Parte 2: Valutazione

Lo studente dovrà rispondere ad almeno 3 tra i seguenti quesiti.

Quesito 1. Qual è la differenza fra steganografia e crittografia?

Quesito 2. Qual è il metodo utilizzato per attaccare i sistemi crittografici di Cesare e Vigenère?

Quesito 3. i) Si consideri a^2 con a numero intero. Provare che il resto della divisione per 4 del numero a^2 è 0 oppure 1.

ii) Usare il punto precedente per trovare i possibili resti della divisione per 4 del numero $a^2 + b^2$.

Quesito 4. Dimostrare che per un numero intero $x \in \mathbb{Z}$ vale

$$\begin{cases} x \equiv 1 \text{ mod. } 2 \\ x \equiv 1 \text{ mod. } 3 \\ x \equiv 1 \text{ mod. } 5 \end{cases}$$

se e solo se

$$x \equiv 1 \text{ mod. } 30.$$

Quesito 5. i) Quanto vale la funzione di Eulero $\varphi(p)$ con p numero primo?

ii) Calcolare $\varphi(4)$.

iii) Determinare un numero $x \in \mathbb{N}, x \geq 2$ con $x \neq 4$ tale che $\varphi(x) = \varphi(4)$.

Quesito 6. Sia x un numero reale. Dimostrare che se x^m e x^n sono razionali con $m, n \geq 2$ numeri naturali coprimi (cioè $(m, n) = 1$), allora x è razionale. (Suggerimento: usare l'identità di Bézout).

Quesito 7. Denotiamo con (e, n) la chiave pubblica di un sistema crittografico RSA.

a) Detta f la chiave privata, qual è la relazione algebrica che sussiste tra e e f?

b) Perché è così importante che i due grandi fattori primi p e q di n restino segreti?

Quesito 8. Se si hanno a disposizione due numeri primi molto grandi p e q, e quindi il loro prodotto $n = pq$, si può costituire a partire da essi un sistema crittografico RSA. Ricordiamo brevemente come si procede.

a) Come si può scegliere una chiave pubblica e? E come si determina la chiave privata f ad essa associata? Qual è l'algoritmo che ci consente di determinarle?

b) Qual è la prima trasformazione che subisce una breve stringa di testo prima ancora di essere crittografata? Come si completa, quindi, la sua crittografazione?

c) Se la stringa di testo è molto breve (ad esempio di soli 8 caratteri) possiamo concludere che la sua versione crittografata sarà un numero intero (o una classe resto modulo n da esso rappresentata) analogamente piccolo? Perché?