

Sequente Caso

E. se vale secondo Kolmogorov che sequenze sono casuale
se $K(h) = |h| - \text{flage}(h)$.

• Cifrari storici •

Cifrario di Cesare ~~sostituzione~~ trasposizione delle lettere dell'alfabeto per un K (originariamente K=3)

Cifrari e sostituzione

Sostituiscono ogni lettere con una o più lettere seguenti di una regole prefissata

Sost. Monoalfabetica alle stesse lettere nel messaggio corrispondono le stesse lettere nel crittogramma. (c. di Cesare)

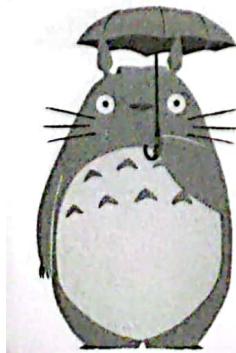
Deboltezze orittoonalisi statistica - le frequenze di lettere e k-grammi rimane uguale.

Sost. polialfabetica alle stesse lettere corrispondono una scelta in un insieme secondo una regola opportuna
~~(Augusto)~~ Cifrario di Augusto Documenti scritti in numeri. Scritti in greco, li confrontava con le seq di lettere nel I libro dell'Iliade e segnava la distanza

Deboltezze difficile da forzare. Bisogna registrare e iscritto la chiave.

Cifrario di Alberti ci sono due dischi, le chiavi cambia ogni volta che nel msg si incontra un carattere speciale.
Variante indice mobile i nr incontri indicano che dopo n caratteri avviene il cambio delle chiavi con le corrispondenze corrispondente

La macchina enigma è basata sul cifrario di Alberti



Cifrario di Vigenère Tabella 26x26 di rotazione dell'alfabeto [≡] (all'inizio). C'è una chiave K che, inesso $K \leq m$, viene ripetuta più volte.

Si procede lettera per lettera sostituendo con le corrispondenti tra le righe che iniziano con x (msg) e le colonne che iniziano con y (chiave)

- Se stesso chiavette perfette - one time Pad -

Cifrari a Trasposizione

Permutazione delle lettere secondo una regola prefissata

Permutazione semplice chiave intero h e permutazione π_h

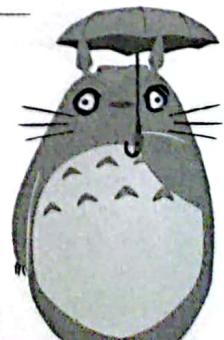
$\{1, 2, \dots, h\}$. Sudolito in blocchi di h lettere e scambio h segmenti π . Nr delle chiavi $h! - 1$ - Difficile ricordare π

Perm. di colonne $N = 2c, r, \pi_h$ con $c < r$ nr di colonne e righe di una tabella di lavoro. H è decomposto in blocchi di $c \times r$ caratteri, che vengono disposti nelle tavole in modo regolare. Poi le colonne vengono permutate secondo π , viene riportato c seguenti per colonne

Cifrario a griglie c'è una scheda perforata, sovrapposta griglie a una pagine. Griglie di $m \times n$ (verticale) $q \times q$, q pari. S (telle trasparenti) = $q^2/4$. Vengono scelte in modo che non si sovrappongano sotto 3 rotazioni di 90°

Debolezza STVolio dei q -grammi che indicazioni sulle permutazioni

is draw



• Ci froni perfetti •

Caratteristiche sicurezza inconcioneate - ~~l'attacco~~
bruteforce invile. Serve avere le chiavi.

Definizione Un cifrario è perfetto se $H_m = H_S = H_C$
scritto, $P(H=m) = P(H=m | c=c)$, cioè le conoscenze
di c non aumentano la informazioni disponibili.

Messaggio e crittogramma sono scorretti.

One Time pad

Idee: chiave lunghezza non rivilizzabile consente
messaggio. Si utilizzate lo xor: $C(m, k) = m \oplus k$.

Cifrario perfetto:
1 - Tutti i msg hanno lunghezza n
2 - Tutte le sequenze sono msg possibili
3 - chiave
scelta perfettamente a caso

$$P = \frac{1}{2^n}$$

ATTACCHI Bruteforce - non ha senso, ogni K genera un msg
Problema: generare le sequenze di bit casuali

• Ci froni Simmetrici •

Principi di Shannon

Diffusione: Testo in chiaro distribuito su tutto: il crittogramma

confusione: messaggio e chiave devono essere
combinati in modo complesso



..

