

Elementi di Crittoanalisi

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

<http://www.dia.unisa.it/professori/ads>



Marzo 2017

Indice

- Tipi di attacchi
- Crittoanalisi di
 - Cifrario a sostituzione
 - Cifrario di Hill
 - Cifrario di Vigenère

Cifrari simmetrici

chiave privata k

chiave privata k

$$C \leftarrow \text{CIFRA}(k, M)$$

$$M \leftarrow \text{DECIFRA}(k, C)$$



Alice

messaggio M

C

canale insicuro



Bob



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,

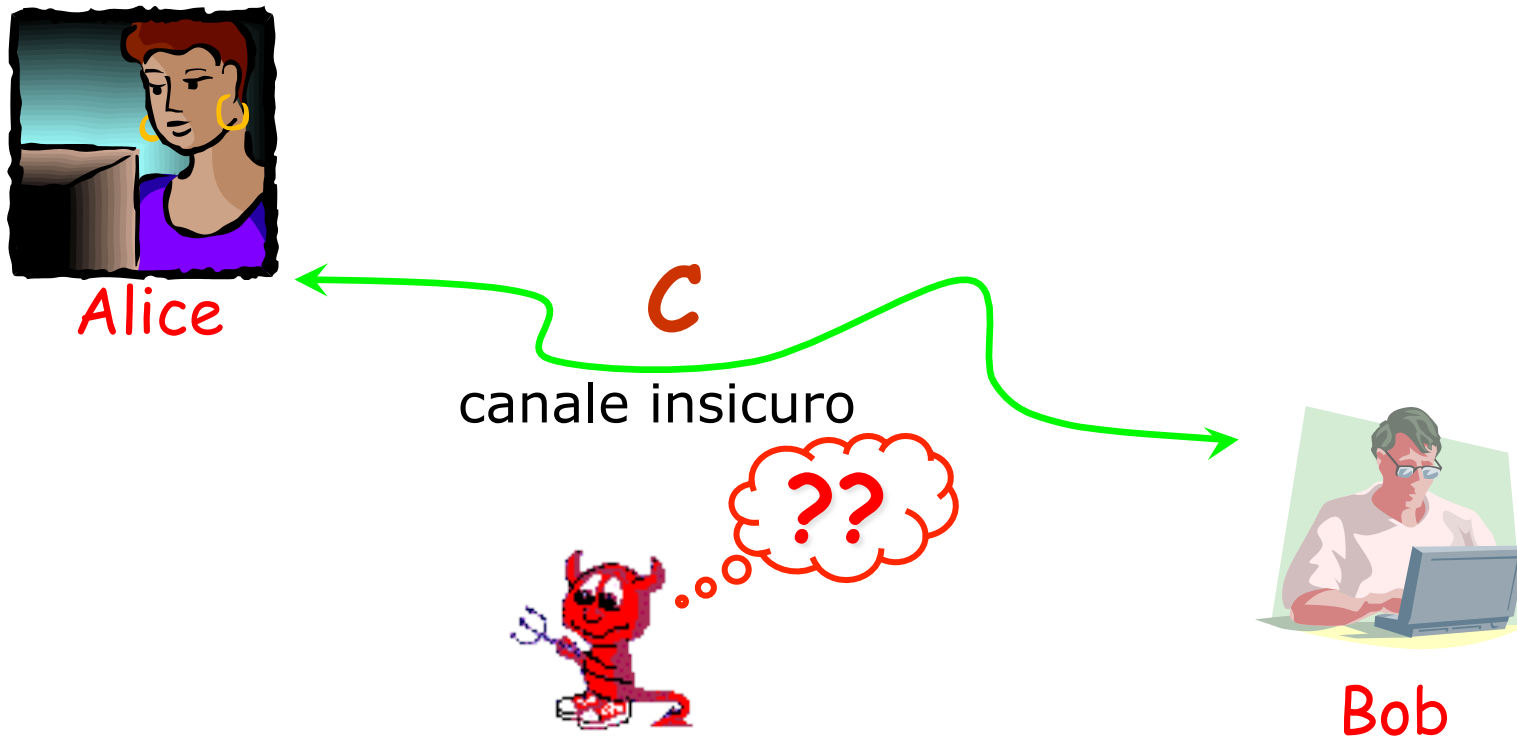
"La Cryptographie Militarie" [1883]

Crittoanalisi

- Tipi di attacchi:
 - Known Ciphertext Attack
 - Known Plaintext Attack
 - Chosen Plaintext Attack
 - Chosen Ciphertext Attack



