Cifrari Simmetrici

Prof. Francesco Bergadano

Dipartimento di Informatica
Università di Torino

Cifrario

Sistema che permette di

- **Cifrare**
- **Decifrare**
- **Generare e Gestire chiavi crittografiche**

Cifrari

Aperti: il metodo per cifrare e decifrare è pubblico

Chiusi: tutto è segreto/classificato

Cifrari aperti

Principio di Kerkhoffs [La cryptographie militaire, 1883]:

metodi e algoritmi segreti prima o poi verranno conosciuti dall'avversario, il segreto deve essere concentrato nelle chiavi.

Cifrari aperti

In generale, vogliamo evitare il concetto di "security through obscurity":

Ottenere sicurezza nascondendo informazioni o inventando metodi complessi per recuperare le stesse, metodi che però potranno essere studiati e rilevati dal nostro avversario

Cifrari aperti

Simmetrici: chiavi condivise

Asimmetrici: chiavi diverse per chi cifra e per ci decifra

Cifrari Simmetrici

Caratteristiche dei cifrari simmetrici

- Mittente e ricevente condividono una stessa chiave
- Per cifrare e decifrare si usa la stessa chiave
- Cifratura e decifratura sono efficienti
- E' difficile o praticamente impossibile decifrare senza conoscere la chiave, perché manca l'informazione necessaria

