Esercizi di crittografia
Foglio 3

1. Costruite un registro a scorrimento lineare di lunghezza 5 avente periodo massimo.

2. La stringa 0000100011 è stata ottenuta da un registro a scorrimento lineare di lunghezza 5. Ricostruite il registro.

3. Trovate una stringa binaria di lunghezza 8 che non può essere stata prodotta da un registro a scorrimento lineare di lunghezza 4.

4. Avete intercettato la stringa

   00001101101110101011111101110100110111100100111100001011000101010101 01

   e avete ragione di credere che sia un messaggio in ASCII a 7 bit, cifrato con un registro a scorrimento lineare a 7 bit, e che le prime due lettere del messaggio in chiaro siano `SU`. Decrittate il messaggio.

5. La chiave pubblica RSA di Bob è $(8633, 151)$:

   (a) cifrate il messaggio 5000 da trasmettere a Bob;

   (b) fattorizzate 8633;

   (c) trovate la chiave privata di Bob;

   (d) decifrate il messaggio 8119 che è stato inviato a Bob.