• DES •

Messaggio svolto in 8 blocchi di 64 bit, cifrati indipendentemente. Chiave di 64 bit: 56 caselli a 8 posizioni. Posso $r = 16$ in cui si ripetono le operazioni.

FASI DEL DES

Permutazioni: P_1 , permutazione iniziale, P_T , opposta di P_1 , T (trasposizione) scartate; bit di controllo

Funzioni: CT - 8 bit in ingresso non sono presenti in uscita

Finzi EP - 16 bit sono duplicati

S-BOX 8 tabelline che ricevono 6 bit in ingresso e ne restituiscono 4 bit estremamente somma il nr di righe, i 4 centrali per le 4 colonne. Viene restituito il valore nelle celle in binario

Permutazione Φ permutazione finale di 32 bit. Genera DES

ATTACCHI chosen plain test \Rightarrow coppie $(m_1, c_1), (m_2, c_2)$ e confronto con $c \leq m \leq n$ se $c_1 = n$ occ \hat{n}

Variante: 3 DES idea: concatenare più copie del DES.

• AES •

Variante del DES che usa chiave di 128 bit, 192 o 256
Opera su blocchi da 128

FASI

② Gestione della chiave il blocco chiave viene considerato come 16 byte (4×4), esteso alle 4x4 colonne

$$w(t) = \begin{cases} w(t-1) \oplus w(4t-1) & \text{se } 4 \nmid t \\ T(w(4t-1)) \oplus w(4t-1) & \text{se } 4 \mid t \end{cases}$$

con T non lineare che usa le S-Box

mette al sicuro dagli attacchi che indovinano i bit delle chiavi



Sommo le chiavi fin sopra con il msg, poi 10 fesi
che consistono di 4 posseaggi ripetuti.

Substitute bytes uso l'S-Box

shift rows e mix columns mescolano righe e colonne

Add round key aggiunge le chiavi in xor

NB nella fase 10 non faccio mix columns

Substitute bytes - avviene trasformazione via S-Box

Shift rows - shift ciclici su righe 0, 1, 2, 3 posizioni

Mix columns - Moltiplicazioni colonne per una matrice 4x4 -
così dipende da tutti i byte delle colonne

Add round key - xor bit a bit con le chiavi

Sicurezza nessun attacco ad oggi più grado di compromissione

AES anche a 192 bit.

Esistono attacchi più efficienti del brute force con 6 fasi,
ma ~~non~~ ne usano almeno 10.

* Attacchi side-channel sfruttano debolezze delle piattaforme - non è nostro competente

Cifrari a blocchi

Se i blocchi sono simili è possibile risetare el
messaggio - soluzione CBC

si concatenano i blocchi fra loro con 80
bit a bit con il blocco ^{criptato} precedente



• Crittografie a chiavi pubbliche •

Sia One Time Pad che AOS richiedono un metodo per scambiarsi le chiavi in sicurezza - come fare?
Prime proposte Protocollo DH

Vengono delineati due tipi di cifrari:

Simmetrici: chiave di cifratura = decifratura (o facilmente calcolabile) - chiave segrete

Asimmetrici: chiave cifratura ≠ decifratura, Cifratura pubblica, decifratura privata. Esiste coppia $\langle K_{pub}, K_{priv} \rangle$ per ogni utente. Funzione di cifratura e decifratura disponibili a tutti

Caratteristiche: correttezza, chiavi facili da generare, impossibile che i utenti le abbiano uguale, facile per A decifrare il crittogramma e per B decifrare, ma difficile se non si ha K_{priv} (l'ère).

Funzione di cifratura: one way Trapdoor

• RSA •

Si basa sulla moltiplicazione di due nr primi - calcolo $n = p \cdot q$ è facile ma l'inverso è difficile, utilizza l'algebra modulare.