Termini equivalenti

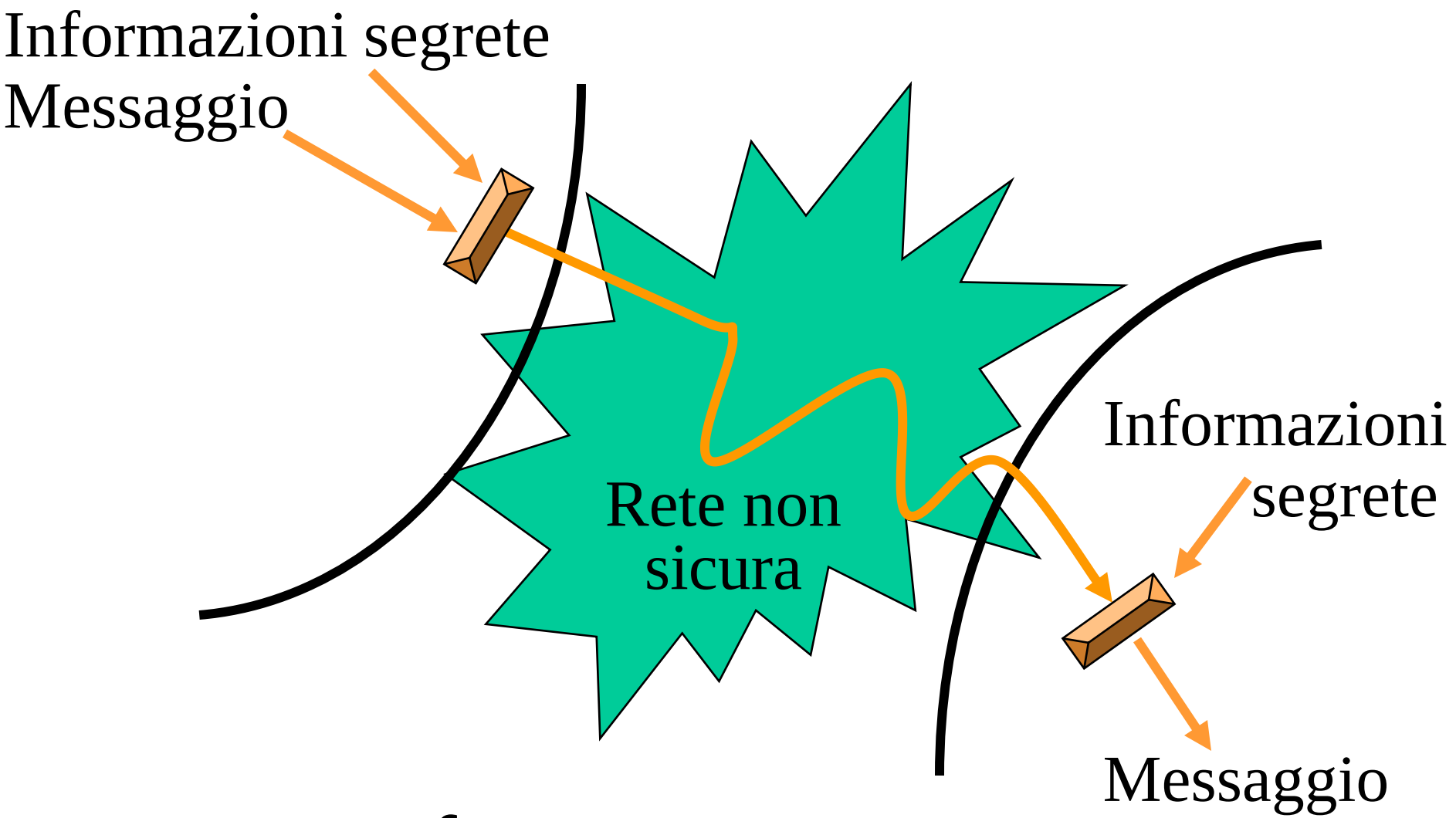
Cifrari simmetrici

=

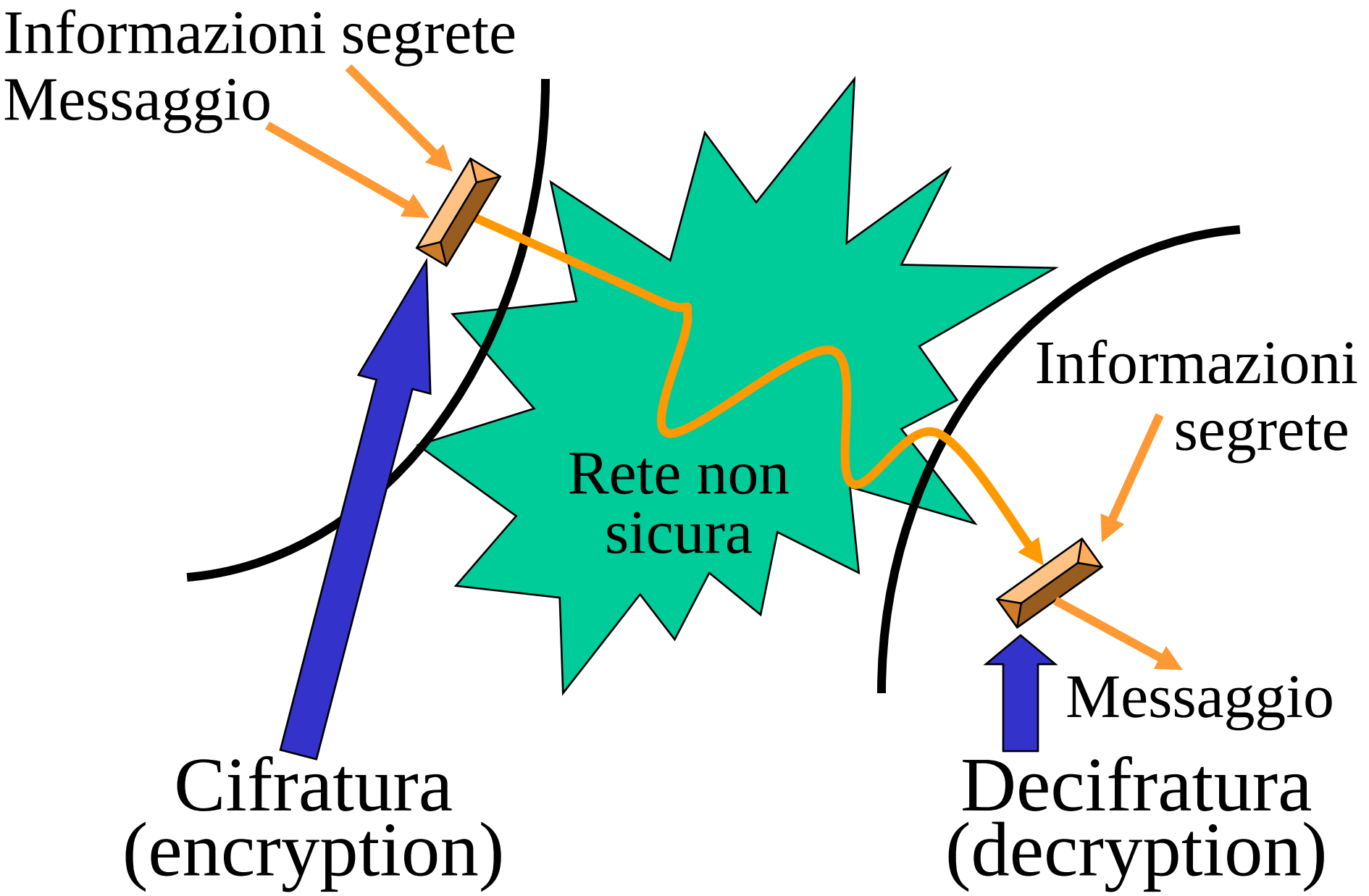
Cifrari convenzionali

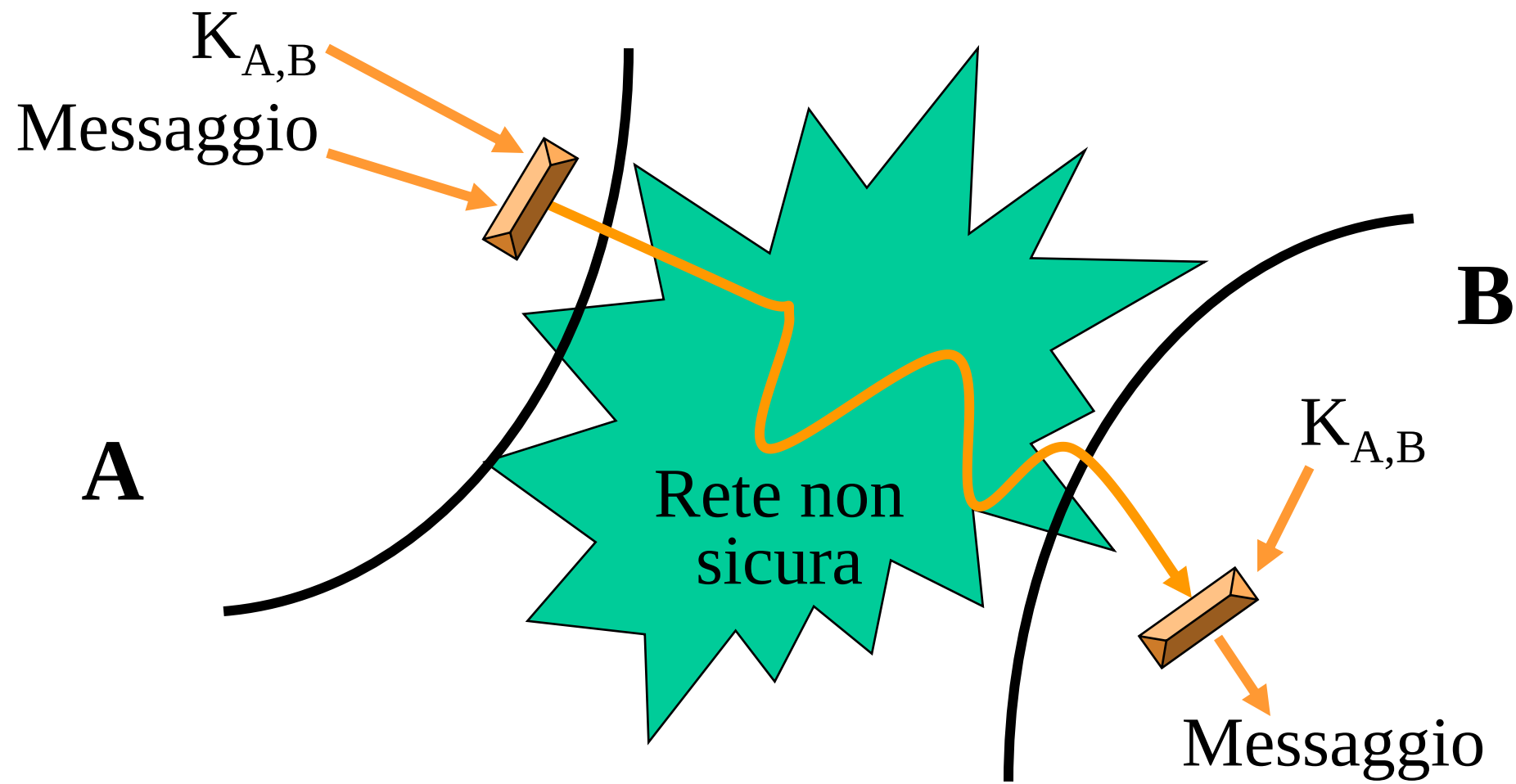
=

Cifrari a chiave condivisa



Cifratura simmetrica


Informazioni segrete
Messaggio
Rete non sicura
Informazioni segrete
Messaggio
Cifratura (encryption)
Decifratura (decryption)



