


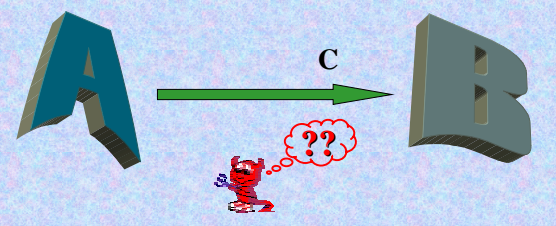
## Crittoanalisi

- ❑ Known Ciphertext Attack
- ❑ Known Plaintext Attack
- ❑ Chosen Plaintext Attack
- ❑ Chosen Ciphertext Attack



Introduzione 0

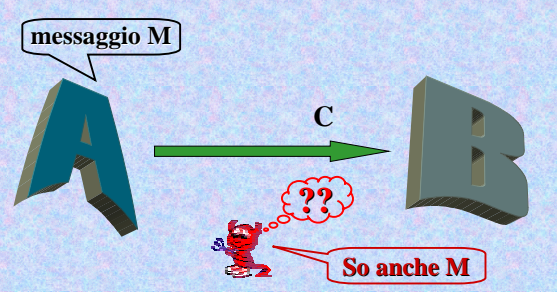
## Known Ciphertext Attack



Introduzione 1

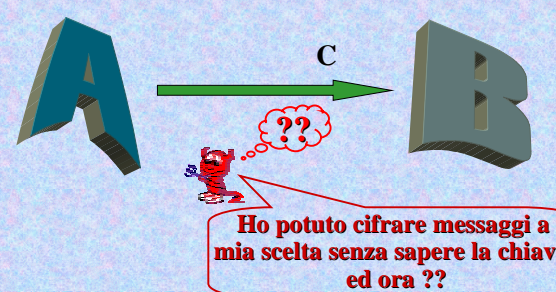
## Known Plaintext Attack

messaggio M



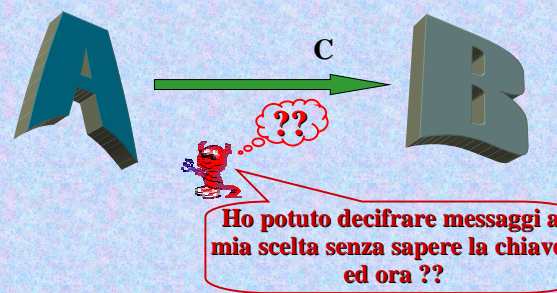
Introduzione 2

## Chosen Plaintext Attack



Introduzione 3

## Chosen Ciphertext Attack



Introduzione 4

## Principio di Kerckhoffs

La sicurezza di un crittosistema deve dipendere **solo** dalla segretezza della chiave e **non** dalla segretezza dell'algoritmo usato.

Jean Guillaume Hubert Victor Francois Alexandre Auguste Kerckhoffs von Nieuwenhof (1835-1903), filologo olandese, *"La Criptographie Militaire"* [1883]

Introduzione 5

### Cifrari a sostituzione polialfabetica

Cifrario di Vigenère [1586] (Blaise de Vigenère, 1523-1596)

$M = M_0M_1M_2\dots M_n$   $\xrightarrow{\text{testo in chiaro}}$   $C_i \leftarrow M_i + K_i \pmod{26}$   $\xrightarrow{\text{testo cifrato}}$   $C = C_0C_1C_2\dots C_n$

$K = K_0K_1K_2\dots K_{t-1}$   
**chiave**

Testo in chiaro: CODICE MOLTO SICURO	Chiave: REBUS
CODIC EMOLT OSICU RO	testo in chiaro
REBUS REBUS REBUS RE	chiave
TSECU VQPFL FWJWM IS	testo cifrato

Introduzione 6

### Cifrari a sostituzione polialfabetica

Cifrario di Vigenère [1586] (Blaise de Vigenère, 1523-1596)

$M = M_0M_1M_2\dots M_n$   $\xrightarrow{\text{testo in chiaro}}$   $C_i \leftarrow M_i + K_i \pmod{26}$   $\xrightarrow{\text{testo cifrato}}$   $C = C_0C_1C_2\dots C_n$

$K = K_0K_1K_2\dots K_{t-1}$   
**chiave**

- ❑ Considerato inviolabile per molto tempo
- ❑ Numero possibili chiavi =  $26^t$
- ❑ Crittoanalisi: Known Ciphertext Attack

Introduzione 7

### Test di Kasiski

Friedrich Kasiski [1863]


testo cifrato ...WPIXFGHDAFNV TV... KLXFGLO

Introduzione 8

### Test di Kasiski

Friedrich Kasiski [1863]

testo cifrato ...WPIXFGHDAFNV TV... KLXFGLO


 XFG cifra lo stesso testo in chiaro!

