1

CRYPTOGRAPHY - CRITTOGRAFIA
CRYPTOLOGY - CRITTOLOGIA
CRYPTOANALYSIS - CRITTOANALISI

CIFRARE - DECIFRARE

ATTACCHI DEL CRITTOANALISTA

- Ciphertext only ho solo il ciphertext C^*
- Known Plaintext $C^* \to P^*$
  ho decifrato un ciphertext a caso
- chosen Plaintext
  scelgo $P^{\text{scelto}} \xrightarrow[\text{ottengo}]{} C^{\text{scelto}}$
- chosen Ciphertext
  scelgo $C^{\text{scelto}} \xrightarrow[\text{ottengo}]{} P^{\text{scelto}}$

APPLICAZIONI CRITTOGRAFICHE (2)

- confidenzialità
- integrità dei dati
- autenticazione
  - entità ⇔ IDENTIFICAZIONE
  - origine dei dati (creatore e tempo di creazione dei dati)
- non ripudio — non rifiuto dell'esecuzione di transazione

impossibile nel caso di

Chiavi simmetriche

$\{M\}_{KAB} \rightarrow$ (V) Victor verifier

(A) $\rightarrow \{M\}_{KAB}$ (B)

K_{AB} $\qquad$ K_{AB}

Bob è sicuro di Alice (!) l'autenticazione è automatica

ma Bob non può provare a Victor che Alice ha mandato il messaggio: infatti anche Bob ha K_{AB} e potrebbe aver forgiato lui $\{M\}_{KAB}$.

possibile con chiavi asimmetriche
chiavi pubbliche

Firme Digitali

(3)

Testo + Firma

Identificazione

- Username + password

segreto

la password può essere rubata

- Feige-Fiat-Shamir

Zero Knowledge Methods

prova dell'identità senza rivelare il segreto

Stabilimento delle chiavi

Condivisione del Segreto

Protocolli di sicurezza

Moneta Elettronica

anonimato

	CIFRARI CLASSICI mod m	Keyspace $\mathbb{Z}_m$ → esempio $m=26$	CIPHERTEXT ONLY	KNOWN PLAINTEXT	CHOSEN PLAINTEXT	CHOSEN CIPHERTEXT
A BLOCCHI	SHIFT	$m=26$ 2^{5}	Forza Bruta	1 coppia	1 coppia	1 coppia
	AFFINE	$m\varphi(m)=312 \approx 2^{9}$	Forza Bruta	2 coppie	2 coppie	2 coppie
	SUBSTITUTION	$m!=26!\approx 10^{26} \approx 2^{78}$	ATTACCO SULLE FREQUENZE BINGO!	m coppie	m coppie	m coppie
	VIGENERE dimensione chiave n, n massimo $= m$	$m^m=26^{26}\approx 10^{36}$ esempio $n=m$ $\approx 2^{119}$	ATTACCO SULLE FREQUENZE BINGO!	$m(n)$ coppie	$m(n)$ coppie	$m(n)$ coppie
	HILL matrici $d \times d$ esempio $d=m=26$ matrici $(m \times m)$	$m^{m^2}=26^{676}\approx 10^{956}$ esempio $d=26=m$ $\approx 2^{3178}$	Forza Bruta	$d \times d$ coppie BINGO!	$d \times d$ coppie	$d \times d$ coppie
A CASCATA / A FLUSSO	STREAM (mod 2) periodo stream $= d$; $d_{max}=2^n-1$: n dimensione dello SR	$2^d=2^{2^n-1}\approx 10^{646.000.000}$ esempio per $n=31$: $2^{31}-1\approx 2 \cdot 10^9$	Forza Bruta	un $2n$ bit coppie BINGO!	$2n$ bit coppie	$2n$ bit coppie

$\log_2 10 \approx 3,3246$

Cifrari classici

plaintext

$n=26$ $\quad a-z \equiv \{0,1,2\ \dots\ 25\} \equiv$

$\equiv A-Z$

ciphertext

$n = 2 \times 13$

$\varphi(n) = 1 \times 12 = 12$

SHIFT

$$C \equiv P + K \pmod{26}$$

$$P \equiv C - K \pmod{26}$$

$K = \{0,1\,..\,25\}$

$K \in Z_{26}$

4 attacchi

Solo testo cifrato — esaustivo forza bruta $\#$ tentativi $= |K| = 26$

oppure nella frequenza delle lettere se "L" è la più frequente in C allora la congettura è che corrisponda a "e"

$L=11$, $e=4$ $\quad K = 11-4=7$

è più lungo della ricerca a forza bruta!

<u>testo in chiaro noto</u>

basta un carattere P noto qui confonde se cifro $t = 19$ e $D = 3$

allora $\underline{K = 3 - 19 = -16 = 10 \pmod{26}}$.

<u>testo in chiaro scelto</u>

scelgo $P = a = 0$

e $\underline{c = 0 + K = K}$

se $C = \underline{H} = 7$ $\quad C = H = \underline{7 = K}$

<u>testo cifrato scelto</u>

scelgo $C = A = 0$

$P = C - K = -K$

se $P = h = 7$ $\quad K = -7 = 19 \pmod{26}$

AFFINE

$$\begin{cases} C = aP + b \pmod{26} \\ P = a^{-1}(C - b) \quad \text{mcd}(a, 26) = 1 \end{cases}$$

ok

$a = 9$
$b = 2$

se

$|a| = \phi(26) = 12$

$|b| = 26$

Solo testo cifrato

esaustivo # chiavi
$= n\,\phi(n) = 26 \times 12 = 312$

conteggio frequenze
è più lungo!

Testo in chiaro noto

due lettere del plaintext
e due ciphertext bastano in genere
(serve l'inversione)

$P = if \;;\; C = PQ$

$(8,5) \to (15,16)$

$$\begin{cases} 8a + b \equiv 15 \pmod{26} \\ 5a + b \equiv 16 \end{cases}$$

sottraendo $3a \equiv -1 \equiv 25 \pmod{26}$

$3 \nmid 26$ OK $3a \equiv 25$ $a \equiv 3^{-1} \times 25 \equiv 9 \times 25 \equiv 225 \equiv 17 \pmod{26}$

in altri casi NO! $3^{-1} \equiv 3^{11} \bmod 26 = 9$ da cui $8 \times 17 + b \equiv 15$ $b \equiv 9$

Una lettera dimunisce lo spazio della ricerca esaustiva (3)

$P \Leftrightarrow C$

es $g \Leftrightarrow T$ $\qquad 6a+b \equiv 19 \pmod{26}$

$\downarrow$ cerco solo i $\phi(n) = 12$ valori possibili per a

Testo in chiaro scelto

$$P \equiv ab \equiv (0,1)$$

noto $\rightarrow C \equiv (c_1, c_2)$ $c_1 \equiv b$

$$0 \cdot a + b \equiv c_1 \rightarrow b \equiv c_1$$

$$a + c_1 \equiv c_2 \rightarrow a \equiv c_2 - c_1 \pmod{26}$$

Testo cifrato scelto

$$\begin{cases} C \equiv AB \equiv (0,1) \\ P \equiv (p_1, p_2) \end{cases}$$

noto $\rightarrow$ P

$$p_1 a + b = 0$$

$$p_2 a + b = 1$$

$$a(p_2 - p_1) = 1 \qquad \boxed{(p_2 - p_1) = a^{-1}}$$

$p_1 = -a^{-1} b$

$-p_1 = a^{-1} b$

$\boxed{b = -a p_1}$

$$p_2 = a^{-1}(1-b) = a^{-1} - a^{-1} b$$

$$p_2 - a^{-1} = -a^{-1} b \qquad a^{-1} b = a^{-1} - p_2$$

$$\boxed{b = 1 - a p_2}$$

SOSTITUZIONE

(4)

attacco **ciphertext only** soccombe al conteggio frequenze monogrammi, digrammi

frequenze di monogrammi

a	0,082
b	0.015
c	0.028
d	0.043
→ e	0.127
f	0.022
g	0,020

- digrammi
- trigrammi

ecc.

26

scelgo una permutazione tra 26! come chiave K

a	b	c	d	e	f	g	...	w	x	y	z
X	N	Y	A	H	P	Q	...	M	S	T	R

\# chiavi $26! \cong 4 \cdot 10^{26}$

esempio TRAPPE

520 caratteri ciphertext

382 si scoprono con monogrammi $\overset{1}{e} \Leftrightarrow H$

e digrammi 381 !

debolissimo

VIGENERE

Known plaintext — servono tanti caratteri quanto la lunghezza del blocco

Chosen plaintext — $P = 00000$ $C = K$

Chosen ciphertext — $C = 0000$ $P = -K$

ciphertext only — nulle frequenze

5

- ~~lunghezza della~~ trova la chiave
- trova la chiave

Keyword $K \equiv (k_1, k_2 \dots k_n)$ lunga n

che indica lo shift dei vari caratteri di plaintext presi a blocchi di n.

ad es. $K = (21, 4, 2, 19, 14, 17)$ $(n = 6)$

plaintext	h	e	r	e	i	s	h	o	w	i	t	w	o...
key	21	4	2	19	14	17	21	4	2	19	14	17	21...
ciphertext	C	I	T	X	W	J	C	S	Y	B	H	N	J...

$\longleftarrow n \longrightarrow$

$C = P + K$

Forza Bruta
\# chiavi 26^n
max $26^{26} = 6 \times 10^{36}$

Testo in chiaro noto

servono abbastanza caratteri noti per trovare la chiave

$$K = C - P$$

testo in chiaro scelto

per $P = aaa\dots = 000\dots$

$C = K$

testo cifrato scelto

per $C = AAAA\dots = 000\dots$

$P = -K$

Attacco

<u>Solo testo cifrato</u>

(6)

Vigenere

è polialfabetico la lettera

può $n=6$

e appare con $\underline{n}$ lettere cifrate

$e=4$ diverse

$$4+21 \equiv 25 \equiv Z$$
$$4+4 \equiv 8 \equiv I$$
$$4+2 \equiv 6 \equiv G$$
$$4+19 \equiv 23 \equiv X$$
$$4+17 \equiv 21 \equiv V$$

e Z può venire anche da $v \equiv 21+4 \equiv Z$

e allora le lettere cifrate tendono a essere distribuite uniformemente con frequenza 1/26.

Trovare la lunghezza della chiave

<u>Vedi Trappe</u> sposto il ciphertext di k lettere a destra e vado a vedere le "coincidenze"

Tabella: displacement coincidenze

spostamento	1	2	3	4	5	6	7
coincidenze	14	14	16	14	24	12	14

7

Molto probabilmente

$n=5$ key lenght

Trovare la chiave

$n=5$ determinato

testo cifrato XYZABCXFFCKMABAE

5

1^a 6^a 11^a 16^a

cerco le lettere più frequenti

A 0
B 0
C 7 ← la più frequente è la "e"
⋮
X 6
Y 1
Z 0

es $G \to e$

$e = 4$ $K_1 = 2 = c$

$G = 6$

2^a 7^a 12^a

allora la più frequente $S = e$

$S=18$ $K_2=14$

e cw' va 8

$\{2, 14, 3, 4, 18\} = \{\text{codes}\}$

keyword

Shift
affine
substitution
} cifrari a sostituzione di caratteri singoli

Vigenere
Hill
} cifrari a permutazione di blocchi di caratteri

Diffusione
Confusione
} Solo Hill

DIFFUSIONE

se cambio un carattere di testo in chiaro cambiano molti caratteri cifrati (la statistica delle frequenze delle lettere, digrammi etc, del plaintext si diffonde su molti caratteri del ciphertext)

CONFUSIONE

la chiave non è relazionata semplicemente al testo. Cioè ogni carattere del cifrato dipende da varie parti della chiave

Cifrario di Hill

la chiave è una matrice $n \times n$ $(\bmod m)$ ad es. $m = 26$.