Modello a chiavi simmetriche o condivise

Definizioni

Testo in chiaro (Plaintext o Cleartext):

Testo prima della encryption

Testo cifrato (Ciphertext)

Testo dopo l'operazione di encryption

Cifrari simmetrici ‘pre-informatici’

Character-oriented

- Cifrario di Cesare e cifrari monoalfabetici a 1 lettera
- Cifrario di Playfair (monoalfabetico a 2 lettere)
- Cifrario di Vigenère (polialfabetico)

Bit-oriented

- Cifrario di Vernam e one-time pad (bit-oriented)

Cifrari simmetrici ‘pre-informatici’

A sostituzione

- Un gruppo di caratteri viene sostituito con un altro gruppo di caratteri

A permutazione

- Gruppi di caratteri vengono spostati nel testo

Cifrari monoalfabetici a N lettere

Ogni N-upla di lettere del testo in chiaro viene sostituita sempre dalla stessa sequenza di lettere nel testo cifrato

Cifrari polialfabetici

Una lettera o N-upla di lettere può essere cifrata diversamente (con traformazioni alfabetiche diverse) a seconda della sua posizione nel testo

Cifrario di Cesare

- Numera le lettere dell'alfabeto
- genera una chiave K tra 0 e 20
- per cifrare, sostituisci la lettera numero X con la lettera numero (X+K)%21
- per decifrare, sostituisci X con (X-K)%21

esempio: ***buongiorno*** *con K=3 diventa* ***earqlnruqr***

Il cifrario di Cesare è molto debole

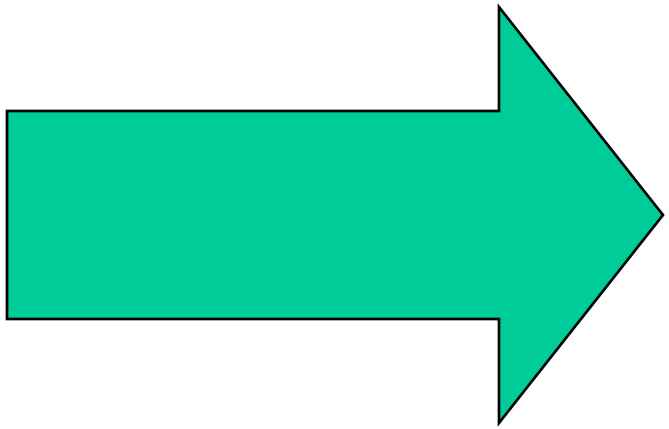
Dato un testo cifrato basta provare a decifrarlo con tutte le chiavi K da 0 a 20, fermandoci quando troviamo un testo di senso compiuto (attacco di tipo ‘forza bruta’ – ‘brute force’, o ‘esaustivo’)

Cifrari monoalfabetici a una lettera

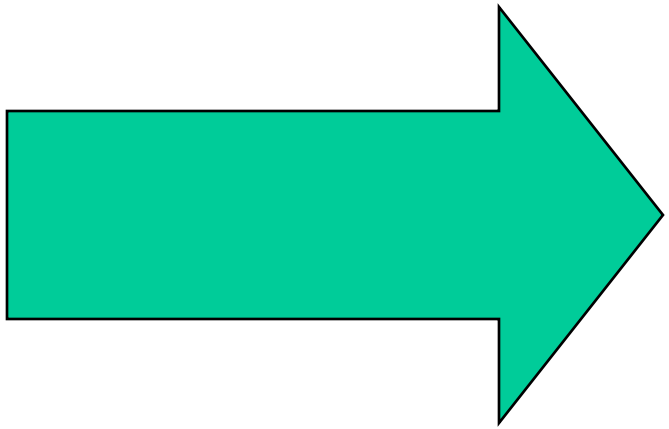
Come il cifrario di Cesare, ma la chiave K identifica una sostituzione arbitraria di ciascuna lettera dell'alfabeto (per esempio a→q, b→z, c→f, …)

abcdefghilmnopqrstuvz

qzfabdeohilmnprstcugv



Esistono N! diverse chiavi per N lettere (tutte le possibili permutazioni), per 21 lettere sono più di 51 miliardi di miliardi di chiavi.



