CRITTOGRAFIA 2020/21 – Appello del 30 gennaio 2021

Esercizio 1 – Cifrari storici

Sia c la cifra decimale di valore maggiore nel proprio numero di matricola, e sia $k = 25 + c$.
Si consideri un cifrario affine in cui si lavora modulo k, e si determini il numero di chiavi possibili. Si scelga infine una chiave e si cifri il proprio cognome.

Esercizio 2 – Scambio di chiavi

L'algoritmo DH per lo scambio pubblico di chiavi è basato sull'uso di un primo p e di un *generatore* g di Z_p^*. Scelti $\boldsymbol{p = 13}$ e $\boldsymbol{g = 2}$:

1. **Verificare** che 2 è un generatore di Z_{13}^*;
2. Presi i due interi *x, y (corrispondenti alle due cifre meno significative* ***e*** *maggiori o uguali a 2 del proprio numero di matricola)* come scelte casuali di due partner che devono costruire una chiave comune, **indicare** come procede l'algoritmo per questi due valori e quale chiave si costruisce.

Esercizio 3 – RSA

Sia M il proprio numero di matricola, e sia M' il numero composto dalla prima e dall'ultima cifra di M. Siano quindi p il più piccolo numero primo maggiore di M', e q il numero primo successivo a p. **Costruire** i parametri di un cifrario RSA impiegando p e q scelti sopra. Impiegare l'algoritmo di Euclide Esteso per il calcolo della chiave segreta indicando i calcoli eseguiti.

Esercizio 4 – Protocollo BB84

Dare un esempio di applicazione del protocollo BB84 **(in presenza** di crittoanalista sul canale):

- si usi la sequenza di 18 bit ottenuta trasformando in binario ogni cifra decimale del proprio numero di matricola, e prendendo per ciascuna di esse i tre bit meno significativi
- si scelgano a caso le basi per imporre e per misurare la polarizzazione dei fotoni
- si utilizzino 4 bit per effettuare il controllo delle intercettazioni.