Crittografia simmetrica: Tecniche classiche

1

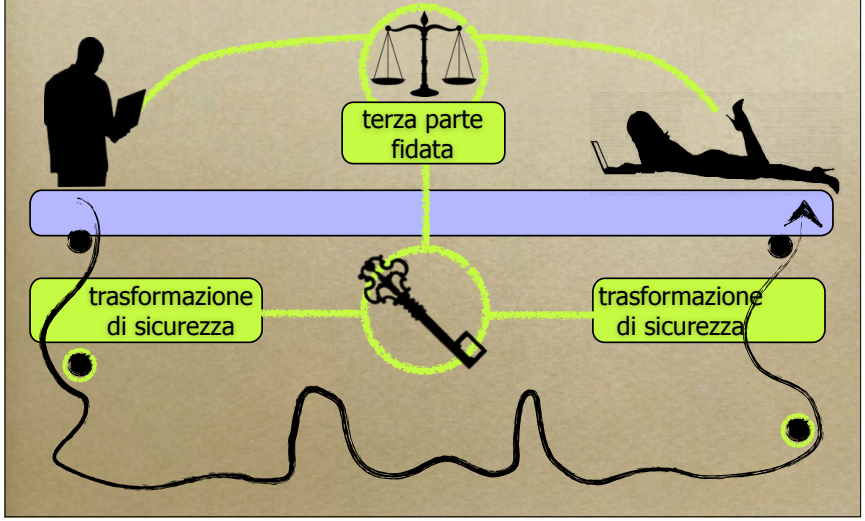
Problema

FURTO DI INFORMAZIONI

- una spia intercetta un messaggio e ne **scopre** il contenuto riservato

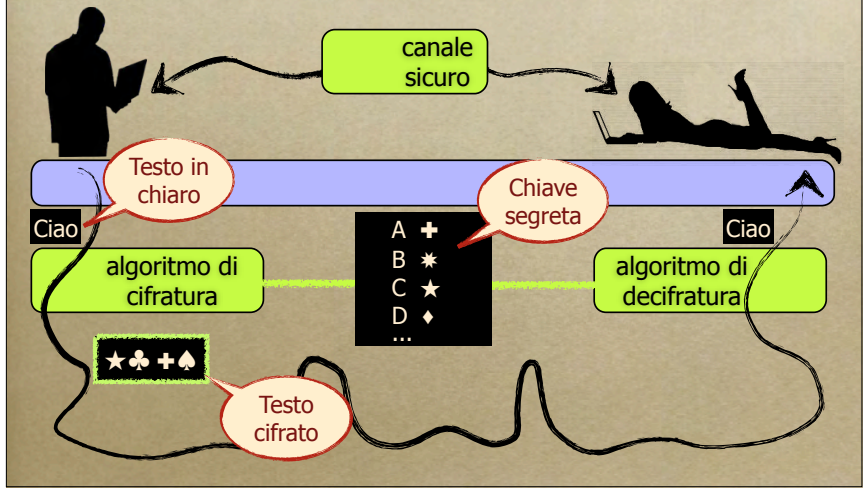
2

Modello generico



3

Crittografia Simmetrica



4

Cifratura monoalfabetica

- Definisco l'alfabeto **A** di partenza
  - è l'alfabeto in cui è scritto il messaggio in chiaro
- Scelgo un alfabeto **A'** di trasformazione
  - è l'alfabeto in cui sarà scritto il messaggio cifrato
  - deve valere **|A|=|A'|**
- Determino una mappatura dei caratteri μ:**A**→**A'**
  - condizione: deve essere invertibile (biunivoca)
  - immediata l'estensione alle stringhe:
    - $\mu(t^0t^1\ldots t^n)=\mu(t^0)\mu(t^1)\ldots\mu(t^n)$
- Quindi dato un messaggio in chiaro M:
  - cifratura: C = μ(M)
  - decfiratura: M = μ^{-1}(C)

Cifratura monoalfabetica

- Facciamo alcune assunzioni che semplificano:
  - l'alfabeto **A** è l'alfabeto dei 26 caratteri della lingua inglese (si può usare anche per l'italiano, avendo cura di togliere gli accenti)
  - scelgo **A'** = **A**
  - quindi μ è una permutazione
- Come si fa per punteggiatura/spazi?
  - nella cifratura vera si rimuovono entrambi (chi decifra il messaggio legalmente dovrebbe comunque essere in grado di comprendere il senso del messaggio)
  - per fare esercizi di analisi crittografica si può decidere di lasciare gli spazi (un po' più facile) o anche la punteggiatura (ancora più facile)

Cifratura monoalfabetica

A ciascun carattere ne viene associato un altro in modo arbitrario (però in modo che due caratteri diversi vengano trasformati in modo diverso, se no è impossibile effettuare il procedimento inverso!)

