Introduzione alla crittografia

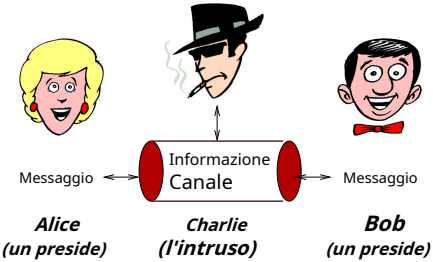
Alessandro Armando

Laboratorio di sicurezza informatica (CSec)
DIBRIS, Università di Genova

Sicurezza del computer

Contorno

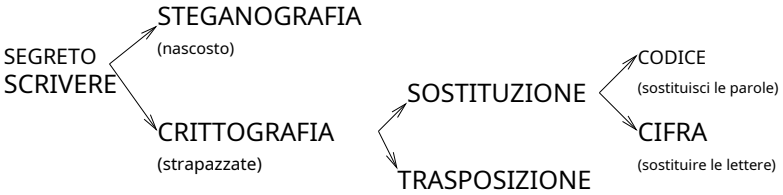
Di cosa si tratta?



- Come ci rivolgiamo? canali inaffidabili in affidabile quelli?

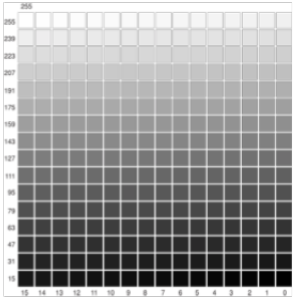
  Riservatezza: Le informazioni trasmesse rimangono segrete.
  Integrità: Informazioni non danneggiate (o rilevate alterazioni).
  Autenticazione: I dirigenti sanno con chi stanno parlando.

- Altri obiettivi desiderabili. Ad esempio, non ripudio.
- La crittografia è la tecnologia abilitante.

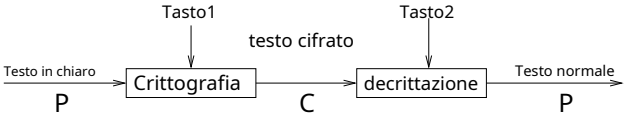


- crittologia: lo studio della scrittura segreta.
- Steganografia: la scienza di nascondere i messaggi in altri messaggi.
- Crittografia: la scienza della scrittura segreta.

Steganografia



Schema crittografico generale



dove $E_{chiave_1}(P) = C$, $D_{chiave_2}(C) = P$

- **La sicurezza dipende dalla segretezza della chiave, non dall'algoritmo**
- Simmetrico algoritmi
  - Key1 = Key2, o sono facilmente derivabili l'uno dall'altro.
- Asimmetrico o chiave pubblica algoritmi
  - Chiavi diverse, che non possono essere derivate l'una dall'altra.Chiave
  - pubblica può essere pubblicato senza compromessi chiave privata.
- La crittografia e la decrittografia dovrebbero essere facili, se le chiavi sono note.

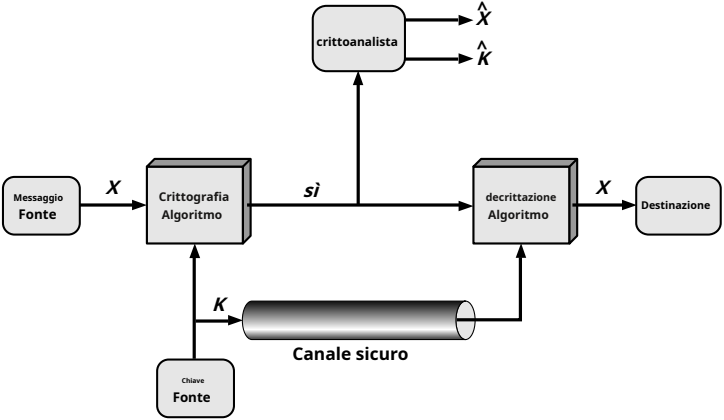
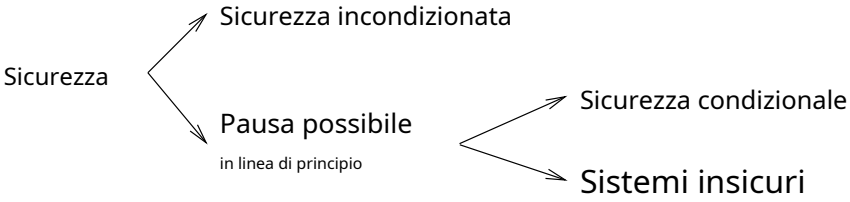


Figura 2.2 Modello di crittografia simmetrica

Classificazione di sicurezza



Sicurezza incondizionata: Il sistema è sicuro anche se l'avversario ha un computing illimitato potere poiché il testo cifrato fornisce informazioni insufficienti per determinare in modo univoco il corrispondente testo in chiaro. Sicurezza misurata utilizzandoteoria dell'informazione.