Known Ciphertext Attack

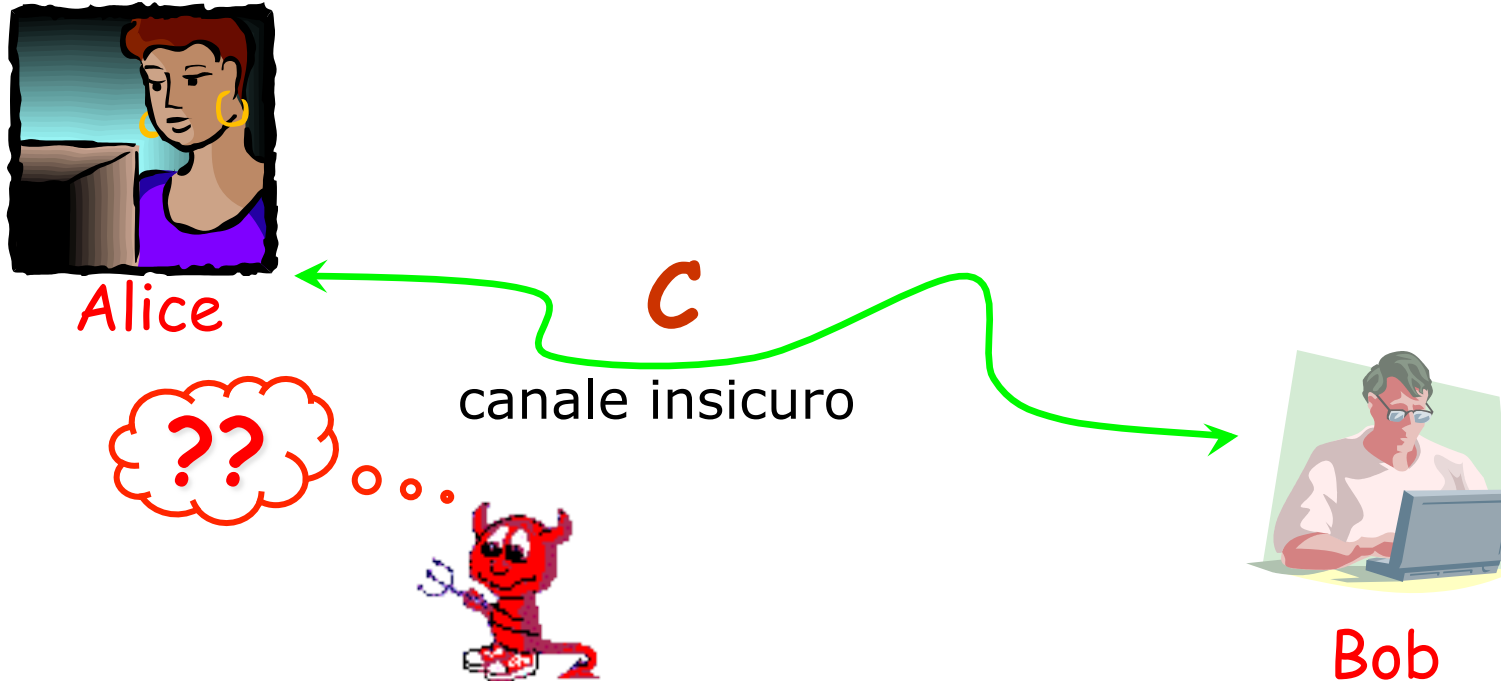


L'avversario conosce solo il testo cifrato

Known Plaintext Attack

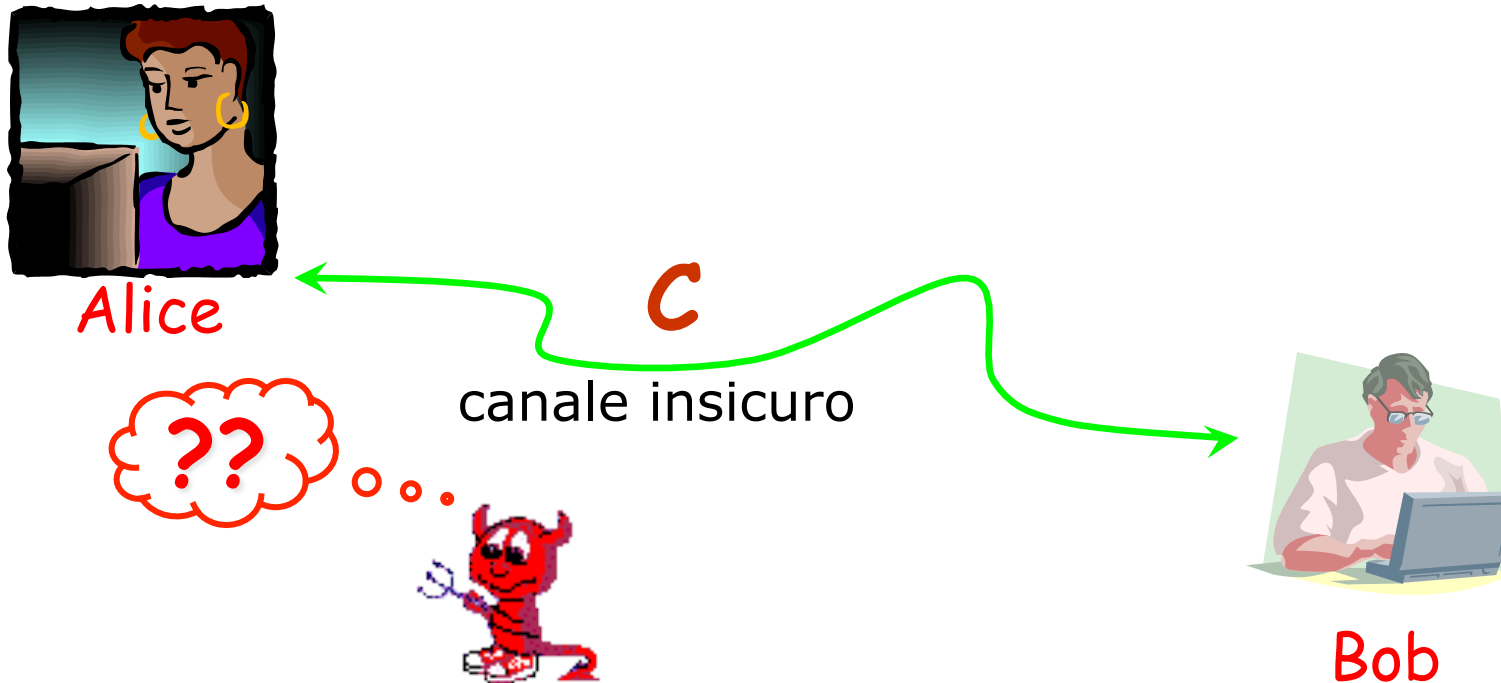


Chosen Plaintext Attack



L'avversario può ottenere la cifratura di testi in chiaro di sua scelta

Chosen Ciphertext Attack



L'avversario può ottenere la decifrazione di
testi cifrati di sua scelta

Known Ciphertext Attack

Cifrario a sostituzione

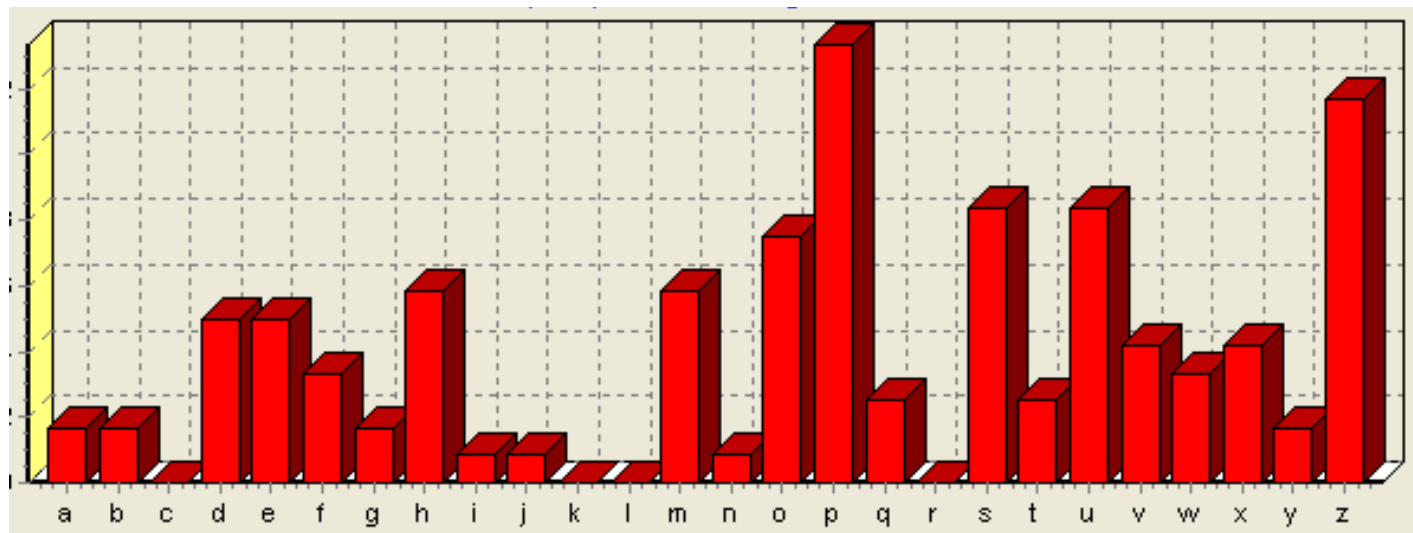
- Assumiamo che il testo in chiaro sia in lingua inglese, senza "spazi" e punteggiatura
- Esempio di testo cifrato:

UZQSOVUOHXMOPVGPOZPEVSGZWS
ZOPFPESXUDBMETSXAIZVUEPHZMD
ZSHZOWSFPAPPDTSVPQUZWYMXUZ
UHSXEPYEPOPDZSZUFPOMBZWPFUP
ZHMDJUDTMOHMQ

Known Ciphertext Attack

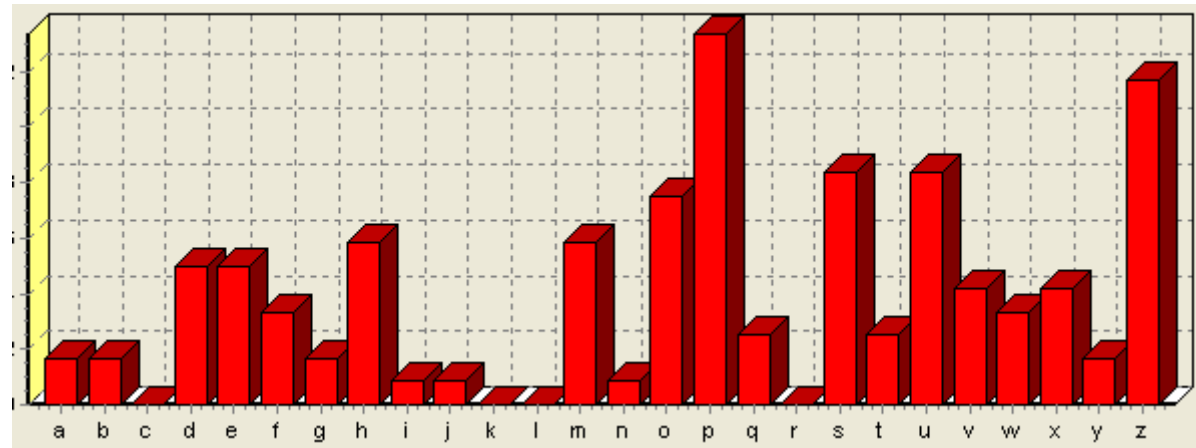
Cifrario a sostituzione

| | | | | | | | | | |
|---|-------|---|------|---|------|---|------|---|---|
| P | 13,33 | H | 5,83 | F | 3,33 | B | 1,67 | C | 0 |
| Z | 11,67 | D | 5,00 | W | 3,33 | G | 1,67 | K | 0 |
| S | 8,33 | E | 5,00 | Q | 2,50 | Y | 1,67 | L | 0 |
| U | 8,33 | V | 4,17 | T | 2,50 | U | 0,83 | N | 0 |
| O | 7,50 | X | 4,17 | A | 1,67 | J | 0,83 | R | 0 |
| M | 6,67 | | | | | | | | |



Known Ciphertext Attack

Cifrario a sostituzione



P = E? Z = T? Digramma più frequente: ZW ... TH?

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSX

T E E TE TH T E E

AIZVUEPHZMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

T E T T E EE E TH T

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

E E E T T E THE ET

Known Ciphertext Attack

Cifrario a sostituzione

Simboli con alta frequenza: S, U, O, M e H

Lettere inglesi con alta frequenza: a,i,n,o,r,s

Sequenza: TH_T ... se fosse una parola ... THAT ... S=A?

Lettera iniziale U seguita da T ... it,nt,ot,rt,st ... U=I?

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSX
IT A I E E TE A THAT E E A I
AIZVUEPHZMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
T I E TA T A E EE A E ITH ITI A
EPYEPOPDZSZUFPOMBZWPFPUPZHMDJUDTMOHMQ
E E E TATI E THE IET I

Known Ciphertext Attack

Cifrario a sostituzione

Sequenza: _ITH ... probabilmente è WITH ... Q=W?

Il messaggio inizia con: IT WA_ ... IT WAS? Quindi O=S?