La colonna di destra (**P**) è una **permutazione** della colonna di sinistra (**X**) e rappresenta μ

Per un alfabeto di 26 caratteri ci sono $26! \simeq 4\times10^{26}$ possibili μ

X	P
a	l
b	u
c	c
d	o
e	z
f	b
g	y
h	m
i	r
j	p
k	a
l	k
m	x

X	P
n	e
o	s
p	h
q	z
r	w
s	i
t	d
u	t
v	j
w	f
x	q
y	n
z	g

Cifratura monoalfabetica

Esempio

il mastino dei baskerville
custodisce il segreto

rk xlidres ozr uliazwjrkkz
ctidsoricz rk izywzds

X	P
a	l
b	u
c	c
d	o
e	z
f	b
g	y
h	m
i	r
j	p
k	a
l	k
m	x

X	P
n	e
o	s
p	h
q	z
r	w
s	i
t	d
u	t
v	j
w	f
x	q
y	n
z	g

Determinare μ

- I due partner che desiderano comunicare devono condividere μ
  - non è facile da ricordare o da comunicarsi a parole
  - più semplice generarla a partire da un codice segreto condiviso
- Vediamo tre modi:
  - con parola chiave
  - con generatore di numeri pseudocasuali
  - con sistema di Cesare (caso particolare)

Con parola chiave

- la sequenza iniziale di lettere è fornita da una parola chiave (sufficientemente lunga e da cui scarto le lettere duplicate) scambiata fra mittente e destinatario
- le lettere successive seguono in ordine alfabetico a partire dall'ultima

c	y
a	z
b	i
c	a
d	v
e	o
f	l
g	p
h	e
i	f
j	g
k	h
l	j
m	k

c	y
n	m
o	n
p	q
q	r
r	s
s	t
t	u
u	w
v	x
w	y
x	b
y	c
z	d

Con numeri pseudocasuali

- Uso un generatore di numeri casuali per "estrarre a sorte" la sequenza dei caratteri nella permutazione
- Il codice segreto che scambio col partner è dato dal seme di inizializzazione del generatore

Sistema di Cesare

I caratteri nell'alfabeto di interesse vengono numerati in base alla loro posizione **p**. **p** va da 0 a **N**-1 (**N** è la dimensione dell'alfabeto).

L'idea è di sostituire ciascun carattere con quello che si trova *k* posti più in là (*k* è la chiave segreta)

Quindi si sceglie una chiave *k*, dove *k* va da 1 a **N**-1. Ad esempio: $k = 5$.

Si calcola poi per ciascun carattere **c**:

$$\mathbf{q} = (\mathbf{p} + k) \bmod \mathbf{N}$$

c	p
a	0
b	1
c	2
d	3
e	4
f	5
g	6
h	7
i	8
j	9
k	10
l	11
m	12

c	p
n	13
o	14
p	15
q	16
r	17
s	18
t	19
u	20
v	21
w	22
x	23
y	24
z	25

Cifratura di Cesare

I caratteri nell'alfabeto di interesse vengono numerati in base alla loro posizione **p**. **p** va da 0 a **N**-1 (**N** è la dimensione dell'alfabeto).

L'idea è di sostituire ciascun carattere con quello che si trova *k* posti più in là (*k* è la chiave segreta)

Quindi si sceglie una chiave *k*, dove *k* va da 1 a **N**-1. Ad esempio: *k* = 5.

Si calcola poi per ciascun carattere **c**:
q = (**p** + *k*) mod **N**

Il carattere **c** in posizione **p** viene quindi sostituito col carattere **y** in posizione **q**

c	p	q	c	p	q
a	0	5	n	13	18
b	1	6	o	14	19
c	2	7	p	15	20
d	3	8	q	16	21
e	4	9	r	17	22
f	5	10	s	18	23
g	6	11	t	19	24
h	7	12	u	20	25
i	8	13	v	21	0
j	9	14	w	22	1
k	10	15	x	23	2
l	11	16	y	24	3
m	12	17	z	25	4

13

Cifratura di Cesare

I caratteri nell'alfabeto di interesse vengono numerati in base alla loro posizione **p**. **p** va da 0 a **N**-1 (**N** è la dimensione dell'alfabeto).

L'idea è di sostituire ciascun carattere con quello che si trova *k* posti più in là (*k* è la chiave segreta)

Quindi si sceglie una chiave *k*, dove *k* va da 1 a **N**-1. Ad esempio: *k* = 5.

Si calcola poi per ciascun carattere **c**:
q = (**p** + *k*) mod **N**

Il carattere **c** in posizione **p** viene quindi sostituito col carattere **y** in posizione **q**

c	p	q	y	c	p	q	y
a	0	5	**f**	n	13	18	
b	1	6		o	14	19	
c	2	7		p	15	20	
d	3	8		q	16	21	
e	4	9		r	17	22	
f	5	10		s	18	23	
g	6	11		t	19	24	
h	7	12		u	20	25	
i	8	13		v	21	0	
j	9	14		w	22	1	
k	10	15		x	23	2	
l	11	16		y	24	3	
m	12	17		z	25	4	

14

Cifratura di Cesare

I caratteri nell'alfabeto di interesse vengono numerati in base alla loro posizione **p**. **p** va da 0 a **N**-1 (**N** è la dimensione dell'alfabeto).

L'idea è di sostituire ciascun carattere con quello che si trova *k* posti più in là (*k* è la chiave segreta)

Quindi si sceglie una chiave *k*, dove *k* va da 1 a **N**-1. Ad esempio: *k* = 5.

