Crittografia nel Paese delle Meraviglie

Luigi Russo

(Soluzioni v0.1 - 13 novembre 2020)

Indice

Indice **i**

1 Introduzione **1**

I Crittografia di Base **3**

2 Sicurezza incondizionata **5**

II Protocolli **7**

Capitolo 1

Introduzione

Parte I

Crittografia di Base

Capitolo 2

Sicurezza incondizionata

Esercizio 2.1 In questo caso è possibile usare un attacco a forza bruta e testare, quindi, tutte e 26 le chiavi per scoprire il messaggio originale. Se, però, si osserva che le lettere R, X e N compaiono alla fine di alcune parole, e si ipotizza che esse siano delle vocali nel messaggio originale, il numero di tentativi si restringe ulteriormente. Per k = **17**, si ha la soluzione:

> Combatti solo le guerre che puoi vincere. . . preparati per le guerre che devi combattere — Della guerra, Carl Von Clausewitz

Esercizio 2.2

> L'arte della guerra ci insegna a confidare non soltanto nella probabilità[1] che il nemico non si presenti, ma sulla nostra preparazione a riceverlo; non soltanto sulla possibilità che non attacchi, ma piuttosto sull'avere reso le nostre posizioni imprendibili — L'arte della guerra, Sun Tzu

Esercizio 2.3 Osservando le sequenze di caratteri ripetuti (come PJ e $KAN\,I$) si determina che la chiave ha lunghezza 6. In un secondo momento, si procede l'analisi e si può ricavare che la chiave è **Scozia**, da cui:

> Non essere il primo a provare le cose nuove e tantomeno l'ultimo a mettere da parte quelle vecchie — Antico proverbio scozzese

Esercizio 2.4

[1] le vocali accentate e gli apostrofi sono stati aggiunti per completezza.

.1 A deve essere una matrice quadrata invertibile: quindi $A \in Z_4^{2\times 2}$ e $\det(A) \neq 0$.

.2 Si divide il messaggio in 6 blocchi m_i da 2 elementi e si applica il prodotto $c_i = A^T \cdot m_i (\bmod 4)$ da cui $c = (c_1, \ldots, c_6) = (013301303301)^T$. Per ottenere m da c si calcolano i blocchi $m_i = (A^{-1})^T \cdot c_i (\bmod 4)$, da cui $m = (m_1, \ldots, m_6) = (100110110110)^T$.

Parte II

Protocolli