

crittoanalisi: principio di Kerckhoffs

L'attaccante, Eve, può conoscere il crittosistema usato da Alice e Bob.

Non conosce la chiave.

Vantaggi:

- è più facile tenere segreta la chiave
 - se la sicurezza si basa sulla chiave, e la chiave viene scoperta, basta cambiare chiave
 - si può usare lo stesso crittosistema per far comunicare diverse coppie di persone
-
- oggi il principio di Kerckhoffs viene inteso in maniera più forte: l'algoritmo deve essere pubblico
 - un sistema che viene molto studiato (e attaccato) è più sicuro
 - meglio che le debolezze, se ci sono, vengano scoperte e rese pubbliche
 - se l'algoritmo è pubblico, non c'è rischio di reverse engineering
 - si possono stabilire standard

crittoanalisi: tipi di attacco

Ciphertext only attack: L'attaccante conosce una stringa y di testo cifrato. Cerca di risalire al testo in chiaro o alla chiave.

Known plaintext attack: L'attaccante conosce una stringa x di testo in chiaro e il corrispondente testo cifrato y . Cerca di risalire alla chiave o di decrittare altri testi cifrati.

Chosen plaintext attack: L'attaccante ha la possibilità di scegliere un testo in chiaro x e di costruire il corrispondente testo cifrato. Cerca di risalire alla chiave o di decrittare altri testi cifrati.

Chosen ciphertext attack: L'attaccante ha la possibilità di scegliere un testo cifrato y e di ottenere il corrispondente testo in chiaro x . Cerca di risalire alla chiave.

crittoanalisi di un cifrario a sostituzione

Dobbiamo decrittare il testo

QANGH TGM YJ 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
GQG XG 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 QYOA H TGQUJ UAKUG OGXHN GGDDA TGOGA SXNYQ UJUAK
UGALL AMUSX YIHAI DABBY VUJAK TYSUN GJJAK NYXHX XYAVG

analisi delle frequenze

frequenze dei caratteri % in italiano

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

analisi delle frequenze

frequenze dei caratteri % nel nostro testo

A 13,52	B 2,41	C 0	D 2,78	E 0	F 0,74	G 11,30	H 4,26	I 0,74
J 6,85	K 2,59	L 1,11	M 1,85	N 4,44	O 2,96	P 1,11	Q 4,44	R 0
S 4,44	T 7,78	U 8,52	V 2,78	W 0	X 6,48	Y 8,89	Z 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](#)
[io](#)Sen 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 So0aH nSe0D JiQeD eBBoV
 aQata StaVi IHeJJ iQPeV inMer noSim etton oneJJ eStHF
 eenei Qa0in ettiD eraQQ enVer eiJFH oQoeD erriS QaJVa
 reJeS tanBe nonSo Qo0ea nVaSS e0aiJ Fatto KJieQ PeHnL
 eJKio rnoIH eStoD eBBoV iJeKn oQaDi toneJ JaLot teKaV
 iHnMe QQPio FaJeK na0ei JIHaJ eaMeM ano0e maStr anton
 ioSen onQPe tHtti JoQPi a0aMa no0ae StroQ iJieK iaDer
 MiaVe JJaDH ntaVe JSHon aSoQP eeraS e0Dre JHStr aeDao
 naBBa Qo0eH naQiJ ieKia 0atHr aaDDe na0ae StroQ iJieK
 iaeLL eMiSt oIHeJ DeBBo ViJeK noSir aJJeK rotHt toeVa

aMeM ano0e 0aStr anton
 ioSen onQPe tHtti JoQPi a0aMa no0ae 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 WWOCT WZZKW UPTKW IFGII
FEGJM LEKLV SNWLI RKUEM VTRLD ALRVI UNUDX SRTRB GOGJK
JZYTQ VTLFT YZXVM VLODX WEAFA ADUWN AOOMM FEUJC TTYJI
NLRRRA GWOKI JTGVA WWBRO YTGDW EAXRK WWOJV 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 (~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 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 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 WEAF A ADUWN AOOMM FEUJC TTYJI
NLRRA 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 DLHZB SKOFV WOKCT SEOXZ WOKCT SXGCM KTGGW 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

Sappiamo che la chiave ha lunghezza 5.

