Fondamenti di Cybersecurity 05-07-2024

Nome: Cognome: Matricola:

1. **Crittoanalisi di un Cifrario Affine ($y=e(x) = ax+b \bmod 26$).**

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.

Supponiamo 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, ...

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

(7 punti / 24)

2. Sia ***n*** un intero positivo. Un **quadrato latino** di ordine *n* è un array ***L*** di n×n degli interi 1, ..., *n*, tale che ognuno degli *n* interi ricorra esattamente una volta in ogni riga e in ogni colonna di *L*. Un esempio di quadrato latino di ordine 3 è come segue:

1	2	3
3	1	2
2	3	1

Nome: Cognome: Matricola:

Dato un qualsiasi quadrato latino L di ordine n, possiamo definire un relativo Crittosistema quadrato latino. Prendiamo $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1, \ldots, n\}$. Per $1 \leq i \leq n$, la regola di crittografia (encryption rule) è definita come $e_i(j) = L(i, j)$ (Quindi ogni riga di L dà origine a una regola di crittografia.)

Domanda: Dimostrare che questo crittosistema quadrato latino raggiunge la *perfect secrecy* a condizione che ogni chiave venga utilizzata con la stessa probabilità. (Suggerimento: Bayes' Theorem)

(5 punti / 24)

3. Che cos'è AES? Fornire lo schema generale di questo cifrario: ad ogni iterazione quali funzioni vengono eseguite? Spiegare brevemente lo scopo di ognuna di queste funzioni.

(4 punti / 24)

4. Descrivere il concetto di anonimizzazione e che cos'è il Routing a Cipolla (Onion Routing); quest'ultimo meccanismo come garantisce l'anonimizzazione del traffico sulla rete?

(4 punti / 24)

5. Unix utilizza un sistema di sicurezza composto da ACL (Access Control List) e Capabilities. Descrivere questi 2 meccanismi e cosa garantiscono assieme.

(4 punti / 24)