Introduzione 9

### Test di Kasiski

Friedrich Kasiski [1863]

testo cifrato ...WPIXFGHDAFNV TV... KLXFGLO

 XFG cifra lo stesso testo in chiaro!  
La distanza tra le "X" è un multiplo di t

Introduzione 10

### Test di Kasiski

Friedrich Kasiski [1863]

testo cifrato ...WPIXFGHDAFNV TV... KLXFGLO

 XFG cifra lo stesso testo in chiaro!  
La distanza tra le "X" è un multiplo di t

Siano  $d_1, d_2, \dots, d_n$  le distanze tra le "X" di "XFG"  
allora  $\text{gcd}(d_1, d_2, \dots, d_n)$  è multiplo di t

Introduzione 11

## Indice di coincidenza

Definito da Wolfe Friedman [1920]

Indice di coincidenza di una stringa  $x_1x_2\dots x_n$   
 $IC(x_1x_2\dots x_n)$  = probabilità che due caratteri,  
 presi a caso in  $x_1x_2\dots x_n$ , siano uguali

Introduzione 12

## Indice di coincidenza

Definito da Wolfe Friedman [1920]

Indice di coincidenza di una stringa  $x_1x_2\dots x_n$   
 $IC(x_1x_2\dots x_n)$  = probabilità che due caratteri,  
 presi a caso in  $x_1x_2\dots x_n$ , siano uguali

Esempi:  $IC(MONO) = 1/6$   
 $IC(ALFA) = 1/6$   
 $IC(GAMMA) = 2/24 = 1/12$

Introduzione 13

## Indice di coincidenza

Definito da Wolfe Friedman [1920]

Indice di coincidenza di una stringa  $x_1x_2\dots x_n$   
 $IC(x_1x_2\dots x_n)$  = probabilità che due caratteri,  
 presi a caso in  $x_1x_2\dots x_n$ , siano uguali

$$= \frac{\sum_{i=0}^{25} \binom{f_i}{2}}{\binom{n}{2}} = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}$$

$f_i$  = numero occorrenze carattere i

Introduzione 14

## Indice di coincidenza

Se  $x_1x_2\dots x_n$  è un testo in Inglese  
 Allora  $IC(x_1x_2\dots x_n) \approx \sum_{i=0}^{25} p_i^2 = 0.065$

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
7.3	1.3	3.5	4.3	12.8	3.0	2.0	3.5	7.8	0.3	0.5	3.7	2.8	7.8	7.5	2.8	0.5	8.5	6.0	9.3	3.0	1.5	1.5	0.5	2.3	0.3
$p_A$	$p_B$	$p_C$	$p_D$	$p_E$	$p_F$	$p_G$	$p_H$	$p_I$	$p_J$	$p_K$	$p_L$	$p_M$	$p_N$	$p_O$	$p_P$	$p_Q$	$p_R$	$p_S$	$p_T$	$p_U$	$p_V$	$p_W$	$p_X$	$p_Y$	$p_Z$

$p_i$  = probabilità carattere i in Inglese

Introduzione 15

## Indice di coincidenza

Se  $x_1x_2\dots x_n$  è un testo in Inglese  
 Allora  $IC(x_1x_2\dots x_n) \approx \sum_{i=0}^{25} p_i^2 = 0.065$

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
7.3	1.3	3.5	4.3	12.8	3.0	2.0	3.5	7.8	0.3	0.5	3.7	2.8	7.8	7.5	2.8	0.5	8.5	6.0	9.3	3.0	1.5	1.5	0.5	2.3	0.3
$p_A$	$p_B$	$p_C$	$p_D$	$p_E$	$p_F$	$p_G$	$p_H$	$p_I$	$p_J$	$p_K$	$p_L$	$p_M$	$p_N$	$p_O$	$p_P$	$p_Q$	$p_R$	$p_S$	$p_T$	$p_U$	$p_V$	$p_W$	$p_X$	$p_Y$	$p_Z$

