Key Exchange, Diffie–Hellman

1. Δίνεται το παρακάτω σχήμα ανταλλαγής κλειδιού[1]:

   (α΄) Η Αλίκη επιλέγει τυχαία $k, r \leftarrow \{0,1\}^n$ και στέλνει στο Βασίλη την τιμή $s := k \oplus r$.

   (β΄) Ο Βασίλης επιλέγει τυχαίο $t \leftarrow \{0,1\}^n$ και στέλνει στην Αλίκη $u := s \oplus t$.

   (γ΄) Η Αλίκη υπολογίζει την τιμή $w := u \oplus r$ και τη στέλνει στο Βασίλη.

   (δ΄) Η Αλίκη χρησιμοποιεί την τιμή k και ο Βασίλης την τιμή $w \oplus t$.

   Να εξετάσετε το παραπάνω σχήμα ως προς την ορθότητα και την ασφάλεια.

2. Εργαζόμαστε στην υποομάδα του $\mathbb{Z}_{23}$ που παράγεται από το 4.

   (α΄) Επιβεβαιώστε ότι η τάξη q της υποομάδας είναι 11.

   (β΄) Προσομοιώστε μια εκτέλεση του πρωτοκόλου για $a = 3$, $b = 5$.

3. Στον πρώτο υποψήφιο ορισμό ασφαλείας για σχήματα ανταλλαγής κλειδιών, αναφέραμε ότι ένα σχήμα που είναι ασφαλές σύμφωνα με τον ορισμό, μπορεί στην πράξη να αποκαλύπτει όλο το κλειδί εκτός από $\log^2(\lambda)$ bits. Εξηγήστε από που προκύπτει το όριο (κατ'ελάχιστο, εξηγήστε γιατί δεν θα μπορούσαμε να αλλάξουμε το όριο σε $\log \lambda$). **Λύθηκε εν μέρει στην τάξη στις 5/4.**

4. Στη διάλεξη αναφερθήκαμε στο γεγονός ότι δεδομένης μίας ομάδας $\mathbb{G}$ τάξης q, όπου q πρώτος, παραγόμενη από το g, μια μεταβλητή A που ακολουθεί την κατανομή $K := g^{x \cdot y}$ όπου $x, y \leftarrow \mathbb{Z}_q$ και μια μεταβλητή B που ακουλουθεί την κατανομή $U := g^z$ όπου $z \leftarrow \mathbb{Z}_q$ έχουν μικρή στατιστική απόσταση. Επιβεβαιώστε αυτό τον ισχυρισμό. **Λύθηκε στην τάξη στις 12/4.**

5. Κατά τη διαδικασία ανταλλαγής κλειδιού, είναι πιθανό να καταλήξουμε σε ένα κλειδί διαφορετικής μορφής από αυτό που θα θέλαμε να χρησιμοποιήσουμε. Σε ένα παράδειγμα από τις σημειώσεις, η διαδικασία ανταλλαγής κλειδιού μας δίνει ένα τυχαίο στοιχείο του $\mathbb{Z}_q$, ενώ εμείς θα επιθυμούσαμε μια συμβολοσειρά από bits. Διατυπώστε ένα απλό αλγόριθμο για να μετατρέψουμε τον ένα ακέραιο από το 0 ως το $q - 1$ σε μια συμβολοσειρά από bits με το μέγιστο δυνατό[2] μήκος. Κατόπιν υπολογίστε τη στατιστική απόσταση των συμβολοσειρών που παράγονται σε σχέση με την ομοιόμορφη κατανομή για το ίδιο μήκος.

6. Σε συνέχεια της προηγούμενης άσκησης, έστω ότι έχουμε κατασκευάσει μία διαδικασία που παράγει συμβολοσειρές s bits μήκους λ σύμφωνα με μια κατανομή S που είναι δ-κοντά στην ομοιόμορφη στο $\{0,1\}^\lambda$. Να δείξετε ότι για ένα οποιοδήποτε ψηφίο s_i $(0 \leq i < \lambda)$ αυτών των συμβολοσειρών, ισχύει ότι η κατανομή που ακολουθεί το ψηφίο, έστω S_i είναι δ-κοντα στην ομοιόμορφη κατανομή στο $\{0,1\}$;

[1] Άσκηση 9.3 (1η έκδοση)/ 10.4 (2η έκδοση) από το Katz & Lindell

[2] Δεν μας ενδιαφέρει να προσθέσουμε τετριμμένα bits που θα είναι σταθερά 0 ή 1