Si calcola poi per ciascun carattere **c**:
q = (**p** + *k*) mod **N**

Il carattere **c** in posizione **p** viene quindi sostituito col carattere **y** in posizione **q**

c	p	q	y	c	p	q	y
a	0	5	**f**	n	13	18	**s**
b	1	6	**g**	o	14	19	**t**
c	2	7	**h**	p	15	20	**u**
d	3	8	**i**	q	16	21	**v**
e	4	9	**j**	r	17	22	**w**
f	5	10	**k**	s	18	23	**x**
g	6	11	**l**	t	19	24	**y**
h	7	12	**m**	u	20	25	**z**
i	8	13	**n**	v	21	0	**a**
j	9	14	**o**	w	22	1	**b**
k	10	15	**p**	x	23	2	**c**
l	11	16	**q**	y	24	3	**d**
m	12	17	**r**	z	25	4	**e**

15

Cifratura di Cesare

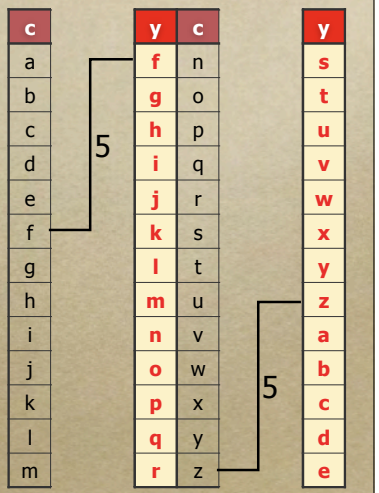
I caratteri nell'alfabeto di interesse vengono numerati in base alla loro posizione **p**. **p** va da 0 a **N**-1 (**N** è la dimensione dell'alfabeto).

L'idea è di sostituire ciascun carattere con quello che si trova *k* posti più in là (*k* è la chiave segreta)

Quindi si sceglie una chiave *k*, dove *k* va da 1 a **N**-1. Ad esempio: *k* = 5.

Si calcola poi per ciascun carattere **c**:
q = (**p** + *k*) mod **N**

Il carattere **c** in posizione **p** viene quindi sostituito col carattere **y** in posizione **q**



16

Cifratura di Cesare

Esempio

il mastino dei baskerville
custodisce il segreto

nq rfxynst ijn gfxpjwanqqj
hzxytinxhj nq xjlwjyt

c
a
b
c
d
e
f
g
h
i
j
k
l
m

y	c
f	n
g	o
h	p
i	q
j	r
k	s
l	t
m	u
n	v
o	w
p	x
q	y
r	z

y
s
t
u
v
w
x
y
z
a
b
c
d
e

Violazione

- Una spia può tentare di violare la cifratura
  - a patto che conosca l'alfabeto A o ancora meglio la lingua del messaggio in chiaro
- Due modi:
  - FORZA BRUTA: prova tutte le possibili mappature μ
    - è davvero fattibile solo se non sono troppe
    - per esempio con il sistema di Cesare questo tipo di attacco è abbastanza facile!
  - ANALISI CRITTOGRAFICA (solo se conosce la lingua del messaggio in chiaro)

Esercizio 1

vg avmj

jngfba n ubyzrf: unlznexrg natbyb benatr fgerrg

px ajrkq vjrcq jpjc

Cesare a forza bruta…

Analisi crittografica

- I primi crittoanalisti furono gli arabi
  - nel X sec. D.C. sotto la dinastia Abbaside la cifratura era ampiamente utilizzata per i documenti di governo
  - usavano principalmente la cifratura monoalfabetica, con la variante di introdurre dei simboli nel codice in aggiunta alle lettere (es.: a → +, b → #, etc.)
- Si posero il problema di "rompere" un codice senza ricorrere alla forza bruta (ossia senza andare per tentativi)
  - uno studio che necessitava di adeguate competenze matematiche, statistiche e linguistiche
  - non per niente i codici monoalfabetici erano stati considerati inviolabili per secoli

Analisi crittografica

- Anche la religione diede il suo contributo
  - gli studiosi del Corano intrapresero sofisticate analisi linguistiche per scoprire la cronologia esatta delle rivelazioni di Maometto
  - ritenevano che alcune parole fossero più nuove di altre, e pertanto cercavano di stabilire la cronologia in base alla frequenza di tali parole (più parole nuove = testo più recente)
  - questo li portò ad analizzare anche la frequenza delle singole lettere.
- Abu Yūsuf Ya'qūb ibn 'Isḥāq aṣ-Ṣabbāḥ al-Kindī: "Manoscritto sulla Decifrazione dei Messaggi Crittografici"
  - testo scoperto solo nel 1987 negli Archivi Ottomani di Istanbul
  - propone la tecnica dell'analisi delle frequenze.

Analisi delle frequenze

- Bisogna conoscere la lingua del testo originale, e il testo da decifrare deve essere sufficientemente lungo
  - la frequenza delle singole lettere nella lingua considerata può essere assunta come nota, per lo meno per le lettere più frequenti
  - si calcolano le frequenze dei simboli nel testo cifrato, e in base ad esse si possono fare ipotesi ragionevoli almeno su quelli più frequenti
- Più in generale si possono analizzare anche:
  - frequenze di digrammi, trigrammi, etc.
  - parole sicuramente presenti nel testo in determinate posizioni (es. firma del mittente)
  - pattern ricorrenti (ad es. per codici scritti in linguaggi di programmazione)

Analisi delle frequenze

- Naturalmente non è un metodo "sicuro" che fornisca una sequenza di passi predeterminata
  - È possibile infatti prevenirla scrivendo messaggi che volontariamente scombinano le frequenze
- In molti alfabeti europei la **E** è una lettera molto frequente, mentre la **Z** lo è poco...
  - "dalla zambia allo zaire, le zone di ozono aizzano le zebre che vanno a zonzo a zig zag"
  - nel 1969, il romanziere francese Georges Perec scrisse un intero romanzo di 200 pagine senza usare la lettera **e**: "La Disparition"
  - Il romanziere inglese Gilbert Adair riuscì a tradurlo sempre senza usare la **e**: il titolo è "A Void"

Esempio (S.Singh - The Cracking Code Book)

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: "DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?" OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

