crittoanalisi di un cifrario di Vigenère

Dobbiamo decrittare il testo:

```
DLSVH RLTFB LPJVT NPTKQ SAXZT WXOCT WZZKW UPTKW IFGII
FEGJM LEKLV SNWLI RKUEM VTRLD ALRVI UNUDX SRTRB GOGJK
JZYTQ VTLFT YZXVM VLODX WEAFA ADUWN AOOMM FEUJC TTYJI
NLRRA GWOKI JTGVA WWBRO YTGDW EAXRK WXOJW DLYZB MLZRA
MWRVK GDZVW UNOUM FEGCQ VTHFZ FPUVQ DNAZV GXKSI KEGMI
AYWLM AEKDX ALYGI JRKIM AWZVZ JZXVI UPTKW DPMYM SWRZV
LZXEW DLHZB SKOFV WOKCT SEOXZ WOKCT SXGCM KTGGW KEGTW
EPGHC AWGJC VTAEI YCGEZ MAKKI YWORB SLVZK UZYLT ELXVI
UTTHC WNKEB GAGJA AOGCT WFRKQ EPIRX SYTVL WWBZT DLMXQ
GOOXQ WSGMM EBAVT DLTFB LPIFV LCUZT KZRZB GPXR
```

crittoanalisi di un cifrario di Vigenère – lunghezza della chiave

- il cifrario di Vigenère è facile da decrittare se si conosce la lunghezza della chiave
- metodo di Babbage-Kasiski ($\sim$1860) per determinare m= lunghezza della chiave
- due segmenti identici di testo in chiaro a distanza δ, con $\delta \equiv 0 \pmod{m}$ vengono cifrati nello stesso modo
- nel testo cifrato, si osservano le ripetizioni di stringhe di lunghezza almeno tre e le distanze fra queste ripetizioni
- si ipotizza che la chiave m divida il MCD di queste distanze

cerchiamo le ripetizioni nel testo:

DLSVH RLTFB LPJVT NPTKQ SAXZT WXOCT WZZKW UPTKW IFGII
FEGJM LEKLV SNWLI RKUEM VTRLD ALRVI UNUDX SRTRB GOGJK
JZYTQ VTLFT YZXVM VLODX WEAFA ADUWN AOOMM FEUJC TTYJI
NLRRA GWOKI JTGVA WWBRO YTGDW EAXRK WXOJW DLYZB MLZRA
MWRVK GDZVW UNOUM FEGCQ VTHFZ FPUVQ DNAZV GXKSI KEGMI
AYWLM AEKDX ALYGI JRKIM AWZVZ JZXVI UPTKW DPMYM SWRZV
LZXEW DLHZB SKOFV WOKCT SEOXZ WOKCT SXGCM KTGGW KEGTW
EPGHC AWGJC VTAEI YCGEZ MAKKI YWORB SLVZK UZYLT ELXVI
UTTHC WNKEB GAGJA AOGCT WFRKQ EPIRX SYTVL WWBZT DLMXQ
GOOXQ WSGMM EBAVT DLTFB LPIFV LCUZT KZRZB GPXR

$\delta_1 = 415 = 5 \cdot 83$
$\delta_2 = 10$
$\delta_3 = 220 = 4 \cdot 5 \cdot 11$
la lunghezza della chiave è probabilmente 5

crittoanalisi di un cifrario di Vigenère

Dobbiamo decrittare il testo:

- DLSVH RLTFB LPJVT NPTKQ SAXZT WXOCT WZZKW UPTKW IFGII
  FEGJM LEKLV SNWLI RKUEM VTRLD ALRVI UNUDX SRTRB GOGJK
  JZYTQ VTLFT YZXVM VLODX WEAFA ADUWN AOOMM FEUJC TTYJI
  NLRRA GWOKI JTGVA WWBRO YTGDW EAXRK WXOJW DLYZB MLZRA
  MWRVK GDZVW UNOUM FEGCQ VTHFZ FPUVQ DNAZV GXKSI KEGMI
  AYWLM AEKDX ALYGI JRKIM AWZVZ JZXVI UPTKW DPMYM SWRZV
  LZXEW DLHZB SKOFV WOKCT SEOXZ WOKCT SXGCM KTGGW KEGTW
  EPGHC AWGJC VTAEI YCGEZ MAKKI YWORB SLVZK UZYLT ELXVI
  UTTHC WNKEB GAGJA AOGCT WFRKQ EPIRX SYTVL WWBZT DLMXQ
  GOOXQ WSGMM EBAVT DLTFB LPIFV LCUZT KZRZB GPXR

