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

Οδηγίες : Κάθε θέμα είναι 2.5 βαθμοί.

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 $\langle p, m, g, h, H(\cdot) \rangle$, όπου m k-bit πρώτος και η g είναι υποομάδα τάξης m στο $\mathbb{Z}_p^*$, και το μυστικό κλειδί $\langle p, g, h, x \rangle$ με $h = g^x$. Ισχύει ότι $H : \mathbb{Z}_p^* \to \{0,1\}^k$ είναι μια συνάρτηση κατακερματισμού (hash). Η συνάρτηση $\mathcal{E}$ με είσοδο $M \in \{0,1\}^k$ επιστρέφει την τιμή $\langle g^r, H(h^r) \oplus M \rangle$ όπου $\oplus$ συμβολίζει την πράξη exclusive-or μεταξύ δυαδικών συμβολοακολουθιών. Για την απόδειξη, φανταζόμαστε ότι το $H : \mathbb{Z}_p^* \to \{0,1\}^k$ λειτουργεί σαν τυχαίο μαντείο. (1) Διατυπώστε την υπόθεση DDH 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 DDH.

Άσκηση 2 Έχετε δύο νομίσματα από τα οποία τα ένα είναι κίβδηλο. Το κίβδηλο επιστρέφει γράμματα με πιθανότητα $3/4$ ενώ το άλλο επιστρέφει γράμματα με πιθανότητα $1/2$. Τα νομίσματα είναι αδιαχώριστα 'με το μάτι.' (1) Δώστε τον τύπο της στατιστικής απόστασης μεταξύ δύο πιθανοτικών κατανομών. (2) 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 μικρότερη του $1/4$. Σε κάθε περίπτωση δώστε πλήρη αιτολόγηση της απάντησης σας. Σημείωση: ο αλγόριθμος σας δεν πρέπει να χρησιμοποιεί άλλη πηγή τυχαιότητας πέρα από τα νομίσματα.

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 δεν είναι πρωτόκολλο μηδενικής γνώσης για τίμιους επαληθευτές για το διακριτό λογάριθμο x του h βάσει του g στην υποομάδα $\langle g \rangle$ τάξης m της G.

1. Ο prover διαλέγει τυχαία ρ από το $\mathbb{Z}_m$ και στέλνει το $y = g^\rho$ στον verifier.
2. Ο verifier διαλέγει ένα k bit c τυχαίο από το $\mathbb{Z}_m$ και το στέλνει στον prover.
3. Ο prover στέλνει στον verifier την τιμή t που ορίζεται σαν $t = \rho + (c + x)$.
4. Ο verifier ελέγχει αν ισχύει το $g^t = yg^c h$ και αν ισχύει επιστρέφει 1.

Άσκηση 4 Να διατυπώσετε την ασφάλεια για ηλεκτρονικές υπογραφές (unforgeability against adaptive chosen message attacks). Κατόπιν να διατυπώσετε την υπόθεση RSA. Να ορίσετε τους αλγόριθμους $\langle \mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify} \rangle$ για τις ηλεκτρονικές υπογραφές του συστήματος RSA. Μετά με βάση το τυχαίο μαντείο του τύπου $H : \mathbb{Z}_n^* \to \{0,1\}^k$ να δείξετε ότι ικανοποιήται ο ορισμός της ασφάλειας.