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod m$$

$$\det M = ad - bc$$

deve essere (2) $\text{mcd}(\det M, m) = 1$
(1) $\det M \neq 0$

(2) implica per default (1)
infatti $\underbrace{\text{mcd}(0, m) = m \neq 1}_{\text{per definizione}}$

---

se $c_{ij} \in \mathbb{Z}_{26}$

$26 = 2 \times 12 \rightarrow \varphi(26) = 12$

deve essere $\underline{\text{mcd}(\det M, 26) = 1}$

$$[1 \times n][n \times n] = [1, n]$$
$$P \times M = C$$

ove P è un vettore riga a $\underline{n}$ componenti

Esempio
$$M=\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$$

②

$$P=(a\ b\ c) = (0,1,2)$$

$$(0,1,2)\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \equiv (0,23,22) \pmod{26}$$

$$C=(0,23,22)=(A\,X\,W).$$

$$\operatorname{mcd}(\det M, 26)=1$$

$$\det M \equiv 1(5\times8-6\times9)-2(4\times8-6\times11)+3(4\times9-5\times11)$$
$$\equiv -3 \pmod{26} \equiv 23$$

$$\det M^{-1} = 23^{-1} \bmod 26 \equiv 17 \pmod{26}$$

Allora

$$M^{-1}=\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}^{-1} = \frac{\begin{bmatrix} ei-fh & ch-bi & bf-ce \\ fg-di & ai-cg & cd-af \\ dh-eg & bg-ah & ae-bd \end{bmatrix}}{\det M = a(ei-fh)-b(di-fg)+c(dh-eg)}$$

③

aggiunta

cofattore → Trasposta

inversa
$$M^{-1} = \frac{1}{\det M} \underbrace{\left(C_{ij}\right)^T}_{\text{aggiunta}} = \frac{1}{|M|} \begin{pmatrix} c_{11} & c_{21} & c_{j1} \\ c_{12} & & \\ c_{1i} & & c_{ji} \end{pmatrix}$$

cofattori
ove $C_{ij} = (-1)^{i+j} M_{ij}$ minori
cofattori

M_{ij} = minori sono i determinanti delle matrici che restano cancellando riga i e colonna j

---

Allora
$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} = M$$

$$C_{ij} = \begin{pmatrix} (5\times 8 - 6\times 9) & -(4\times 8 - 6\times 11) & +(4\times 9 - 5\,11) \\ -(2\times 8 - 3\times 9) & +(1\times 8 - 3\times 11) & -(1\times 9 - 2\times 11) \\ +(2\times 6 - 3\times 5) & -(1\times 6 - 3\times 4) & +(1\times 5 - 2\times 4) \end{pmatrix} =$$

$$= \begin{pmatrix} -14 & 34 & -19 \\ 11 & -25 & 13 \\ -3 & 6 & -3 \end{pmatrix}$$

4

$$c_{ij}^{T} = \begin{pmatrix} -14 & 11 & -3 \\ 34 & -25 & 6 \\ -19 & 13 & -3 \end{pmatrix}$$

$$M^{-1} = (-3)^{-1} \begin{pmatrix} -14 & 11 & -3 \\ 34 & -25 & 6 \\ -19 & 13 & -3 \end{pmatrix} =$$

$17(-14) = -238$
$= -4 = 22$

$$= 17 \begin{pmatrix} -14 & 11 & -3 \\ 34 & -25 & 6 \\ -19 & 13 & -3 \end{pmatrix} = \begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix}$$

$$M \cdot M^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$= I$ (matrice identité)

$$1 = (\overset{22}{1 \times 22} + \overset{12}{2 \times 6} + \overset{45}{3 \times 15}) = 79 \bmod 26$$
$$= 1$$

$$-238 = -9 \times 26 + r$$

$$-8 = -26 + 18$$

$$r = -4 \bmod 26 = 22$$

decifro $C \equiv (0, 23, 22) \bmod 26$ 5

$$\begin{pmatrix} 0 & 23 & 22 \end{pmatrix} \begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 & 2 \end{pmatrix} \pmod{26}$$

OK

Cifrari

Affine - attacchi

Vigenere = attacchi
Substitution = attacchi
Blocchi - Hill attacchi

$$M = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \bmod 3$$

$$\text{Det } M = (1\times4 - 2\times3) \bmod 3 = -2 \bmod 3 = 1$$

$$\begin{cases} \text{deve essere } \neq 0 \quad \text{ok} \\ \text{deve essere } \quad mcd(1, 3) = 1 \quad \text{ok} \end{cases}$$

Per esempio

$$M = \begin{pmatrix} 15 & 22 \\ 11 & 3 \end{pmatrix} \bmod 26$$

$$\det M = (45 - 242) = -197 \equiv -15 \equiv 11 \pmod{26}$$

$mcd(11, 26) = 1$ ok

$\varphi(26) = 12$

$$11^{-1} = 11^{11} \equiv 19 \bmod 26$$

$$11 \cdot 19 \equiv 1 \pmod{26}$$

allora

$$M^{-1} = \frac{1}{19}\begin{pmatrix} 3 & -22 \\ -11 & 15 \end{pmatrix} = 19\begin{pmatrix} 3 & 4 \\ 15 & 15 \end{pmatrix} = \begin{pmatrix} 5 & 24 \\ 25 & 25 \end{pmatrix}$$

$$M M^{-1} = \begin{pmatrix} 15 & 22 \\ 11 & 3 \end{pmatrix}\begin{pmatrix} 5 & 24 \\ 25 & 25 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

infatti $15\cdot 5 + 22\cdot 25 \equiv 625 \equiv 1$; $15\cdot 24 + 22\cdot 25 \equiv 0$

$11\cdot 5 + 3\cdot 25 \equiv 0$; $11\cdot 24 + 3\cdot 25 \equiv 1$

Attacco <u>Known plaintext</u>

se M è $n\times n$, devo avere $\underline{n}$ blocchi di Plaintext di dimensione n, noti cui corrispondono n blocchi di Ciphertext di dimensione n, noti.

Per l'attacco devo conoscere a priori la dimensione della matrice M, e cioè n.

Per esempio supponiamo che sia $n=2$

Supponiamo di lavorare mod 26 con 26 lettere dell'alfabeto A-Z inglese numerate $0 \div 25$.

Allora ecco il Plaintext

$$P = \underset{7,\,14,\,20,\,19}{\underline{|\,h\,o\,|\,u\,t\,|}}$$ due blocchi da 2

Supponiamo che il ciphertext sia

$C = $ Z W P L

25, 22, 15, 11,

Allora scrivo l'equazione matriciale $P \cdot M = C$

$$\begin{pmatrix} 7 & 14 \\ 20 & 19 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 15 & 11 \end{pmatrix} \pmod{26}$$

Si noti che le matrici $\tilde{P}$ e $\tilde{C}$ hanno det $\perp$ 26 e cioè

$$\det\begin{pmatrix} 7 & 14 \\ 20 & 19 \end{pmatrix} = 133-280 = -147 \bmod 26$$
$$= -17 \bmod 26 = 9$$

$9 \equiv 3 \times 3$

$$\mathrm{mcd}(9, 26) = 1 \text{ ok}$$

Però in questo caso

$$\det\begin{pmatrix} 25 & 22 \\ 15 & 11 \end{pmatrix} = 275-330 = -55 \bmod 26 =$$
$$= -3 \bmod 26 =$$
$$= 23 \bmod 26$$

non è vero $\forall \tilde{C}'$

$$\mathrm{mcd}(23, 26) = 1 \text{ ok}$$

$$\det M \equiv \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ad-bc)$$

deve essere $\mathrm{mcd}[(ad-bc), 26] = 1$ $\quad (ad-bc) \neq 0$

allora invertiamo $\underset{\sim}{P}$

$$P^{-1} = \begin{pmatrix}7 & 14\\ 20 & 19\end{pmatrix}^{-1} = 9^{-1}\begin{pmatrix}19 & -14\\ -20 & 7\end{pmatrix} = 9^{-1}\begin{pmatrix}19 & -14\\ -20 & 7\end{pmatrix}$$

$$9^{-1} = 9^{11} \bmod 26 = 3 \qquad 3\times 9 \equiv 27$$

o

$$P^{-1} = \begin{pmatrix}5 & 10\\ 18 & 21\end{pmatrix} \bmod 26$$

allora

$$M \equiv P^{-1}\cdot C \pmod{26}$$

$$M \equiv \begin{pmatrix}5 & 10\\ 18 & 21\end{pmatrix}\begin{pmatrix}25 & 22\\ 15 & 12\end{pmatrix} \equiv \begin{pmatrix}15 & 12\\ 11 & 3\end{pmatrix}$$

<u>Trovata!</u>

infatti

$$P\cdot M = C$$

$259 \bmod 26 = 25$

$$\begin{pmatrix}7 & 14\\ 20 & 19\end{pmatrix}\begin{pmatrix}15 & 12\\ 11 & 13\end{pmatrix} = \begin{pmatrix}25 & 22\\ 15 & 12\end{pmatrix}$$

Hill attacco chosen plaintext

Scelgo P e ottengo C

NOTO n

scelgo P così

n blocchi lunghi n lettere

$$\begin{cases} \underbrace{baa\ldots a}_{n} = 100\ldots 0 \\ aba\ldots a = 010\ldots 0 \\ \vdots \\ aaa\ldots a = 000\ldots 1 \end{cases}$$

$P \cdot M = C$

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} M \end{pmatrix} = \begin{pmatrix} M \end{pmatrix} = C$$

mi arriva direttamente

$C = M$

Chosen ciphertext

scelgo C e ottengo P

Scelgo C come ho fatto per P e faccio

$C M^{-1} = P$ $\qquad C = I$

$$I \cdot M^{-1} = P$$

mi avrei direttamente $P = M^{-1}$

causes error propagation (12)

Diffusion Full

Diffeme & Confusione   Vigènere &
Hillsi   Substitution
NO

se si cambia un carattere di P
molti caratteri di C cambiano

e viceversa

la chiave K non è relazionata
sufficiente con il C ciphertext.
ogni carattere di C dipende da
molte porzioni della chiave

Esercizio

attacco al cifrario di Hill
testo in chiaro scelto

2x2
mod 26

$ba \to HC \quad (1,0) \to (7,2)$

$zz \to GT \quad (25,25) \to (6,19)$

qual'è M ?