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

Queste lettere sono:

DRLNSWWUI
FLSRVAUSG
JVYVWAAFT
NGJWYEDM
MGUFVFDGK
AAAJAJUDS
LDSWSWSKK
EAVYMYSUE
UWGAWESWD
GWEDLLKG

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

```

frequenze - italiano

```

                                X
                                X  X
X                                X  X
X                                X  X
X  X  X      X
X  X  X      X
X  X  X  X XX  XXX
X  X  X  X XX  XXX
X XXX  X  X XX  XXX
X XXX  X  X XXX XXXX
X XXX X X  XXXXX XXXXX
XXXXXXXXXX XXXXXXXXXXXXX  X
ABCDEFGHIJKLMNOPQRSTUVWXYZ

```

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

```

X
X
X      X      X
X      X      X
X    X    X
X    X    X
X  XX  X      X      XXX
X  XX  X      X      XXX
X   XXXX   XXX      X   XXX  X
X   XXXX   XXXX     X   XXX  X
X   XXXX   XXXXXX  XX   XXX  X
X   XXXX   XXXXXXX  XXXXXXX  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
ZLKOEOTE
PWTCWLZL
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
ABCDEFGHIJKLMN OPQRSTUVWXYZ

```

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
TORNQ LABIT AZION EDELL ATIGR EDELL AMALE SIAPO STACO
MEQU 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 di un cifrario affine

XKLJS UJNXD YBUJT YOBLR GXUJD XKJWL TYXSX
ALYQX LAAJY RGXWX UXNNX KBRGJ LKLVX YQXRG
XRBNX KLUJN XDYLJ SJYQX KYBUX SOBL

la sostituzione è del tipo $e_{a,b}(x) = ax + b = y$:
basta trovare due coppie (x_1, y_1) e (x_2, y_2) tali che
 $ax_1 + b = y_1$ e $ax_2 + b = y_2$ per determinare a, b .

analisi delle frequenze

frequenze dei caratteri % in italiano

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

crittoanalisi di un cifrario affine

Sono 99 caratteri, così distribuiti

A	B	C	D	E	F	G	H	I
3	6	0	3	0	0	4	0	0
J	K	L	M	N	O	P	Q	R
10	6	10	0	5	2	0	3	5
S	T	U	V	W	X	Y	Z	
4	2	6	1	2	18	9	0	

Probabilmente $e \rightarrow X$
quindi $4a + b = 23$.

Proviamo $a \rightarrow J$
allora $a \cdot 0 + b = 9$.

La congruenza $4a \equiv 14 \pmod{26}$
ha due soluzioni: $a = 10$ (che non può essere)
e $a = -3 = 23$.
10 non va bene: $(10, 26) \neq 1$.

Proviamo la sostituzione $y = 23x + 9$. Si ha $23^{-1} = 17$,
quindi $x = 17(y - 9)$.

Decifrando, si ha

erix faqec vufao vhuig befac erani ovexe
ivpei ddavg benef eqqer ugbai riwev pegbe
guqer ifaqe cviix avper vufex hui

Proviamo $a \rightarrow L$

allora $a \cdot 0 + b = 11$.

e $4a + b = 23$.

La congruenza $4a \equiv 12 \pmod{26}$

ha le due soluzioni $a = 3$ e $a = 16$.

16 non va bene: $(16, 26) \neq 1$.

Proviamo la sostituzione $y = 3x + 11$. Si ha $3^{-1} = 9$, quindi $x = 9(y - 11)$.

Decifrando, si ha

erail diseg nodiu nboac hedig eriva unele
fante affin cheve desse rochi arame ntech
ecose radis egnai linte rnode lboa

crittoanalisi del cifrario di Hill

- 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 $i = 1, \dots, m$

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

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

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

crittoanalisi del cifrario di Hill

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

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
- $\begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 10 \\ 20 \end{pmatrix}$