CRYPTO HOMEWORK

1. Quanto dovrebbero essere grandi i numeri primi p e q per poter cifrare con RSA un blocco di 18 bit di plaintext ? Fornire un esempio.

2. Se p=467 e q=479, calcolare la chiave segreta nel sistema RSA, sapendo che la chiave pubblica è e=73443.

3. Dato un 'ElGamal cryptosystem' con modulo q=1283 and g=653, lasciamo che l'utente scelga k=977. Calcolare la chiave pubblica e la versione cifrata del messaggio m=751.

4. E' la funzione identità, che restituisce in output il valore in input, una buona funzione crittografica di checksum? Perchè o perchè no?

5. Un sistema ECC usa una curva ellittica $E_{11}(2,5)$ con punti P le cui coordinate (x,y) soddisfano la congruenza $y^2 = x^3 + 2x+5$ mod11. Dati i punti P=(3,4) e Q=(8,7), trovare i punti P+Q, P+P, e Q+Q.

6. La chiave pubblica RSA di Yolanda è (e=7, n=15). Xavier le spedirà uno di due messaggi, o SELL (rappresentato dall'intero 2) o BUY (rappresentato dall'intero 4), criptati con la sua (di lei) chiave pubblica. Noi osserviamo il testo cifrato 8.
   a. SENZA calcolare la chiave privata, stabilire quale messaggio era stato spedito.
   b. Descrivere succintamente 2 metodi per impedire questo tipo di 'forward search attack'
   c. Adesso calcolare la chiave pubblica di Yolanda e verificare la correttezza della risposta alla parte a)

7. Supponiamo che Alice e Bob abbiano le chiavi pubbliche RSA in un file su un server. Comunicano regolarmente usando messaggi confidenziali autenticati. Eva vuole leggere i messaggi ma non riesce a 'rompere' il sistema e calcolare le chiavi private di Alice e Bob. Riesce comunque ad introdursi nel server ed a modificare il file che contiene le chiavi private di Alice a Bob.
   a) Come dovrebbe Eva modificare il file in modo da poter leggere i messaggi confidenziali tra Alice e Bob, e contraffare i messaggi da ciascuno di loro?
   b) Come potrebbero Alice e/o Bob scoprire l'inganno di Eva sulle loro chiavi?