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$(1,0)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a,b)$$

allora
$a=7$
$b=2$

$$(-1,-1)\begin{pmatrix} 7 & 2 \\ c & d \end{pmatrix} = (-7-c),(-2,-d) =$$
$$= [-(7+c), -(2+d)]$$

$-(7+c) = 6 \qquad c = -13 = 13$

$-(2+d) = 19 \qquad d = -21 = 5$

mod 26

ciphertext ELNI (M) Hill 2x2
plaintext dont
(a) trovare M.

(b) se C = ELNK
come cambia M'?

dont = (3, 14) (13, 19)
ELNI = (4, 11) (13, 8)

$$\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix} M = \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix}$$

$\det\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix} = 5 \mod 26$

$\det^{-1} \equiv 5^{-1} \equiv 21 \equiv 5^{11} \mod 26$

$$\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}^{-1} \equiv 21 \begin{pmatrix} 19 & -14 \\ -13 & 3 \end{pmatrix} \equiv \begin{pmatrix} 9 & 18 \\ 13 & 11 \end{pmatrix}$$

$\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}\begin{pmatrix} 9 & 18 \\ 13 & 11 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ok

$$M = \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix} \text{ ok}$$

ELNK = (4, 11)(13, 10)

(b) $\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix} M = \begin{pmatrix} 4 & 11 \\ 13 & 10 \end{pmatrix}$ si trova un cambiamento! Cambia tutta la colonna

$$M' = \begin{pmatrix} 10 & 19 \\ 13 & 19 \end{pmatrix}$$

Esempio* $M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ cifrario Hill mod 26

* Non valida per il cifrario

trova due plaintext che producono lo stesso ciphertext – det M mod 26 = 24 ≠ 1 No! mcd(24,26)=2

$$P = (x, y)$$

$$C = (x + 3y, 2x + 4y) \bmod 26$$

ci sono molti (x,y) che producono lo stesso testo cifrato

troviamo i plaintext che producono cifertext del tipo (0,*)

$$x = -3y \bmod 26$$

basta trovare ora due y diversi tali che producano lo stesso valore di −2y

$$2(-3y) + 4y = -2y \pmod{26}$$

es y=4 e y=17

$-2y = -8 \bmod 26 = 18$
$-2y = -34 \bmod 26 = 18$
$-8 \bmod 26$

$P_1 = (4,18), P_2 = (17,18)$.

$$M = \begin{pmatrix} 1 & 1 \\ 3 & 4 \end{pmatrix} \bmod 26 \qquad \det M = 4-3 = 1$$

OK

$$\begin{cases} P = (x, y) \\ C = (x+3y,\ x+4y) \bmod 26 \end{cases}$$

molti (x, y) producono lo stesso ciphertext

troviamo i plaintext che producono

$$\text{ciphertext} = (0, *) \quad * \text{ any}$$

allora dove essere $\quad x = -3y \bmod 26$

Basta trovare due diversi y che

$$-3y + 4y = y \pmod{26}$$

producono lo stesso risultato y

es $\quad y_1 = 5 \qquad 5 \bmod 26 \equiv 5$

$\quad\ \ y_2 = 31 \qquad 31 \bmod 26 \equiv 5$

allora $\cancel{P_1(5, 11),\ P_2(31, 1)}$ $\qquad x_1 = -3 \times 5 = -15 \equiv 11$

$x_2 = -3 \times 31 = -93 \equiv -15 \equiv 1$

$\cancel{P_1(5,} \quad \cancel{P_2(31}$ $\quad P_1 = (11, 5) \quad P_2 = (1, 5)$

①

Cifrario di Hill $M \equiv n \times n$

Key size? quante chiavi diverse? $m = 26$

se 2×2 # chiavi $= \underline{157.248}$

$\boxed{n=2}$

$\downarrow$

$34{,}4\%$ utili

su

$K \equiv (a, b, c, d) \bmod 26$

senza vincoli è $26^4 = \underline{456.976}$ su 100%

Ma c'è il vincolo

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv (ad - bc) \equiv 1 \pmod{26}$$

e cioè

$$\gcd((ad-bc), 26) = 1$$

$\underline{26 = 2 \times 13}$

FACCIAMO UN ESEMPIO $m = 4$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod 4$ $\mathbb{Z}_4 \equiv \{0, 1, 2, 3\}$

quante chiavi?

teorico $= 4^4 = 256$

Ma deve essere $\text{mcd}[(ab - cd), 4] = 1$

4 è pari i suoi coprimi sono 1 e 3

allora $(ab - cd)$ deve essere DISPARI $(\neq 0)$

prendiamo $x = ad \quad \mathbb{Z}_4 \times \mathbb{Z}_4$

$y = bc \quad \mathbb{Z}_4 \times \mathbb{Z}_4$

ciascuno x e y hanno 16 combinazioni

Ricordo che ($P \equiv$ pari) ($D \equiv$ dispari)

$P \times P = P$, $P \times D = D \times P = P$, $D \times D = D$

solo il prodotto tra dispari è dispari

allora sulle 16 risultano

$0\times 0 = 0$ 0×1 0×2 0×3 1×0

(0) 8 ZERO 2×0 3×0 $2\times 2 \equiv 4 \equiv 0 \pmod 4$

(2) 4 PARI $1\times 2 \equiv 2$; $2\times 1 \equiv 2$; $2\times 3 \equiv 6 \equiv 2$; $3\times 2 \equiv 6 \equiv 2 \pmod 4$

(1, 1, 3, 3) 4 DISPARI $1\times 1 \equiv 1$; $1\times 3 \equiv 3$; $3\times 1 \equiv 3$

$3\times 3 \equiv 9 \equiv 1 \pmod 4$

16

Solo 4 su 16 sono dispari.

Considero ora (1) $x - y = ad - bc = D$ dispari (1 o 3)

Ricordo che

$P \pm P = P$, $P \pm D = D \pm P = D$; $D \pm D = P$

Solo se uno dei due è dispari (mentre l'altro è zero oppure pari) allora la (1) è dispari

tutte le combinazioni sono tra X e Y
di cui ciascuno ha 4 dispari ~~e~~ su 16
allora   tra pari anche zero

$$\begin{array}{ccccc} & D-D & D-P & P-D & P-P \\ \text{Combinazioni complessive} = & (4 \times 4) + & (4 \times 12) + & (12 \times 4) + & (12 \times 12) = 256 \end{array}$$

di cui quelle dispari sono chiavi valide

$$\underset{D-P}{(4 \times 12)} + \underset{P-D}{(12 \times 4)} = \underline{96}$$

Per cui $\frac{\text{valide}}{\text{totali}} = \frac{96}{256} = 37{,}5\%$ compressione dello spazio delle chiavi

Si osservi che ne servono

$$\lfloor \log_2(96) \rfloor + 1 = 7 \text{ bit}$$

$$\log_2(256) = 8 \text{ bit}$$

lunghezza "binaria" della chiave equivalente

ho compresso di un bit

Ecco il numero di chiavi nel cifrario di Hill 2x2

Modulo	Numero chiavi
1	0
2	6
3	48
4	96
5	480
6	288
7	2016
8	1536
9	3888
10	2880
11	13200
12	4608
13	26208
14	12096
15	23040
16	24576
17	78336
18	23328
19	123120
20	46080
21	96768
22	79200
23	267168
24	73728
25	300000
26	157248
27	314928
28	193536
29	682080
30	138240
31	892800

$m=4$

$m=8$

$m=16$ $\quad 2^x$

$m=32$

anche
nel caso $n=2$ $m=26$ (4)

$$\frac{\#\text{ chiavi valide}}{\#\text{ chiavi possibili}} = \frac{157.248}{456.976} = 34.7\%$$

$m = 2 \times 13$

keysize in bit $\lfloor \log_2(157.248) \rfloor + 1 = \underline{18}$ bit

$\lfloor \log(456,976) \rfloor + 1 = \underline{19}$ bit

$(456,976) = \frac{5,659}{18,8}$

comprensione di un bit $\lg_2 = \frac{\log_{10}(157.248)}{\log_{10} 2} = \frac{5,196}{0,301} = 17,2$

---

nel caso $m = 26 = 2 \times 13$

$$mcd[(ad-bc), 26] = 1$$

quindi il det M deve essere diverso da zero, dispari (non multiplo di 2), e

diverso da 13.

in $\mathbb{Z}_{26}$ ci sono uno ZERO
13 DISPARI
12 PARI

$\overline{26}$

in $\mathbb{Z}_{26}^*$ ci sono $\underline{12}$ dei 13 dispari

infatti $\varphi(26) = 12$ tutti tranne il 13!

1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 applicando lo stesso procedimento per trovare $ad - bc \Rightarrow$ DISPARI

si ottiene

per $x = ad$ e $y = bc$ $26 \times 26 = 676$

$P \cdot P = P$
$P \cdot D = D P = P$
$D \cdot D = D$

di cui solo $13 \times 13 = 169$ sono dispari le altre no 507

allora x tutti i 13 dispari finora validi sarebbero

$$(169 \times 507) + (507 \times 169)$$

$$= 2 \times 85683 = 171.366$$

un numero di dispari non lontano dai 157.268 divisi da 13.

I numeri 13 sono quindi 14.098 su 171.366

circa l'8,27% non lontano dalla distribuzione "uniforme" $\frac{1}{13} \cong 7{,}7\%$.

anche se sono un po' di più di 13.182.

(1)

Cifrario di Hill

$n \times n \quad 32 \times 32 = 2^5 \times 2^5 = \underline{1024} = 2^{10}$

coefficienti della matrice M

$\det M \equiv 1 \pmod{m}$

Scelta di $m = 256 = 2^8$

es. in $GF(2^8)$

$\gcd(\det M, 2^8) = 1$

$(\underline{\det M \equiv \text{dispari}})$

$\log_{10} 2 = 3{,}098$

$\log_2 10 = 3{,}322$

Quante chiavi?

$\#\text{chiavi possibili} = (256)^{1024} = \approx 1{,}1 \times 10^{2466} \approx 2^{2466 \times \log_2 10} \approx 2^{2{,}466 \times 3{,}322} \approx 2^{8.192}$

$(2^8)^{1024} = 2^{8192}$

$\boxed{\text{è come avere una chiave binaria a 8.192 bit}}$

 # chiavi valide

$\det M_{32 \times 32}$ = numero dispari $\in \mathbb{Z}_{256} \equiv \{0, -255\}$

127 dispari in 256

(2)

se fossero ~~...~~ i det M uniformemente distribuiti allora le chiavi valide sarebbero

$$\simeq \frac{2^{8192}}{2} = \underline{2^{8.191}}$$

Probabilmente, non sono uniformemente distribuiti ci sono più ZERI e pochi dispari

8000 bit is safe?

