Elementi di Crittografia
Esercitazione

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. Descrivere la cifratura e la decifratura in un round di un generico cifrario di Feistel. Spiegare perché non è necessario che la funzione F sia iniettiva.