Nome: [redacted]

Fondamenti di Cybersecurity 12-09-2025

Cognome: [redacted]

Matricola: [redacted]

1. Shift Cipher.

$y = e_k(x) = (x+k) \bmod 26$,

$d_k(y) = (y-k) \bmod 26$, $x, y, k \in Z_{26} = \{0, \ldots, 25\}$.

Supponiamo che Eve abbia intercettato il seguente testo cifrato con uno *Shift Cipher* e una *chiave k ignota*, dove $0 \leq k \leq 25$.

Ciphertext = "KYGSKJOIEHKXYKIAXOZE"

a) Calcolare il plaintext del ciphertext di cui sopra (o in altre parole determinare la chiave ***k***) utilizzando il metodo di ***exhaustive key search.***

*Vi ricordo che la chiave **k** che viene utilizzata per cifrare il plaintext, utilizzando uno Shift Cipher, prende valori fra 0 e 25, e quando si utilizza il metodo di exhaustive key search ci si ferma quando si ottiene un testo che ha senso.*

b) Lo Shift cipher è un cifrario sicuro? Giustificare chiaramente la vostra risposta.

c) Lo Shift cipher è un caso speciale di DUE altri cifrari che abbiamo visto a lezione. Quali sono? Giustificare chiaramente e esaustivamente la vostra risposta.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

(10 punti / 30)

2. Modes of operation of the Block ciphers.

Spiegare in modo dettagliato due modi di operazione fra i 3 modi (visti a lezione) che permettono di trasformare/convertire un Block Cipher in uno Stream Cipher. Illustrare le funzioni di Encryption e Decryption con delle figure.

(7 punti / 30)

3. Denial of Service (DoS).

a) Definire in modo dettagliato il DoS.

b) Che cos'è il Distributed Denial of Service (DDoS)?

c) Fornire e spiegare in modo dettagliato e preciso il DoS nel caso del protocollo TCP per una architettura Client-Server durante la fase dello stabilimento della connessione.

(7 punti / 30)

4. Autenticazione/Password.

a) Cosa sono le **Hash chains**?

b) Qual è il problema principale delle Hash chains e come viene risolto questo problema? ***[Rispondere in modo chiaro e dettagliato]***

(6 punti / 30)