Sicurezza condizionale: Il sistema può essere rotto in linea di principio, ma questo richiede di più potenza di calcolo di quella che avrebbe un avversario realistico. Sicurezza misurata utilizzandoteoria della complessità.

Criptoanalisi

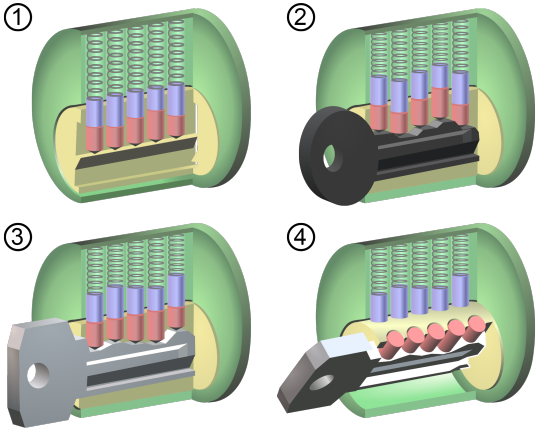
- Crittoanalisi: scienza del recupero del testo in chiaro dal testo cifrato senza la chiave.
- Ma l'obiettivo tipico è recuperare la chiave non solo il
- messaggio Approcci generali:
  - attacco di forza bruta
  - attacco crittoanalitico

Attacco a forza bruta

- È sempre possibile: prova semplicemente ogni chiave Il suo costo
- (molto) dipende dalla dimensione della chiave
- Presuppone che il testo in chiaro sia noto o riconoscibile

Dimensione chiave (bit)	Numero di chiavi	Tempo richiesto a 1 decrittazione/μS	Tempo richiesto alle 10_6 decrittazioni/μS
32	$2_{32} = 4.3 \times 10_9$	$2_{31}\mu$s=35,8 minuti $2_{55}\mu$	2,15 ms
56	$2_{56} = 7.2 \times 10_{16}$	s=1142 anni $2_{127}\mu$s=5.4	ore 10.01
128	$2_{128} = 3.4 \times 10_{38}$	$\times 10_{24}$ anni $2_{167}\mu$s=5.9 $\times 10$	5.4 $\times 10_{18}$ anni 5.
168	$2_{168} = 3.7 \times 10_{50}$	$_{36}$ anni 2 $\times 10_{26}\mu$s=6.4 $\times 10$	9 $\times 10_{30}$ anni 6.4
26 caratteri (permuta.)	$26! = 4 \times 10_{26}$	$_{12}$ anni	$\times 10_6$ anni

Analogia con la sicurezza fisica: serratura a chiave Tumbler



Analogia con la sicurezza fisica: casseforti

- La sicurezza delle casseforti è valutata in base al grado di protezione fornito contro un tentativo di attacco con scasso.
- Classe TL-X (per $X = 15, 30, 40$):[1]

  La porta resiste con successo all'ingresso per X minuti [...] quando viene attaccata con comuni utensili manuali, strumenti di raccolta, utensili elettrici meccanici o portatili, punte di molatura, trapani in metallo duro e dispositivi o meccanismi di applicazione della pressione.

- supponendo che[2]

  il laboratorio riceve preventivamente le planimetrie dei campioni da testare affinché la volta, la sua struttura, la sua composizione, il suo assemblaggio ed eventuali punti deboli possano essere approfonditi preventivamente

[1] https://www.safeandvaultstore.com/pages/burglary-ratings
[2] https://www.bunkerkit.com/en/performances/vault/

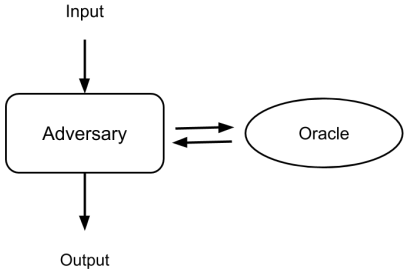
Modello di attacco

Possiamo pensare all'avversario come a un gioco:

Ingresso: Qualunque avversario necessariamente conosce fin dall'inizio, ad es. chiave pubblica, distribuzione di testi in chiaro, ecc.

Oracolo: Informazioni sui modelli avversario può ottenere durante un attacco. Diversi tipi di informazioni caratterizzano diversi tipi di attacchi.

Produzione: Qualunque cosa voglia l'avversario per calcolare, ad esempio, chiave segreta, informazioni parziali su testo normale, ecc. Vince se riesce.

