pq$ με πρώτους p, q 20 δυαδικών ψηφίων ο καθένας.

(α) Υπολογίστε θεωρητικά και επαληθεύστε πειραματικά την περίοδο της γεννήτριας. Εξηγήστε γιατί πρέπει να είναι μικρό το $\gcd(p-1, q-1)$.

(β) Υλοποιήστε το εξής πείραμα ελέγχου ψευδοτυχαιότητας: θεωρώντας block των 16 bit σαν ζεύγη ακεραίων στο $\{0, \ldots, 255\}^2$, θεωρήστε τους ως σημεία στο επίπεδο, στο τετράγωνο με κορυφές $(0, 0), (255, 255)$. Στη συνέχεια μετρήστε πόσα σημεία βρίσκονται εντός κύκλου με κέντρο το σημείο $(127.5, 127.5)$ και ακτίνα 127.5: ο λόγος αυτών προς το συνολικό πλήθος θα πρέπει να πλησιάζει το $\pi/4$.

(β.i) Αν θεωρήσετε την παραπάνω διαδικασία σαν μέθοδο υπολογισμού του π, πόσα σημεία χρειάζεται να πάρετε για να πετύχετε ακρίβεια 2,3,4 δεκαδικών ψηφίων; Δώστε θεωρητική εκτίμηση (υποθέτοντας ότι η πιθανότητα κάθε bit εξόδου να είναι ίσο με '1' είναι 1/2) και συγκρίνετε με τα πειραματικά αποτελέσματα.

(β.ii)* Συγκρίνετε με την παραλλαγή όπου το bit εξόδου της γεννήτριας είναι η ισοτιμία των δυαδικών ψηφίων των αριθμών x_i $(= x_{i-1}^2 \bmod n)$ αντί για το λιγότερο σημαντικό τους ψηφίο.

(γ)* Ελέγξτε την γεννήτρια (και στις δύο εκδοχές της) με κάποια από τα τεστ που αναφέρονται σε αυτή την δημοσίευση:
`https://pdfs.semanticscholar.org/cf0a/fe558c2638db24a0527a4725fe0ae82cc88b.pdf`
Τι παρατηρείτε;

Άσκηση 3. 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 4. 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 κατακερματισμού 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 5. Έστω $F : \{0,1\}^n \to \{0,1\}^n$ ψευδοτυχαία συνάρτηση. Εξετάστε τις παρακάτω συναρτήσεις ως προς την ψευδοτυχαιότητα τους:

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

Άσκηση 6. Θέλουμε να κατασκευάσουμε μια συνάρτηση σύνοψης από δύο άλλες συναρτήσεις σύνοψης H_1, H_2 για τις οποίες γνωρίζουμε ότι τουλάχιστον η μία είναι ελεύθερη συγκρούσεων. Εξετάστε αν οι παρακάτω συναρτήσεις είναι ελεύθερες συγκρούσεων.

1. $H_3(m) = H_1(m)||H_2(m)$.
2. $H_4(m) = H_1(H_2(m))$.

(*): άσκηση bonus.

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*.