

## CRITTOGRAFIA: raccolta di esercizi (cifrari storici).

### Esercizio 1

**Decifrare** i seguenti crittogrammi (di messaggi in lingua inglese):

1. YMNXCJWHNXJNXJFXD (Cifrario Cesare con chiave  $k \neq 3$ )
2. REXETSIH ONSICESI UCIFTFID REHTLIET (Cifrario a permutazione semplice,  $h = 8$ )

### Esercizio 2

Dato un cifrario affine (mod 26), si fa un attacco di tipo testo in chiaro scelto (*chosen plain-text attack*) usando il testo *hahaha*. Il testo cifrato è *nonono*. Determinare la funzione di cifratura.

### Esercizio 3

Se nei cifrari affini si lavora modulo 27 invece che modulo 26, quante sono le chiavi possibili? E se si lavora modulo 29?

### Esercizio 4

Questo esercizio ha lo scopo di dimostrare che un cifrario affine iterato ha la stessa sicurezza di un cifrario singolo.

Si considerino i due cifrari affini:

$$C_1(x) = (a_1 * x + b_1) \text{ mod } 26,$$

$$C_2(x) = (a_2 * x + b_2) \text{ mod } 26.$$

**Dimostrare** che esiste un cifrario affine  $C_3$  tale che  $C_3(x) = C_2(C_1(x))$ .

### Esercizio 5

Il crittogramma  $c = \text{MBR OJFGA SWNTE CNK QJDIL NURW MBR XHMR}$  è stato ottenuto cifrando il messaggio  $m = \text{THE QUICK BROWN FOX JUMPS OVER THE GATE}$  con un cifrario a sostituzione monoalfabetica completo.

1. Quanta informazione relativa alla chiave si può determinare conoscendo la coppia  $m, c$  ?
2. Quante chiavi differenti potrebbero essere state usate per cifrare il messaggio  $m$ ?
3. **Decifrare** il crittogramma MBR TRHLRP WHE HTHV CWND PNEYNE ZNN, che è stato cifrato usando la stessa chiave usata per cifrare  $m$ .

### Esercizio 6

Usando il metodo di Vigenère, **cifrare** il messaggio CRITTOGRAFIA impiegando come chiave le prime 4 lettere del proprio cognome. **Spiegare** inoltre come tale cifrario possa essere attaccato.

Si ricorda che la tabella di Vigenère è la seguente:

A	B	C	...	X	Y	Z
B	C	D	...	Y	Z	A
...	...					...
Z	A	B	...	W	X	Y

### Esercizio 7

Si deve cifrare il messaggio APPELLODIFEBBRAIO impiegando come chiave una permutazione arbitraria e segreta delle 26 lettere dell'alfabeto.

1. **Mostrare** la permutazione scelta e il crittogramma ottenuto.
2. **Calcolare** il numero di prove necessario per condurre un attacco esauriente sulle chiavi.
3. **Discutere** la possibilità di un attacco più efficiente confrontandolo con quello del punto 2.

**Esercizio 8**

Spiegare cosa s'intende per crittoanalisi statistica e come essa possa essere impiegata nell'attacco ai cifrari a sostituzione monoalfabetica e polialfabetica.

**Esercizio 9**

Spiegare cosa s'intende per cifrario (storico) a griglia, indicare come si costruisce una griglia e quante griglie diverse si possono costruire per ogni dimensione scelta.

**Esercizio 10**

Esporre come funziona il cifrario di de Vigenère e descrivere il principale attacco che può essere condotto contro di esso.

**Esercizio 11**

Illustrare il funzionamento del cifrario di Alberti.