Esercizi di crittografia
Foglio 1

1. Decrittare il seguente testo, cifrato col cifrario di Cesare:

SVFOBYZBYLVOWKXYXONOMBSDDKBOWKMKZSBOVKCMBSDDEBKNOVWSDDOXDO.

abcdefghijklmnopqrstuvwxyz
KLMNOPQRSTUVWXYZABCDEFGHIJ

SVFOBYZBYLVOWKXYXONOMBSDDKBOWKMKZSBOVKCMBSDDEBKNOVWSDDOXDO →
ilveroproblemanonedecrittaremacapirelascritturadelmittente

2. Decrittare il seguente testo, cifrato col cifrario di Cesare numerico:

24 25 24 24 5 16 5 17 5 24 9 17 5 24 13 7 5 9 5 22 13 11 19
22 9 25 18 5 9 21 25 5 4 13 19 18 9 13 18 11 22 5 18 8 9 20
9 22 16 9 5 16 24 22 9 23 7 13 9 18 4 9 (18 19 0 5 16 13 23)

t $\longrightarrow$ 24, u $\longrightarrow$ 25 ... a $\longrightarrow$ 5

Tutta la matematica è a rigore una equazione in grande
per le altre scienze (Novalis)

3. Decrittare il seguente messggio cifrato con un cifrario monoalfabetico:

‘‘SF GSJ KZKZ E GJFPJ NSAAJ. CQZTZCHZ 31 GSFSZNTS ZF GEOE ADE, TSUSOS KEN 31 CSJNHS ADE AS OJHJ SH QH GEOE, IZ ...QH GSFSZNTJ ZF CSJNHJ.’’

‘‘SF GSJ KZKZ E GJFPJ KJUENJ. CQZTZCHZ 10000 FSNE ZF GEOE ADE, TSUSOS KEN 31 CSJNHS ADE AS OJHJ SH QH GEOE, IZ ...10000 ZF CSJNHJ. ZF KNSGJ CSJNHJ, KJS MZOPZ.’’ (CSJNCSJ CZMEN)

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ

c ghelmnfop brstu idv    a
```

4. Quanti cifrari affini si possono costruire, avendo un alfabeto di 26 lettere? E avendo un alfabeto di 21, 25 o 27 lettere?

5. Costruire un cifrario affine $[7, 5]$ (con la regola $X = 7x + 5$). Decifrare la parola `PJYXLIID` sapendo che è stato usato un cifrario affine di tipo $[7, b]$ ($X = 7x + b$) e che il testo in chiaro è un nome proprio italiano.

6. È possibile costruire un cifrario moltiplicativo (su di un alfabeto di 26 lettere) che non fissi alcuna lettera? E che ne fissi esattamente una?

7. (Usiamo un alfabeto di 26 lettere.)

- Trovare l'equazione della trasformazione affine tale che

$$\mathtt{e} \longrightarrow \mathtt{Q}, \qquad \mathtt{h} \longrightarrow \mathtt{Z}.$$

- Trovare la trasformazione inversa.