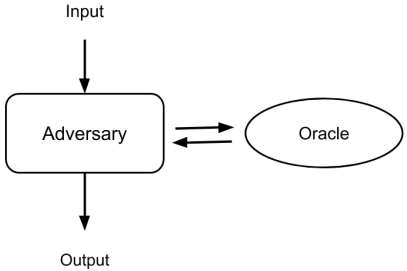


Tipi di attacchi

- **Solo testo cifrato**
  - **Dato:** $C_1 = E_K(m_1), \ldots, C_n = E_K(m_n)$
  - **Dedurre:** $m_1, \ldots, m_n$ o algoritmo per calcolare m_{n+1} a partire dal $C_{n+1} = E_K(m_{n+1})$
- **Testo in chiaro conosciuto**
  - **Dato:** $m_1, C_1 = E_K(m_1), \ldots, m_n, C_n = E_K(m_n)$
  - **Dedurre:** Chiave inversa o algoritmo da calcolare m_{n+1} a partire dal $C_{n+1} = E_K(m_{n+1})$
- **Testo in chiaro scelto** Come sopra ma il crittoanalista può scegliere $m_1, \ldots, m_n$.
- **Testo in chiaro adattivo scelto** Il crittoanalista non solo può scegliere il testo in chiaro, ma può modificare il testo in chiaro in base ai risultati della crittografia.
- **Testo cifrato scelto** Il crittoanalista può scegliere diversi testi cifrati da decifrare e ottiene l'accesso al testo in chiaro decifrato.

Come costruire una definizione di sicurezza

1. Specifica un oracolo (un tipo di attacco).
2. Definisci cosa deve fare l'avversario per vincere la partita, cioè una condizione sulla sua uscita.
3. Il sistema è sicuro secondo la definizione, se presente efficiente l'avversario vince la partita con solo trascurabileprobabilità.



Contorno

Crittografia/decrittografia

- *UN*, il alfabeto, è un insieme finito.
- $M \subseteq A^?$ è il spazio messaggi. *m M* è un testo in chiaro (messaggio). *C* è il
- spazio del testo cifrato, il cui alfabeto può differire da *m*. *K* denota la
- spazio chiave di chiavi.
- Ogni *e K* determina una funzione biunivoca da *m* a *C*, denotato da E_e. E_e è il funzione di crittografia (o trasformazione).
- Per ciascuno *D K*, D_D denota una biiezione da *C* a *m*. D_D è il funzione di decrittazione.
- applicando E_e (o D_D) è chiamato crittografia (o decrittazione).

Crittografia/decrittografia (segue)

- Un schema di crittografia (o cifra) consiste in un insieme $\{E_e : e\ K\}$ e un insieme corrispondente $\{D_D : D\ K\}$ con la proprietà che per ciascuno $e\ K$ c'è un unico $D\ K$ tale Quello $D_D = E_e$; cioè,

$$D_D(E_e(m)) = m \qquad \text{per tutti } m\ M.$$

- I tasti e e D sopra forma a coppia di chiavi, talvolta indicato con (e, d). Possono essere identici (es.il chiave simmetrica).

- Per costruire uno schema di crittografia richiede la correzione di uno spazio per i messaggi m, uno spazio di testo cifrato C, e uno spazio chiave K, così come le trasformazioni di crittografia $\{E_e : e\ K\}$ e corrispondenti trasformazioni di decrittazione $\{D_D : D\ K\}$.

Un esempio

Permettere $m = \{m_1, m_2, m_3\}$ e $C = \{C_1, C_2, C_3\}$. Ce ne sono 3! = 6 biiezioni da m a C. Lo spazio chiave $K = \{1, 2, 3, 4, 5, 6\}$ specifica queste trasformazioni.

$$
\begin{array}{lll}
E_1 & E_2 & E_3 \\
m_1 \to C_1 & m_1 \to C_1 & m_1 \to C_2 \\
m_2 \to C_2 & m_2 \to C_3 & m_2 \to C_1 \\
m_3 \to C_3 & m_3 \to C_2 & m_3 \to C_3 \\
\\
E_4 & E_5 & E_6 \\
m_1 \to C_2 & m_1 \to C_3 & m_1 \to C_3 \\
m_2 \to C_3 & m_2 \to C_1 & m_2 \to C_2 \\
m_3 \to C_1 & m_3 \to C_2 & m_3 \to C_1
\end{array}
$$

Supponiamo che Alice e Bob siano d'accordo sulla trasformazione E_6. Per crittografare m_1, Alice calcola $E_6(m_1) = C_3$. Bob decifra C_3 invertendo le frecce sul diagramma per E_6 e osservando che C_3 punta a m_1.