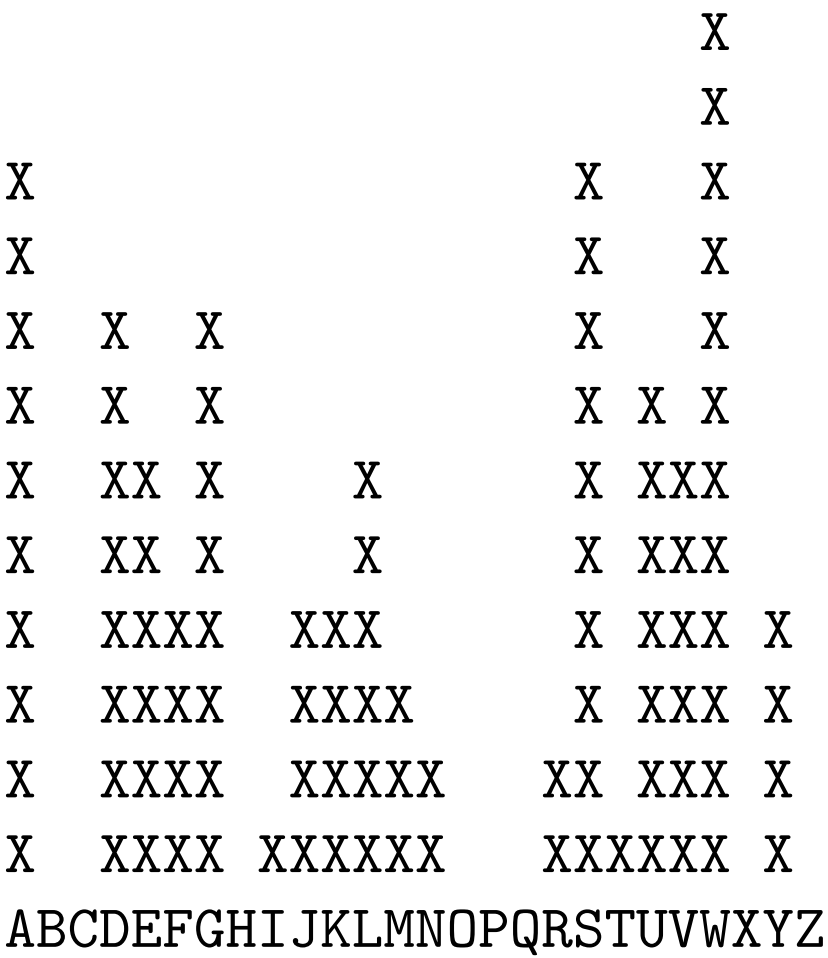
Sappiamo che la chiave ha lunghezza 5.

Le lettere in posizione $1, 1+5, 1+10, \ldots 1+5k$
sono state cifrate con lo stesso cifrario additivo.