{attacco del testo in chiaro noto! Come si contrasta? (Vedremo con GF(8)) !!}

$n = \boxed{16 \times 16} = 256$

$(2^8)^{256} = 2^{1024}$

{chiave di 1000 bit? valida}

$\boxed{\det M = \text{dispari}}$

STREAM CIPHERS - OTP & LFSR

One-Time Pad

(1)

GILBERT VERNAM & JOSEPH MAUBORGNE
1918

messaggio M $|M| = b$, bit

Chiave K $|K| = b$, bit

$$C = M \oplus K$$

$$M = C \oplus K$$

Metodo di cifratura perfetta se

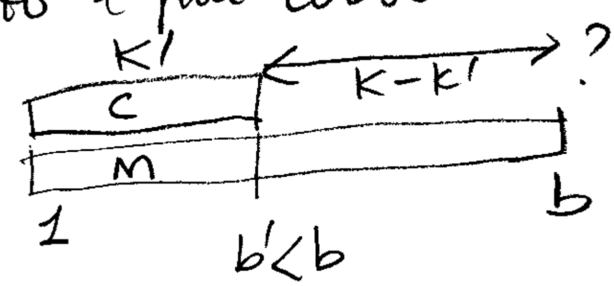
(1) $b \gg 0$ $b \to \infty$

(2) K è scelta in modo casuale

(3) e viene usata una sola volta

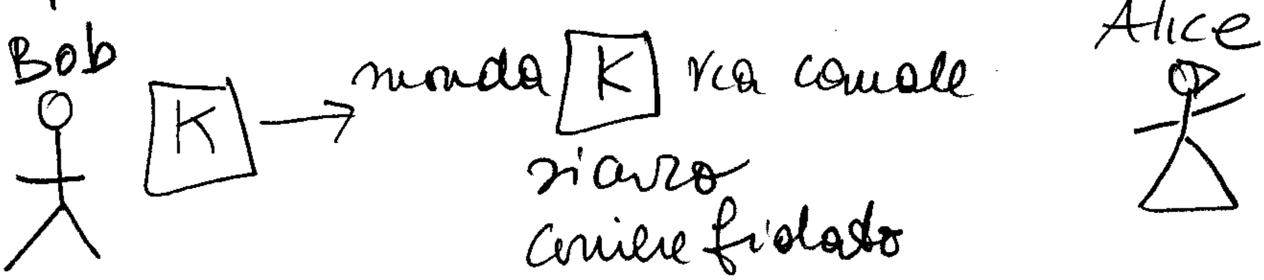
È imbattibile per attacchi ciphertext only.

- Nel caso di chosen plaintext, o chosen ciphertext se il testo è più corto di b anche se troviamo la chiave K' non sappiamo



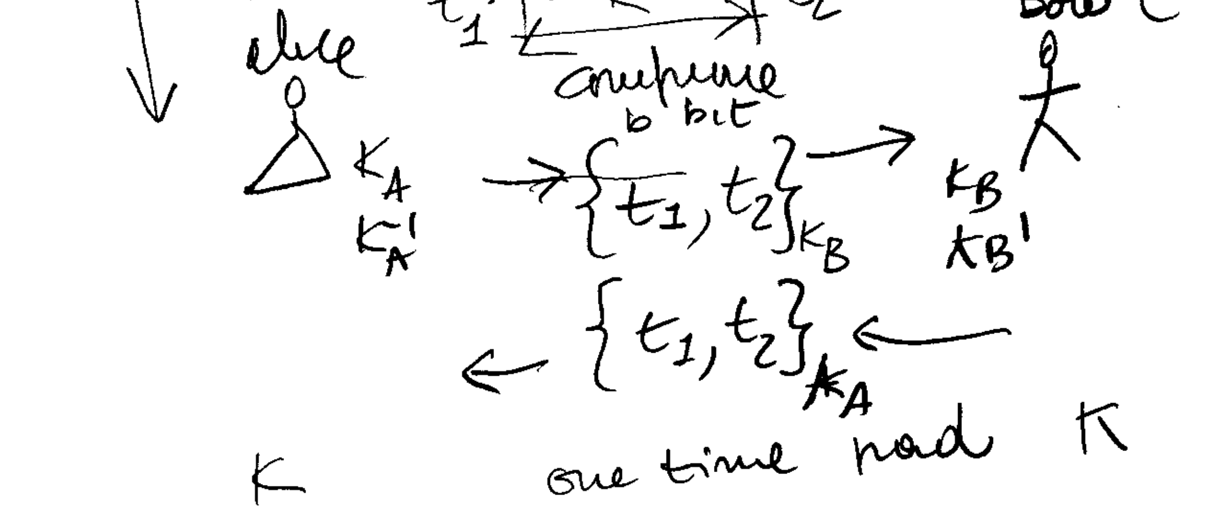
nulla del resto della chiave K fino a b bit.
Inoltre se trovo la chiave, questa viene usata una volta sola!

generazione di un numero casuale binario lungo b, bit.
è un problema si generano solo numeri pseudocasuali (non del tutto casuali).



Chiave molto lunga e trasmissione "fidata".
Per esempio posso mandare una chiave "seme" lunga $b' \ll b$ e il ricevente la usa per generare K lunga b.

3° metodo di MAURER, RABIN, DING.



Generazione di bit pseudocasuali

In "C" la libreria contiene rand() che genera numeri pseudocasuali tra 0 e 65.535.

Un generatore congruenziale lineare

produce i numeri $x_1, x_2 \ldots$ ove

$$X_n \equiv a X_{n-1} + b \pmod{\underline{m}}$$

$$1 \leq n \leq \infty$$

X_0 e' il SEME

mentre a, b e m sono parametri

in rand(), $m = 2^{16} = 64.536$ $0 \leq X_n \leq 64.535$, $a = X_1$; $b = X_2$

Questi generatori sono insicuri nel senso che osservando la una sequenza di bit si può prevedere la sequenza dei bit successivi con alta probabilità.

Due modi per creare bit non predicibili:

Funzioni one-way "unidirezionali"

$y = f(x)$ easy to compute

$x = f^{-1}(y)$ infattibile computazionalmente, computationally infeasible

essendo $f^{-1}[f(\bullet)] = \bullet$

(4)

Prendiamo un SEME s a caso

$$x_0 = f(s) \qquad j=0$$

$$x_j = f(s+j); \quad j = 1,2,3 \dots$$

1 - DISPARI
0 - PARI

se b_j è il bit meno significativo di x_j allora $b_0, b_1, b_2, \dots$ è una sequenza pseudocasuale di bit.

$$f \equiv DES; \; SHA$$

BLUM-BLUM-SHUB (BBS) generatore di bit pseudocasuali

generatore dei residui quadratici

Si generano due primi grandi p e q

$$p \equiv q \equiv 3 \pmod 4$$

Si pone

$$n = p \cdot q$$

e si sceglie un intero a caso $x \perp n$

$$mcd(x, n) = 1$$

SEME $\quad x_0 = x^2 \pmod n$

1. $x_j \equiv x_{j-1}^2 \pmod n$
2. $b_j \equiv$ è il bit meno significativo di x_j

LFSR Linear Feedback Shift Register

$x_1 \equiv 0,\ x_2 \equiv 1,\ x_3 \equiv 0,\ x_4 \equiv 0,\ x_5 \equiv 0$

vettore inizializzazione $\{0,1,0,0,0\}$

Coefficienti della ricorrenza lineare di lunghezza uguale a m (intero>0) [n indice corrente]

$$x_{n+m} = c_0 x_n + c_1 x_{n+1} + \dots + c_{m-1} x_{n+m-1} \pmod 2$$

es. $m = 5$

$$x_{n+5} \equiv x_n + x_{n+2} \pmod 2$$

$c_i \in \mathbb{Z}_2$

coefficienti $\{ \overset{c_0}{1}, \overset{c_1}{0}, \overset{c_2}{1}, \overset{c_3}{0}, \overset{c_4}{0} \}$ $c_i <^{0}_{1}$ mod 2

la ricorrenza è periodica di periodo d_{max}, ove

inoltre $2^m - 1 = d_{max} =$ periodo massimo della ricorrenza $\quad 2^5 - 1 = 31$ periodo max

altro esempio

$m = 31$ $\quad x_{n+31} = x_n + x_{n+3} \pmod 2$

$$d_{max} = 2^{31} - 1 \cong 2 \times 10^9$$ due miliardi di cifre!

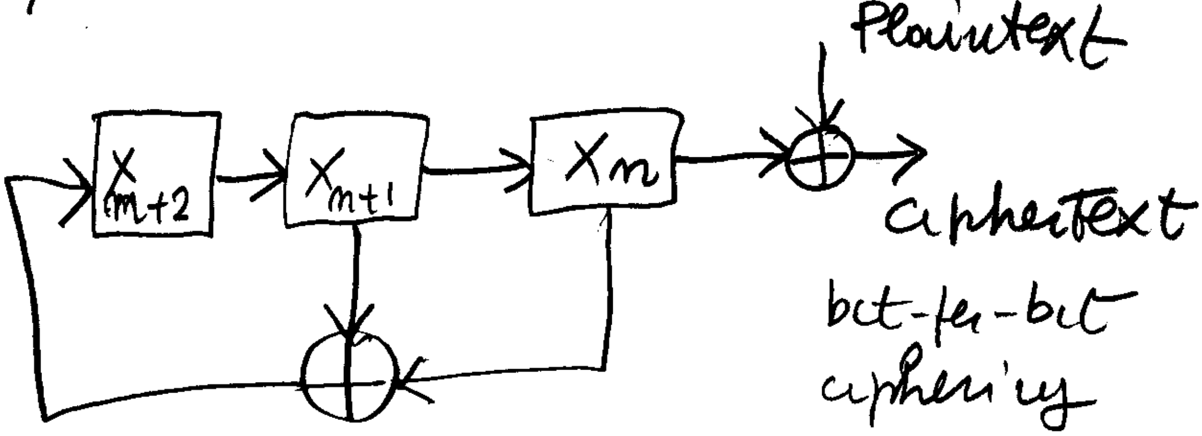
Realizzazione con registri a scorrimento (shift registers)

esempio

$$X_{n+3} = X_n + X_{n+1} \pmod 2$$

$m = 3$

$d = d_{max} = 2^3 - 1 = 7$



clocked bit shift

i bit nei box sono spostati da un clock

$$C = P \oplus K$$

$m = 3$ $\quad X_{n+3} = X_n \oplus X_{n+1}$

Vettore iniziale $[x_1, x_2, x_3]$ $\quad n=1, n+1=2, n+2=3$

Attacco "known plaintext" alla scoperta della chiave (sequenza di bit generata da uno scorrimento lineare di lunghezza m)

$$P \Leftrightarrow C$$

es. $\underbrace{101}_{a \text{ bit}}$ $\quad \underbrace{100}_{a \text{ bit}}$

allora faccio $P \oplus C = K'$ lunga "a" bit

$a < d$ lunghezza chiave

Si può attaccare e servono pochi bit $2m$ $\quad d_{max} = 2^m - 1$

Supponiamo di conoscere il segmento di 12 bit iniziale

011|010|111|100|

della sequenza

011|010|111|100|010|011|010|111|...