Contorno

Crittografia a chiave simmetrica

- Considera uno schema di crittografia $\{E_e : e \ K\}$ e $\{D_D : D \ K\}$. Lo schema è chiave simmetrica se per ogni coppia associata (e, d) è computazionalmente "facile" da determinare D solo sapendo e e per determinare e a partire dal D. In pratica $e = D$.
- Altri termini: tasto singolo, una chiave, chiave condivisa, e crittografia convenzionale. mittente e
- destinatario condividono una chiave comune
- tutti gli algoritmi di crittografia classici sono a chiave simmetrica (era l'unico tipo di crittografia prima dell'invenzione della chiave pubblica negli anni '70)
- di gran lunga il più utilizzato

Cifrari a blocchi, cifrari a flusso e codici

- UN cifrario a blocchi è uno schema di crittografia che suddivide il messaggio in chiaro in stringhe (blocchi) di lunghezza fissa T e crittografa un blocco alla volta.
- UN cifrario a flusso è uno in cui la lunghezza del blocco è 1. Al
- contrario, codici lavorare su parole di lunghezza variabile.

Codici

- Traduzione data da a 'libro dei codici'.

Parola	Codice
...	...
Il	**1701**
segreto	**5603**
guai	**4008**
Quello	**3790**
io	**2879**
set	**0524**
...	...

Codici

- Traduzione data da a 'libro dei codici'.

Parola	Codice
...	...
Il	**1701**
segreto	**5603**
guai	**4008**
Quello	**3790**
io	**2879**
set	**0524**
...	...

2327 6605 1702 9853 0001 0970 3190 8817 1320 0000 =1701 5603 4008
3790 2879 0524 7946 =
2879 2870 6699 1702 3982 5550 8102 7354 0000 =

Codici

- Traduzione data da a 'libro dei codici'.

Parola	Codice
...	...
Il	**1701**
segreto	**5603**
guai	**4008**
Quello	**3790**
io	**2879**
set	**0524**
...	...

2327 6605 1702 9853 0001 0970 3190 8817 1320 0000 = Faccio il male, e prima comincio a litigare.1701 5603 4008 3790 2879 0524 7946
2879 2870 6699 1702 3982 5550 8102 7354 0000 = Le marachelle segrete che ho messo a nudo= Mi metto alle dolorose accuse di altri.

(Riccardo III, atto I, scena 3)

Contorno

Cifrari a sostituzione semplice

- **KHOOR ZRUOG** = **CIAO MONDO**
  cifra di Cesare: ogni carattere di testo in chiaro è sostituito dal carattere tre a destra modulo 26.
- **Zl anzr vf Nqnz** = **Il mio nome è Adam**
  ROT13: sposta ogni lettera di 13 posti. Sotto Unix:
  tr a-zA-Z n-za-mN-ZA-M
- **2-25-5 2-25-5** = **CIAO CIAO**Alfanumerico:
  sostituire i numeri con le lettere.

Quanto sono difficili da crittare? Cesare? Generale?

Cifrari a sostituzione semplice

- **KHOOR ZRUOG** = **CIAO MONDO**
  cifra di Cesare: ogni carattere di testo in chiaro è sostituito dal carattere tre a destra modulo 26.
- **Zl anzr vf Nqnz** = **Il mio nome è Adam**
  ROT13: sposta ogni lettera di 13 posti. Sotto Unix:
  tr a-zA-Z n-za-mN-ZA-M
- **2-25-5 2-25-5** = **CIAO CIAO**Alfanumerico: sostituire i numeri con le lettere.

Quanto sono difficili da crittare? Cesare? Generale?

Cifrari a sostituzione semplice

- **KHOOR ZRUOG** = **CIAO MONDO**
  cifra di Cesare: ogni carattere di testo in chiaro è sostituito dal carattere tre a destra modulo 26.
- **Zl anzr vf Nqnz** = **Il mio nome è Adam**
  ROT13: sposta ogni lettera di 13 posti. Sotto Unix:
  tr a-zA-Z n-za-mN-ZA-M
- **2-25-5 2-25-5** = **CIAO CIAO**Alfanumerico: sostituire i numeri con le lettere.

Quanto sono difficili da crittare? Cesare? Generale?

Cifrari a sostituzione semplice

- **KHOOR ZRUOG** = **CIAO MONDO**
  cifra di Cesare: ogni carattere di testo in chiaro è sostituito dal carattere tre a destra modulo 26.
- **Zl anzr vf Nqnz** = **Il mio nome è Adam**
  ROT13: sposta ogni lettera di 13 posti. Sotto Unix:
  tr a-zA-Z n-za-mN-ZA-M
- **2-25-5 2-25-5** = **CIAO CIAO**Alfanumerico: sostituire i numeri con le lettere.

Quanto sono difficili da crittare? Cesare? Generale?

