1) α) Βρείτε τα σημεία της ελλειπτικής καμπύλης $E: y^2 = x^3 + x + 6$ πάνω στο Z_{11}. Βρείτε τα διηλάσια των σημείων αυτών.

β) Η Alice και ο Bob χρησιμοποιούν το κρυπτοσύστημα Elgamal πάνω στην καμπύλη αυτή. και βάση το σημείο $B = (3,6)$.
Ο Bob επιλέγει σαν ιδιωτικό κλειδί το 7.
Η Alice θέλει να κρυπτογραφήσει το άγνο κείμενο $m = (7,9)$ και επιλέγει σαν ιδιωτικό κλειδί της το $k=3$.
Ποιο θα είναι το κ.κ που θα στείλει στον Bob; Πως θα αποκρυπτογραφήσει ο Bob το κ.κ που θα πάρει;

γ) Συμφέρει από απόψη ταχύτητας την διαδικασία του κρυπτο b με το σύνηθες κρυπτοσύστημα elgamal.
Τι σχέση έχει η διαδικασία του κρυπτο b με το πρόβλημα του διακριτού λογαρίθμου (DLP); 3

2) Έστω ο 3x3 πίνακας $K = \begin{pmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 9 & 11 \end{pmatrix}$

α) κρυπτογραφήστε με το σύστημα Hill το α.κ monica

β) Βρείτε τον αντίστροφο του και αντίστοιχα τον αντίστροφο του. Υπάρχει το αντίστροφο κλειδί; γιατί; 3
αντίστοιχα αποκρυπτογραφήστε το κ.κ. (με τον ίδιο πίνακα-κλειδί K)
BOT

3) α) Δείξτε ότι ο 5ος αριθμός Fermat $F_5 = 2^{2^5} + 1$ είναι σύνθετος
Υπόδειξη: Ξεκινήστε από την σχέση $5 \cdot 2^7 = -1 \bmod 641$ 15

β) Δείξτε ότι $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$ για κάθε φυσικό n
Υποδ. Για $n=1$ $7/49$ για $n=2$ $7/1393$ 15

γ) Υπολογίστε το σύμβολο $\left(\frac{8773}{1373}\right)$ και βάσει αυτού υπολογίστε το $773^{686} \bmod 1373$. Ποιο κριτήριο χρησιμοποιήσατε; 2

Θεωρείτε για σύμβολο Legendre ή Jacobi;
Μπορείτε να τυποποιήσετε την διαδικασία υπολογισμού του $\left(\frac{773}{1373}\right)$ σε μια αλγοριθμική διαδικασία;

GNN