Parte 2: Valutazione

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

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

Nella steganografia il messaggio non viene alterato, bensì nascosto. Nella crittografia il messaggio viene invece cifrato, cioè se ne rende incomprensibile il significato attraverso una alterazione del messaggio stesso attuata per mezzo di un processo segreto ma reversibile.

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

Principalmente il metodo basato sull'analisi delle frequenze, una volta che sia nota la lingua con la quale è stato scritto il testo originale. Nel caso più complesso di Vigenère appare indispensabile comprendere dapprima quale sia la lunghezza della chiave di cifratura, e questo è possibile attraverso la ricerca delle ripetizioni di sequenze di caratteri, rilevandone la distanza.

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.

Se a è pari, allora è divisibile per 2, e così a^2 è divisibile per 4, cioè a^2 è congruo a 0 modulo 4. Se, al contrario, a è dispari, allora è della forma $a = b+1$ con b intero pari. Così $a^2 = (b+1)^2 = b^2+2b+1$. Ora b^2+2b è divisibile per 4, ed allora a^2 è congruo a 1 modulo 4.

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

Se a e b sono entrambi pari, allora per quanto visto nel punto precedente sia a^2 che b^2 sono congrui a 0 modulo 4, e così pure a^2+b^2 è congruo a 0 modulo 4. Se invece uno dei due è pari e l'altro è dispari, allora il quadrato del primo è congruo a 0 modulo 4 mentre il quadrato del secondo è congruo a 1 modulo 4, ed allora a^2+b^2 è congruo a 1 modulo 4. Infine, se a e b sono entrambi dispari, allora sia a^2 che b^2 sono congrui a 1 modulo 4, e così a^2+b^2 è congruo a 2 modulo 4. I resti possibili sono in definitiva $0, 1$ e 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

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

Il sistema di congruenze afferma esattamente che $x-1$ è divisibile per 2, per 3 e per 5. Essendo $2, 3, 5$ interi a due a due coprimi, ciò equivale e richiedere che $x-1$ è divisibile per il prodotto $2 \cdot 3 \cdot 5$, cioè per 30.

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

Vale $p-1$, poiché ogni classe $\neq \bar{0}$ in $\mathbb{Z}_p$ è invertibile, essendo rappresentata da un intero coprimo con p.

ii) Calcolare $\varphi(4)$.

$\varphi(4) = \varphi(2^2) = 2^2 - 2 = 2$.

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

Ad esempio $x = 3$, poiché $\varphi(3) = 3-1 = 2 = \varphi(4)$.

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).

Per Bézout, esistono numeri interi α e β tali che $1 = \alpha m + \beta n$. Allora $x = x^1 = x^{\alpha m + \beta n} = (x^m)^\alpha \cdot (x^n)^\beta$ dove entrambi i fattori $(x^m)^\alpha$ e $(x^n)^\beta$ sono razionali, essendo x^m e x^n numeri razionali per ipotesi, ed α e β esponenti interi.

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?

La relazione è $ef \equiv 1 \mod \varphi(n)$, cioè $\bar{e}$ e $\bar{f}$ sono classi l'una l'inversa dell'altra in $\mathbb{Z}_{\varphi(n)}$.

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

Perchè la conoscenza di p e q è equivalente alla conoscenza di $\varphi(n) = (p-1)(q-1)$ e, una volta noti sia la chiave pubblica (e, n) che $\varphi(n)$, si ottiene subito la chiave privata f (che rappresenta la classe inversa di e modulo $\varphi(n)$) attraverso l'algoritmo di Euclide esteso applicato alla coppia $(\varphi(n), e)$.

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?

Si deve scegliere un intero e, con $1 < e < \varphi(n)$, che sia coprimo con $\varphi(n)$. Per fare ciò, ci si avvale dell'algoritmo di Euclide esteso il quale, una volta determinato un corretto valore di e, fornisce attraverso l'identità di Bézout la chiave privata f (che rappresenta la classe inversa di e modulo $\varphi(n)$).

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?

Dopo aver individuato l'alfabeto con m simboli utilizzato per scrivere il messaggio, ed aver associato ad ogni simbolo dell'alfabeto il numero intero che rappresenta la corrispondente posizione ordinale, si interpreta la stringa S di testo quale numero intero X, con $0 < X < \varphi(n)$, del quale S rappresenta la scrittura m-aria. Si completa quindi la crittografazione di S considerando la classe resto rappresentata da X^e modulo $\varphi(n)$.

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?

No, non vi è una corrispondenza diretta tra la lunghezza del testo in chiaro S ed il valore del numero intero che ne rappresenta la cifratura, poiché in ogni caso il numero intero X^e ottenuto dal processo descritto al punto precedente sarà, in generale, molto grande, probabilmente maggiore di $\varphi(n)$, e la cifratura finale di S coincide con il resto della divisione di X^e per $\varphi(n)$, il cui valore non dipende più dalla lunghezza di S.