Fondamenti di Cybersecurity 10-07-2025

Nome: Cognome: Matricola:

1. Crittoanalisi di un Cifrario Affine ($y = e(x) = ax+b \pmod{26}$, $a, b \in Z_{26}$)

Molte tecniche di crittoanalisi sfruttano le proprietà statistiche della lingua (Inglese in questo esercizio). Diversi autori hanno stimato le frequenze relative delle 26 lettere compilando statistiche da numerosi romanzi, riviste e quotidiani. Le stime nella seguente Tabella sono state ottenute da Beker e Piper. Sulla base di queste probabilità, Beker e Piper suddividono le 26 lettere in cinque gruppi come segue:

TABLE 2.1: Probabilities of occurrence of the 26 letters

letter	probability	letter	probability
A	.082	*N*	.067
B	.015	*O*	.075
C	.028	*P*	.019
D	.043	*Q*	.001
E	.127	*R*	.060
F	.022	*S*	.063
G	.020	*T*	.091
H	.061	*U*	.028
I	.070	*V*	.010
J	.002	*W*	.023
K	.008	*X*	.001
L	.040	*Y*	.020
M	.024	*Z*	.001

1. *E*, having probability about 0.120
2. *T, A, O, I, N, S, H, R*, each having probability between 0.06 and 0.09
3. *D, L*, each having probability around 0.04
4. *C, U, M, W, F, G, Y, P, B*, each having probability between 0.015 and 0.028
5. *V, K, J, X, Q, Z*, each having probability less than 0.01.

Possiamo vedere dalla Tabella (come abbiamo visto anche a lezione) che la lettera **E** è la lettera più frequente, **R** è mediamente frequente e **Z** è pochissimo frequente.

Supponiamo adesso che Oscar abbia intercettato il testo cifrato mostrato nell'esempio seguente:

Ciphertext =

"FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLRHHRH"

In questo ciphertext la lettera A appare 2 volte, la lettera R appare 8 volte, …, e la lettera Z 0 volte. Questo ciphertext è composto solo da 57 caratteri, ma è sufficiente per critto-analizzare un cifrario affine.

1) Determinare la funzione di decifratura ***d(y)***, ovvero determinare i valori di **a** e **b** del Cifrario Affine utilizzando l'analisi statistica della lingua Inglese (vedi tabella sopra). (Suggerimento: $e_K(E)=?$, $e_K(T)=?$, $e_K(?)=A$, …, $e_K(?)=R$). ***Vi ricordo che le scelte di a e b devono essere valide!***

2) Calcolare il plaintext del ciphertext di cui sopra (Ciphertext-only attack).

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

E

(10 punti / 30)

Fondamenti di Cybersecurity 10-07-2025

Nome: Cognome: Matricola:

2. **Perfect Secrecy.**
   a) Definire in modo dettagliato il concetto di Perfect Secrecy (o la Sicurezza Perfetta di Shannon).
   b) Fornire e spiegare in modo dettagliato e preciso il nome di un cipher che gode di questa proprietà.
   c) Dimostrare che questo cipher soddisfa la perfect secrecy.

(7 punti / 30)

3. **RC4.**
   a) Che cos'è RC4?
   b) Come viene generata la keystream di RC4?
   c) La procedura di generazione della keystream è perfetta? Si o No? Giustificare in modo esaustivo la vostra risposta.

(7 punti / 30)

4. **Autenticazione.**
   a) Descrivere in modo chiaro e dettagliato il concetto di autenticazione fornendo degli esempi di metodi per poter autenticarsi ad un sistema informatico in rete.
   b) Il concetto di **Multifactor Authentication** cosa aggiunge al metodo classico di autenticazione dal punto di vista sicurezza? Come devono essere i diversi fattori di autenticazione?

(6 punti / 30)