crittoanalisi di un cifrario a sostituzione

Dobbiamo decrittare il testo

```
QANGH TGMYJ XGHTN AVUNG TTYSH LUXYU OUAUD UQQYJ UJAXX
YNUTY NGKGB BUGMA XASLG KJUGX YQANG HTGMY JXGHT DABBY
VUJAK TYTYT ANGHT JAKTY VUJHS SYOGH TSAOD JUQAD ABBYV
GQGXG SXGVU IHAJJ UQPAV UTMAN TYSUO AXXYT YTAJJ ASXHF
AATAU QGOUT AXXUD ANGQQ ATVAN AUJFH YQYAD ANNUS QGJVG
NAJAS XGTBA TYTSY QYOAG TVGSS AOGUJ FGXXY KJUAQ PAHTL
AJKUY NTYIH ASXYD ABBYV UJAKT YQGDU XYTAJ JGLYX XAKGV
UHTMA QQPUY FGJAK TGOAU JIHGJ AGMAM GTYOA OGSXN GTXYT
UYSAT YTQPA XHXXU JYQPU GOGMG TYOGA SXNYQ UJUAK UGDAN
MUGVA JJGDH TXGVA JSHYT GSYQP AANGS AODNA JHSXN GADGY
TGBBG QYOAH TGQUJ UAKUG OGXHN GGDDA TGOGA SXNYQ UJUAK
UGALL AMUSX YIHAJ DABBY VUJAK TYSUN GJJAK NYXHX XYAVG
```

analisi delle frequenze

frequenze dei caratteri % in italiano

A	B	C	D	**E**	F	G	H	**I**
10,41	0,95	4,28	3,82	**12,62**	0,75	2,01	1,10	**11,62**
J	K	L	M	N	**O**	P	Q	R
0	0	6,61	2,58	6,49	**8,71**	3,20	0,75	6,70
S	T	U	V	W	X	Y	Z	
6,04	6,06	3,04	1,51	0	0	0	0,93	

analisi delle frequenze

frequenze dei caratteri % nel nostro testo

A	B	C	D	E	F	**G**	H	I
13,52	2,41	0	2,78	0	0,74	**11,30**	4,26	0,74
J	K	L	M	N	O	P	Q	R
6,85	2,59	1,11	1,85	4,44	2,96	1,11	4,44	0
S	T	**U**	V	W	X	**Y**	Z	
4,44	7,78	**8,52**	2,78	0	6,48	**8,89**	0	

proviamo A=e

QeNGH TGMYJ XGHTN eVUNG TTYSH LUXYU OUeUD UQQYJ UJeXX
YNUTY NGKGB BUGMe XeSLG KJUGX YQeNG HTGMY JXGHT DeBBY
VUJeK TYTYT eNGHT JeKTY VUJHS SYOGH TSeOD JUQeD eBBYV
GQGXG SXGVU IHeJJ UQPeV UTMeN TYSUO eXXYT YTeJJ eSXHF
eeTeU QGOUT eXXUD eNGQQ eTVeN eUJFH YQYeD eNNUS QGJVG
NeJeS XGTBe TYTSY QYOeG TVGSS eOGUJ FGXXY KJUeQ PeHTL
eJKUY NTYIH eSXYD eBBYV UJeKT YQGDU XYTeJ JGLYX XeKGV
UHTMe QQPUY FGJeK TGOeU JIHGJ eGMeM GTYOe OGSXN GTXYT
UYSeT YTQPe XHXXU JYQPU GOGMG TYOGe SXNYQ UJUeK UGDeN
MUGVe JJGDH TXGVe JSHYT GSYQP eeNGS eODNe JHSXN GeDGY
TGBBG QYOeH TGQUJ UeKUG OGXHN GGDDe TGOGe SXNYQ UJUeK
UGeLL eMUSX YIHeJ DeBBY VUJeK TYSUN GJJeK NYXHX XYeVG

Digrammi frequenti in italiano (nell'ordine):

er, es, on, re, el, en, de, di, si, ti, la, al
Nel nostro testo:

AN (9), YT (9), AJ (6), VU (5).
(le nostre vocali sono probabilmente G, U, Y)

G=a, N=r, ?? Y=o, T=n, U=i ??.

