Elementi di Crittografia
Esercitazione
marzo 2012

1. Determinare il cifrario affine tale che `ma` $\rightarrow$ `IC`.

2. Determinare il registro a scorrimento lineare (oppure la ricorrenza lineare) sapendo che il numero di stati è 5 e il PT 1010111001 dà luogo al CT 1111100100.

3. Sia dato un crittosistema, e supponiamo di poter effettuare 2^{20} cifrature (o decifrature) al secondo. Se la chiave ha 40 bit, quanto tempo ci vuole per un attacco a forza bruta? Cosa succede se invece raddoppiamo la lunghezza della chiave (sempre con 2^{20} cifrature al secondo)?

4. Mostrare che il cifrario additivo è a segretezza perfetta se ogni chiave viene usata con probabilità pari a $\frac{1}{26}$.

5. Determinare il cifrario di Hill tale che `hgcd` $\rightarrow$ `UHRW` e la lunghezza di un blocco è 2.

6. Supponiano di sapere che la cifratura del messaggio "attack at dawn" con un One-Time Pad sia `6c73d5240a948c86981bc294814d` (il testo in chiaro è codificato con l'ASCII a 8-bit e il testo cifrato è scritto in esadecimale). Qual è la cifratura del messaggio "attack at dusk" con un cifrario OTP con la stessa chiave? (*dal corso di Dan Boneh*)