α	#	%
a	3	0.9
b	25	7.4
c	27	8.0
d	14	4.1
e	5	1.5
f	2	0.6
g	1	0.3
h	0	0.0
i	11	3.3
j	18	5.3
k	26	7.7
l	25	7.4
m	11	3.3

α	#	%
n	3	0.9
o	38	11.2
p	31	9.2
q	2	0.6
r	6	1.8
s	7	2.1
t	0	0.0
u	6	1.8
v	18	5.3
w	1	0.3
x	34	10.1
y	19	5.6
z	5	1.5

Esempio (S.Singh - The Cracking Code Book)

PCQ VMJYPD LBYK LYSO
KBXBJXWXV BXV ZCJPO EYPD
KBXBJYUXJ LBJOO KCPK. CP LBO
LBCMKXPV XPV IYJKL PYDBL,
QBOP KBO BXV OPVOV LBO
LXRO CI SX'XJMI, KBO JCKO XPV
EYKKOV LBO DJCMPV ZOICJO
BYS, KXUYPD: "DJOXL EYPD, ICJ
X LBCMKXPV XPV CPO PYDBLK Y
BXNO ZOOP JOACMPLYPD LC
UCM LBO IXZROK CI FXKL XDOK
XPV LBO RODOPVK CI XPAYOPL
EYPDK. SXU Y SXEO KC ZCRV XK
LC AJXNO X IXNCMJ CI UCMJ
SXGOKLU?"
OFYRCDMO, LXROK IJCS LBO
LBCMKXPV XPV CPO PYDBLK

α	#	%
a	3	0.9
b	25	7.4
c	27	8.0
i	11	3.3
j	18	5.3
k	26	7.7
l	25	7.4
m	11	3.3

α	#	%
n	3	0.9
o	38	11.2
p	31	9.2
v	18	5.3
w	1	0.3
x	34	10.1
y	19	5.6
z	5	1.5

O X P
e t a

25

Esempio (S.Singh - The Cracking Code Book)

PCQ VMJYPD LBYK LYSO
KBXBJXWXV BXV ZCJPO EYPD
KBXBJYUXJ LBJOO KCPK. CP LBO
LBCMKXPV XPV IYJKL PYDBL,
QBOP KBO BXV OPVOV LBO
LXRO CI SX'XJMI, KBO JCKO XPV
EYKKOV LBO DJCMPV ZOICJO
BYS, KXUYPD: "DJOXL EYPD, ICJ
X LBCMKXPV XPV CPO PYDBLK Y
BXNO ZOOP JOACMPLYPD LC
UCM LBO IXZROK CI FXKL XDOK
XPV LBO RODOPVK CI XPAYOPL
EYPDK. SXU Y SXEO KC ZCRV XK
LC AJXNO X IXNCMJ CI UCMJ
SXGOKLU?"
OFYRCDMO, LXROK IJCS LBO
LBCMKXPV XPV CPO PYDBLK

O X P
e t a

26

Esempio (S.Singh - The Cracking Code Book)

PCQ VMJYPD LBYK LYSO
KBXBJXWXV BXV ZCJPO EYPD
KBXBJYUXJ LBJOO KCPK. CP LBO
LBCMKXPV XPV IYJKL PYDBL,
QBOP KBO BXV OPVOV LBO
LXRO CI SX'XJMI, KBO JCKO XPV
EYKKOV LBO DJCMPV ZOICJO
BYS, KXUYPD: "DJOXL EYPD, ICJ
X LBCMKXPV XPV CPO PYDBLK Y
BXNO ZOOP JOACMPLYPD LC
UCM LBO IXZROK CI FXKL XDOK
XPV LBO RODOPVK CI XPAYOPL
EYPDK. SXU Y SXEO KC ZCRV XK
LC AJXNO X IXNCMJ CI UCMJ
SXGOKLU?"
OFYRCDMO, LXROK IJCS LBO
LBCMKXPV XPV CPO PYDBLK

O X P
e t a

	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
O	1	9	0	3	1	1	1	0	1	4	6	0	1	2	2	8	0	4	1	0	0	3	0	1	1	2
X	0	7	0	1	1	1	1	0	2	4	6	3	0	3	1	9	0	2	4	0	3	3	2	0	0	1
P	1	0	5	6	0	0	0	0	0	1	1	2	2	0	8	0	0	0	0	0	0	11	0	9	9	0

27

Esempio (S.Singh - The Cracking Code Book)

PCQ VMJYPD LBYK LYSO
KBXBJXWXV BXV ZCJPO EYPD
KBXBJYUXJ LBJOO KCPK. CP LBO
LBCMKXPV XPV IYJKL PYDBL,
QBOP KBO BXV OPVOV LBO
LXRO CI SX'XJMI, KBO JCKO XPV
EYKKOV LBO DJCMPV ZOICJO
BYS, KXUYPD: "DJOXL EYPD, ICJ
X LBCMKXPV XPV CPO PYDBLK Y
BXNO ZOOP JOACMPLYPD LC
UCM LBO IXZROK CI FXKL XDOK
XPV LBO RODOPVK CI XPAYOPL
EYPDK. SXU Y SXEO KC ZCRV XK
LC AJXNO X IXNCMJ CI UCMJ
SXGOKLU?"
OFYRCDMO, LXROK IJCS LBO
LBCMKXPV XPV CPO PYDBLK

