CRITTOGRAFIA: raccolta di esercizi d'esame (RSA, DH).

Esercizio 1
1. **Spiegare** in cosa consiste il cifrario RSA e **dimostrarne** la correttezza.
2. **Darne un esempio** di applicazione impiegando parametri numerici molto piccoli per cifrare il messaggio costituito dalle due cifre meno significative del proprio numero di matricola.

Esercizio 2
Posto che si scopra un algoritmo polinomiale per calcolare la funzione di Eulero, **spiegare** in termini matematici quale influenza la scoperta avrebbe sul cifrario RSA.

Esercizio 3
Per la costruzione di una coppia di chiavi RSA si sceglie il numero n come prodotto di due primi p e q considerando le seguenti possibilità:
1) $p = \Theta(n^{1/2})$, $q = \Theta(n^{1/2})$. 2) $p = O(n^{1/3})$, $q = O(n^{2/3})$.
3) $p = \Theta(n^{1/3})$, $q = \Theta(n^{1/3})$. 4) $p = O(\log n)$, $q = O(n/\log n)$.
Per ciascuna di queste possibilità **spiegare con precisione** se la scelta è corretta e consigliabile.

Esercizio 4
Si consideri un cifrario RSA con $p = 7$, $q = 11$, $e = 13$.
1. **Determinare** il valore della chiave privata d.
2. Qual è la dimensione dei blocchi per la cifratura?
3. **Cifrare** 100011001010.

Esercizio 5
Si consideri il cifrario RSA con chiave pubblica $n = 55$, $e = 7$.
1. **Cifrare** il messaggio $m = 10$.
2. **Forzare** il cifrario trovando p, q, d.
3. **Decifrare** il crittogramma $c = 35$.

Esercizio 6
Siano x, y, n tre interi positivi arbitrari, con $x < n$, $y < n$. Poniamo che si scopra un algoritmo di algebra modulare di complessità $O(d^2)$ per calcolare, se esiste, il logaritmo discreto di y in base x modulo n, con $d = \Theta(n)$ oppure $d = \Theta(\log n)$.
Spiegare in termini matematici, per i due suddetti valori di d, quale influenza la scoperta avrebbe sull'algoritmo DH (Diffie-Hellman) per lo scambio segreto di chiavi.

Esercizio 7
Si consideri il protocollo basato sull'algoritmo DH con $g = 3$ e $p = 353$, e siano $x = 97$ e $y = 233$.
Calcolare X, Y e la chiave k. [**Sol.** $k[session] = 160$]

Esercizio 8
Due utenti A, B vogliono costruire una chiave segreta di sessione impiegando il protocollo basato sull'algoritmo DH. A tale scopo concordano su una coppia pubblica di interi $<p,g>$, con $p = 11$ (p è piccolo per costruire il nostro esempio), e $g = 6$.

1. **Dimostrare** che la coppia <11,6> è adatta per il protocollo DH.
2. Posto che A e B scelgano come numeri "casuali" segreti x, y la terza e la quarta cifra del numero di matricola del candidato, **creare** la chiave di sessione **indicando i calcoli eseguiti da A e B**.

Esercizio 9
Considerando il cifrario RSA:

1. Discutere se è possibile scegliere un valore pari per il parametro e.
2. Siano e ed e' due valori scelti per la chiave pubblica tali che e' è ottenuto da e cambiando un bit da 0 a 1. Dimostrare che MCD(e, e') = 1.

Esercizio 10
Nonostante il cifrario RSA sia considerato un cifrario sicuro, alcune sue implementazioni possono rendere insicura la cifratura. Si consideri ad esempio la cifratura di un messaggio m di 64 bit con una chiave pubblica RSA $<e, n>$, dove $e = 3$ e n è un numero di 512 bit.

- **Spiegare** perché la cifratura di m è completamente insicura.
- **Decifrare** il crittogramma $c = 33076161$ nel caso in cui $n = 100082119$.

Esercizio 11
Si supponga che Eve intercetti un crittogramma $c = m^e \bmod n$ diretto ad Alice. Si supponga inoltre che Alice sia disposta a decifrare per Eve qualsiasi crittogramma c', a patto che c' sia diverso da c.

Descrivere come Eve possa decifrare m in tempo polinomiale, richiedendo ad Alice la decifrazione del crittogramma $c' = c\, x^e$, dove $x < n$ è un intero casuale, co-primo con n.

Esercizio 12
Alice vuole mandare un messaggio cifrato a Bob usando il cifrario RSA, ma non conosce la sua chiave pubblica. Quindi invia un email a Bob chiedendogli la chiave. Bob risponde inviando $K[pub] = < e, n >$.
Eve <u>intercetta</u> il messaggio, <u>sostituisce</u> e con un nuovo intero e' coprimo con e, e <u>invia</u> la chiave modificata $K'[pub] = < e', n >$ ad Alice.
Alice usa $K'[pub]$ per cifrare il messaggio m, e invia il crittogramma $c' = m^{e'} \bmod n$ a Bob.
Dato che m è stato cifrato con la chiave sbagliata, Bob non può decifrare e quindi rimanda la sua chiave pubblica ad Alice, chiedendole di inviare nuovamente il messaggio cifrato. A questo punto Alice invia il crittogramma corretto $c = m^e \bmod n$.

Mostrare come Eve (che ha spiato lo scambio di messaggi e conosce e, e', c, c') possa risalire al messaggio in chiaro m.

[***Suggerimento***: sfruttare il fatto che e ed e' sono coprimi.]