QeraH naMoJ XaHnr eVira nnoSH LiXoi OieiD iQQoJ iJeXX
orino raKaB BiaMe XeSLa KJiaX oQera HnaMo JXaHn DeBBo
ViJeK nonon eraHn JeKno ViJHS SoOaH nSeOD JiQeD eBBoV
aQaXa SXaVi IHeJJ iQPeV inMer noSiO eXXon oneJJ eSXHF
eenei QaOin eXXiD eraQQ enVer eiJFH oQoeD erriS QaJVa
reJeS XanBe nonSo QoOea nVaSS eOaiJ FaXXo KJieQ PeHnL
eJKio rnoIH eSXoD eBBoV iJeKn oQaDi XoneJ JaLoX XeKaV
iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe OaSXr anXon
ioSen onQPe XHXXi JoQPi aOaMa noOae SXroQ iJieK iaDer
MiaVe JJaDH nXaVe JSHon aSoQP eeraS eODre JHSXr aeDao
naBBa QoOeH naQiJ ieKia OaXHr aaDDe naOae SXroQ iJieK
iaeLL eMiSX oIHeJ DeBBo ViJeK noSir aJJeK roXHX XoeVa

```
QeraH naMoJ XaHnr eVira nnoSH LiXoi OieiD iQQoJ iJeXX
orino raKaB BiaMe XeSLa KJiaX oQera HnaMo JXaHn DeBBo
ViJeK nonon eraHn JeKno ViJHS SoOaH nSeOD JiQeD eBBoV
aQaXa SXaVi IHeJJ iQPeV inMer noSiO eXXon oneJJ eSXHF
eenei QaOin eXXiD eraQQ enVer eiJFH oQoeD erriS QaJVa
reJeS XanBe nonSo QoOea nVaSS eOaiJ FaXXo KJieQ PeHnL
eJKio rnoIH eSXoD eBBoV iJeKn oQaDi XoneJ JaLoX XeKaV
iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe OaSXr anXon
ioSen onQPe XHXXi JoQPi aOaMa noOae SXroQ iJieK iaDer
MiaVe JJaDH nXaVe JSHon aSoQP eeraS eODre JHSXr aeDao
naBBa QoOeH naQiJ ieKia OaXHr aaDDe naOae SXroQ iJieK
iaeLL eMiSX oIHeJ DeBBo ViJeK noSir aJJeK roXHX XoeVa
```

X=t

```
QeraH naMoJ taHnr eVira nnoSH Litoi OieiD iQQoJ iJett
orino raKaB BiaMe teSLa KJiat oQera HnaMo JtaHn DeBBo
ViJeK nonon eraHn JeKno ViJHS SoOaH nSeOD JiQeD eBBoV
aQata StaVi IHeJJ iQPeV inMer noSim etton oneJJ eStHF
eenei QaOin ettiD eraQQ enVer eiJFH oQoeD erriS QaJVa
reJeS tanBe nonSo QoOea nVaSS eOaiJ Fatto KJieQ PeHnL
eJKio rnoIH eStoD eBBoV iJeKn oQaDi toneJ JaLot teKaV
iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe maStr anton
ioSen onQPe tHtti JoQPi aOaMa noOae StroQ iJieK iaDer
MiaVe JJaDH ntaVe JSHon aSoQP eeraS eODre JHStr aeDao
naBBa QoOeH naQiJ ieKia OatHr aaDDe naOae StroQ iJieK
iaeLL eMiSt oIHeJ DeBBo ViJeK noSir aJJeK rotHt toeVa



                                  aMeM anoOe OaStr anton
ioSen onQPe tHtti JoQPi aOaMa noOae StroQ iJieK iaDer
```

M=v, S=s, O=m.....

la sostituzione è

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
G	L	Q	V	A	F	K	P	U	-	-	J	O	T	Y	D	I	N	S	X	H	M	-	-	-	B

il testo in chiaro è:

```
cerau navol taunr edira nnosu bitoi mieip iccol ilett
orino ragaz ziave tesba gliat ocera unavo ltaun pezzo
dileg nonon eraun legno dilus somau nsemp licep ezzod
acata stadi quell iched inver nosim etton onell estuf
eenei camin ettip eracc ender eilfu ocoep erris calda
reles tanze nonso comea ndass email fatto gliec heunb
elgio rnoqu estop ezzod ilegn ocapi tonel labot tegad
iunve cchio faleg namei lqual eavev anome mastr anton
iosen onche tutti lochi amava nomae stroc ilieg iaper
viade llapu ntade lsuon asoch eeras empre lustr aepao
nazza comeu nacil iegia matur aappe namae stroc ilieg
iaebb evist oquel pezzo dileg nosir alleg rotut toeda
```