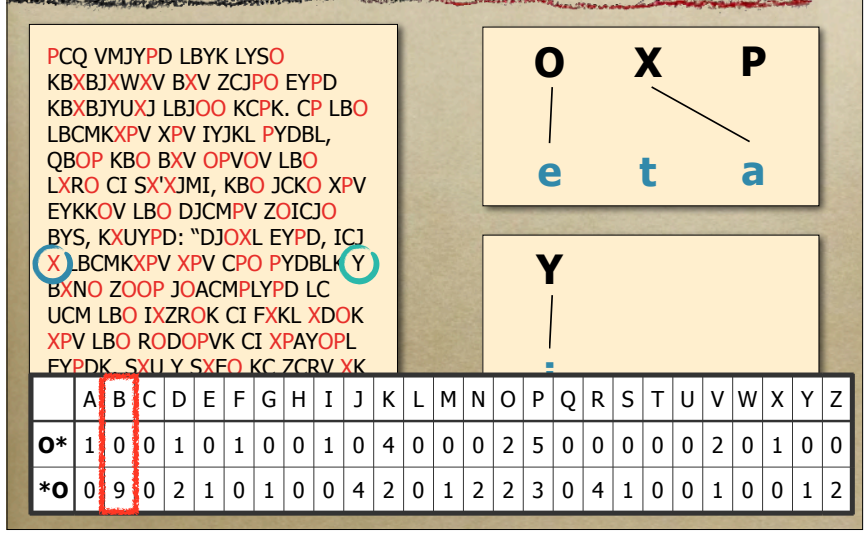
O X P
e t a

Y
i

28

Esempio (S.Singh - The Cracking Code Book)

PCQ VMJYPD LBYK LYSO
KBXBJXWXV BXV ZCJPO EYPD
KBXBJYUXJ LBJOO KCPK. CP LBO
LBCMKXPV XPV IYJKL PYDBL,
QBOP KBO BXV OPVOV LBO
LXRO CI SX'XJMI, KBO JCKO XPV
EYKKOV LBO DJCMPV ZOICJO
BYS, KXUYPD: "DJOXL EYPD, ICJ
X LBCMKXPV XPV CPO PYDBLK Y
BXNO ZOOP JOACMPLYPD LC
UCM LBO IXZROK CI FXKL XDOK
XPV LBO RODOPVK CI XPAYOPL
EYPDK. SXU Y SXEO KC ZCRV XK
LC AJXNO X IXNCMJ CI UCMJ
SXGOKLU?"
OFYRCDMO, LXROK IJCS LBO
LBCMKXPV XPV CPO PYDBLK

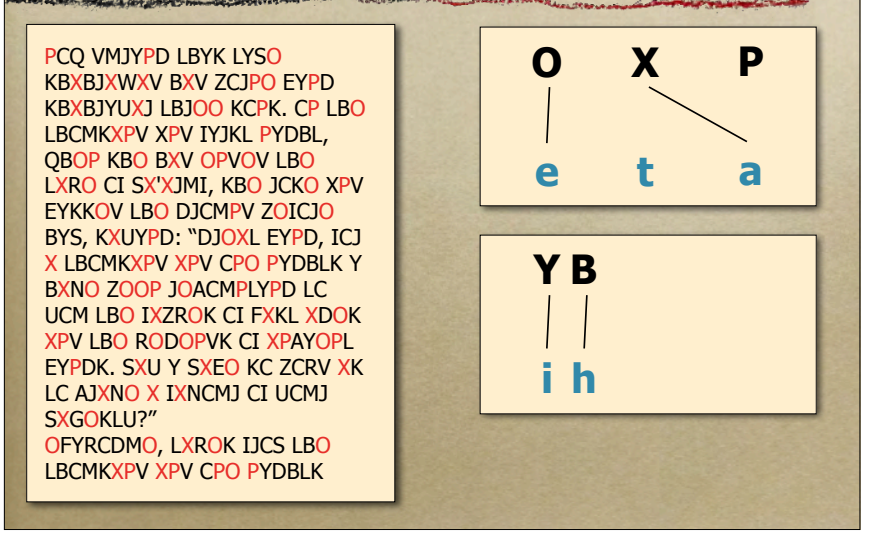


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O*	1	0	0	1	0	1	0	0	1	0	4	0	0	0	2	5	0	0	0	0	0	2	0	1	0	0
***O**	0	9	0	2	1	0	1	0	0	4	2	0	1	2	2	3	0	4	1	0	0	1	0	0	1	2

29

Esempio (S.Singh - The Cracking Code Book)

