Διαγώνισμα Σεπτεμβρίου | Κρυπτογραφία | Επώνυμο: Όνομα: Α.Μ.:

Οδηγίες : Οι ασκήσεις 1,3 είναι για 3 μονάδες και οι ασκήσεις 2,4 για δύο μονάδες.

Άσκηση 1 Έστω το εξής κρυπτοσύστημα $\langle \mathcal{G}, \mathcal{E}, \mathcal{D} \rangle$: η $\mathcal{G}$ με είσοδο 1^k παράγει το δημόσιο κλειδί $\langle n, e, H(\cdot) \rangle$, όπου n k-bit σύνθετος και το μυστικό κλειδί $\langle d, p, q \rangle$. Ισχύει ότι $e \cdot d = 1 \bmod \phi(n)$, $n = pq$ (όπως στο RSA) καθώς και $H : \mathbb{Z}_n \to \{0,1\}^k$ είναι μια συνάρτηση κατακερματισμού (hash). Η συνάρτηση $\mathcal{E}$ με είσοδο $M \in \{0,1\}^k$ διαλέγει r τυχαίο και επιστρέφει την τιμή $\langle r^e \bmod n, H(r) \oplus [r]_k \oplus M \rangle$ όπου $\oplus$ συμβολίζει την πράξη exclusive-or μεταξύ δυαδικών συμβολοακολουθιών και $[a]_k$ τα k least significant bits του a. Για την απόδειξη, φανταζόμαστε ότι το $H : \mathbb{Z}_n^* \to \{0,1\}^k$ λειτουργεί σαν τυχαίο μαντείο.

(1) Διατυπώστε την υπόθεση RSA και το μοντέλο ασφάλειας IND-CPA.

(2) Περιγράψτε πως πιστεύετε οτι πρέπει να δουλεύει η διαδικασία της αποκρυπτογράφησης $\mathcal{D}$.

(3) Δείξετε ότι το κρυπτοσύστημα ικανοποιεί ασφάλεια τύπου IND-CPA στο μοντέλο τυχαίου μαντείου κάτω από την υπόθεση RSA.

(4) Αν αφαιρούσαμε τον όρο $H(r)$ απο τα κρυπτογραφήματα θα μπορούσε η συνάρτηση κρυπτογράφησης να είναι ασφαλής κατά IND-CPA; αιτιολογήστε την απάντηση σας. (χωρίς να δώσετε πλήρη απόδειξη).

Άσκηση 2 Έχετε ένα κίβδηλο νομίσματα το οποίο επιστρέφει γράμματα με πιθανότητα $p < 1/2$. (1) Δώστε τον τύπο της στατιστικής απόστασης μεταξύ δύο πιθανοτικών κατανομών. (2) Μια ρίψη του νομίσματος τι απόσταση έχει από την ομοίομορφη κατανομή στο $\{0,1\}$; (3) Περιγράψτε έναν αλγόριθμο που τερματίζει πάντοτε και πλησιάζει την ομοιόμορφη κατανομή στο $\{0,1\}$ όσο καλύτερα γίνεται (με τη έννοια της στατιστικής απόστασης). Κατέλάχιστον ο αλγόριθμος σας πρέπει να έχει στατιστική απόσταση το πολύ $1/2 - 2p(1-p)$. Πόσες φορές ο αλγόριθμος σας ρίχνει το νόμισμα; (4) Δείξτε ότι ο αλγόριθμος σας είναι καλύτερος από μια απλή ρίψη του νομίσματος. Σε κάθε περίπτωση δώστε πλήρη αιτολόγηση των απάντησεων σας. Σημείωση: ο αλγόριθμος σας δεν πρέπει να χρησιμοποιεί άλλη πηγή τυχαιότητας πέρα από το νόμισμα.