Non è possibile, in generale, decifrare provando manualmente tutte le possibili chiavi, come nel caso del cifrario di Cesare.

I cifrari monoalfabetici a una lettera sono tuttavia molto deboli

Questo è dovuto alla possibile presenza di regolarità statistiche o di porzioni di testo fisso nel messaggio originario.

Il principale metodo per decifrare il testo senza conoscere la chiave consiste nell'analisi della frequenza delle lettere nel testo cifrato (crittanalisi statistica)

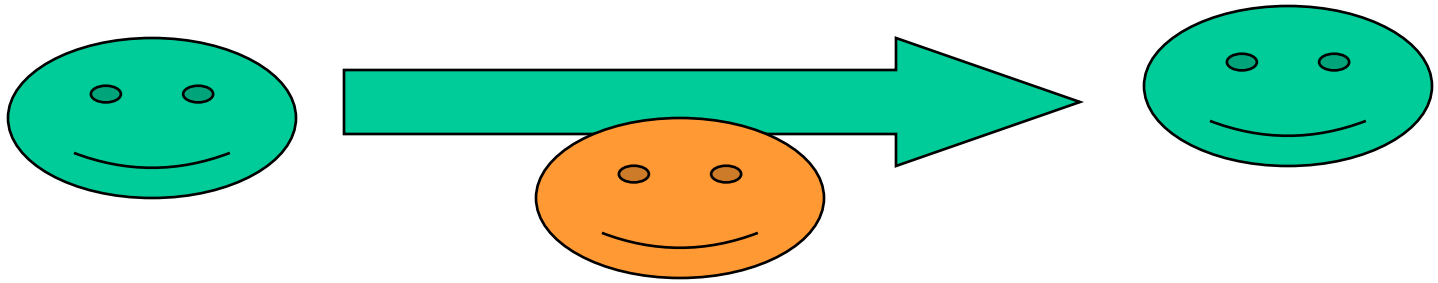
Frequenza delle lettere in Inglese

a	**7.25**	**n**	**7.75**
b	**1.25**	**o**	**7.5**
c	**3.5**	**p**	**2.75**
d	**4.25**	**q**	**0.5**
e	**12.75**	**r**	**8.5**
f	**3.0**	**s**	**6.0**
g	**2.0**	**t**	**9.25**
h	**3.5**	**u**	**3.0**
i	**7.75**	**v**	**1.5**
j	**0.25**	**w**	**1.5**
k	**0.5**	**x**	**0.5**
l	**3.75**	**y**	**2.25**
m	**1.25**	**z**	**0.25**

Lettere in ordine di frequenza

e	**12.75**	**u**	**3.0**
t	**9.25**	**p**	**2.75**
r	**8.5**	**y**	**2.25**
i	**7.75**	**g**	**2.0**
n	**7.75**	**v**	**1.5**
o	**7.5**	**w**	**1.5**
a	**7.25**	**b**	**1.25**
s	**6.0**	**m**	**1.25**
d	**4.25**	**q**	**0.5**
l	**3.75**	**x**	**0.5**
h	**3.5**	**k**	**0.5**
c	**3.5**	**z**	**0.25**
f	**3.0**	**j**	**0.25**

Ciphertext Only Attack



Attacco a un cifrario monoalfabetico

- Confrontare la frequenza delle lettere nel testo cifrato con la frequenza delle lettere nella lingua o nel linguaggio del testo in chiaro
- Ipotizzare (altre) possibili corrispondenze tra lettere del testo cifrato e lettere del testo originario
- Verificare se il testo così parzialmente decifrato è possibile nella lingua del testo in chiaro, e, in caso contrario, annullare una parte delle corrispondenze ipotizzate

Cifrari monoalfabetici

- Più il testo cifrato è lungo più è facile decifrare
- Se esistono parti di testo fisse il compito è estremamente facilitato
- Se esistono parti di testo probabili il compito è facilitato
- Esempio: decifrare un testo di circa 150 caratteri

Cifrari monoalfabetici a N lettere

Ogni sequenza di N lettere viene sostituita con una sequenza fissata di N lettere. Per esempio, per N=2, aa→qe, ab→zi, …, ba→df, …, zz→kf.

Il cifrario è migliore di quello per N=1, ma rimane comunque possibile una analisi statistica. L'analisi è facile se il testo cifrato è lungo o se alcune parti del testo in chiaro sono note o probabili.