• RICHIAMI MD! •

Funzione di Euler numero di intari en e coprim. $\phi(n)$

Se $n = p \rightarrow \phi(p) = p-1$ se $n = p \cdot q$, $\phi(n) = (p-1)(q-1)$

$$e^{-1} \equiv a^{\phi(n)-1} \pmod n$$



le c. a chiavi pubbliche necessita 2n chiavi totali
invece di $n(n-1)/2$ sono però molto più lenti e
esposti ad attacchi chosen plain text

Soluzione: **cifrati ibridi** - chiave pubblica x
scambio chiavi, privata x messaggi (AES)

• RSA •

Fasi:

Creazione delle chiavi Si sceglie per q molto grande, calcola
 $n = p \cdot q$, $\phi n = (p-1)(q-1)$. Sceglie poi $e < \phi n$ coprimo
calcola $d = e^{-1} \bmod \phi n$, rende pubblico $K_{pub} \langle e, n \rangle$,
 $K_{priv} = \langle d \rangle$

Messaggio $m < n$, altrimenti in blocchi di $\lceil \log_2 n \rceil$ bit.

Nella pratica ~~$m \in \mathbb{Z}^b$~~ $m \in \mathbb{Z}^{b \leq n}$

Cifratura $c = m^e \bmod n \rightarrow c < n$

Decifratura $m = c^d \bmod n$

Correttezza $c^d \bmod n = (m^e \bmod n)^d \bmod n = m^d \bmod n = m$

Sicurezza legate alla diff. di fattorizzazione un n molto grande.

calcolo di $m = \sqrt[n]{c} \bmod n$ almeno difficile come fattorizz.

Fattorizzazione: complessità sub-esponenziale $O(2^{\frac{n}{\log n}})$ con $b = \log_2 n + 1$

NON è un problema NP-Hard, polinomiale su m quantistica.

richiede moduli molto grandi

per molti grandi

$p-1$ e $q-1$ ^{augmentare} sottrarre primo grande

$\text{MCD}(p-1, q-1)$ molto piccolo (id. = 2) $\rightarrow \frac{p-1}{2} \frac{q-1}{2}$ coprimi

non devono essere vicini oppure ~~primo~~ ~~primo~~

$$p^2 \# q^2 \approx n$$



~~Attacchi all'RSA~~ Protocollo DH

A e B scelgono un primo molto grande e un generatore g per \mathbb{Z}_p^* . g è pubblica.

A e B scelgono a caso un esponente $a \in \mathbb{Z}_{p-1}$, calcolano $A = g^a \text{ mod } p$ e $B = g^b \text{ mod } p$, li inviano sul canale, poi calcolano $K = B^a \text{ mod } p$ e $A^b \text{ mod } p = g^{ab} \text{ mod } p$. Quelle sono chiavi.

Attacchi la sicurezza si basa sul logaritmo discreto, che è un problema difficile, esponenziale nelle dimensioni dell'input. Vulnerabile a Man in The Middle

Cifrario di El Gamal

Creazione delle chiavi: si sceglie p e g , poi da intero $x \in [2, p-2]$ si calcola $y = g^x \text{ mod } p$. $(p_{\text{pub}} = \langle p, g, y \rangle, p_{\text{priv}} = x)$

Cifratura: si scrive sequenza binaria, tratta come intero ($m < p$, altrimenti blocca), si sceglie $r \in [2, p-2]$, si calcola $c = g^r \text{ mod } p$ e $d = m \cdot y^r \text{ mod } p$

Decifratura: $n = d \cdot c^{-r} \text{ mod } p \quad | \quad (m \cdot y^r \cdot (g^r)^{-r}) \text{ mod } p = m$

Sicurezza basata su logaritmo discreto



• Curve ellittiche •

~~Punto~~ Punto di vista matematico

Formule $y^2 = x^3 + cx + b$ (curve di Weierstrass) [definite su \mathbb{F}_p]

altra forma: $E(a, b)$

Somma

Se $P \neq Q$ $x_s = \lambda^2 - x_p - x_q$ $\lambda = \frac{4a + 4p}{x_q - x_p}$
 $4s^2 - 4p + \lambda(x_p - x_s)$

$P = Q$ uguali no $\lambda = \frac{3x_p^2 + a}{2y_p}$

$P = -Q$ $s = 0$

La curva fa parte di un gruppo \mathbb{G}_p se $4a^3 + 27b^2 \pmod p \neq 0$

Inverso di un punto $-P = (x, -y) \in (x, p-y \pmod p)$

La sicurezza si basa sul p. del log discreto $Q = kP$
 $k \in \log_p Q$

DH su curve ellittiche costruzione di una chiave

A e B scelgono una curva appropriata e un punto B di ordine grande^(*) $[B \sim g]$. curva e B pubblici.