$p_i$  = probabilità carattere i in Inglese

Se  $x_1x_2\dots x_n$  sono caratteri scelti a caso  
 Allora  $IC(x_1x_2\dots x_n) \approx \sum_{i=0}^{25} \left(\frac{1}{26}\right)^2 = 0.038$

Introduzione 16

## Indice di coincidenza

Se  $x_1x_2\dots x_n$  è un testo in Italiano  
 Allora  $IC(x_1x_2\dots x_n) \approx \sum_{i=0}^{25} p_i^2 = 0.075$

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
10.3	0.9	4.3	3.8	12.6	0.8	2.0	1.1	11.6	0.0	0.0	6.6	2.6	6.6	8.7	3.2	0.6	6.7	6.1	6.1	3.0	1.5	0.0	0.0	0.0	0.9
$p_A$	$p_B$	$p_C$	$p_D$	$p_E$	$p_F$	$p_G$	$p_H$	$p_I$	$p_J$	$p_K$	$p_L$	$p_M$	$p_N$	$p_O$	$p_P$	$p_Q$	$p_R$	$p_S$	$p_T$	$p_U$	$p_V$	$p_W$	$p_X$	$p_Y$	$p_Z$

$p_i$  = probabilità carattere i in Italiano

Se  $x_1x_2\dots x_n$  sono caratteri scelti a caso  
 Allora  $IC(x_1x_2\dots x_n) \approx \sum_{i=0}^{25} \left(\frac{1}{26}\right)^2 = 0.038$

Introduzione 17

**t = 1 ?**

testo cifrato  $C_0C_1...C_n$

Se  $t = 1$  allora  $IC(C_0C_1...C_n) = IC(M_0M_1...M_n)$

$$IC(C_0C_1...C_n) \approx \begin{cases} 0.075 & \text{se } t=1 \\ 0.038 & \text{se } t \neq 1 \end{cases}$$

Non proprio!  
Comunque lontano da 0.065

Introduzione 18

**t = 2 ?**

testo cifrato  $C_0C_1...C_n$

Se  $t = 2$  allora  $IC(C_0C_2...) = IC(M_0M_2...)$   
 $IC(C_1C_3...) = IC(M_1M_3...)$

$$IC(C_0C_2...) \approx \begin{cases} 0.075 & \text{se } t=2 \\ 0.038 & \text{se } t \neq 2 \end{cases}$$

Comunque lontano da 0.065

Introduzione 19

**t = 3 ?**

testo cifrato  $C_0C_1...C_n$

Se  $t = 3$  allora  $IC(C_0C_3...) = IC(M_0M_3...)$   
 $IC(C_1C_4...) = IC(M_1M_4...)$   
 $IC(C_2C_5...) = IC(M_2M_5...)$

$$IC(C_0C_3...) \approx \begin{cases} 0.075 & \text{se } t=3 \\ 0.038 & \text{se } t \neq 3 \end{cases}$$