Cifrari monoalfabetici a N lettere

Il cifrario è più sicuro rispetto all'attacco esaustivo

Es. per N=2, numero di chiavi:
|{aa,ab,…,az,ba,…,bz,…,za,…,zz}|!=(21*21)!

Ma è ancora possibile la crittanalisi statistica

Esempio di cifrario monoalfabetico a 2 lettere: il cifrario di Playfair

Si sceglie come chiave una parola arbitraria, per esempio ‘security’, e si prepara una tabella così:

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

Il cifrario di Playfair

sostituire

- lettere ripetute inserendo una lettera riempimento
- lettere sulla stessa riga con lettere successive a dx
- lettere sulla stessa colonna con lettere in basso
- lettera(rigaI,colonnaJ),lettera(rigaK,colonnaM) con lettera(rigaI,colonnaM),lettera(rigaK,colonnaJ)

Il cifrario di Playfair - esempio

K = ‘security’

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

C(‘buona giornata’) = C(‘buona giornatax’) =

‘arpoy halcpbyhu’ (x = lettera riempitivo)

Debolezze del cifrario di Playfair

- Rimane possibile un'analisi statistica, esaminando la frequenza delle coppie di lettere nel linguaggio del testo in chiaro
- Più il testo cifrato è lungo più è facile decifrare
- Se esistono parti di testo fisse il compito è estremamente facilitato
- Se esistono parti di testo probabili il compito è facilitato

Cifrari polialfabetici

L’analisi statistica risulta molto più difficile con un cifrario polialfabetico, ove una lettera viene sostituita ogni volta in modo diverso, a seconda della sua posizione nel testo

Cifrario di Vigenère

- Selezionare una chiave $K=K_0K_1\ldots K_{n-1}$, dove ogni sottochiave K_i consiste in un numero tra 0 e 20
- Per cifrare sostituire la lettera T_J del testo con la lettera $(T_J+K_{(J\%n)})\%21$, ovvero applicare alla lettera T_J il cifrario di Cesare corrisponte alla sottochiave $K_{(J\%n)}$ individuata dalla posizione J di T_J nel testo

Cifrario di Vigenère - esempio

n = 5

K = $K_0K_1 \ldots K_4$ = 10,3,1,20,0

Testo =	b	u	o	n	a	g	i	o	r	n	a	t	a
	10	3	1	20	0	10	3	1	20	0	10	3	1
→	n	a	p	m	a	s	n	p	q	n	m	z	b

Cifrario di Vigenère

- Ottenere la chiave $K=K_0K_1\ldots K_{n-1}$, dove ogni sottochiave K_i consiste in un numero tra 0 e 20
- Per decifrare sostituire la lettera C_J del testo cifrato con la lettera $(C_J-K_{(J\%n)})\%21$

Debolezze del cifrario di Vigenère

Supponiamo si conosca n, allora è possibile fare la stessa analisi dei cifrari monoalfabetici per lettere che distano n posizioni nel testo (per esse vale la stessa sostituzione)

- Più il testo cifrato è lungo più è facile decifrare
- Se esistono parti di testo fisse il compito è estremamente facilitato

Da caratteri --- a bit

- La sostituzione alfabetica diventa $\oplus$
- $\oplus$ trasforma un bit X in qualsiasi altro bit Y, utilizzando una opportuna chiave K
- $\oplus$ trasforma 8 bit X in qualsiasi altra sequenza di 8 bit Y, utilizzando una opportuna chiave K di 8 bit – ovvero sostituisce X con Y

Cifrario di Vernam (analogo al cifrario di Vigenère, ma bit oriented)

- Selezionare una chiave binaria $K=K_0K_1\ldots K_{n-1}$
- Sostituire il bit T_J del testo con il bit $T_J \oplus K_{(J\%n)}$, ovvero applicare l'operazione di OR esclusivo a ogni bit T_J del testo, utilizzando il bit $K_{(J\%n)}$ della chiave individuato dalla posizione J di T_J nel testo

