Elementi di Crittografia
Esercitazione
9 giugno 2011

1. In un cifrario di Vigenère, il PT `pippo` viene cifrato nel CT `PTXRS`. Determinare la chiave.
2. Determinare il cifrario affine tale che
   - `ciao` $\to$ `SWIA`.
   - `ciao` $\to$ `GIOK`.
   - `ciao` $\to$ `AYSW`.
3. Determinare il registro a scorrimento lineare (oppure la ricorrenza lineare) sapendo che il numero di stati è 4 e
   - il PT 00110100 dà luogo al CT 10101111;
   - il PT 00110100 dà luogo al CT 10100101.
4. Determinare il cifrario di Hill tale che `dbgd` $\to$ `LGBR` e la lunghezza di un blocco è 2.
5. La chiave RSA di Alice è $N = 7 \cdot 11$ con $e = 17$ esponente pubblico di cifratura.
   - Determinare l'esponente privato di decifratura d.
   - Cifrare il messaggio 3 da inviare a Alice.
   - Alice deve firmare il messaggio 4. Determinare la coppia (messaggio, firma).
6. Bob sceglie $p = 13, g = 2$ e esponente privato $a = 5$. Cifrare con il crittosistema di Elgmal il messaggio $x = 6$. Decifrare il CT così ottenuto.

(a) Descrivere un cifrario a sostituzione. Trattare brevemente la sua crittoanalisi. Dare un esempio di sostituzione involutoria, in cui cioè la stessa chiave è usata per cifrare e per decifrare.

(b) Trattare brevemente un crittosistema a blocchi a scelta fra DES e AES.

(c) Trattare il problema del logaritmo discreto, discutendo brevemente le applicazioni in crittografia.

(d) Dare la definizione e un esempio di crittosistema a segretezza perfetta.

(e) Dare la definizione di numero pseudoprimo. Mostrare che il numero 15 è uno pseudoprimo in base 4.

(f) Sia (N, e) la chiave pubblica RSA di Alice. Spiegare perché se Eve riesce a fattorizzare N, allora può decifrare i messaggi per Alice.

(g) Descrivere il cifrario di Vigenère, accennando alle sue debolezze.

(h) Cosa è un attacco ciphertext only? Cos'è un attacco known plaintext?

Soluzioni

1. alice
2.
   - $y = 5x + 8$
   - $y = 9x + 14$
   - $y = 17x + 18$
3.
   - $z_{i+4} = z_{i+3} + z_{i+2}$
   - $z_{i+4} = z_{i+3} + z_i$
4. $K = \begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}$
5.
   - $d = 53$
   - 75
   - 9
6. per $h = 7$, la cifratura è $(11, 3)$