Se si sa che si sta parlando del Vietcong ... la sequenza IET ... potrebbe far parte di VIETCONG

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSX
IT WAS DISCLOSED YESTERDAY THAT SEVERAL INFORMAL
AIZ VUEPHZ HMDZSHZOWSFPAPPD TSVP QUZWYMXUZUHSX
BUT DIRECT CONTACTS HAVE BEEN MADE WITH POLITICAL
EPYEPOPDZSZUFPOMBZWPFPUPZHMDJUDTMOHMQ
REPRESENTATIVES OF THE VIETCONG IN MOSCOW

Known Plaintext Attack

Cifrario di Hill

- Supponiamo di conoscere m coppie (P_j, C_j) dove $C_j = K \times P_j$
 - La chiave K è una matrice $m \times m$
- Si considerino le matrici
 - $X = (p_{ij})$ ogni riga ha uno dei testi in chiaro
 - $Y = (c_{ij})$ ogni riga ha uno dei testi cifrati
- $Y = K \times X$ e quindi $K = Y \times X^{-1}$
 - Se X non è invertibile occorrono altre coppie P_i/C_i fino ad avere X invertibile

Known Plaintext Attack

Cifrario di Hill

Sia **PQCFKU** la cifratura Hill di **FRIDAY** per $m=2$

➤ $FR=(5,17) \rightarrow PQ=(15,16)$

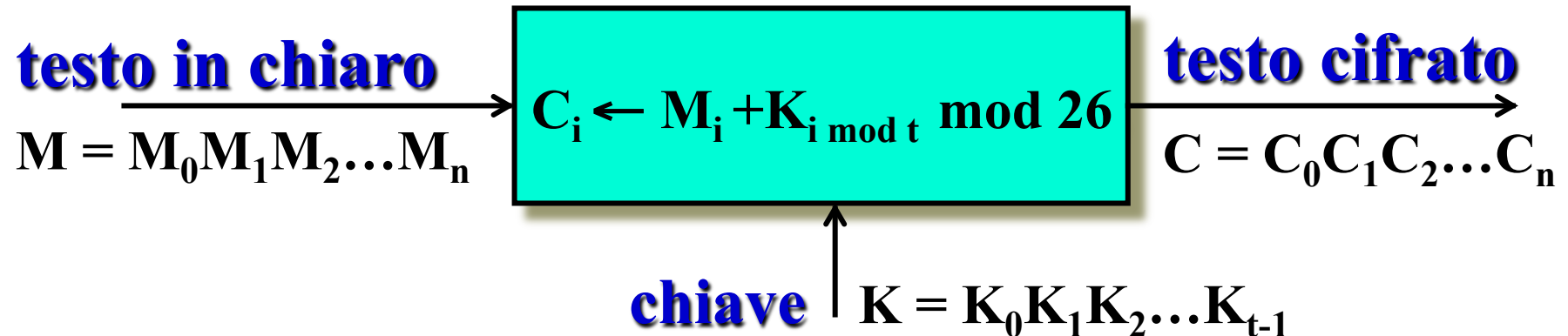
➤ $ID=(8,3) \rightarrow CF=(2,5)$

➤ Si ha
$$\underset{Y}{\begin{bmatrix} 15 & 2 \\ 16 & 5 \end{bmatrix}} = K \underset{X}{\begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}} \pmod{26}$$

➤
$$X^{-1} = \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} \quad K = Y \times X^{-1} = \begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$$

Cifrari a sostituzione polialfabetica

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

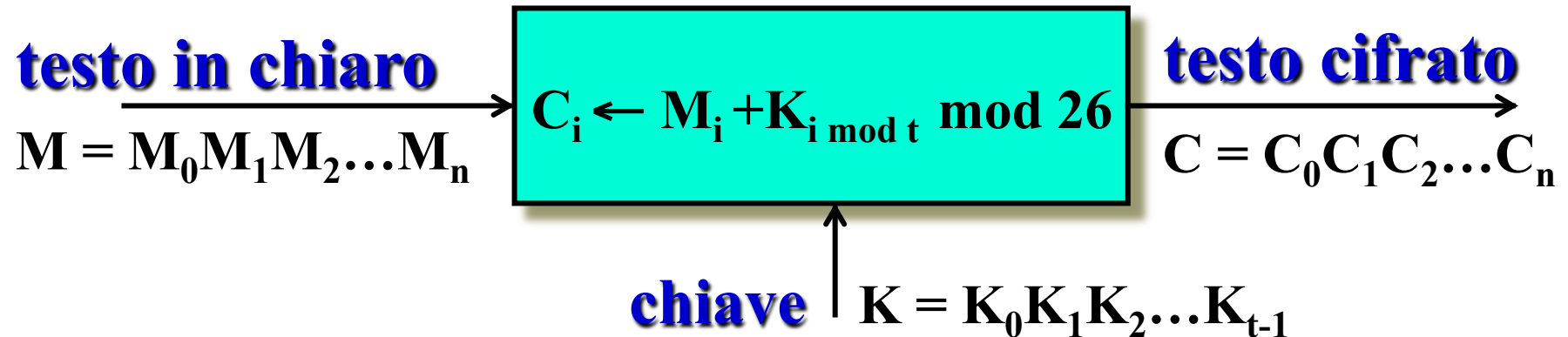


Testo in chiaro: CODICE MOLTO SICURO Chiave: REBUS
 CODIC EMOLT OSICU RO testo in chiaro
 REBUS REBUS REBUS RE chiave

 TSECU VQPFL FWJWM IS testo cifrato

Cifrari a sostituzione polialfabetica

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



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

Known Ciphertext Attack

Cifrario di Vigenère

- Determinare la lunghezza t della chiave
 - **Test di Kasiski**: studio delle ripetizioni
- Dividere il testo cifrato in t sottotesti
 - Ogni sottotesto corrisponde ad un cifrato con shift
- Effettuare l'analisi delle frequenze per ognuno dei sottotesti

Test di Kasiski

Friedrich Kasiski [1863]

testo cifrato ...WPIXFGHDAFNV TV... KLXFGLQ

Test di Kasiski

Friedrich Kasiski [1863]

testo cifrato ...WPIXFGHDAFNV TV... KLXFGLQ



XFG cifra lo stesso testo in chiaro!

Test di Kasiski

Friedrich Kasiski [1863]

testo cifrato ...WPIXFGHDAFNV TV... KLXFGLQ



XFG cifra lo stesso testo in chiaro!

La distanza tra le "X" è un multiplo di t

Test di Kasiski

Friedrich Kasiski [1863]

testo cifrato ...WPIXFGHDAFNV TV... KLXFGGLQ



XFG cifra lo stesso testo in chiaro!