Cifrario di Vernam - esempio

n = 5

K = $K_0K_1 \ldots K_4$ = 0,0,1,0,1

Testo = 1 1 0 0 1 0 1 0 1 0 0

0 0 1 0 1 0 0 1 0 1 0

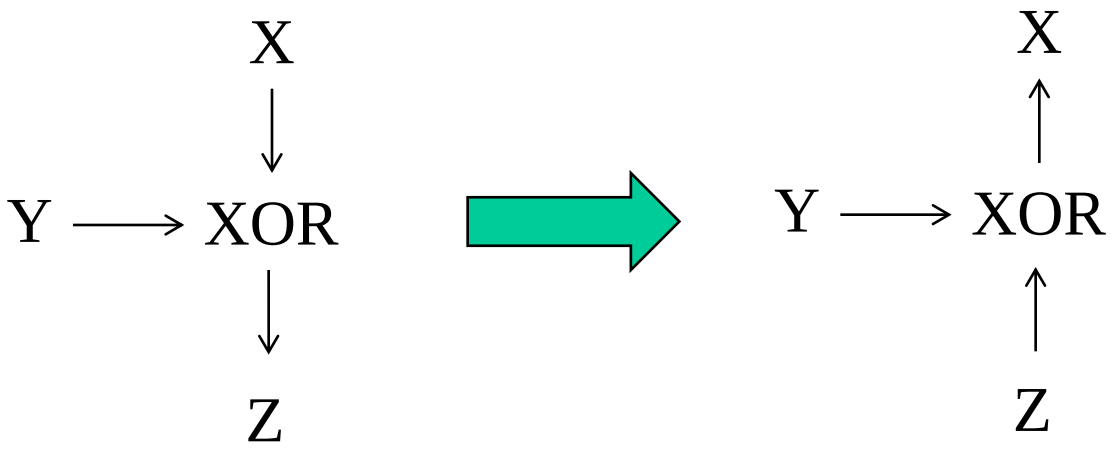
$\rightarrow$ 1 1 1 0 0 0 1 1 1 1 0

OR esclusivo (XOR)

Se X xor Y = Z allora Z xor Y = X

Infatti X xor Y xor Y = Z xor Y, quindi

X xor 0 = Z xor Y, e pertanto X = Z xor Y



Cifrario di Vernam - esempio

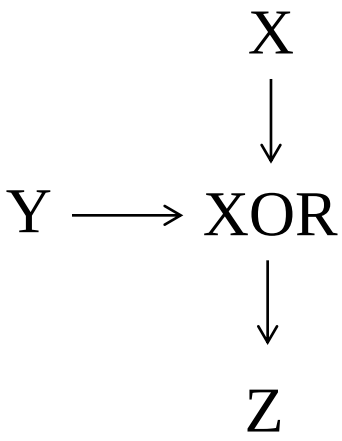
n = 5

K = $K_0K_1 \ldots K_4$ = 0,0,1,0,1

Testo = 1 1 0 0 1 0 1 0 1 0 0 X

0 0 1 0 1 0 0 1 0 1 0 Y

$\rightarrow$ 1 1 1 0 0 0 1 1 1 1 0 Z



Se X xor Y = Z allora Z xor Y = X

Infatti X xor Y xor Y = Z xor Y, quindi

X xor 0 = Z xor Y, e pertanto X = Z xor Y

Debolezze del cifrario di Vernam

Supponiamo si conosca n, allora è possibile fare una analisi statistica su bit che distano n posizioni, con riferimento alla frequenza di particolari gruppi di bit nell'insieme dei possibili testi di partenza

- Più il testo cifrato è lungo più è facile decifrare
- Se esistono parti di testo fisse il compito è estremamente facilitato

One time pad

Come il cifrario di Vernam, ma dove la chiave ha la stessa lunghezza del testo

Questo è l'unico cifrario totalmente sicuro, ma non ha rilevante utilità pratica (tanto vale scambiarsi in modo sicuro il messaggio, invece della chiave!)

Cifrari a permutazione

Le lettere vengono scambiate di posizione, non sostituite

esempio: sistemare il testo su N colonne, scambiare le lettere invertendo le colonne secondo una permutazione segreta di N elementi

Cifrari a permutazione

1 2 3 4 5	3 4 2 1 5
b u o n a	o n u b a
s e r a	r a e s x

K = 3 4 2 1 5

Buona sera onubaraesx

Debolezze dei cifrari a permutazione

E’ possibile elaborare successivi raffinamenti di ipotesi di permutazione basandosi sulla frequenza di digrafi e trigrafi, o sulla presenza di testo fisso o probabile

Il cifrario migliora significativamente effettuando più permutazioni in cascata con diverse chiavi, e ancor più combinandolo con tecniche di sostituzione.

Cifrari simmetrici ‘moderni’

- Macchine a rotori
- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)