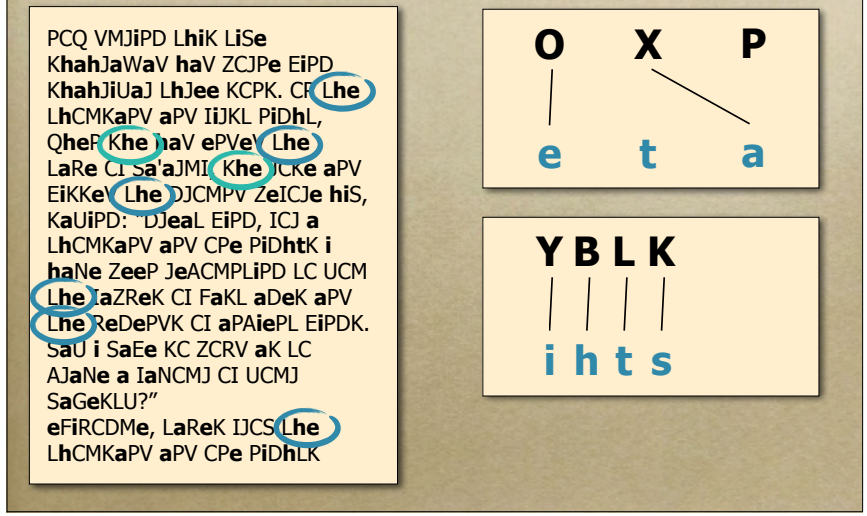
PCQ VMJYPD LBYK LYSO
KBXBJXWXV BXV ZCJPO EYPD
KBXBJYUXJ LBJOO KCPK. CP LBO
LBCMKXPV XPV IYJKL PYDBL,
QBOP KBO BXV OPVOV LBO
LXRO CI SX'XJMI, KBO JCKO XPV
EYKKOV LBO DJCMPV ZOICJO
BYS, KXUYPD: "DJOXL EYPD, ICJ
X LBCMKXPV XPV CPO PYDBLK Y
BXNO ZOOP JOACMPLYPD LC
UCM LBO IXZROK CI FXKL XDOK
XPV LBO RODOPVK CI XPAYOPL
EYPDK. SXU Y SXEO KC ZCRV XK
LC AJXNO X IXNCMJ CI UCMJ
SXGOKLU?"
OFYRCDMO, LXROK IJCS LBO
LBCMKXPV XPV CPO PYDBLK



30

Esempio (S.Singh - The Cracking Code Book)

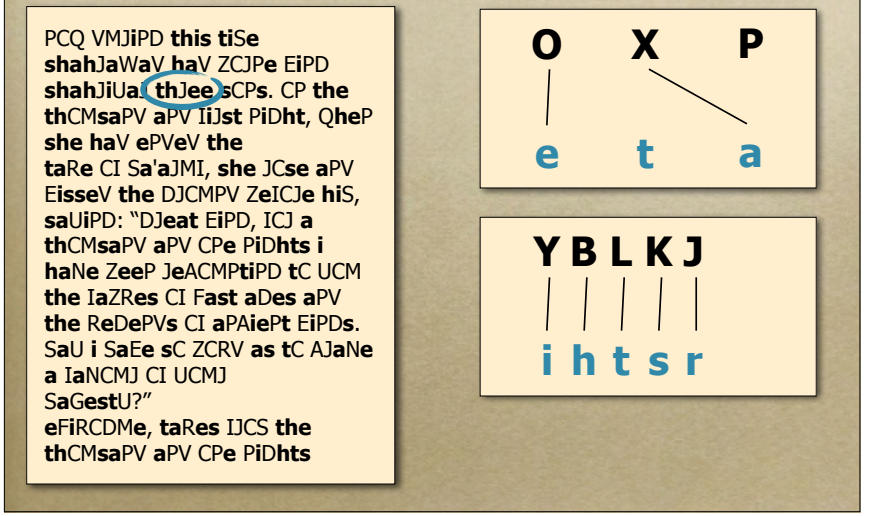
PCQ VMJiPD LhiK LiSe
KhahJaWaV haV ZCJPe EiPD
KhahJiUaJ LhJee KCPK. CP Lhe
LhCMKaPV aPV IiJKL PiDhL,
QheP Khe haV ePVeV Lhe
LaRe CI Sa'aJMI, Khe JCKe aPV
EiKKeV Lhe DJCMPV ZeICJe hiS,
KaUiPD: "DJeaL EiPD, ICJ a
LhCMKaPV aPV CPe PiDhtK i
haNe ZeeP JeACMPLiPD LC UCM
Lhe IaZReK CI FaKL aDeK aPV
Lhe ReDePVK CI aPAiePL EiPDK.
SaU i SaEe KC ZCRV aK LC
AJaNe a IaNCMJ CI UCMJ
SaGeKLU?"
eFiRCDMe, LaReK IJCS Lhe
LhCMKaPV aPV CPe PiDhLK



31

Esempio (S.Singh - The Cracking Code Book)

PCQ VMJiPD **this tiSe**
shahJaWaV **ha**V ZCJPe EiPD
shahJiUaJ **thJee**sCPs. CP **the**
thCM**sa**PV **a**PV I**i**J**st** PiD**ht**, Q**he**P
she haV ePVeV **the**
taRe CI Sa'**a**JMI, **she** JCse **a**PV
E**i**sse**V the** DJCMPV **Ze**ICJe **hi**S,
saUiPD: "DJ**eat** EiPD, ICJ **a**
thCM**sa**PV **a**PV CPe PiD**hts i**
haNe ZeeP JeACMP**ti**PD **t**C UCM
the IaZRes CI **F**ast **a**Des **a**PV
the ReDePV**s** CI **a**PA**ie**P**t** EiPDs.
SaU **i** SaEe **s**C ZCRV **as t**C AJaNe
a IaNCMJ CI UCMJ
SaG**est**U?"
eFiRCDMe, **ta**Res IJCS **the**
thCM**sa**PV **a**PV CPe PiD**hts**



32

Esempio (S.Singh - The Cracking Code Book)

PCQ VMriPD **this** tiSe
shahraWaV **ha**V ZCrPe EiPD
shahriU**ar three s**CP**s**. CP **the**
thCM**sa**PV **a**PV **)irst** PiD**ht**, Q**he**P
she haV ePVeV **the**
taRe CI Sa'**ar**MI, **she** rCs**e** **a**PV
E**isse**V **the** DrCMPV ZeICr**e hi**S,
saUiPD: "D**reat** EiPD, ICr **a**
thCM**sa**PV **a**PV)CPe PiD**hts i**
haNe ZeeP **re**ACMP**ti**PD **t**C UCM
the IaZR**es** CI F**ast** a**Des** **a**PV
the ReDePV**s** CI **a**PA**ie**P**t** EiPD**s**.
SaU **i** SaEe sC ZCRV **as t**C AraNe
a IaNCM**r** CI UCM**r**
Sa**Gest**U?"
eFiRCDM**e**, **ta**R**es** IrCS **the**
thCM**sa**PV **a**PV)CPe PiD**hts**