Cifrari a sostituzione semplice

- **KHOOR ZRUOG** = **CIAO MONDO**
  cifra di Cesare: ogni carattere di testo in chiaro è sostituito dal carattere tre a destra modulo 26.
- **Zl anzr vf Nqnz** = **Il mio nome è Adam**
  ROT13: sposta ogni lettera di 13 posti. Sotto Unix:
  tr a-zA-Z n-za-mN-ZA-M
- **2-25-5 2-25-5** = **CIAO CIAO**Alfanumerico:
  sostituire i numeri con le lettere.

Quanto sono difficili da crittare? Cesare? Generale?

CHIAVE	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva nffu nf
2	bgufs uif uphb qbsuz meet me after
3	the toga party ldds ld zesdq sgd snfz
4	ozqsx kccr kc ydrcp rfc rmey nyprw
5	jbbqync o btwzm qb xlxpanqbo ozqsx
6	uznyl Nby niau julns fxxm fx tymxk max
7	mhzt itkmr ewwl ew sxlwj LZW lgys
8	hsjlq dvvk dv rwkvi kyv kfxr grikp cuuj
9	cu qvjuh jxu jewq fqhjo btti bt puitg
10	IWT idvp epgin ASSH come othsf HVS
11	hcuo dofhm zrrg ZR nsgre Gur gbtn
12	cnegl yqqf YQ mrfqd FTQ FASM bmdfk
13	xppe xp lqepc esp ezrl alcej legno wo
14	kpdob dro dyqk zkbdi vnnc vn jocna
15	CQN cxpj yjach ummb um inbmz bpm
16	bwoi xizbg tlla tl hmaly aol avnh whyaf
17	skkz sk glzkx ZNK zumg vgxze rjjy rj
18	fkyjw ymj ytlf ufwyd qiix qi ejxiv xLI
19	xske tevxc
20	
21	
22	
23	
24	
25	

Figura 2.3 Crittoanalisi a forza bruta di Caesar Cipher

Cifrari a sostituzione monoalfabetica

- Idea chiave: generalizzare il cifrario di Cesare consentendo una sostituzione arbitraria.
- Permettere K essere l'insieme di tutte le permutazioni dell'alfabeto UN. Definisci per ciascuno e K una trasformazione della crittografia E_e sulle corde $m = m_1 m_2 \cdots m_n$ M come

$$E_e(m) = e(m_1)e(m_2) \cdots e(m_n) = C_1 C_2 \cdots C_n = C$$

- per decifrare C, calcola la permutazione inversa $D = e^{-1}$ e

$$D_D(C) = D(C_1)D(C_2) \cdots D(C_n) = m$$

- E_e è un cifrario a sostituzione semplice o un cifrario a sostituzione monoalfabetica.

Esempio:

Pianura:	**ABCDEFGHIJKLMNOPQRSTUVWXYZ**
Cifra:	**DKVQFIBJWPESCXHTMYAUOLRGZN**
Testo in chiaro:	**SEWEWEWISHTOREPLACELETTERS**
Testo cifrato:	**WIRFRWAJUHYFTSDVFSFUUFYA**

Esempio: cifrari affini

- Un *cifra affine* è un cifrario a sostituzione monoalfabetica tale che

$$e(m) = (un \cdot m + B) \text{ modalità } |A|$$

dove un e B sono numeri interi positivi e sono la chiave del cifrario.

- Affinché il cifrario sia invertibile, un e $|A|$ deve essere *relativamente primo*, ovvero l'unico intero positivo che divide entrambi deve essere 1.
- La funzione di decrittazione è

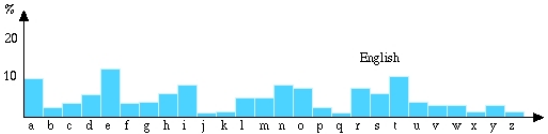
$$D(C) = un^{-1}(c - b) \bmod |A|,$$

dove un^{-1} è l'inverso moltiplicativo modulare di un modulo $|A|$, cioè soddisfa l'equazione

$$1 = un \cdot un^{-1} \text{modalità } |A|$$

(In)sicurezza dei cifrari a sostituzione

- Gli spazi chiave sono in genere enormi. 26 lettere $26!$ chiavi possibili.
- Tuttavia, possono essere facilmente decifrati utilizzando l'analisi della frequenza (lettere,
- digrammi, ecc.). Frequenze per l'inglese basate su libri/articoli di data mining.