La distanza tra le "X" è un multiplo di t

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

Test di Kasiski

Data la chiave RUN:

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------------|---|---|---|---|---|---|---|---|------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R | U | N | R | U | N | R | U | N | R | U | N | R | U | N | R | U | N | R | U | N | R | U | N | | | |
| t | o | b | e | o | r | n | o | t | t | o | b | e | t | h | a | t | i | s | t | h | e | q | u | e | s | t |
| K | I | O | V | I | E | E | I | G | K | I | O | V | N | U | R | N | V | J | N | U | V | K | H | V | M | G |
| ← 9 characters → | | | | | | | | | ← 6 characters → | | | | | | | | | | | | | | | | | |

ogni volta che la stringa RUNR cifra la stringa
to be, si ha lo stesso testo cifrato KIOV

$\text{gcd}(9,6)=3$ è un multiplo di t

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

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: $IC(\text{MONO}) = 1/6$

$IC(\text{ALFA}) = 1/6$

$IC(\text{GAMMA}) = 2/24 = 1/12$

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

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

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

è il numero di modi
di scegliere un
sottoinsieme di k
oggetti da un
insieme di n oggetti

f_i = numero occorrenze carattere i

Indice di coincidenza

Se $x_1x_2\dots x_n$ è un testo in Inglese

$$\text{Allora } IC(x_1x_2\dots x_n) \approx \sum_{i=0}^{25} p_i^2 = 0.065$$

p_i = probabilità carattere i in Inglese

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 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_0 | p_1 | p_2 | p_3 | p_4 | p_5 | p_6 | p_7 | p_8 | p_9 | p_{10} | p_{11} | p_{12} | p_{13} | p_{14} | p_{15} | p_{16} | p_{17} | p_{18} | p_{19} | p_{20} | p_{21} | p_{22} | p_{23} | p_{24} | p_{25} |

Infatti, la probabilità che

- entrambi siano AA è p_0p_0
- entrambi siano BB è p_1p_1
- ...

Indice di coincidenza

Se $x_1x_2\dots x_n$ è un testo in Inglese

$$\text{Allora } IC(x_1x_2\dots x_n) \approx \sum_{i=0}^{25} p_i^2 = 0.065$$

p_i = probabilità carattere i in Inglese

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 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_0 | p_1 | p_2 | p_3 | p_4 | p_5 | p_6 | p_7 | p_8 | p_9 | p_{10} | p_{11} | p_{12} | p_{13} | p_{14} | p_{15} | p_{16} | p_{17} | p_{18} | p_{19} | p_{20} | p_{21} | p_{22} | p_{23} | p_{24} | p_{25} |

Se $x_1x_2\dots x_n$ sono caratteri scelti a caso

$$\text{Allora } IC(x_1x_2\dots x_n) \approx \sum_{i=0}^{25} \left(\frac{1}{26}\right)^2 = 0.038$$

Indice di coincidenza

Se $x_1x_2\dots x_n$ è un testo in Italiano

$$\text{Allora } IC(x_1x_2\dots x_n) \approx \sum_{i=0}^{25} p_i^2 = 0.075$$

p_i = probabilità carattere i in Inglese

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 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_0 | p_1 | p_2 | p_3 | p_4 | p_5 | p_6 | p_7 | p_8 | p_9 | p_{10} | p_{11} | p_{12} | p_{13} | p_{14} | p_{15} | p_{16} | p_{17} | p_{18} | p_{19} | p_{20} | p_{21} | p_{22} | p_{23} | p_{24} | p_{25} |

Se $x_1x_2\dots x_n$ sono caratteri scelti a caso

$$\text{Allora } IC(x_1x_2\dots x_n) \approx \sum_{i=0}^{25} \left(\frac{1}{26}\right)^2 = 0.038$$

Ipotesi $t=1$?



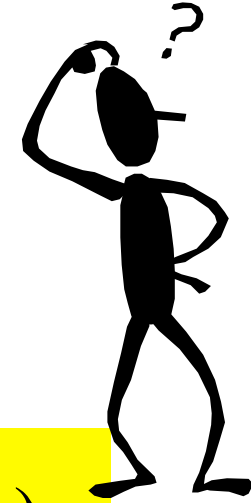
testo cifrato $C_0C_1\dots C_n$

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

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

Comunque lontano da 0.075

Ipotesi $t=2$?



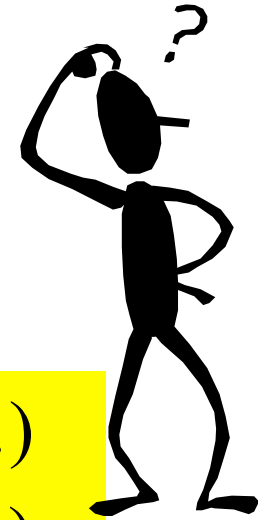
testo cifrato $C_0C_1\dots C_n$

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

$$\begin{cases} IC(C_0C_2\dots) \approx 0.075 & \text{se } t=2 \\ IC(C_1C_3\dots) \approx 0.038 & \text{se } t \neq 2 \end{cases}$$

Comunque lontano da 0.075

Ipotesi $t=3$?



testo cifrato $C_0C_1\dots C_n$

Se $t = 3$ allora $IC(C_0C_3\dots) = IC(M_0M_3\dots)$

$IC(C_1C_4\dots) = IC(M_1M_4\dots)$

$IC(C_2C_5\dots) = IC(M_2M_5\dots)$

$$\begin{array}{l} IC(C_0C_3\dots) \approx \\ IC(C_1C_4\dots) \approx \\ IC(C_2C_5\dots) \approx \end{array} \left\{ \begin{array}{ll} 0.075 & \text{se } t=3 \\ 0.038 & \text{se } t \neq 3 \end{array} \right.$$