di periodo 15 generata da una ricorrenza lineare.
Come si determinano i coefficienti?
Noi conosciamo la lunghezza m. Cominciamo con $m=2$
($m=1$ è una sequenza costante)

$$x_{n+2} = c_0 x_n + c_1 x_{n+1} \qquad m=2$$

con vettore $x_1 = 0$; $x_2 = 1$ ($n=1$; $n=2$)
iniziale
e usiamo i valori noti
Known Plaintext

$$\begin{cases} x_3 = c_0 x_1 + c_1 x_2 = 1 \\ x_4 = c_0 x_2 + c_1 x_3 = 0 \end{cases} \pmod 2$$

otteniamo le equazioni

$$1 \equiv c_0 \cdot 0 + c_1 \cdot 1$$
$$0 \equiv c_0 \cdot 1 + c_1 \cdot 1 \qquad \pmod 2$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

la cui soluzione è $c_0 = 1$ e $c_1 = 1$ ($\det M = 1$)
per cui $x_{n+2} = x_n + x_{n+1}$: ma NON è così perché

$$x_6 = 0 \neq x_4 + x_5 = 0 + 1$$

Proviamo quindi $m=3$.

l'equazione matriciale per $m=3$ diventa (8)

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \pmod{2}$$

il $\det M = 0 \bmod 2$.

prendiamo allora $m=4$

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

che è risolubile e risulta $c_0 = 1;\ c_1 = 1$
$c_2 = 0;\ c_3 = 0$

per cui $\underline{X_{n+4} \equiv X_n + X_{n+1}} \pmod{2}$

che è la sequenza corretta!

ora il periodo risulta esattamente $2^4 - 1 = 15 = d_{max}$

in quanto il polinomio

$$f(x) = X^4 + X + 1 \quad \text{in } \mathbb{Z}_2[X]$$

risulta irriducibile e primitivo in

$\mathbb{Z}_2[X] \pmod{X^4 + X + 1}$.

in genere

$$X_{n+m} \equiv c_0 X_n + c_1 X_{n+1} + \quad + c_{m-1} X_{n+m-1} \pmod 2$$

m

con $c_i \in \mathbb{Z}_2$ $\quad 0 \leq i \leq m-1$

$2^m - 1 = d_{max}$ lunghezza massima della ricorsa

se il Polinomio

$$f(X) = X^m + c_{m-1} X^{m-1} \dots + c_0$$

è irriducibile mod 2, allora risulta: $\boxed{d = \frac{2^m - 1}{k}}$

allora il periodo divide 2^m-1 $\longrightarrow$ $d \mid 2^m - 1$ $\quad \boxed{2^m - 1 = k d}$ per certi k

e cioè $2^m - 1$ è multiplo di $\underline{d}$

primi di Mersenne

ma se $2^m - 1 = p$ primo es $m = 31$

$$2^{31} - 1 \simeq 2 \times 10^9 \text{ bit}$$

il periodo è massimo $\boxed{d = 2^m - 1 = d_{max}}$

Vediamo!

10

$$\pi(x) = x^m + c_{m-1} x^{m-1} + c_{m-2} x^{m-2} + \dots + c_0$$

è irriducibile modulo 2

$\mathbb{Z}_2[x] \pmod{\pi(x)}$ è il

Campo $GF(2^m)$

---

tutti i polinomi sono generatori se 2^m-1 è primo in $GF^*(2^m)$: x ad esempio

e tutti gli elementi si generano

$$x^1 \equiv x,\ x^2;\ x^3\ ,\ x^{2^m-1}.$$

pertanto $d = 2^m-1$ è il periodo della ricorrenza

$$x^{2^m-1} \equiv 1 \pmod{\pi(x)}$$

$\boxed{\text{Definizione}}$ $\boxed{\text{In generale}}$

$$x \cdot x^{m-1} = x^m \equiv c_0 + c_1 x + c_2 x^2 + \dots$$
$$\dots + c_{m-1} x^{m-1}$$

moltiplicazione per "x"

$$M_x = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ \vdots & & \cdots & & \vdots \\ 0 & 0 & \cdots & 1 & c_{m-1} \end{pmatrix} \qquad M_x^{2^m-1} \equiv I$$

$$I = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

10 BIS

Supponiamo che conosciamo

$$x_n, x_{n+1}, \dots x_{n+m-1}$$

allora calcoliamo

$$\begin{pmatrix} x_n \dots x_{n+m-1} \end{pmatrix} M_X = \left(x_{n+1}, x_{n+2}, \dots, (c_0 x_n + \dots c_{m-1} x_{n+m-1})\right)$$
$$= \left(x_{n+1}, x_{n+2}, \dots, x_{n+m}\right)$$

per cui la moltiplicazione per M_X fa scorrere gli indici di 1.

Se si moltiplica a destra per M_X^j si fanno scorrere gli indici di j

$$(x_1 \dots x_m) \, M_X^j = (x_{1+j} \dots x_{m+j})$$

Se $M_X^j = I$ si torna al vettore iniziale $(x_1, \dots x_m)$

Ma per Lagrange si ha che $M_X^{2^m-1} = I$ per cui sappiamo che

$$x_1 \equiv x_{2^m} \; ; \; x_2 \equiv x_{2^m+1} \; \dots$$

La sequenza si ripete con periodo $d = k$ intero positivo più piccolo per cui $x^k \equiv 1 \pmod{z(x)}$

e $k \mid 2^m - 1$, essendo x radice primitiva di $GF(2^m)$

per esempio $m=3$ $\quad GF(2^3)$ $\quad$ 11

$$f(x) = x^3 + x + 1 \qquad 2^3 - 1 = 7 = p$$

in generale
ove
$$f(x) = x^m + c_{m-1} x^{m-1} + \quad + c_1 x + c_0$$

$$\{c_{m-1}, c_{m-2}, \dots c_2, c_1, c_0\}$$

$$m-1 = 2$$

$$f(x) = \{\overset{c_2}{0}, \overset{c_1}{1}, \overset{c_0}{1}\}$$

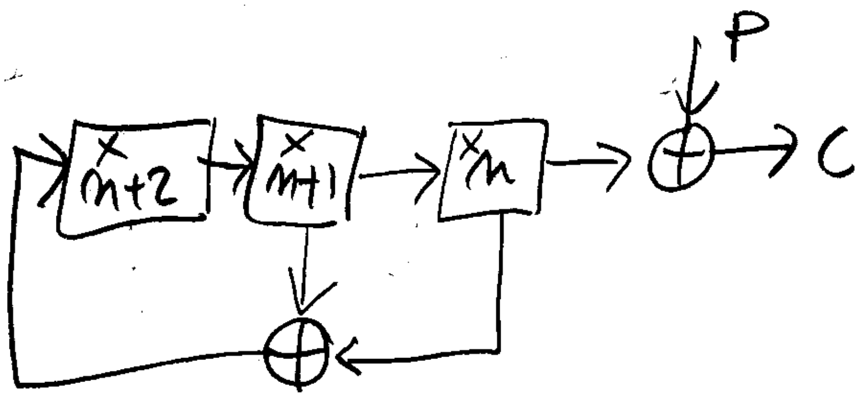
con incremento è

$c_0 = 1$
$c_1 = 1$
$c_2 = 0$

$$x_{n+3} = c_0 x_n + c_1 x_{n+1} + c_2 x_{n+2}$$

il periodo della sequenza è $d = 2^3 - 1 = 7$ bit

$$\boxed{x_{n+3} = x_n + x_{n+1}}$$



Registro LFSR a 3 bit $\quad VI \equiv \{x_1, x_2, x_3\}$
a scrambler - scrambler

$n = 31 = p$ 12

$2^{31}-1$ $\qquad 2^{p}-1 =$ primo

$2^{31} = 2.147.483.648 -$
1

$2^{31}-1 \Rightarrow \underline{2.147.483.647}$

primo numero di **Mersenne**

No generatori

$$\phi(2^{31}-1) = 2^{31}-2 = 2.147.483.646$$

No irriducibili e primitivi

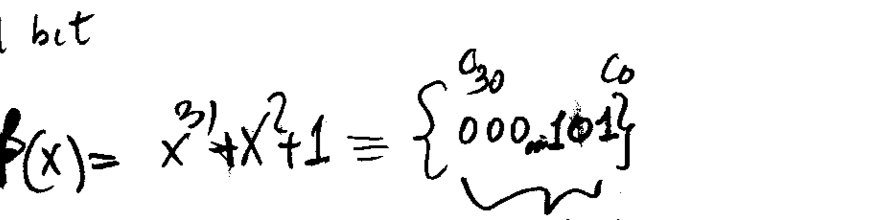
$$\frac{\phi(2^{31}-1)}{31} = \frac{2^{31}-2}{31} = 69.273.666$$

$n=31$

31 bit

$$f(x) = x^{31}+x^2+1 \equiv \{\underbrace{\overset{c_{30}}{0}00\ldots10\overset{c_0}{1}}_{31\text{ bit}}\}$$

$$X_{m+31} = X_m + X_{m+2}$$



per craccare uno scrambler m=31 bastano 62=2m known plaintext bits e corrispondenti ciphertext bits

scrambler per TPR MP3 MP4

$$V1 = \{x_1, x_2 \ldots x_{31}\}$$

in generale attacco "Known plaintext" alla chiave (13)

Per scoprire una ricorrenza lineare di lunghezza m servono $2m$ bit

bit : $x_1, x_2 \dots x_{2m}$

si effettua il calcolo

$$\textcircled{1} \quad \begin{pmatrix} x_1 & x_2 & \dots & x_m \\ x_2 & x_3 & \dots & x_{m+1} \\ \vdots & & \ddots & \vdots \\ x_m & x_{m+1} & \dots & x_{2m-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \end{pmatrix} = \begin{pmatrix} x_{m+1} \\ x_{m+2} \\ \vdots \\ x_{2m} \end{pmatrix}$$

la matrice è invertibile (mod 2)

se non c'è alcuna ricorrenza di lunghezza inferiore a m che è soddisfatta da $x_1, x_2 \dots x_{2m-1}$.

Teorema Sia $x_1, x_2, x_3 \dots$ la sequenza di bit prodotta da una ricorrenza lineare mod 2. Per ogni $n \geq 1$, sia M_n. Sia N la lunghezza della più corta ricorrenza che genera la sequenza $x_1 \div x_{2m-1}$

$$M_n \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_2 & x_3 & \dots & x_{n+1} \\ x_n & x_{n+1} & \dots & x_{2n-1} \end{pmatrix}$$

allora $\begin{cases} \det(M_N) \equiv 1 \pmod 2 \\ \det(M_n) \equiv 0 \quad \text{per } n > N \end{cases}$

Supponiamo di conoscere i primi 100 bit della chiave generata da una sequenza lineare di lunghezza incognita m.

Per $m = 2, 3, 4 \ldots$ si costruisca la matrice $M_m \equiv (m \times m)$ e si calcoli il determinante. Se trovo valori consecutivi di m avanzati rendono $\det M_m \equiv 0 \pmod 2$ STOP. L'ultimo m^* che dà $\det M_{m^*} \equiv 1 \pmod 2$ è probabilmente la lunghezza della sequenza $m = m^*$.