O	X	P
e	t	a

Y	B	L	K	J	P	V
i	h	t	s	r	n	d

33

Esempio (S.Singh - The Cracking Code Book)

n**C**Q **d**M**rin**D **this** tiSe
shahraW**ad had** ZC**rne** E**in**D
shahriU**ar three s**C**ns**. C**n the**
thCM**sand** **)nd** I**irst ni**D**ht**,
Q**hen she had ended the**
taRe CI Sa'**ar**MI, **she** rC**se and**
E**issed the** DrCM**nd** ZeICr**e hi**S,
saU**in**D: "D**reat** E**in**D, ICr **a**
thCM**sand and** C**ne ni**D**hts i**
haNe Z**een re**ACM**ntin**D **t**C UCM
the IaZR**es** CI F**ast** a**Des and**
the ReD**ends** CI **an**A**ient** E**in**D**s**.
SaU **i** SaEe sC ZCR**d as t**C AraNe
a IaNCM**r** CI UCM**r**
Sa**Gest**U?"
eFiRCDM**e**, **ta**R**es** IrCS **the**
thCM**sand and** C**ne ni**D**hts**

O	X	P
e	t	a

Y	B	L	K	J	P	V
i	h	t	s	r	n	d

34

Esempio (S.Singh - The Cracking Code Book)

noQ **durin**D **this** tiSe
shahraW**ad had** Z**orne** E**in**D
shahriU**ar three sons**. **on the**
thousand and I**irst** nYD**ht**,
Q**hen she had ended the**
taRe **o**I Sa'**aru**I, **she rose and**
E**issed the** D**round** ZeI**ore hi**S,
saU**in**D: "D**reat** E**in**D, **)or a**
thousand and one niD**hts i**
haNe Z**een re**A**ountin**D **to** U**ou**
the IaZR**es o**I F**ast** a**Des and**
the ReD**ends o**I **an**A**ient** E**in**D**s**.
SaU **i** SaEe **so** ZoR**d as to** AraNe
a IaN**our o**I U**our**
Sa**Gest**U?"
eFiR**oDue**, **ta**R**es** IroS **the**
thousand and one niD**hts**

O	X	P
e	t	a

Y	B	L	K	J	P	V
i	h	t	s	r	n	d

35

Esempio (S.Singh - The Cracking Code Book)

noQ **during this** tiSe
shahraW**ad had** Z**orne** E**ing**
shahriU**ar three sons**. **on the**
thousand and I**irst night**,
Q**hen she had ended the**
taRe **o**I Sa'**aru**I, **she rose and**
E**issed the ground** ZeI**ore hi**S,
saU**ing**: "**great** E**ing**, **)or a**
thousand and one nights i
haNe Z**een re**A**ounting to** U**ou**
the IaZR**es o**I F**ast** a**ges and**
the R**egends o**I **an**A**ient** E**ings**.
SaU **i** SaEe **so** ZoR**d as to** AraNe
a IaN**our o**I U**our**
Sa**Gest**U?"
eFiR**ogue**, **ta**R**es** IroS **the**
thousand and one nights

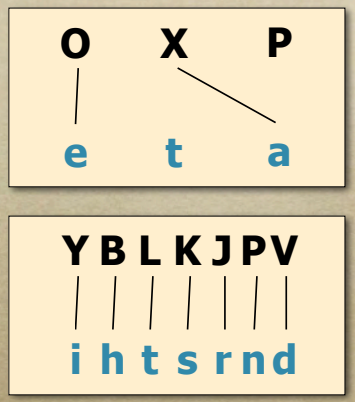
O	X	P
e	t	a

Y	B	L	K	J	P	V
i	h	t	s	r	n	d

36

Esempio (S.Singh - The Cracking Code Book)

now during this time shahrazad had borne king shahriyar three sons. on the thousand and first night, when she had ended the tale of ma'aruf, she rose and kissed the ground before him, saying: "great king, for a thousand and one nights i have been recounting to you the fables of past ages and the legends of ancient kings. may i make so bold as to crave a favour of your majesty?"
epilogue, tales from the thousand and one nights



Esercizio 2

Tm fizbuzfzp ha uidtop m'abzqdiep.
Cadeop htoop vt eupbudiotop bpb fpuvd fdiepbd
dg d eotop upbezgditop gtz fza upsd abt utoozqt speet.

Esercizio 3

La cifratura monoalfabetica è molto usata nei romanzi gialli. Tipicamente la chiave è la prima frase di un libro; volendo cambiare la chiave il mittente e il destinatario devono solo comunicarsi il nuovo libro da utilizzare.
Ecco un esempio tratto da *Parlando con uno Sconosciuto* di Ruth Rendell.
Si provi a decifrare il messaggio:

SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA

considerando che è stato cifrato usando la prima frase del libro *The Other Side of Silence*, che racconta la storia della spia Kim Philby:

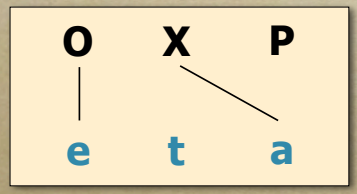
The snow lay thick on the steps and the snowflakes driven by the wind looked black in the headlights of the cars.