Comunque lontano da 0.075

Esempio

RLEYFBDOQSMCATCEZCBAPTHRJPCGRONVZMCHZOEBPKRNRVVCNHFEEACOZNGS
SIOGHFUIZCOKIGIUKONGFEIRUPCFVOTVCBBERDRZMFSCCSXEESFUEYFJVNGF
BIEQWRLEYZJMIRBRLAFWBLNGFBKTBO SVSGFJEGRFTZENDSVNQSSSTOEGPVFVU
VIAQWGZUZSUIAHBQIOZCOKOEWRDRGUIARIORMCWBT OFHJVRNRBCLNZUIACO
SKERWMGOAHFTHRWWZCBBHZUAUFCEQIFIIISQRRPVFIEARB JAZQPIPVITVNFV
CZLROMCOPQIZODIFJTNHSRSSCSDAMWPEERGF XNVWVGUAHPZNP IJZLYOHFCRG
TREYOEUA EWDFMVB DZACSS IICWHCINFQFIACNVDVZBXOQCWV LRFJMENZMFNGO
ORNQCTZDVBVFBZBJCVOOCAPEVRDVGUVNQSSJIRFBCLRBURRFWJENHCWZGBZ
GZEVBOLOIWTVNVZBT OFHJVRNTPIMNHB UAYRFGOFWUFDVHSVGECTJIGCSIEAH
JJCRBEVACDPXGVOURAQIFDOAHJTOAHJXUVZVEOQSUKOVZTRNZOSKIACMRLGF
PTOAJPTEYCNSAERBZLESTVGBBFUAVAPCTVQPTUMNPCIVBGZLNQIVIAJFIOYC
GRNACTFMVUMZAE SBLNNGFXAGOMTHRBPEEPVJRLCFJDOISEVRYCQLRPVFJINR
JWRBBUVCBAFGEESTVMCWPUIFIMVMHFBUIZWMRNBQIVGHOSUAACBJEGHFETEW
PEEACOCOQWTTEEBBKOFHPRUAHBCCBBUIAFGF XNBWOHURZMRLH BHREIOTKATW
PXAVOERGYWBCTEWNFNNGWEZNB AFGIHCTTUECFUI SCSDACWVTOZIOVPRFVEBHC
OGEMNPCAPCTKAFOMVCBBVEPRBEZOYSOKORQPETVBVFPBWTZRBAQVIADPXGVS
JEVNZMFNPSMCIVBFITRSJEIFDJRNHFJEPCOUOYCTJAGISRDRRVMMBBUZEZVZ

Indice di coincidenza

□ $t = 1 ?$

$$IC(C_0 C_1 \dots C_n) = 0.045$$

Indice di coincidenza

$$\begin{array}{l} \square t = 1 ? \quad IC(C_0 C_1 \dots C_n) = 0.045 \\ \square t = 2 ? \quad \left\{ \begin{array}{l} IC(C_0 C_2 \dots) = 0.0463 \\ IC(C_1 C_3 \dots) = 0.0438 \end{array} \right. \end{array}$$

Indice di coincidenza

| | |
|------------------------------------|---|
| <input type="checkbox"/> $t = 1 ?$ | $IC(C_0 C_1 \dots C_n) = 0.045$ |
| <input type="checkbox"/> $t = 2 ?$ | $\left\{ \begin{array}{l} IC(C_0 C_2 \dots) = 0.0463 \\ IC(C_1 C_3 \dots) = 0.0438 \end{array} \right.$ |
| <input type="checkbox"/> $t = 3 ?$ | $\left\{ \begin{array}{l} IC(C_0 C_3 \dots) = 0.0431 \\ IC(C_1 C_4 \dots) = 0.0459 \\ IC(C_2 C_5 \dots) = 0.0456 \end{array} \right.$ |

Indice di coincidenza

| | |
|------------------------------------|---|
| <input type="checkbox"/> $t = 1 ?$ | $IC(C_0 C_1 \dots C_n) = 0.0445$ |
| <input type="checkbox"/> $t = 2 ?$ | $\left\{ \begin{array}{l} IC(C_0 C_2 \dots) = 0.0463 \\ IC(C_1 C_3 \dots) = 0.0438 \end{array} \right.$ |
| <input type="checkbox"/> $t = 3 ?$ | $\left\{ \begin{array}{l} IC(C_0 C_3 \dots) = 0.0431 \\ IC(C_1 C_4 \dots) = 0.0459 \\ IC(C_2 C_5 \dots) = 0.0456 \end{array} \right.$ |
| <input type="checkbox"/> $t = 4 ?$ | $\left\{ \begin{array}{l} IC(C_0 C_4 \dots) = 0.0448 \\ IC(C_1 C_5 \dots) = 0.0421 \\ IC(C_2 C_6 \dots) = 0.0495 \\ IC(C_3 C_7 \dots) = 0.0437 \end{array} \right.$ |

Indice di coincidenza

□ $t = 5$?

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

Tutti vicini a 0.075

$t = 5$

Cifrario di Vigenère: Crittoanalisi

- Determinare la lunghezza della chiave t
 - uso dell'indice di coincidenza
- Determinare il valore della chiave $K_0K_1K_2\dots K_{t-1}$
 - uso dell'indice mutuo di coincidenza
 - K_0 usato per $C_0 C_t C_{2t} \dots$
 - K_1 usato per $C_1 C_{t+1} C_{2t+1} \dots$
 - ...
 - K_{t-1} usato per $C_{t-1} C_{2t-1} C_{3t-1} \dots$

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

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

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

$IMC(ALFA;GAMMA) = 4/20$

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

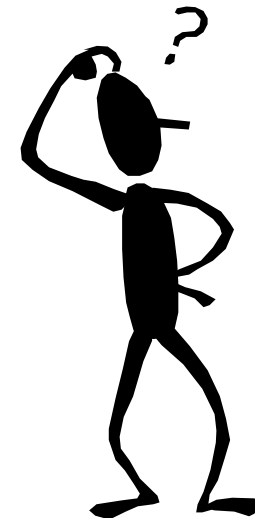
$$= \frac{\sum_{i=0}^{25} f_i \cdot f'_i}{n \cdot n'}$$

f_i = numero occorrenze carattere "i" in $x_1x_2\dots x_n$

f'_i = numero occorrenze carattere "i" in $y_1y_2\dots y_{n'}$

Indice mutuo di coincidenza

Quale è il valore medio di $IMC(C_0C_+C_{2+}\dots; C_1C_{+1}C_{2+1}\dots)$?



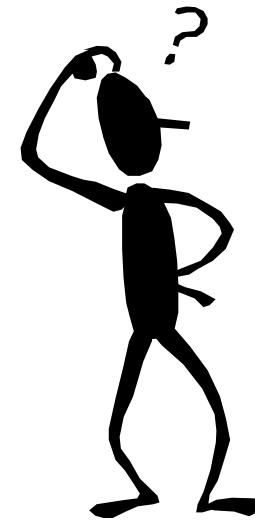
Indice mutuo di coincidenza

Quale è il valore medio di $IMC(C_0 C_+ C_{2+} \dots; C_1 C_{+1} C_{2+1} \dots)$?

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

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

...



Indice mutuo di coincidenza

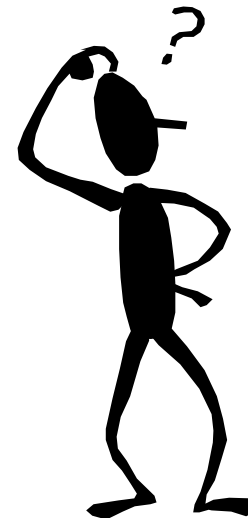
Quale è il valore medio di $IMC(C_0 C_1 C_2 \dots; C_1 C_{+1} C_{2+1} \dots)$?