Ora si applica l'equazione (1) con $M^{-1}_{m^*}$ per calcolare

$$\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m^*-1} \end{pmatrix} = M^{-1}_{m^*} \begin{pmatrix} x_{m+1} \\ x_{m+2} \\ \vdots \\ x_{2m} \end{pmatrix}$$

Calcolati i coefficienti si verifica se generano i primi 100 bit. Se non è verificato, <u>bisogna provare con valori più elevati di m.</u>

Esempio

$m=3 \quad 2^3-1=7=d$

$r(x) = x^3 + x + 1$ irriducibile in $\mathbb{Z}_2(x)$ di grado 3

$$z(x) = x^m + c_{m-1} x^{m-1} + \dots + c_1 x + c_0$$

$$z(x) = x^3 + (0)x^2 + 1 \cdot x + 1$$

$c_2 = 0$
$c_1 = 1$
$c_0 = 1$

$$x_{n+3} = x_n + x_{n+1}$$

supponiamo $x_1 = 1$; $x_2 = 0$; $x_3 = 0$

sequenza

$$\overbrace{1\ 0\ 0\ 1\ 0\ 1\ 1}^{\text{periodo}}\ \overbrace{1\ 0\ 0\ 1\ 0\ 1\ 1}^{\text{periodo}}\ 1$$

$$\begin{array}{ccccccccccccccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 & x_{10} & x_{11} & x_{12} & x_{13} & x_{14} & x_{15} \end{array}$$

$$M_3 = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_4 \\ x_3 & x_4 & x_5 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} x_4 \\ x_5 \\ x_6 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

$\det M_3 = 1$ ok $\quad \begin{cases} c_0 = 1 \\ c_2 = 0 \\ c_1 = 1 \end{cases}$ ok!

5BIS

La sequenza generata da una ricorrenza lineare di lunghezza $m=3$ comincia con

001110

trovare i seguenti 4 elementi della sequenza

Scriviamo l'equazione

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \pmod 2$$

da cui $c_0 = 1$; $c_1 = 0$ e $c_2 = 1$ per cui la ricorrenza è

$$k_{n+3} \equiv k_n + k_{n+2} \pmod 2$$

i successivi termini sono

1 0 0 1

Si consideri la sequenza con vettore iniziale (V) $k_1 = 1$; $k_2 = 0$; $k_3 = 1$ definita da ($m=3$) ricorrenza lineare: $K_{n+3} = k_n + k_{n+1} + k_{n+2}$. (1) (mod 2)

Questa sequenza può essere generata da una di lunghezza $m=2$. Qual'è

sequenza (1) con vettore iniziale (V) è

1 0 1 0 1 0 1 0 1 0 . . .

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad c_0 = 1 \quad c_1 = 0$$

$$K_{n+2} = K_n \pmod 2$$

Per ovviare all'attacco ai LFSR si possono usare le ricorrenze "non lineari", del tipo

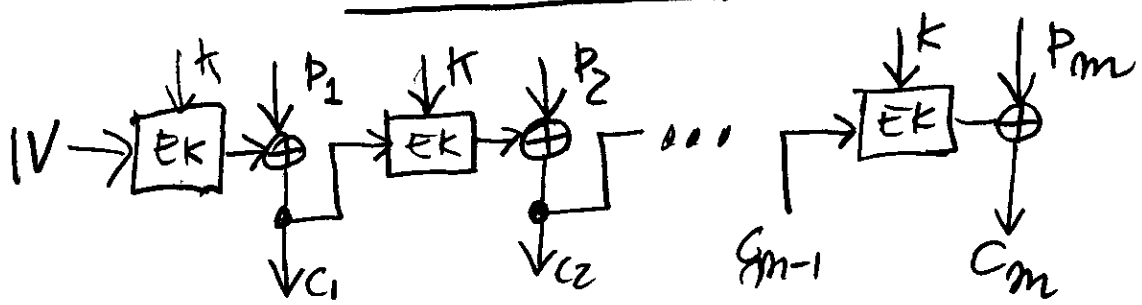
$$X_{n+3} \equiv X_{n+2} \cdot X_n + X_{n+1}$$

molto più difficili da attaccare.

Osservazione Modo di funzionamento

Cipher Feedback Mode CFB

è simile a OTP e LFSR



in pratica la chiave K, la lunghezza m e il vettore iniziale IV costituiscono la chiave da usare in XOR con il testo. Se $m = 64$ e $|P_i| = 64$ bit e $|IV| = 64$ bit. Un testo di $2^{12} \equiv 4096$ bit è cifrato XOR con una "chiave" lunga uguale prodotta da K usata da DES operante sui bit di testo fino al 4032-esimo bit e sul vettore IV.

CFB può essere usato per rivelare errori di trasmissione.

Publickey crittografia algoritmi

RSA ① Fattorizzazione
Rabin ② Radici quadrati
ElGamal ③ Logaritmi discreti
Diffie-Hellman

in $\mathbb{Z}_p$ in $GF(p^n)$ in ECC

campi gruppo abeliano

in lattice = reticoli
campi rigini ai reticoli multidimensionali

altri
- McEliece
- Knapsack
- Quantum

meccanismi

- Identity based encryption - IBE
- Zero-Knowledge - Fiat-Shamir-Feige
- secret sharing - Shamir schemes

cifrari a blocchi e a catene

Attacchi del crittoanalista

① ciphertext only - forza bruta e teoria dell'informazione crittoanalisi
② Known Plaintext-
③ Chosen Plaintext-
④ Chosen ciphertext-

crittoanalisi

Crittoanalisi

Crittoanalisi differenziale attacco chosen plaintext

Crittoanalisi lineare attacco known plaintext

basati sulla alta probabilità di occorrenza di codici all'ultimo round dei cifrari a blocchi del tipo DES e AES

block ciphers
iterated-ciphers

SUBSTITUTION-PERMUTATION NETWORK
SPN

P, C vettori binari di lunghezza ℓm

ℓm - block length del cifrario a blocchi

S-box substitution box
è la permutazione

$$\pi_S : \{0,1\}^\ell \to \{0,1\}^\ell$$

P-box permutation box
è la permutazione

$$\Pi_P : \{1, \ldots, \ell m\} \to \{1, \ldots, \ell m\}$$

degli ℓm bit del blocco

S- sostituisce parole binarie es $\ell = 4$
es $\ell = 4$

$\to a_1 a_2 a_3 a_4 \to b_1 b_2 b_3 b_4 \leftarrow$

a_bit ingresso
b-bit uscita

P- permuta i bit singoli
es.

$\ell = m = 4$

16 bit

P = Plaintext = x

stringa binaria lunga b-bit

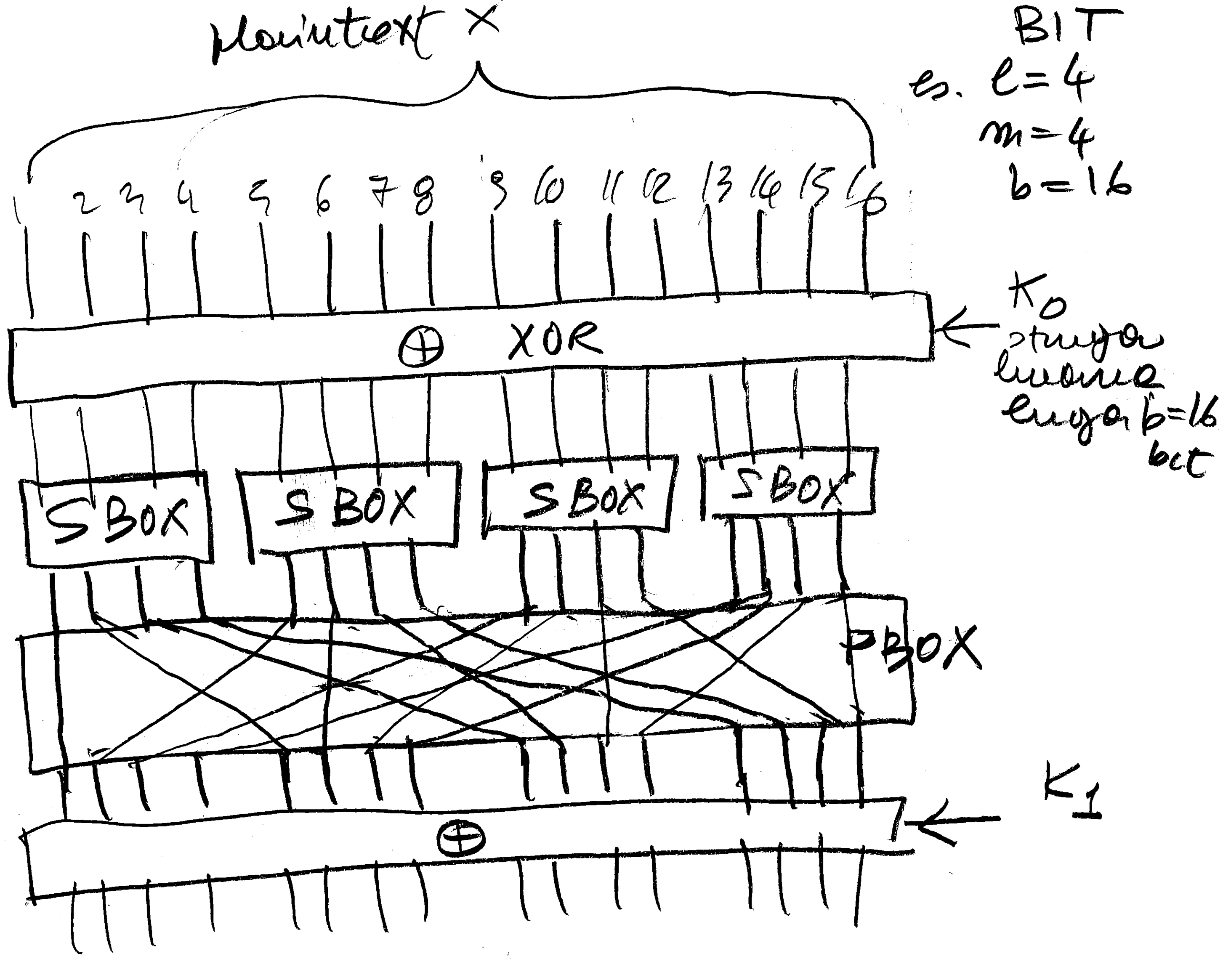
ora assumiamo che $b = m \cdot l$

ove

$$m = \frac{b}{l}$$

l = lunghezza in bit dei blocchi di sostituzione

$b = l \cdot m$ = lunghezza in bit dei blocchi di permutazione



$l=4$ corrispondono parole di 4 bit codice hex 4bit

es.