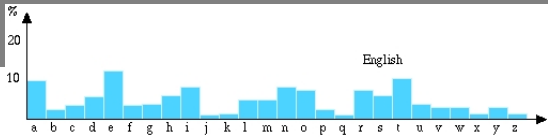


? Serdhrapvrf sbe Ratyvfu onfrq ba qngn-zvavat obbxf/negvpyrf. Facile

- da applicare, tranne che per testi brevi e atipici
  Da Zanzibar allo Zambia e allo Zaire, le zone di ozono fanno correre bizzarri zigzag alle zebre.

? Più sofisticatezza necessaria per mascherare le regolarità statistiche.

Esempio



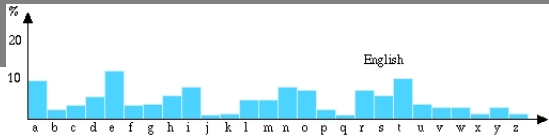
Dato il testo cifrato:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- Conta le frequenze relative delle lettere
- Da quando **P** e **Z** si verificano più frequentemente, immagino che corrispondano a **E** e **T** rispettivamente.
- Conta le frequenze dei diagrammi relativi.
- Da quando **Z W** si verifica più frequentemente, immagino che corrisponda a **NS** (che è il diagramma che ricorre più frequentemente in inglese)
- Quindi **ZWP** è **IL**
- Procedendo per tentativi ed errori finalmente ottieni:

E' STATO COMUNICATO IERI CHE SONO STATE AVVENUTI ALCUNI CONTATTI INFORMALI MA DIRETTI CON RAPPRESENTANTI POLITICI DEL VIET CONG A MOSCA

Esempio



Dato il testo cifrato:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- Conta le frequenze relative delle lettere
- Da quando **P** e **Z** si verificano più frequentemente, immagino che corrispondano a **E** e **T** rispettivamente.
- Conta le frequenze dei diagrammi relativi.
- Da quando **Z W** si verifica più frequentemente, immagino che corrisponda a **NS** (che è il diagramma che ricorre più frequentemente in inglese)
- Quindi **ZWP** è **IL**
- Procedendo per tentativi ed errori finalmente ottieni:

E' STATO COMUNICATO IERI CHE SONO STATE AVVENUTI ALCUNI CONTATTI INFORMALI MA DIRETTI CON RAPPRESENTANTI POLITICI DEL VIET CONG A MOSCA

Cifrari a sostituzione omofonica

- A ogni $un\ A$ associare un insieme $h(un)$ di stringhe di T simboli, dove $h(un)$, $un\ A$ sono disgiunti a coppie. UN cifrario a sostituzione omofonica sostituisce ciascuno un con una stringa scelta a caso da $h(un)$. Per decifrare una stringa C di T simboli, si deve determinare un un ? UN tale che C ? $h(un)$. La chiave per il cifrario sono gli insiemi $h(un)$.
- **Esempio:** $UN = \{x, y\}$, $h(X) = \{00, 10\}$, e $h(si) = \{01, 11\}$. Il testo in chiaro xy crittografa a uno di 0001, 0011, 1001, 1011.
- Razionale: rende più difficile l'analisi della frequenza. Costo: espansione dei dati e più lavoro per la decrittazione.

Cifrari a sostituzione polialfabetica

- Idea (Leon Alberti): nascondere la distribuzione utilizzando la famiglia di mappature.
- UN cifrario a sostituzione polialfabetica è un cifrario a blocchi con lunghezza di blocco T sopra l'alfabeto UN dove:
  - lo spazio chiave K consiste di sequenze di permutazioni su UN della forma $(e_1, \ldots, e_T)$.
  - Crittografia di $m = m_1 m_2 \cdots$ sotto chiave $e = (e_1, \cdots, e_T)$ è $E_e(m) = C_1 C_2 \cdots$, dove $C_{io} = e_{(io \bmod T)}(m_{io})$ per $io = 1, 2, \ldots$
  - Chiave di decrittazione per e è $D = (e_1^{-1}, \cdots, e_T^{-1})$.

Esempio: cifrari di Vigenère

- Le permutazioni sono definite in termini di una sequenza di numeri $K_1, \ldots, K_T$ nel seguente modo:

$$e_{io}(B) = (B + K_{io}) \text{ modalità } |A| \qquad \text{per tutti } B\ A \text{ e } io = 1, \ldots, T$$

- Esempio: inglese ($n = 26$), con $K = K_1, K_2, K_3$ insieme a $K_1 = 3$, $K_2 = 7$, e $K_3 = 10$:

$m =$ **THI SCI PHE RIS CER TAI NLY NOT SEC URE** $E_e(m) =$
WOS VJS SOO UPC FLB WHS QSI QVD VLM XYO

One-time pad (cifrario di Vernam)

- UN pad di una volta è un cifrario a flusso definito su $UN = \{0, 1\}$. Messaggio $m_1 \cdots m_n$ è crittografato da a *scelto a caso* stringa chiave binaria $K_1 \cdots K_n$.

$$E_{K_1 \cdots K_n}(m_1 \cdots m_n) = (m_1 ? K_1) \cdots (m_n ? K_n) (C$$
$$D_{K_1 \cdots K_n}(C_1 \cdots C_n) = {}_1 ? K_1) \cdots (C_n ? K_n)$$

- Esempio:

$$\begin{array}{rcl} m & = & 010111 \\ K & = & 110010 \\ \hline C & = & 100101 \end{array}$$

- Poiché ogni sequenza di tasti è ugualmente probabile, lo è anche ogni testo in chiaro!