Άσκηση 3 (1) Να ορίσετε τι είναι ένα πρωτόκολλο μηδενικής γνώσης για μία γλώσσα $\mathcal{L} = \{x \mid \exists w : R(x,w) = 1\}$ (όπου R πολυωνυμικός αλγόριθμος με έξοδο στο $\{0,1\}$) δίνοντας τις τρεις ιδιότητες : πληρότητα (completeness), ορθότητα (soundness), μηδενική γνώση (zero-knowledge). Να δώσετε μόνο τη 'μαθηματική διατύπωση' των ιδιοτήτων - εξηγήσεις 'υψηλού επιπέδου'/περιγραφικές στα Ελληνικά δεν χρειάζονται και θα προσμετρηθούν αρνητικά. Επίσης να εξηγήσετε τι σημαίνει η ιδιότητα μηδενικής γνώσης για τίμιους επαληθευτές (honest verifier zero-knowledge).

(2) Να δείξετε οτι το παρακάτω πρωτόκολλο είναι πρωτόκολλο μηδενικής γνώσης για τίμιους επαληθευτές (και τις 3 ιδιότητες) για την ορθή κατασκευή κρυπτογραφήματος μέσω του συστήματος ElGamal με δημόσιο κλειδί (G, g, m, g, h). Συγκεκριμένα, ο prover έχει σαν είσοδο το $(C, D) = (g^r, h^r M)$ και το r ενώ ο ο verifier έχει σαν είσοδο το $(C, D) = (g^r, h^r M)$ και το M.

1. Ο prover διαλέγει τυχαία ρ από το $\mathbb{Z}_m$ και στέλνει το $G = g^\rho, H = h^\rho$ στον verifier.
2. Ο verifier διαλέγει ένα c τυχαίο από το $\mathbb{Z}_m$ και το στέλνει στον prover.
3. Ο prover στέλνει στον verifier την τιμή t που ορίζεται σαν $t = \rho + cr \bmod m$.
4. Ο verifier ελέγχει αν ισχύει το $g^t = G \cdot C^c$ και αν ισχύει το $h^t = H \cdot (D/M)^c$ και σε αυτήν την περίπτωση επιστρέφει 1 (αλλιώς 0).

Στην επιχειρηματολογία που θα παραθέσετε μπορείτε να υποθέσετε οτι είναι γνωστό το ακόλουθο (που έχουμε δείξει): αν ένας (κακός) prover είναι πειστικός στον verifier με πιθανότητα α τότε με ένα μόνο rewinding επιτυγχάνουμε δύο πειστικές conversations που έχουν διαφορετική δεύτερη κίνηση με πιθανότητα τουλάχιστον $\alpha^2/4 - 2^{-k}$.

Άσκηση 4 Το σύστημα ηλεκτρονικών υπογραφών βασισμένο στο πρωτόκολλο του Schnorr έχει δημόσιο κλειδί $\langle G, g, m, g, h \rangle$, και ιδιωτικό κλειδί $x = \log_g h$. Μια υπογραφή για το M είναι της μορφής $\langle g^t, c = H(M), s = t + cx \rangle$ όπου το t διαλέγεται τυχαία από το $\mathbb{Z}_m$ και το $H(\cdot)$ είναι συνάρτηση hash που θεωρείται σαν τυχαίο μαντείο.

Θεωρείστε το επόμενο πρωτόκολλο τυφλών υπογραφών για τις υπογραφές του Schnorr. Ο χρήστης με είσοδο M διαλέγει το r από το $\mathbb{Z}_m$ τυχαία και στέλνει το $c' = H(M)/r$ στον server. Ο server απαντά με τις τιμές $s = t + c'x = t + cx/r$ για t τυχαίο από το $\mathbb{Z}_m$ και υπολογίζει το $y = g^t$ και στέλνει στον χρήστη τα y, s. Ο χρήστης τελικά επιστρέφει την τιμή $\langle y^r, H(M), rs \rangle$.

Ικανοποιεί το παραπάνω πρωτόκολλο την ιδιότητα της ασφάλειας για τον σερερ ; Δικαιολογήστε πλήρως την απάντηση σας.