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

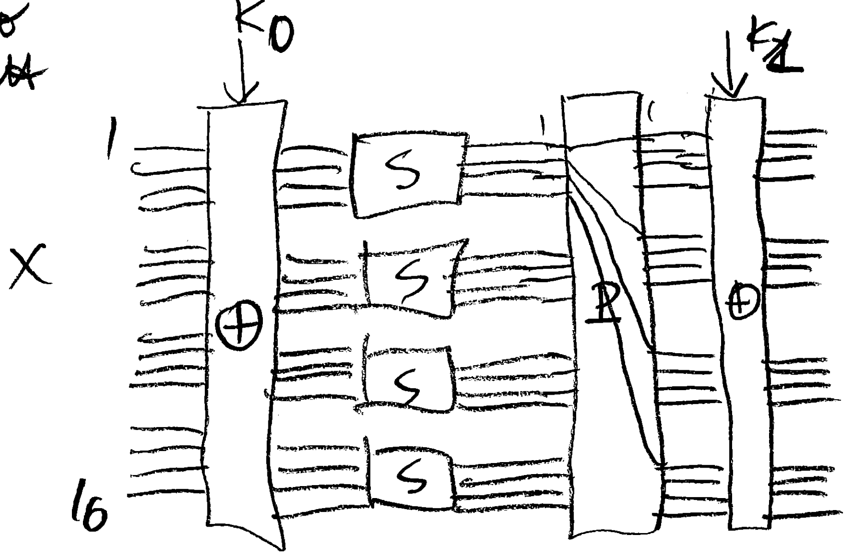
$a_i \updownarrow b_i$

LOOK-UP TABLE

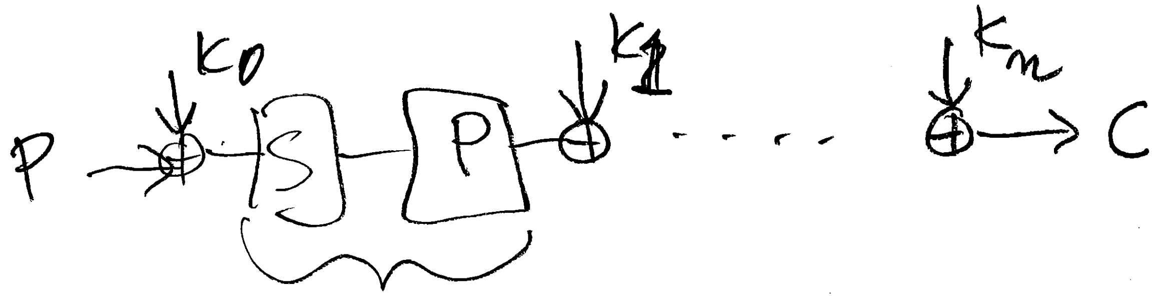
$m=4$

z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi_P(z)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

$l \cdot m = 16$ bit
Blocco lunghezza



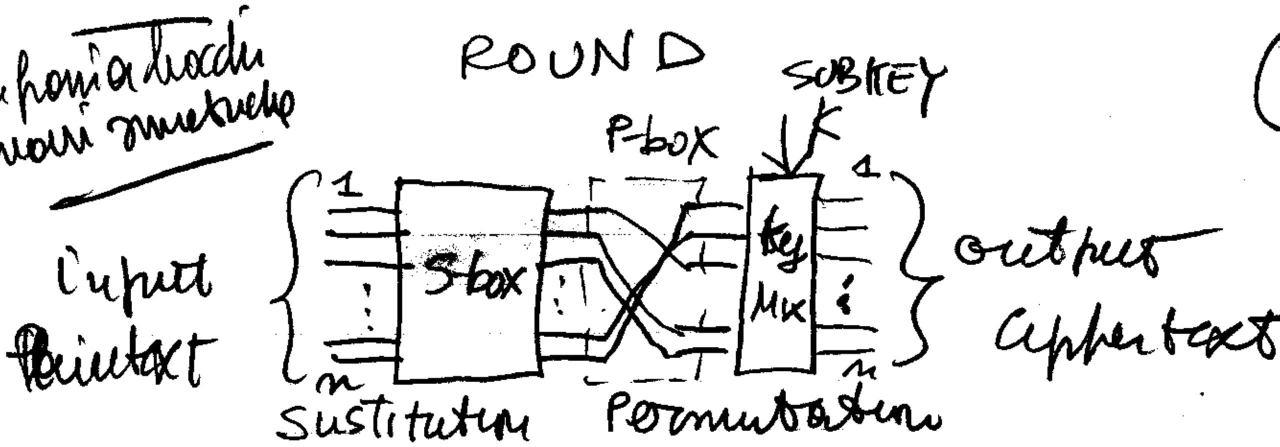
1st ROUND of n ROUNDS



$K_i \quad 0 \le i \le n$ $\qquad$ n - # Rounds

$K_S \rightarrow$ chiavi di round generati da una chiave "seed" - <u>seme</u> (chiave di sessione $K_{A,B}$)

le permutazioni dei blocchi devono simmetriche



es. $n = 16$ blocchi da 4 bit {hex}

SBox input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
output	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

DES S_1 BOX first row

PBox input	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
output	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

<u>Known Plaintext attack</u> - <u>Crittoanalisi lineare</u>

noti u bit d'ingresso del Plaintext X_i $1 \le i \le u$
v bit d'uscita del Ciphertext Y_j $1 \le j \le v$

si approssima il round

$$X_{i1} \oplus X_{i2} \oplus \cdots \oplus X_{iu} \oplus Y_{j1} \oplus Y_{j2} \oplus \cdots \oplus Y_{jv}$$

si noti che

se $X_1 \oplus X_2 = 0$ allora $X_1 = X_2$

$X_1 \oplus X_2 = 1$ allora $X_1 \neq X_2$ e $X_2 = \overline{X_1}$

<u>Chosen Plaintext attack</u> - <u>Crittoanalisi differenziale</u>

ΔX $\quad \xrightarrow{X} \boxed{\text{cif}} \rightarrow Y$ $\quad \underline{\Delta Y}$
$\quad \xrightarrow{X'} \boxed{\text{cif}} \rightarrow Y'$

probabilità di occorrenza di ΔY data una <u>scelta ΔX</u>

$\Delta X = X' \oplus X$ $\qquad \Delta Y = Y' \oplus Y$ $\qquad \underline{(\Delta X, \Delta Y) = \text{differenziale}}$

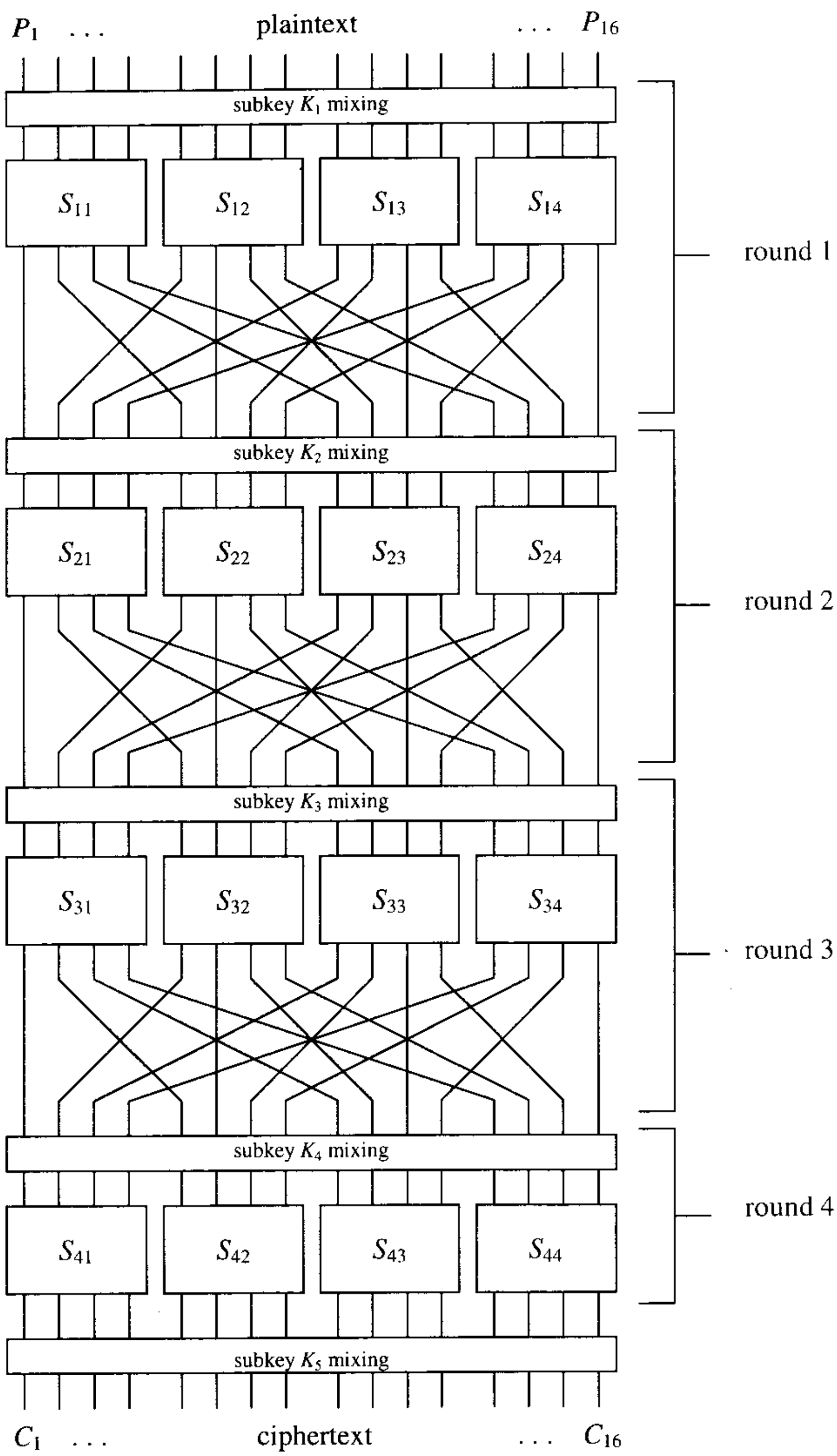
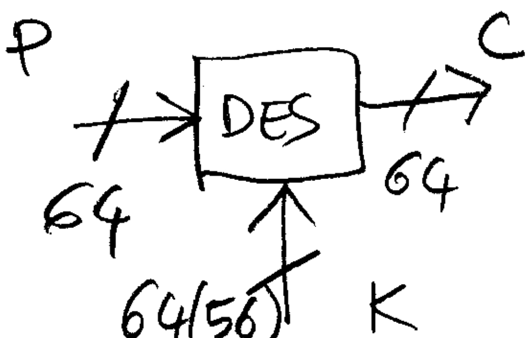


Figure 1. Basic Substitution-Permutation Network (SPN) Cipher

- DES 1977 e (AES 2001)
- SIMPLIFIED DES
- CRITTOANALISI DIFFERENZIALE X 3 ROUND
- DES at a glance
- MODES OF OPERATION ECB-CBC-CFB-OFB-CTR
- MEET-IN-THE MIDDLE ATTACKS