Comunque lontano da 0.065

Introduzione 20

**Esempio**

RLEYFBDOQSMCATCEZCBAPTHRJPCGRONVZMCHZOEPPKRNRVVNCNHFEEACOZNGS  
SIOGHFUIZCOKIGIUKONGFEIRUPCFVOTVCBBERDRZMFSCCSXEEFSUEYFJVNGF  
BIEQWRLEYZJMIRBRLAFWBLNGFBKTBOSVSGFJEGRFTZENDSVNQSSSTOEGFVUVU  
VIAQWGZUSUIAHBQIOZCOKOEWPRDRGULARIORMCWTOFHVJVRNRCBCLNZUIACO  
SKERWMOAHFTHRHWZCBHZAUFCEQIFIIISQRRPVFIEARBJAZQP IPVITVNFV  
CZLROMCOPQIZODIFJTNHSRSCSDAMWPEERGFVXVVMGUAHPZNP IJZLYOHFCRG  
TREYOEUAEBWDFMVBZACSSII CWHCINQF IACNVVZBXOQCWVLR FJ MENZMNGO  
ORNQCTZDVBFVVBZBJCVOOCAPEVRDVGUVNQSSJIRFBCLRBURRFWJENHCWZGBZ  
GZEVBOLWIWTVNVZBT OFHJV RNTPI MNHBUAYRFGOFWUFDVHSVGECTJIGCSIEAH  
JJCRBEVACDPXGVOURAQIFDOAHJTOAHJXUVZVEOQSUKOVZTRNZOSKIACMRIGF  
PTOAJPTEYCNSAERBZLESTVGBBFUAVAPCTVQPTUMNPCIVBGZLNQIVIAJFIOYC  
GRNACTFMVUMZAESBLNNGFXAGOMTHRBPPEPVJRLCFJDOISEVRYCQLRPVFIJNR  
JWRBBUVCBAPFGEESTVMCWPUFIMVMHFBUJZWMRNBQIVGHOSUAACBJEGHFETEW  
PEEACOCOQWTTTEBBKOFHPRUAHBCCBBUIAFGFYNBWOHURZMRLHBHREIOTKATW  
PXAVOERGYWBCTEWPNFNGWEZNBAGIHCCTTUECFUISCSDACVWTOZIOVPRFVBHC  
OGEMNPCAPCTKAFOMVCBBVEPRBEZOYSOKORQPETVBFPEWTZRBAQVIADFXGVS  
JEVNZMFPNSMCIVBFITRSJEIPDJRNHFJEP COUOYCTJAGISDRDRVVMBBUZEZV

Introduzione 21

**Indice di coincidenza**

$t = 1 ? \quad IC(C_0C_1...C_n) = 0.045$

Introduzione 22

**Indice di coincidenza**

$t = 1 ? \quad IC(C_0C_1...C_n) = 0.045$   
  $t = 2 ? \quad \begin{cases} IC(C_0C_2...) = 0.0463 \\ IC(C_1C_3...) = 0.0438 \end{cases}$

Introduzione 23

### Indice di coincidenza

- t = 1 ?  $IC(C_0C_1...C_n) = 0.045$
- t = 2 ?  $\left\{ \begin{array}{l} IC(C_0C_2...) = 0.0463 \\ IC(C_1C_3...) = 0.0438 \end{array} \right.$
- t = 3 ?  $\left\{ \begin{array}{l} IC(C_0C_3...) = 0.0431 \\ IC(C_1C_4...) = 0.0459 \\ IC(C_2C_5...) = 0.0456 \end{array} \right.$

Introduzione 24

### Indice di coincidenza

- t = 1 ?  $IC(C_0C_1...C_n) = 0.045$
- t = 2 ?  $\left\{ \begin{array}{l} IC(C_0C_2...) = 0.0463 \\ IC(C_1C_3...) = 0.0438 \end{array} \right.$
- t = 3 ?  $\left\{ \begin{array}{l} IC(C_0C_3...) = 0.0431 \\ IC(C_1C_4...) = 0.0459 \\ IC(C_2C_5...) = 0.0456 \end{array} \right.$
- t = 4 ?  $\left\{ \begin{array}{l} IC(C_0C_4...) = 0.0448 \\ IC(C_1C_5...) = 0.0421 \\ IC(C_2C_6...) = 0.0495 \\ IC(C_3C_7...) = 0.0437 \\ IC(C_4C_8...) = 0.044 \end{array} \right.$

Introduzione 25

### Indice di coincidenza

- t = 5 ?  $\left\{ \begin{array}{l} IC(C_0C_5...) = 0.0710 \\ IC(C_1C_6...) = 0.0721 \\ IC(C_2C_7...) = 0.0805 \\ IC(C_3C_8...) = 0.0684 \\ IC(C_4C_9...) = 0.0759 \end{array} \right.$

Tutti vicini a 0.075  
t = 5

Introduzione 26

### Cifrario di Vigenère: Crittoanalisi

- Determinare la lunghezza della chiave t
  - uso dell'indice di coincidenza
- Determinare il valore della chiave  $K_0K_1K_2...K_{t-1}$ 
  - uso dell'indice mutuo di coincidenza
  - $K_0$  usato per  $C_0C_1C_2...$
  - $K_1$  usato per  $C_1C_{t+1}C_{2t+1}...$
  - ...
  - $K_{t-1}$  usato per  $C_{t-1}C_{2t-1}C_{3t-1}...$

