ΣΕΜΦΕ Θ. Αξιώματα και Κρυπτογραφία Ιανουάριος 2009

1) Αν ΜΚΔ $(m,n)=1$ τότε $m^{\varphi(n)}+n^{\varphi(m)}\equiv 1 \bmod mn$

2) α) Δείξτε ότι $\varphi(3n)=3\varphi(n)$ αν και μόνο αν $3|n$

β) Υπολογίστε το $939^{1344} \bmod 1469$

γ) Δείξτε ότι $18! \equiv -1 \bmod 437$.

Στο β) απαιτείται ένας απλός πολλαπλασιασμός. Στο γ) χρειάζεστε πολλές και διαιρέτες.

3) α) Σχεδιάστε περίπου την ελλειπτική καμπύλη $y^2=x^3+x+3$ επί του $\mathbb{R}$. Η τιμή $x=-1$ τέμνει την καμπύλη; Αν ναι σε πόσα σημεία;

β) Πόσα και ποιά σημεία έχει η ελ. καμπύλη $y^2=x^3+x+3$ επί του $\mathbb{Z}_7$. Κατασκευάστε τον πίνακα πρόσθεσης της ομάδας.
Αν το σημείο $P(4,1)$ ανήκει στην ελ. καμπύλη υπολογίστε γεωμετρικά το $2P$, το $3P$.

4) Θεωρούμε τον αλγόριθμο του Merkle-Hellman του προβλήματος του σακιδίου (knapsack problem) με την υπεραυξανόμενη ακολουθία 2, 3, 6, 13, 27, 52, $N=31$ και μέτρο $m=105$ (modulo)

α) Κρυπτογραφήστε το μήνυμα 011000 110101 101110

β) Αποκρυπτογραφήστε το κρυπτομήνυμα που προέκυψε στο α)

γ) Τι γνωρίζετε για την ασφάλεια της μεθόδου;

5) Δείξτε ότι το σύστημα κρυπτογράφησης ElGamal ισοδυναμεί με επίλυση του προβλήματος Diffie-Hellman (DHP)