A e B scelgono $n_A, n_B < n$ cesvoli. Calcolano $P_A = n_A \cdot B$ e $P_B = n_B \cdot B$ e li scambiano. Poi calcolano $K_{\text{session}} = n_A \cdot P_B / n_B \cdot P_A = n_A \cdot n_B \cdot B$. K è un punto, $K_{\text{session}} = x_K \pmod {2^{256}}$



di Gmail su curve ellittiche maneggiare msg cifrati
Algoritmo di Koblitz

Bisogna inserire il messaggio in un punto sulle curve ellittiche.

Se metto $m = x_p$, ho probabilità di circa $\frac{1}{2}$ che sia un residuo quadratico \rightarrow non va bene.

Algoritmo di Koblitz

Scelgo intero h (pubblico) tale che $(n+1)^{\frac{1}{h}} < p$

$x = mh + i$ con $0 \leq i < h$ \Rightarrow h tentativi

vedo se è residuo quadratico, altrimenti $i++$ fallimento $(\frac{x}{i})^h$, migliore

Scambio di messaggi

Si fissano curve, punto B e vengono costruite le copie dichiarate come su DH.

m viene convertito con Koblitz, poi si sceglie $r < n$ casuale, calcola $V = rB$ e $W = P_m + rP_B$. Invia $\langle V, W \rangle$, B decifra calcolando $W - n_B \cdot V = P_m$, ricava $m = \lfloor \frac{x_p}{h} \rfloor$

DIMOSTRAZ. $W - n_B V = P_m + rP_B - n_B V = P_m + r(n_B B) - n_B rP_B \in P_m$

Sicurezza (1) - Trovare n_B da P_B - log discreto

(2) conoscendo r e $P_m = W - rP_B$ - log discreto

L'attacco index calculus non è possibile - non

esiste la moltiplicazione fra punti

Pollard - patologico + efficiente (2^{62})



② Identificazione ②

Funzioni hash one-way

Deve essere - computazionalmente facile calcolare $y = f(x)$; difficile calcolare $x = f^{-1}(y)$, difficile determinare x_1, x_2 se $f(x_1) = f(x_2)$
cioè oltre elementi in collisione

Firme digitali - protocollo 3

U calcola $h(m)$ e genera $f : D \rightarrow h(m), K_{priv}$, calcola
separatamente C e spedisce $\langle U, C, f \rangle$
V decifra C e calcola $c(f, K_{pub})$, se $c = h(m)$, V

Protocollo zero-Knowledge

Fiat-Shamir

P sceglie p, q molto grandi, calcola $n = p \cdot q$, sceglie $s < n$, calcola $t = s^2 \pmod{n}$. Rende noto $\langle t, n \rangle$.

V (per K volte): - chiede a P di generare $r < n$ casuale, calcola $v = r^2 \pmod{n}$ e lo dà a V. V genera un bit casuale e lo comunica a P. P calcola $z = r \cdot s^e \pmod{n}$.

V calcola $x \equiv z^2 \pmod{n}$, $(rs^e)^2 = vt^e$ se $x \equiv vt^e \pmod{n}$, V, altrimenti $\not\equiv p$.

Non si può usare sempre $e=1$ altrimenti P mostrerebbe $\frac{t}{z}$ come b .

• Quantum computing •

Protocollo BB84

A invia S_A codificata.

B interpreta S_A con basi casuali e comunica ad A le basi.

A dice quali sono quelle comuni $\sim \frac{|S_A|}{2}$

A e B calcolano S_A^n e S_B^n , comunicano una porzione in posizioni prestabilite (S_A^n , S_B^n). Se sono uguali, allora $S_A^n - S_B^n = S_A^i - S_B^i$ viene usata come chiave.

Attacchi

Eve non può decifrare S_A in copie perché non è possibile produrre una copia uguale di stati incerti, quindi deve inviare il messaggio ricevuto, ma questo porta le basi comuni che A e B a essere vicine a i e l'intrusione viene notata, quando si scambiano S_A^n e S_B^n (che non sono uguali)

Rumore

Possono essere corrotti dai bit a causa del rumore di trasmissione. Si stabilisce quindi il QBER (quantum bit error rate). Il nr di bit diversi tra S_A^n e S_B^n deve essere < QBER.

Attacco II



Eve potrebbe decifrare solo alcuni bit, stando sotto il QBER. È opportuno che le chiavi vengano cifrate con una f. hash one-way.