Introduzione 27

### Indice mutuo di coincidenza

Indice mutuo di coincidenza di  $x_1x_2...x_n$  e  $y_1y_2...y_n$

$IMC(x_1x_2...x_n; y_1y_2...y_n)$  = probabilità che un carattere in  $x_1x_2...x_n$ , ed uno in  $y_1y_2...y_n$ , presi a caso, siano uguali

Introduzione 28

### Indice mutuo di coincidenza

Indice mutuo di coincidenza di  $x_1x_2...x_n$  e  $y_1y_2...y_n$

$IMC(x_1x_2...x_n; y_1y_2...y_n)$  = probabilità che un carattere in  $x_1x_2...x_n$ , ed uno in  $y_1y_2...y_n$ , presi a caso, siano uguali

Esempi:  $IMC(CIA;CIAO) = 3/12 = 1/4$   
 $IMC(ALFA;GAMMA) = 4/20$

Introduzione 29

### Indice mutuo di coincidenza

Indice mutuo di coincidenza di  $x_1x_2\dots x_n$  e  $y_1y_2\dots y_n$

$IMC(x_1x_2\dots x_n; y_1y_2\dots y_n)$  = probabilità che un carattere in  $x_1x_2\dots x_n$ , ed uno in  $y_1y_2\dots y_n$ , presi a caso, siano uguali


$$= \frac{\sum_{i=0}^{25} f_i \cdot f'_i}{n \cdot n'}$$

$f_i$  = numero occorrenze carattere  $i$  in  $x_1x_2\dots x_n$   
 $f'_i$  = numero occorrenze carattere  $i$  in  $y_1y_2\dots y_n$

Introduzione 30

### Indice mutuo di coincidenza

Quale è il valore medio di  $IMC(C_0C_1C_2\dots; C_1C_{t+1}C_{2t+1}\dots)$  ?




Introduzione 31

### Indice mutuo di coincidenza

Quale è il valore medio di  $IMC(C_0C_1C_2\dots; C_1C_{t+1}C_{2t+1}\dots)$  ?

Probabilità di prendere AA =  $p_{-K_0} p_{-K_1}$   
 Probabilità di prendere BB =  $p_{1-K_0} p_{1-K_1}$   
 ...




Introduzione 32

### Indice mutuo di coincidenza

Quale è il valore medio di  $IMC(C_0C_1C_2\dots; C_1C_{t+1}C_{2t+1}\dots)$  ?

Probabilità di prendere AA =  $p_{-K_0} p_{-K_1}$   
 Probabilità di prendere BB =  $p_{1-K_0} p_{1-K_1}$   
 Probabilità di prendere CC =  $p_{2-K_0} p_{2-K_1}$   
 ...



Introduzione 33

### Indice mutuo di coincidenza

Quale è il valore medio di  $IMC(C_0C_1C_2\dots; C_1C_{t+1}C_{2t+1}\dots)$  ?

Probabilità di prendere AA =  $p_{-K_0} p_{-K_1}$   
 Probabilità di prendere BB =  $p_{1-K_0} p_{1-K_1}$   
 Probabilità di prendere CC =  $p_{2-K_0} p_{2-K_1}$   
 ...

$$IMC(C_0C_1C_2\dots; C_1C_{t+1}C_{2t+1}\dots) \approx \sum_{i=0}^{25} p_{i-K_0} p_{i-K_1} = \sum_{h=0}^{25} p_h p_{h+K_0-K_1}$$

Introduzione 34

### Indice mutuo di coincidenza

valore di $K_0-K_1$	media IMC
0	0.065
1, 25	0.039
2, 24	0.032
3, 23	0.034
4, 22	0.044
5, 21	0.033
6, 20	0.036
7, 19	0.039
8, 18	0.034
9, 17	0.034
10, 16	0.038
11, 15	0.045
12, 14	0.039
13	0.043

$K_0-K_1=0 \Rightarrow$  **media IMC = 0.065**  
 $K_0-K_1 \neq 0 \Rightarrow$  **media IMC  $\leq$  0.045**

**Inglese**

Introduzione 35

### Indice mutuo di coincidenza

valore di $K_0-K_1$	media IMC
0	0.075
1, 25	0.033
2, 24	0.034
3, 23	0.034
4, 22	0.047
5, 21	0.027
6, 20	0.032
7, 19	0.026
8, 18	0.027
9, 17	0.023
10, 16	0.024
11, 15	0.027
12, 14	0.015
13	0.021