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 = $p_{2-K_0} p_{2-K_1}$

...



Indice mutuo di coincidenza

Quale è il valore medio di $\text{IMC}(C_0 C_t C_{2t} \dots; C_1 C_{t+1} C_{2t+1} \dots)$?

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 = $p_{2-K_0} p_{2-K_1}$

...

$$\begin{aligned} \text{IMC}(C_0 C_t C_{2t} \dots; C_1 C_{t+1} C_{2t+1} \dots) \\ \approx \sum_{i=0}^{25} p_{i-K_0} p_{i-K_1} = \sum_{h=0}^{25} p_h p_{h+K_0-K_1} \end{aligned}$$

Dipende solo dallo shift relativo delle due stringhe: $K_0 - K_1 \pmod{26}$

Uno shift relativo di ℓ ha la stessa stima di $26 - \ell$ infatti: $\sum_{h=0}^{25} p_h p_{h+\ell} = \sum_{h=0}^{25} p_h p_{h-\ell}$

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

Indice mutuo di coincidenza

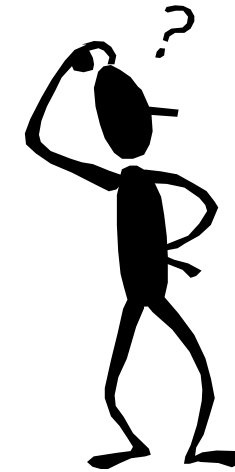
| valore di K_0-K_1 | media IMC |
|------------------------|--------------|
| 0 | 0.075 |
| 1, 25 | 0.033 |
| 2, 24 | 0.034 |
| 3, 23 | 0.034 |
| 4, 22 | 0.047 |
| 5, 21 | 0.027 |
| 6, 20 | 0.032 |
| 7, 19 | 0.026 |
| 8, 18 | 0.027 |
| 9, 17 | 0.023 |
| 10, 16 | 0.024 |
| 11, 15 | 0.027 |
| 12, 14 |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

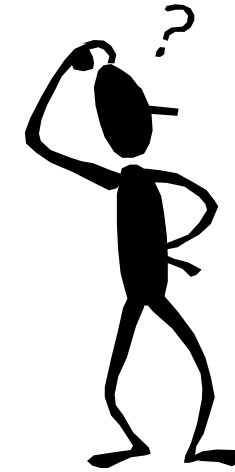
Ipotesi $K_0 - K_1 = 0$?



testo cifrato $C_0 C_1 \dots C_n$

Se $K_0 - K_1 = 0$ allora $\text{IMC}(C_0 C_t \dots; C_1 C_{t+1} \dots) \approx 0.075$

Ipotesi $K_0 - K_1 = 0$?

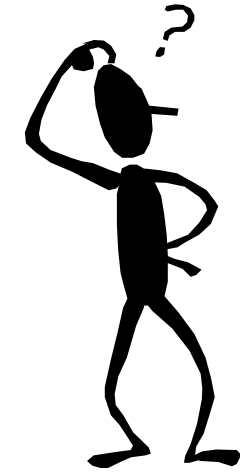


testo cifrato $C_0 C_1 \dots C_n$

Se $K_0 - K_1 = 0$ allora $\text{IMC}(C_0 C_t \dots; C_1 C_{t+1} \dots) \approx 0.075$

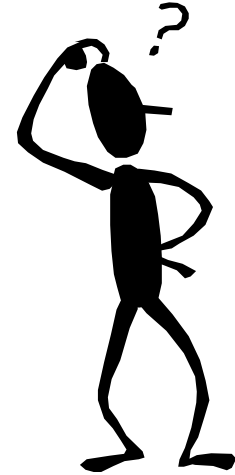
$$\text{IMC}(C_0 C_t \dots; C_1 C_{t+1} \dots) \begin{cases} \approx 0.075 & \text{se } K_0 - K_1 = 0 \\ \approx 0.047 & \text{se } K_0 - K_1 \neq 0 \end{cases}$$

Ipotesi $K_0 - K_1 = 1$?



testo cifrato $C_0C_1\dots C_n$

Ipotesi $K_0 - K_1 = 1$?



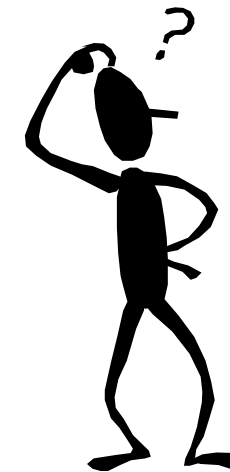
testo cifrato $C_0 C_1 \dots C_n$

$$Y_i \leftarrow C_i - 1 \pmod{26}$$

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

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

Ipotesi $K_0 - K_1 = 2$?



testo cifrato $C_0 C_1 \dots C_n$

Ipotesi $K_0 - K_1 = 2$?



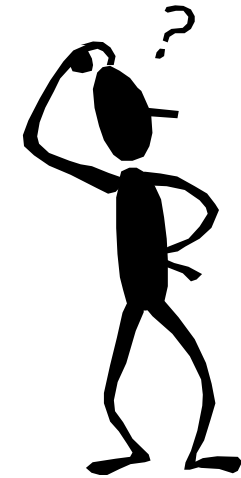
testo cifrato $C_0C_1\dots C_n$

$$Y_i \leftarrow C_i - 2 \pmod{26}$$

Se $K_0 - K_1 = 1$ allora $\text{IMC}(Y_0Y_t\dots; C_1C_{t+1}\dots) \approx 0.075$

$$\text{IMC}(Y_0Y_t\dots; C_1C_{t+1}\dots) \begin{cases} \approx 0.075 & \text{se } K_0 - K_1 = 2 \\ \approx 0.047 & \text{se } K_0 - K_1 \neq 2 \end{cases}$$

Ipotesi $K_0 - K_1 = 3$?



testo cifrato $C_0C_1\dots C_n$

$$Y_i \leftarrow C_i - 3 \pmod{26}$$

Se $K_0 - K_1 = 1$ allora $\text{IMC}(Y_0Y_t\dots; C_1C_{t+1}\dots) \approx 0.075$

$$\text{IMC}(Y_0Y_t\dots; C_1C_{t+1}\dots) \begin{cases} \approx 0.075 & \text{se } K_0 - K_1 = 3 \\ \approx 0.047 & \text{se } K_0 - K_1 \neq 3 \end{cases}$$

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 !