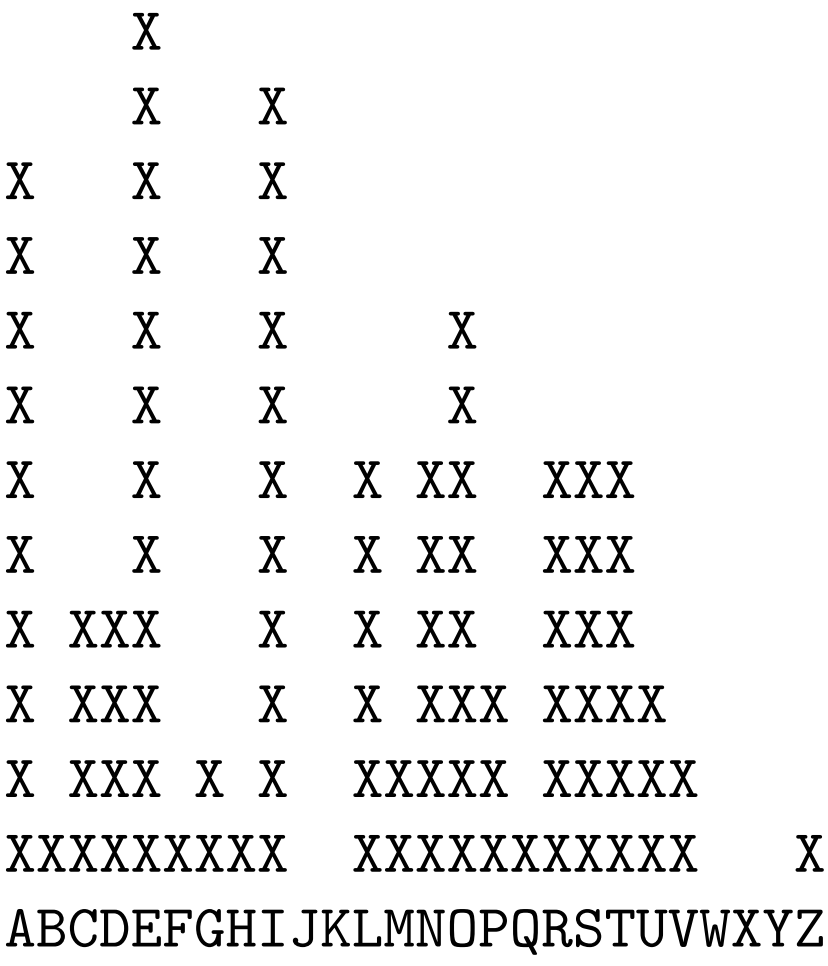
Queste lettere sono:

DRLNSWWUI
FLSRVAUSG
JVYVWAAFT
NGJWYEWDM
MGUFVFDGK
AAAJAJUDS
LDSWSWSKK
EAVYMYSUE
UWGAWESWD
GWEDLLKG

analisi delle frequenze delle lettere di posto $1 + 5k$



frequenze - italiano



analisi delle frequenze delle lettere di posto $1 + 5k$

```
                                X
                                X
X                             X   X
X                             X   X
X   X   X                     X   X
X   X   X                     X X X
X   XX  X     X               X XXX
X   XX  X     X               X XXX
X   XXXX   XXX                X XXX X
X   XXXX   XXXX               X XXX X
X   XXXX   XXXXX            XX XXX X
X   XXXX  XXXXXX            XXXXXX X
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

dunque lo shift è a $\rightarrow$ S

Stesso ragionamento per le lettere di posto $2 + 5k$: le lettere sono:

LLPPAXZPF
EENKTLNRO
ZTZLEDOET
LWTWTAXLM
WDNETPNXE
YELRWZPPW
ZLKOEOXTE
PWTCAWLZL
TNAOFPYWL
OSBLPCZP

analisi delle frequenze delle lettere di posto $2 + 5k$

```
          X
          X
          X   X
    X     X   X   X
    X     X   X   X  X
    X     X   X   X  X  X
    X     X  XX   X  X  X
    X     X XXX   X  X  X
    X     X XXX   X  X  X
X   X     X XXX   X  XX X
X   X     X XXX   X  XX X
X XXXX   XX XXX X X  XXXX
XXXXXX   XXXXXX XXX  XXXX
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

dunque lo shift è a $\rightarrow$ L

Procedendo analogamente per le posizioni $3 + 5k$, $4 + 5k$, $5k$ si trova che il testo in chiaro è:

```
LAMEZ ZANOT TEDEL VENTI APRIL EMILL EOTTO CENTO QUARA
NTASE TTEUN ACQUA ZZONE DILUV IALEA CCOMP AGNAT ODASC
ROSCI DIFOL GOREE DAIMP ETUOS ISOFF IDIVE NTOSU BISSA
VALAS OLITA RIAES ELVAG GIAMO MPRAC EMISO LASIT UATAS
ULLEC OSTEO CCIDE NTALI DIBOR NEOEI LCUIN OMEBA STAVA
INQUE ITEMP IASPA RGERE ILTER ROREA CENTO LEGHE ALLIN
TORNO LABIT AZION EDELL ATIGR EDELL AMALE SIAPO STACO
MEAQU ILASU DIUNA GRANR UPETA GLIAT AAPIC COSUL MAREA
CINQU ECENT OPASS IDALL EULTI MECAP ANNED ELVIL LAGGI
ODIGI EHAVE MQUEL LANOT TECON TROIL SOLIT OERA
```

e la chiave è SLGRI