$K_0-K_1=0 \Rightarrow$  **media IMC = 0.075**  
 $K_0-K_1 \neq 0 \Rightarrow$  **media IMC  $\leq$  0.047**

**Italiano**

Introduzione 36

### $K_0-K_1=0$ ?

testo cifrato  $C_0C_1...C_n$

Se  $K_0-K_1=0$  allora  $IMC(C_0C_1...; C_1C_{t+1}...) \approx 0.075$

Introduzione 37

### $K_0-K_1=0$ ?

testo cifrato  $C_0C_1...C_n$

Se  $K_0-K_1=0$  allora  $IMC(C_0C_1...; C_1C_{t+1}...) \approx 0.075$

$$IMC(C_0C_1...; C_1C_{t+1}...) \begin{cases} \approx 0.075 & \text{se } K_0-K_1=0 \\ \approx 0.047 & \text{se } K_0-K_1 \neq 0 \end{cases}$$

Introduzione 38

### $K_0-K_1=1$ ?

testo cifrato  $C_0C_1...C_n$

Introduzione 39

### $K_0-K_1=1$ ?

testo cifrato  $C_0C_1...C_n$

$Y_i \leftarrow C_i - 1 \text{ mod } 26$

Se  $K_0-K_1=1$  allora  $IMC(Y_0Y_1...; C_1C_{t+1}...) \approx 0.075$

$$IMC(Y_0Y_1...; C_1C_{t+1}...) \begin{cases} \approx 0.075 & \text{se } K_0-K_1=1 \\ \approx 0.047 & \text{se } K_0-K_1 \neq 1 \end{cases}$$

Introduzione 40

### $K_0-K_1=2$ ?

testo cifrato  $C_0C_1...C_n$

Introduzione 41

**$K_0 - K_1 = 2$  ?**

testo cifrato  $C_0 C_1 \dots C_n$   $Y_i \leftarrow C_i - 2 \pmod{26}$

Se  $K_0 - K_1 = 1$  allora  $IMC(Y_0 Y_1 \dots; C_1 C_{t+1} \dots) \approx 0.075$

$$IMC(Y_0 Y_1 \dots; C_1 C_{t+1} \dots) \begin{cases} \approx 0.075 & \text{se } K_0 - K_1 = 2 \\ \approx 0.047 & \text{se } K_0 - K_1 \neq 2 \end{cases}$$

Introduzione 42

**$K_0 - K_1 = 3$  ?**

testo cifrato  $C_0 C_1 \dots C_n$   $Y_i \leftarrow C_i - 3 \pmod{26}$

Se  $K_0 - K_1 = 1$  allora  $IMC(Y_0 Y_1 \dots; C_1 C_{t+1} \dots) \approx 0.075$

$$IMC(Y_0 Y_1 \dots; C_1 C_{t+1} \dots) \begin{cases} \approx 0.075 & \text{se } K_0 - K_1 = 3 \\ \approx 0.047 & \text{se } K_0 - K_1 \neq 3 \end{cases}$$

Introduzione 43

**Determinare la chiave**

- $K_0 - K_1 = 5$
- $K_1 - K_2 = 6$
- $K_2 - K_3 = 9$
- ...
- $K_{t-2} - K_{t-1} = 5$

**t-1 equazioni in t incognite**

Riesco ad esprimere tutti i  $K_i$  in funzione di  $K_0$  !

Introduzione 44

**Determinare la chiave**

- $K_0 - K_1 = 5$
- $K_1 - K_2 = 6$
- $K_2 - K_3 = 9$
- ...
- $K_{t-2} - K_{t-1} = 5$

**t-1 equazioni in t incognite**

Riesco ad esprimere tutti i  $K_i$  in funzione di  $K_0$  !

**Quanto vale  $K_0$  ?**

Introduzione 45

**Determinare la chiave**

- $K_0 - K_1 = 5$
- $K_1 - K_2 = 6$
- $K_2 - K_3 = 9$
- ...
- $K_{t-2} - K_{t-1} = 5$

**t-1 equazioni in t incognite**

Riesco ad esprimere tutti i  $K_i$  in funzione di  $K_0$  !