  Sicurezza incondizionata (teorica dell'informazione), se la chiave non viene riutilizzata!

- La comunicazione Mosca-Washington in precedenza si assicurava in questo modo.
- Problema? Scambio e sincronizzazione di chiavi lunghe in modo sicuro.

One-time pad (cifrario di Vernam)

- UN pad di una volta è un cifrario a flusso definito su $UN = \{0, 1\}$. Messaggio $m_1 \cdots m_n$ è crittografato da a *scelto a caso* stringa chiave binaria $K_1 \cdots K_n$.

$$E_{K_1 \cdots K_n}(m_1 \cdots m_n) = (m_1 ? K_1) \cdots (m_n ? K_n) (C$$
$$D_{K_1 \cdots K_n}(C_1 \cdots C_n) = {}_1 ? K_1) \cdots (C_n ? K_n)$$

- Esempio:

$$\begin{array}{rcl} m & = & 010111 \\ K & = & 110010 \\ \hline C & = & 100101 \end{array}$$

- Poiché ogni sequenza di tasti è ugualmente probabile, lo è anche ogni testo in chiaro!
  Sicurezza incondizionata (teorica dell'informazione), se la chiave non viene riutilizzata!
- La comunicazione Mosca-Washington in precedenza si assicurava in questo modo.
- Problema? Scambio e sincronizzazione di chiavi lunghe in modo sicuro.

- Le chiavi non devono essere riutilizzate! (Da qui il nome pad "una tantum".) Supponiamo che Alice
- desideri crittografare e inviare a Bob due messaggi m_1 e m_2. Alice decide di crittografare entrambi i
- messaggi utilizzando la stessa chiave di cifratura del flusso S, cioè

$$C_1 = S \oplus m_1 \qquad C_2 = S \oplus m_2$$

- Un avversario, che intercetta C_1 e C_2, può calcolare

$$C_1 \oplus C_2 = (S \oplus m_1) \oplus (S \oplus m_2) = m_1 \oplus m_2$$

- Poiché il testo inglese contiene ridondanza, dato $m_1 \oplus m_2$ l'avversario può recuperare entrambi m_1 e m_2 in chiaro (per sufficientemente a lungo m_1 e m_2).

Durante la seconda guerra mondiale l'Unione Sovietica non poteva produrre abbastanza monoblocchi. . . per stare al passo con l'enorme richiesta. . . Quindi, hanno usato un numero di one-time pad due volte, pensando che non avrebbe compromesso il loro sistema. Il controspionaggio americano durante la seconda guerra mondiale raccolse tutti i cavi internazionali in entrata e in uscita. A partire dal 1946, iniziò un intenso sforzo per irrompere nei messaggi sovietici con la collaborazione degli inglesi e di . . . l'errore sovietico di utilizzare alcuni one-time pad come due time pad, è stato in grado, nei successivi 25 anni, di rompere circa 2900 messaggi, contenenti 5000 pagine delle centinaia di migliaia di messaggi inviati tra il 1941 e il 1946 (quando i sovietici passarono a un sistema diverso).[3]

[3] J. Haynes e H. Klehr. *Venona: decodificare lo spionaggio sovietico in America.* Yale University Press, 1999.

- Una funzione crittografica $E(K, M)$ è *malleabile* se esistono due funzioni $F(X)$ e $G(X)$ tale che

$$F(E(K, M)) = E(KG(m)) \text{ per tutte le chiavi } K \text{ e messaggi } m$$

- $E(K, M)) = K ? m$ è chiaramente malleabile.
  Permettere $F(X) = G(X) = n ? X$ per qualsiasi dato n di dimensioni adeguate.

