

Esercizi di crittografia
Foglio 1

1. Decrittare il seguente testo, cifrato col cifrario di Cesare:
SVF0BYZBYLVOWKXYXONOMBSDDKBOWKMKZSBOVKCMBSDDEBKNOVWSDDOXD0.
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)
3. Decrittare il seguente messaggio 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 KJUNJ. 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)
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. (a) Trovare l'equazione della trasformazione affine tale che

$$e \rightarrow Q, \quad h \rightarrow Z.$$

- (b) Trovare la trasformazione inversa.

Esercizi di crittografia
Foglio 2

1. Decrittare i seguenti testi, sapendo che è stato usato un cifrario di Vigenère e che le chiavi hanno lunghezza 5.

(a) DLSVH RLTFB LPJVT NPTKQ SAXZT WWOCT WZZKW UPTKW IFGII
FEGJM LEKLV SNWLI RKUEM VTRLD ALRVI UNUDX SRTRB GOGJK
JZYTQ VTLFT YZXVM VLODX WEAF A DUWN AOOMM FEUJC TTYJI
NLRR A GWOKI JTGVA WWBRO YTG DW EAXRK WWOJW DLYZB MLZRA
MWRVK GDZVW UNOUM FEGCQ VTHFZ FPUVQ DNAZV GXKSI KEGMI
AYWLM AEKDX ALYGI JRKIM AWZVZ JZXVI UPTKW DPMYM SWRZV
LZXEW DLHQB SKOFV WOKCT SEOXZ WOKCT SXGCM KTG GW KEGTW
EPGHC AWGJC VTAEI YCGEZ MAKKI YWORB SLVZK UZYL T ELXVI
UTTHC WNKEB GAGJA AOGCT WFRKQ EPIRX SYTVL WWBZT DLMXQ
GOOXQ WSGMM EBAVT DLTFB LPIFV LCUZT KZRZB GPXR

(b) CFRWB HFKIT ARWXB PIKDH
RRVZZ AZMIM TCPZM ILEGB
RFRDY XRQHB UVVDI TIGCX
HZKIH GZUPT CUSGH HZPVL
RZENH AFMGF DEHJF TEXVE
TJMBG DFSJK XESTX PWJVM
IFEQE TXVJX PGTZG PVWJE
DCEQH GREMU XKVVK XRQZG
IVIMB VVRYH PJINM TJWJX
URGZG SFGMX SVVZZ TEIMH
HRQZG IVMIH CFVZW TZQPK