**Quanto vale  $K_0$  ?**


**Provo tutti i possibili 26 valori !**

Introduzione 46

**Cifrario di Vigenère: Crittoanalisi**


- Determinare la lunghezza della chiave t
  - uso dell'indice di coincidenza
- Determinare il valore della chiave  $K_0 K_1 K_2 \dots K_{t-1}$ 
  - calcolo delle differenze  $K_0 - K_1, K_1 - K_2, \dots, K_{t-2} - K_{t-1}$
  - uso dell'indice mutuo di coincidenza
  - calcolo di  $K_0$ : prova le 26 possibilità

Introduzione 47


 **Esempio: Determinare la chiave**

$K_1 - K_0$

.0325	.0415	.0422	.0436	.0385	.0444	.0388	.0390	.0347
.0350	.0404	.0315	.0419	.0398	.0370	.0380	.0703	.0314
.0346	.0356	.0436	.0269	.0327	.0298	.0381	.0371	



Introduzione 48

 **Esempio: Determinare la chiave**


$K_1 - K_0 = 16$

.0325	.0415	.0422	.0436	.0385	.0444	.0388	.0390	.0347
.0350	.0404	.0315	.0419	.0398	.0370	.0380	.0703	.0314
.0346	.0356	.0436	.0269	.0327	.0298	.0381	.0371	

$K_2 - K_0 = 25$

.0326	.0341	.0345	.0365	.0245	.0367	.0284	.0393	.0394
.0373	.0358	.0432	.0439	.0399	.0382	.0363	.0334	.0315
.0355	.0449	.0384	.0518	.0403	.0313	.0370	.0738	

Introduzione 49

 **Esempio: Determinare la chiave**

$K_3 - K_0 = 12$

.0380	.0407	.0370	.0381	.0295	.0330	.0415	.0361	.0423
.0411	.0330	.0411	.0705	.0364	.0324	.0361	.0460	.0301
.0321	.0316	.0397	.0355	.0354	.0423	.0390	.0403	

$K_4 - K_0 = 13$

.0401	.0393	.0379	.0353	.0345	.0273	.0357	.0461	.0371
.0439	.0420	.0288	.0412	.0737	.0352	.0350	.0401	.0401
.0328	.0387	.0311	.0403	.0368	.0348	.0370	.0340	


$K_2 - K_1 = 9$

.0361	.0328	.0311	.0389	.0334	.0533	.0355	.0390	.0286
.0741	.0328	.0437	.0325	.0415	.0272	.0406	.0284	.0378
.0428	.0382	.0446	.0380	.0463	.0358	.0395	.0260	

$K_3 - K_1 = 22$

.0465	.0302	.0369	.0320	.0391	.0410	.0361	.0488	.0354
.0447	.0351	.0440	.0297	.0429	.0318	.0309	.0336	.0327
.0442	.0347	.0362	.0328	.0721	.0344	.0412	.0318	

Introduzione 50

 **Esempio: Determinare la chiave**

$K_4 - K_1 = 23$

.0355	.0419	.0339	.0436	.0320	.0408	.0423	.0371	.0470
.0334	.0434	.0374	.0414	.0295	.0400	.0296	.0317	.0375
.0328	.0434	.0355	.0322	.0314	.0711	.0330	.0415	

$K_3 - K_2 = 14$

.0443	.0393	.0421	.0358	.0426	.0318	.0269	.0392	.0318
.0378	.0321	.0363	.0372	.0724	.0348	.0354	.0342	.0533
.0364	.0391	.0324	.0373	.0358	.0315	.0419	.0360	


$K_4 - K_2 = 13$

.0353	.0453	.0415	.0367	.0310	.0374	.0296	.0307	.0446
.0303	.0350	.0321	.0321	.0376	.0779	.0343	.0343	.0357
.0470	.0397	.0478	.0344	.0388	.0369	.0329	.0399	

$K_4 - K_3 = 1$


.0382	.0736	.0368	.0349	.0367	.0414	.0390	.0434	.0293
.0336	.0420	.0351	.0427	.0329	.0388	.0361	.0427	.0327
.0366	.0317	.0326	.0402	.0367	.0450	.0345	.0319	