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 ?



Determinare la chiave

➤ $K_0 - K_1 = 5$

➤ $K_1 - K_2 = 6$

➤ $K_2 - K_3 = 9$

➤ ...

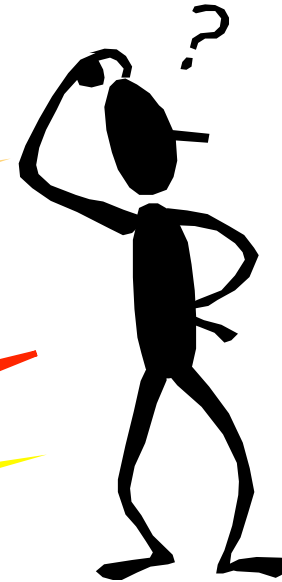
➤ $K_{t-2} - K_{t-1} = 5$

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 !



Cifrario di Vigenère: Crittoanalisi

- ❑ Determinare la lunghezza della chiave t
 - uso dell'indice di coincidenza
- ❑ Determinare il valore della chiave $K_0K_1K_2\dots K_{t-1}$
 - 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

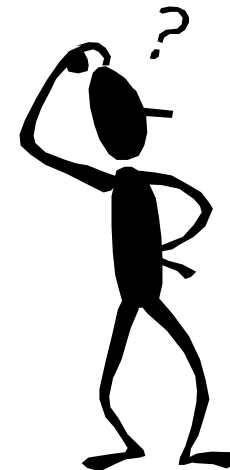
Esempio: Determinare la chiave

$K_1 - K_0$

Ipotesi $K_1 - K_0 = 0$

| | | | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| .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 | |

Ipotesi $K_1 - K_0 = 25$



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 | |

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 | |

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 | |

Esempio: Determinare la chiave

$K_0 - K_1 = 10$

$K_0 - K_2 = 1$

$K_0 - K_3 = 14$

$K_0 - K_4 = 13$

$K_1 - K_2 = 17$

$K_1 - K_3 = 4$

$K_1 - K_4 = 3$

$K_2 - K_4 = 12$

$K_2 - K_3 = 13$

$K_3 - K_4 = 25$

Esempio: Determinare la chiave

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

Eliminare le dipendenze lineari

Esempio: $K_0 - K_3 = 14$
è linearmente dipendente da
 $K_0 - K_1 = 10$ e $K_1 - K_3 = 4$

Esempio: Determinare la chiave

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

$$K_1 = K_0 - 10$$

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

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

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

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

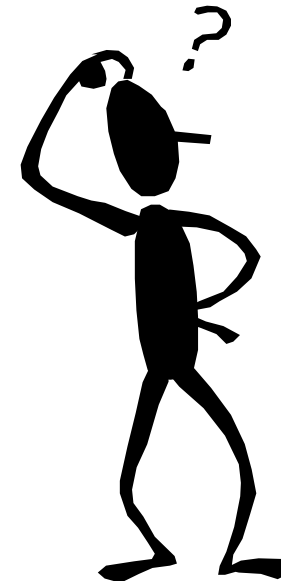
Esempio: Testo in chiaro

QUELRAMODELLAGODICOMOCHEVOLGEAMEZZOGIORNOTRADUECATENENONINTE
RROTTE DIMONTITUTTOASENIEGOLFIASECONDADELLOSPORGEREEDELRIENTR
AREDIQUELLIVIENQUASIAUNTRATTOARESTRINGERSIEAPRENDERCORSOEFIG
URADIFIUMETRAUNPROMONTORIOADESTRAEUNAMPIACOSTIERADALLALTRAPA
RTEEILPONTECHEIVICONGIUNGELEDUERIVEPARCHERENDASAMCORPIUSENSI
BILEALLOCCHIOQUESTATRASFORMAZIONE ESEGNILPUNTOINCUIILLAGOCES
SAELADDARICOMINCIAPERRIPIGLIARPOINOMEDILAGODOVELERIVEALLONTA
NANDOSIDINUOVOLASCIANLACQUADISTENDERSIERALLENTARSIINNUOVIGOL
FIEINNUOVISENILACOSTIERAFORMATADALDEPOSITODITREGROSSITORRENT
ISCENDEAPPOGGIATAADUEMONTICONTIGUILUNODETTOILSANMARTINOLALTR
OCONVOCELOMBARDAILRESEGONEDAIMOLTICOCUZZOLIINFILACHEINVEROLO
FANNOSOMIGLIAREAUNA SEGATALCHENONECHIALPRIMOVERDERLOPURCHESIAD
IFRONTECOME PERESEMPIODISULEMURADIMILANO CHEGUARDANOASETTE TRI
ONENONLODISCERNATOSTOAUNTALCONTRASSEGNOINQUELLALUNGAEVASTAGI
OGAIADAGLIALTRIMONTIDINOMEPIUOSCUROEDIFORMAPIUCOMUNEPERUNBUO
NPEZZOLACOSTASALECONUNPENDIOLENTOECONTINUOPOISIROMPEINPOGGIE
IN VALLONCELLIINERTEEINISPIANATESECONDOLOSSATURADEDUEMONTIEIL

Esercizio

Resistenza del Cifrario di Vigenère rispetto a

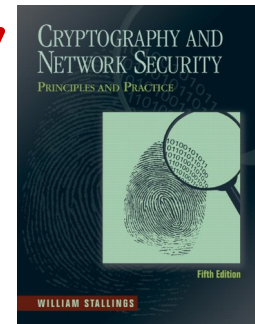
Known Plaintext Attack



Bibliografia

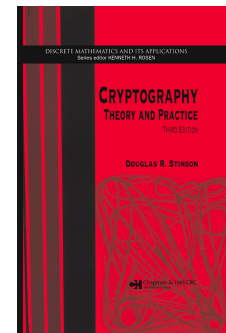
- **Cryptography and Network Security**
by W. Stallings, 2010

- cap. 2



- **Cryptography: Theory and Practice,**
by D. Stinson (2005)

- cap. 1



- Tesina su crittografia classica

- <http://www.dia.unisa.it/professori/ads/>

- Sicurezza su reti, a.a. 1995-1996

Domande?

