Α31 ΚΡΥΠΤΟΓΡΑΦΙΑ
Φυλλάδιο ασκήσεων #4

Θεόδουλος Γαρεφαλάκης

15 Απριλίου 2022

1. (α′) Έστω κυκλική ομάδα G τάξης $2q$. Αποδείξτε ότι ακριβώς τα μισά στοιχεία της G είναι τετράγωνα. Συγκεκριμένα, δείξτε ότι η εικόνα του ομομορφισμού $\rho : G \to G$, $\rho(\alpha) = \alpha^2$ έχει τάξη q.

   (β′) Δείξτε ότι $\alpha \in \mathrm{im}(\rho)$ αν και μόνο αν $\alpha^q = 1$.

2. Έστω κυκλική ομάδα G τάξης $2q$ και γεννήτορας $g \in G$. Δείξτε ότι υπάρχει αποτελεσματικός αλγόριθμος ο οποίος μπορεί να διακρίνει τις τριάδες Diffie-Hellman

$$\{(g, g^a, g^b, g^{ab}) : a \overset{R}{\longleftarrow} \mathbb{Z}_{2q}, b \overset{R}{\longleftarrow} \mathbb{Z}_{2q}\}$$

   από τυχαίες τριάδες

$$\{(g, g^a, g^b, g^c) : a \overset{R}{\longleftarrow} \mathbb{Z}_{2q}, b \overset{R}{\longleftarrow} \mathbb{Z}_{2q}, c \overset{R}{\longleftarrow} \mathbb{Z}_{2q}\}$$

   με πιθανότητα $1/2$. Ειδικότερα, κατασκευάστε ένα αποτελεσματικό αντίπαλο για το παιχνίδι 10.6 του Boneh-Shoup, ο οποίος έχει πλεονέκτημα $1/2$.

3. Έστω κυκλική ομάδα G τάξης πρώτου q και γεννήτορας $g \in G$. Ορίζουμε τη «διαγώνια» απεικόνιση Diffie-Hellman

$$D : G \to G, \;\; D(g^t) = g^{t^2}.$$

   Υπενθυμίζουμε ότι η απεικόνιση Diffie-Hellman ορίζεται ως εξής:

$$DH : G \to G, \;\; DH(g^a, g^b) = g^{ab}.$$

   Αποδείξτε ότι ο υπολογισμός της DH ανάγεται στον υπολογισμό της D. Ειδικότερα, δεδομένου αποτελεσματικού αλγορίθμου $\mathcal{D}$ για τον υπολογισμό της D κατασκευάστε ένα αποτελεσματικό αλγόριθμο για τον υπολογισμό της DH.

4. Έστω φυσικός αριθμός n. Η ομάδα $(\mathbb{Z}_n, +)$ είναι κυκλική τάξης n.

   (α′) Δείξτε ότι το $\overline{g} \in \mathbb{Z}_n$ είναι γεννήτορας αν και μόνο αν $(g, n) = 1$.

   (β′) Περιγράψτε ένα αποτελεσματικό αλγόριθμο για υπολογισμό διακριτών λογαρίθμων στην ομάδα $(\mathbb{Z}_n, +)$.

   (γ′) Υπολογίστε το διακριτό λογάριθμο του $y = \overline{2022}$ ως προς τη βάση $g = \overline{1821}$ στην ομάδα $\mathbb{Z}_{12345678901234567891}$.