$$F(E(K, M)) = n ? (K ? m) = K ? (n ? m) = E(KG(m))$$

- Corollario: puoi trasformare il testo cifrato $C_1 = K ? m_1$ di un dato messaggio noto m_1 nel testo cifrato $C_2 = K ? m_2$ di qualsiasi m_2 di scelta anche se non lo sai K!
  Come? Basta calcolare il $?$ di C_1 e $m_1 ? m_2$. Infatti,

$$C_1 ? (m_1 ? m_2) = (K ? m_1) ? (m_1 ? m_2) = K ? m_2$$

Contorno

Cifrari a trasposizione

- Per la lunghezza del blocco T, permettere K essere l'insieme delle permutazioni su $\{1, \ldots, T\}$. Per ciascuno $e \in K$ e $m \in M$

$$E_e(m) = m_{e(1)} m_{e(2)} \cdots m_{e(T)}$$

- L'insieme di tutte queste trasformazioni si chiama a cifrario a trasposizione.
- per decifrare $C = C_1 C_2 \cdots C_T$ calcolare $D_D(C) = C_{D(1)} C_{D(2)} \cdots C_{D(T)}$, dove D è permutazione inversa.
- Lettere invariate in modo da poter sfruttare l'analisi di frequenza per dittonghi, trittonghi, parole, ecc.

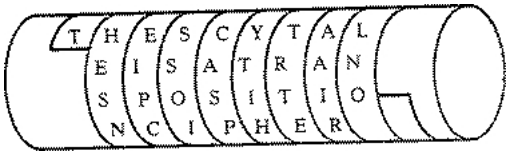
Esempio: cifrari a trasposizione

- C = UNduaenttlyDodioioekounlasciamiToihahvsekeeeleeyqonouv

UN	n	D	io	n	T	h	e	e	n
D	T	h	e	io	o	v	e	sì	o
tu	T	un	K	e	io	S	e	Q	tu
un	io	T	o	T	h	e	io	o	v
e	sì	o	tu	m	un	K	e		

La tabella definisce una permutazione su 1, ..., 50.

- L'idea torna al greco Scytale: avvolgi la cintura a spirale attorno al bastone e scrivici sopra il testo in chiaro.



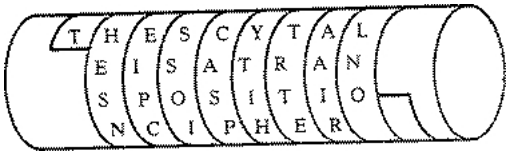
Esempio: cifrari a trasposizione

- C = UNduaenttlyDodioioekounlasciamiToihahvsekeeeleeyqonouv

UN	n	D	io	n	T	h	e	e	n
D	T	h	e	io	o	v	e	sì	o
tu	T	un	K	e	io	S	e	Q	tu
un	io	T	o	T	h	e	io	o	v
e	sì	o	tu	m	un	K	e		

La tabella definisce una permutazione su 1, ..., 50.

- L'idea torna al greco Scytale: avvolgi la cintura a spirale attorno al bastone e scrivici sopra il testo in chiaro.



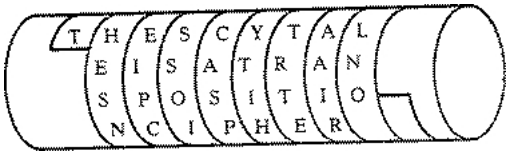
Esempio: cifrari a trasposizione

- C = UNduaenttlyDodioioekounlasciamiToihahvsekeeeleeyqonouv

UN	n	D	io	n	T	h	e	e	n
D	T	h	e	io	o	v	e	sì	o
tu	T	un	K	e	io	S	e	Q	tu
un	io	T	o	T	h	e	io	o	v
e	sì	o	tu	m	un	K	e		

La tabella definisce una permutazione su 1, ..., 50.

- L'idea torna al greco Scytale: avvolgi la cintura a spirale attorno al bastone e scrivici sopra il testo in chiaro.



Contorno

Cifrari compositi

- I cifrari basati solo su sostituzioni o trasposizioni non sono sicuri
- I cifrari possono essere combinati. Però . . .
  - due sostituzioni sono in realtà solo una sostituzione più complessa,
  - due trasposizioni sono in realtà solo una trasposizione, ma
  - una sostituzione seguita da una trasposizione rende un nuovo cifrario più difficile.
- Combinazioni sostituzione-trasposizione della catena di cifrari del prodotto.
- Difficile da fare a mano invenzione di macchine cifrate.

Bibliografia

- William Stallings. *Crittografia e sicurezza di rete* . Quarta edizione, Prentice Hall, 2006.

- Dieter Gollmann. *Sicurezza del computer* . Wiley, 2000.
- Bruce Schneier. *Crittografia applicata*. John Wiley & Sons, New York, 1996.
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. *Manuale di crittografia applicata* . CRC Press, 1996.
  Disponibile online su http://cacr.math.uwaterloo.ca/hac/
- Arthur E. Hutt, Seymour Bosworth, Douglas B. Hoyt. *Manuale sulla sicurezza informatica* . John Wiley & Figli, 1995.