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

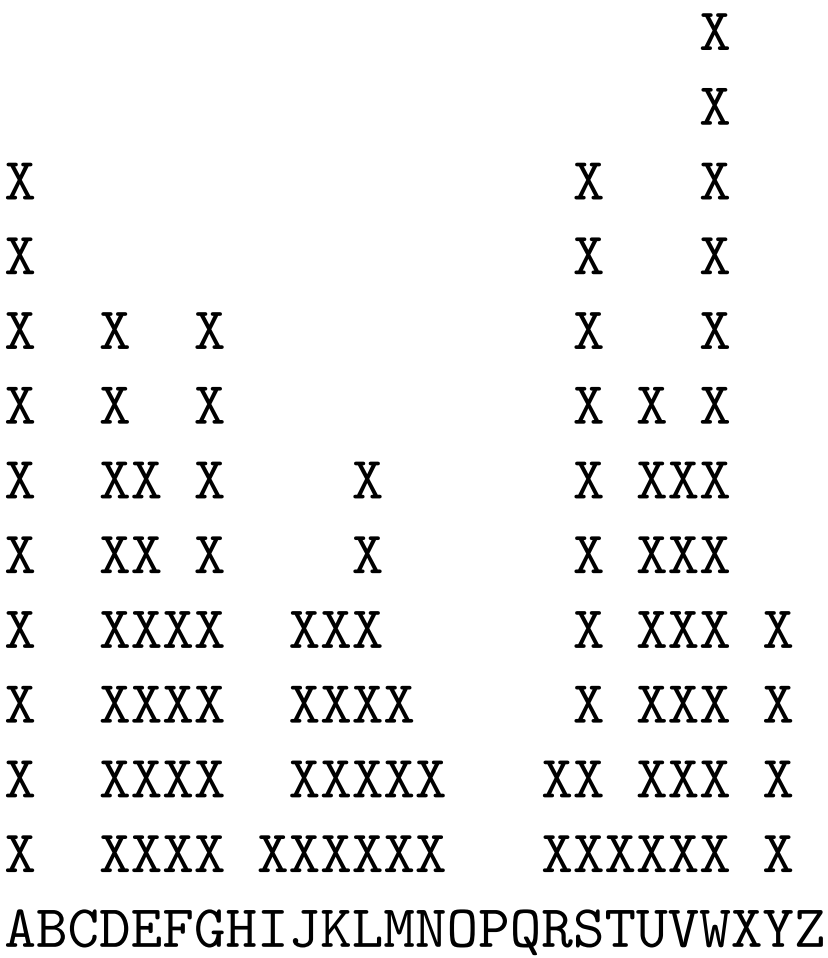
Sappiamo che la chiave ha lunghezza 5.

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

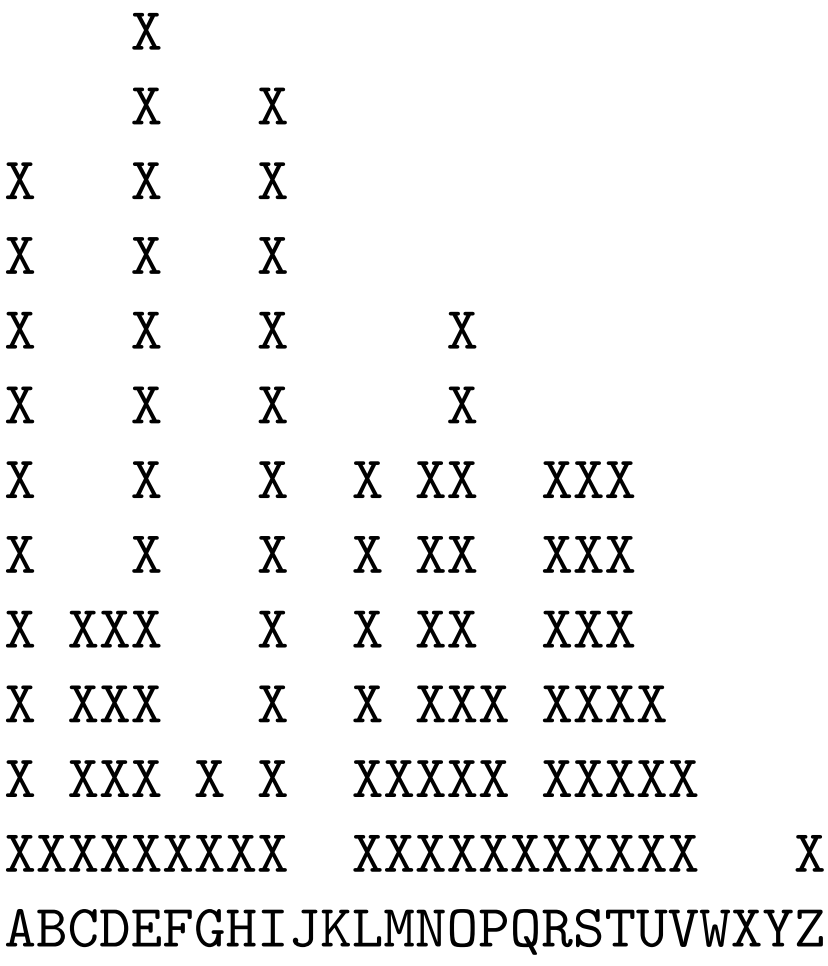
Queste lettere sono:

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

crittoanalisi del cifrario di Hill

- abbastanza resistente a un attacco di tipo ciphertext only
- ma non è difficile da forzare con un attacco known plaintext
- anche qui, bisogna conoscere la lunghezza della chiave m
- e conoscere m coppie
  (testo in chiaro, corrispondente testo cifrato)
- (x_i, y_i) con $e_K(x_i) = y_i$, per $i = 1, \ldots m$

crittoanalisi del cifrario di Hill

- $x_i = \begin{pmatrix} x_{1,i} \\ \vdots \\ x_{m,i} \end{pmatrix} \quad y_i = \begin{pmatrix} y_{1,i} \\ \vdots \\ y_{m,i} \end{pmatrix},$
- quindi bisogna determinare K, la matrice $m \times m$ tale che

$$K \cdot \begin{pmatrix} x_{1,i} \\ \vdots \\ x_{m,i} \end{pmatrix} = \begin{pmatrix} y_{1,i} \\ \vdots \\ y_{m,i} \end{pmatrix}$$

- $K \cdot \begin{pmatrix} x_{1,1} & \cdots & x_{1,m} \\ \vdots & & \vdots \\ x_{m,1} & \cdots & x_{m,m} \end{pmatrix} = \begin{pmatrix} y_{1,1} & \cdots & y_{1,m} \\ \vdots & & \vdots \\ y_{m,1} & \cdots & y_{m,m} \end{pmatrix}$

crittoanalisi del cifrario di Hill

- se $\begin{pmatrix} x_{1,1} & \cdots & x_{1,m} \\ \vdots & & \vdots \\ x_{m,1} & \cdots & x_{m,m} \end{pmatrix}$ è invertibile
- allora $K = \begin{pmatrix} y_{1,1} & \cdots & y_{1,m} \\ \vdots & & \vdots \\ y_{m,1} & \cdots & y_{m,m} \end{pmatrix} \cdot \begin{pmatrix} x_{1,1} & \cdots & x_{1,m} \\ \vdots & & \vdots \\ x_{m,1} & \cdots & x_{m,m} \end{pmatrix}^{-1}$

crittoanalisi del cifrario di Hill - esempio

- supponiamo di sapere che $m = 2$ e che il plaintext `friday` è stato cifrato ottenendo il ciphertext `PQCFKU`
- $e_K \begin{pmatrix} 5 \\ 17 \end{pmatrix} = \begin{pmatrix} 15 \\ 16 \end{pmatrix} \quad e_K \begin{pmatrix} 8 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$
- allora $K = \begin{pmatrix} 15 & 2 \\ 16 & 5 \end{pmatrix} \cdot \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}^{-1}$
- $\det \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} = 9 \quad \text{e} \quad 9^{-1} = 3$
- $\begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}^{-1} = 3 \begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$
- $K = \begin{pmatrix} 15 & 2 \\ 16 & 5 \end{pmatrix} \cdot \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}$

crittoanalisi del cifrario di Hill - esempio

- possiamo verificare che anche ay $\rightarrow$ KU
- $\begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 10 \\ 20 \end{pmatrix}$