Supporto al ragionamento

- Possiamo vedere il ragionamento del crittoanalista come:
  - **camminare nello spazio delle ipotesi…**
  - …fino ad arrivare ad una ipotesi che viene promossa a **SOLUZIONE**

Ipotesi di lavoro

- Un assegnamento parziale di simboli cifrati a lettere dell'alfabeto in chiaro



$\{O=e, X=a\}$

- L'analista può avere la "ragionevole certezza" di un'ipotesi o stare "provandola"

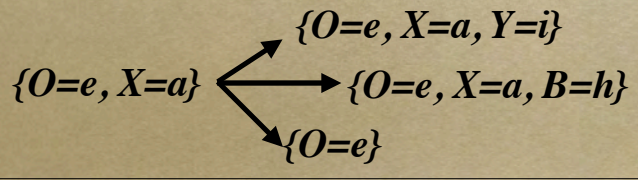
"Effetto" di un'ipotesi

- Un'ipotesi ha un effetto sul "risultato" che permette di valutarne l'attendibilità

PCQ VMJiPD LhiK LiSe
KhahJaWaV haV ZCJPe EiPD
KhahJiUaJ LhJee KCPK. CP Lhe
LhCMKaPV aPV IiJKL PiDhL,
QheP Khe haV ePVeV Lhe
LaRe CI Sa'aJMI, Khe JCKe aPV
EiKKeV Lhe DJCMPV ZeICJe hiS,
KaUiPD: "DJeaL EiPD, ICJ a
LhCMKaPV aPV CPe PiDhtK i
haNe ZeeP JeACMPLiPD LC UCM
Lhe IaZReK CI FaKL aDeK aPV
Lhe ReDePVK CI aPAiePL EiPDK.
SaU i SaEe KC ZCRV aK LC
AJaNe a IaNCMJ CI UCMJ
SaGeKLU?"
eFiRCDMe, LaReK IJCS Lhe
LhCMKaPV aPV CPe PiDhLK

Spazio delle ipotesi

- Grafo in cui:
  - i nodi sono le possibili ipotesi parziali
  - un arco collega due ipotesi se è possibile passare da una all'altra in un passo
- Il passo più piccolo che posso fare è:
  - aggiungere un assegnamento "simbolo cifrato = lettera in chiaro"
  - rimuovere un assegnamento precedentemente fatto



Soluzione

- Una ipotesi diventa una **soluzione** se:
  - assegna una lettera in chiaro ad **ogni** simbolo dell'alfabeto cifrato
  - l'**effetto** che ha sul testo risultante comunica all'analista che la decifratura è riuscita (ossia il messaggio è comprensibile)

Arrivare alla soluzione

- Camminare nello spazio delle ipotesi
  - l'analista fa delle "mosse" (come in un gioco) e ne valuta l'effetto
  - una mossa può corrispondere a più passi nel grafo fatti contemporaneamente:
    - ad esempio: cambiare assegnamento ad un simbolo corrisponde ad effettuare una "rimozione" ed una "aggiunta"
    - oppure: ipotizzare un'intera parola corrisponde a fare tanti assegnamenti in un colpo solo
  - può essere utile poter "tornare indietro" (in gergo tecnico: back-tracking), ma…
    - potrei accorgermi che un'ipotesi era sbagliata solo dopo essere andato molto avanti, e a quel punto voler modificare solo gli assegnamenti di quell'ipotesi, senza tornare sui miei passi fino all'errore

Supportare il processo di analisi

- Ipotesi
  - avere sempre chiara l'ipotesi di lavoro attuale
  - poter vedere il suo effetto sul testo
  - poter segnare un'ipotesi come "ragionevolmente certa"
- Mosse nello spazio delle ipotesi
  - poter vedere quale strada ha portato al punto attuale
  - vedere e riconoscere i "sentieri" già percorsi e scartati
  - essere avvisati se si sta tornando in un punto già visitato (per non muoversi in tondo)
  - essere avvisati se si sta facendo un passo già "fatto e disfatto"
  - potersi segnare il ragionamento che ha portato ad una data ipotesi motivando la/le mosse che hanno condotto lì.

Supportare la singola mossa

- Strumenti che aiutano a fare "il prossimo passo"
  - confronto fra frequenze: simboli cifrati vs. lettere in chiaro nella lingua del messaggio
  - confronto fra frequenze: coppie cifrate vs. coppie in chiaro, vincolando un elemento della coppia (volendo anche con lo spazio per la frequenza delle lettere in fine di parola)
    - vedi quanto fatto con la lettera H nell'esercizio di esempio
    - in italiano quasi tutte le parole finiscono per vocale…
  - ricerca in dizionari per trovare matching fra pattern nel messaggio cifrato e parole della lingua in cui è scritto
    - nell'esercizio di esempio abbiamo fatto corrispondere il pattern L**hJee** alla parola **three**… c'erano altre parole che corrispondevano?

Quindi vorremmo una proposta…

- Che abbia la base di scambio lecito dei messaggi
  - concordare fra partner il sistema da usare
  - cifratura + decifratura di messaggi
- Che contenga anche abbozzati (ma ben studiati livello di analisi progettuale) alcuni strumenti di criptoanalisi
  - Supporto efficace alla "navigazione" dello spazio delle ipotesi
  - Esempi di supporto al ragionamento (frequenze, dizionari)
- Corredato da un'analisi di una possibile estensione che realizzi il gioco a punti attraverso sfide.