Introduzione 51

 **Esempio: Determinare la chiave**

- $K_0 - K_1 = 10$
- $K_0 - K_2 = 1$
- $K_0 - K_3 = 14$
- $K_0 - K_4 = 13$
- $K_1 - K_2 = 17$
- $K_1 - K_3 = 4$
- $K_1 - K_4 = 3$
- $K_2 - K_4 = 12$
- $K_2 - K_3 = 13$
- $K_3 - K_4 = 25$

Introduzione 52

 **Esempio: Determinare la chiave**

- $K_0 - K_1 = 10$
- ~~$K_0 - K_2 = 1$~~
- ~~$K_0 - K_3 = 14$~~
- ~~$K_0 - K_4 = 13$~~
- $K_1 - K_2 = 17$
- ~~$K_1 - K_3 = 4$~~
- ~~$K_1 - K_4 = 3$~~
- ~~$K_2 - K_4 = 12$~~
- $K_2 - K_3 = 13$
- $K_3 - K_4 = 25$

Introduzione 53

### Esempio: Determinare la chiave

- $K_0 - K_1 = 10$
- $K_0 - K_2 = 1$
- $K_0 - K_3 = 14$
- $K_0 - K_4 = 13$
- $K_1 - K_2 = 17$
- $K_1 - K_3 = 4$
- $K_1 - K_4 = 3$
- $K_2 - K_3 = 12$
- $K_2 - K_4 = 13$
- $K_3 - K_4 = 25$

$$K_1 = K_0 - 10$$

$$K_2 = K_1 - 17 = K_0 - 1$$

$$K_3 = K_2 - 13 = K_0 - 14$$

$$K_4 = K_3 - 25 = K_0 - 13$$

Introduzione 54

### Esempio: Determinare la chiave

$$K_1 = K_0 - 10$$

$$K_2 = K_1 - 17 = K_0 - 1$$

$$K_3 = K_2 - 13 = K_0 - 14$$

$$K_4 = K_3 - 25 = K_0 - 13$$

$$K_0 = 1$$

$$K_1 = 17$$

$$K_2 = 0$$

$$K_3 = 13$$

$$K_4 = 14$$

B  
R  
A  
N  
O

Introduzione 55


### Esempio: Testo in chiaro

QUELRAMODELLAGODICOMOCHIEVOLGEAMEZZOGIORNOTRADUECATENENONINTE  
 RROTTEDIMONTITUTTOASENIEGOLFIASECONDADELLOSPORGEREEDELRIENTR  
 AREDIQUELLIVIENQUASIAUNTRATTOARESTRINGERSIEAPRENDERCORSOEFIG  
 URADIFUMETRAUNPROMONTORIOADESTRAEUNAMPIACOSTIERADALLALTRAPA  
 RTEEILPONTECHEVICONGIUNGELEDERIVEPARCHERENDASAMCORPIUSENSI  
 BILEALLOCCHIOQUESTATRASFORMAZIONEESGNILPUNTOINCUIILLAGOCES  
 SAELADDARICOMINCIAPEIRPIGLIARPOINOMEDILAGODOVELERIVEALLONTA  
 NANDOSIDINUOVOLASCIANLAQUADISTENDERSIERALLENTARSIINNUOVIGOL  
 FIEINNUOISENILACOSTIERAFORMATADALDEPOSITODITREGROSSITORRENT  
 ISCENDEAPPOGGIATAADUEMONTICONTIGUILUNODETTOILSANMARTINOLALTR  
 OCCONVOCELOMBARDAILRESEGONEDAIMOLTICOCUZZOLINFILACHEINVEROLO  
 FANNOSOMIGLIAREANASEGATALCHENONECHIALPRIMOVEDERLOPURCHESIA  
 IFRONTECOMEPERESEMPIODISULEMURADIMILANOCHEGUARDANOASETTENTRI  
 ONENONLODISCERNASTOAOUNTALCONTRASSEGNOINQUELLALUNGAEVASTAGI  
 OGAIDAGLIALTRIMONTIDINOMEPIUOSCUROEDIFORMAPIUCOMUNEPERUNBUO  
 NPZEZOLACOSTASALECONUNPENDIOLIENTOCONTINUOPOISIROMPEINPOGGIE  
 INVALLONCELLIINERTEEINISPIANATESECONDOLOSSATURADEUEMONTIEIL

Introduzione 56

## Problema

Resistenza del Cifrario di Vigenère rispetto a  
**Known Plaintext Attack**



Introduzione 57