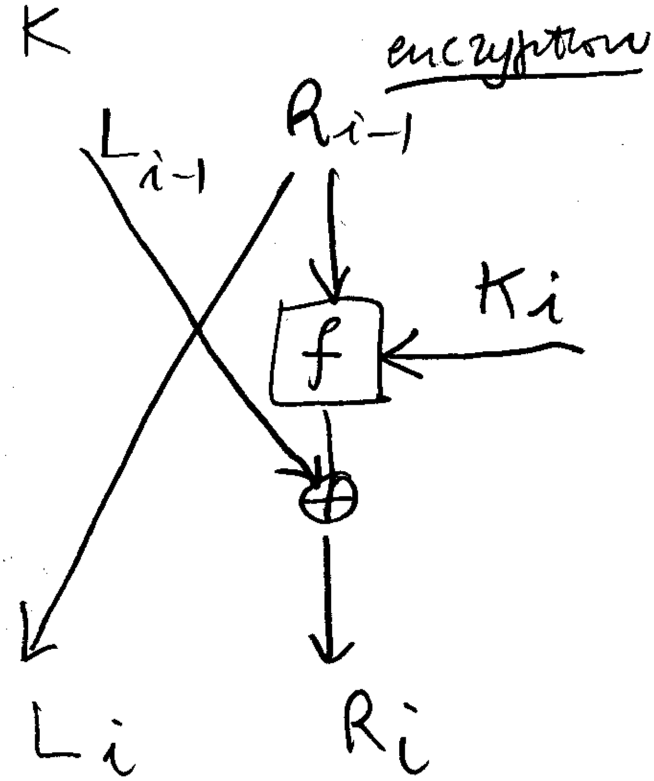
HORST FEISTEL

LUCIFER - IBM 1974

$(L_0, R_0) \rightarrow \boxed{1 \leq i \leq n} \rightarrow (L_n, R_n)$

funzione i-esimo ROUND

$$(1)\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \end{cases}$$

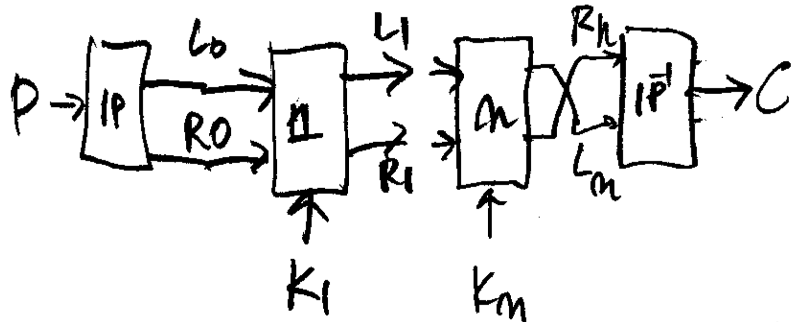


si ha che la funzione (1) è invertibile

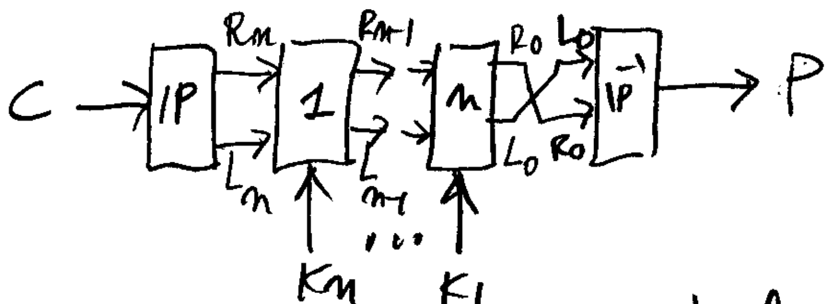
2

$$\begin{cases} L_{i-1} = R_i \oplus f(R_{i-1}, K_i) \\ R_{i-1} = L_i \end{cases}$$

nella decifratura

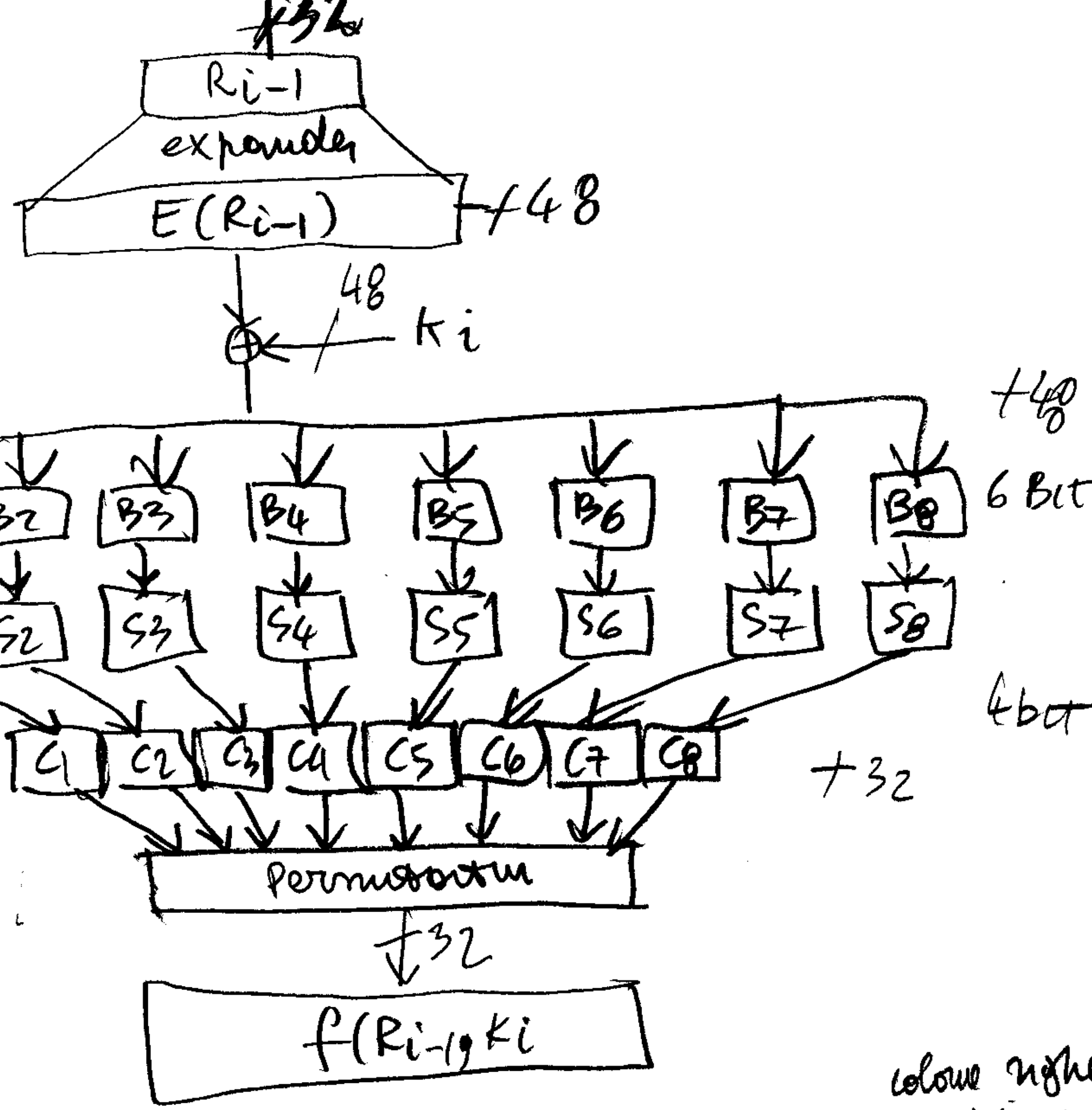


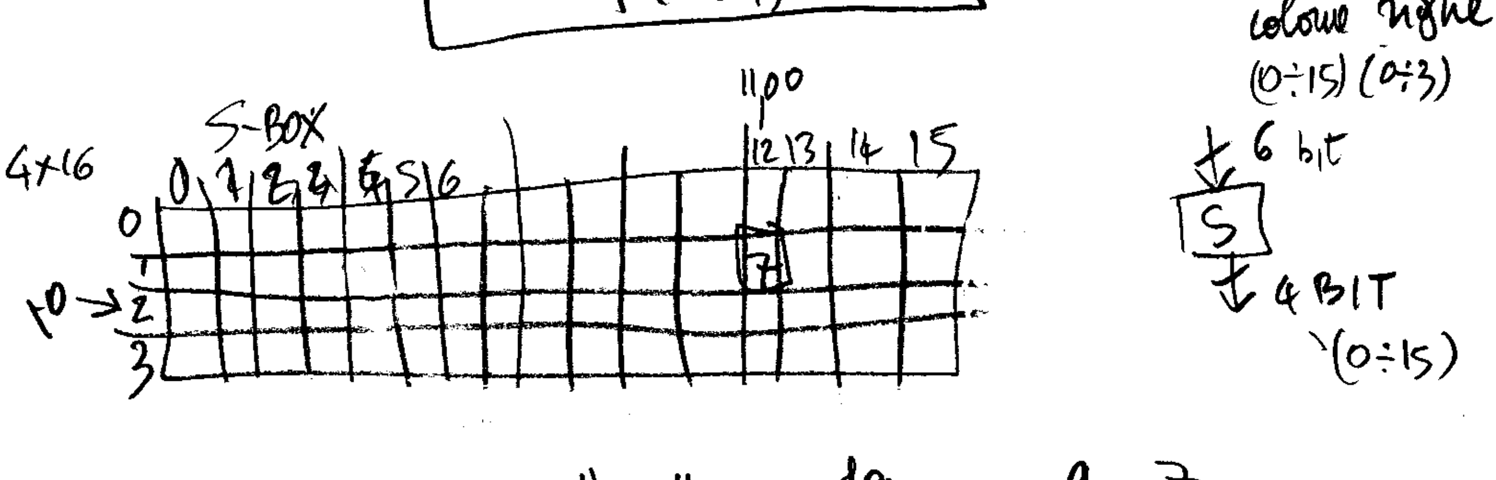
DES: $n=16$



Per decifrare la macchina è la stessa della cifratura basta usare le chiavi di round in ordine inverso. Si noti che il ciphertext è una permutazione di (R_n, L_n) e non (L_n, R_n). In decifratura (R_n, L_n) generano (R_0, L_0) che alla fine invertiti ~~de~~ permutati danno il plaintext
danno $(L_0 R_0)$

la funzione di Feistel $f(R_{i-1}, K_i)$
è la seguente





input colonna 12 "1100"
riga 2 "10"

da a 7
$1\boxed{1100}0$
111000 → 0111

ESERCIZI

Mostrare che se DES cifra con la chiave K il plaintext P in C, allora con $\overline{K}$ si cifra $\overline{P}$ in $\overline{C}$.

Soluzione I è la stringa di tutti "1". Noto che

$$E(\overline{R_{i-1}}) = \overline{E(R_{i-1})} = E(R_{i-1}) \oplus I.$$

Per cui

$$E(\overline{R_{i-1}}) \oplus \overline{K_i} = E(R_{i-1}) \oplus I \oplus K_i \oplus I =$$

$$= E(R_{i-1}) \oplus K_i$$

così che l'ingresso agli S-box non cambia e così come l'uscita non cambia. Ma

$$\overline{L_{i-1}} = L_{i-1} \oplus I$$

per cui la parte destra risulta

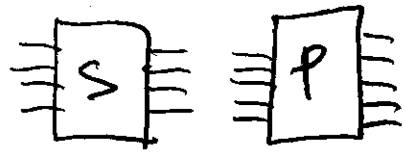
$$\overline{L_{i-1}} \oplus f(R_{i-1}, K_i) = R_i \oplus I = \overline{R_i}$$

mentre la nuova parte sinistra è la stringa complementata $\overline{L_i}$. Poiché è vero ogni round è vero per DES. cvd

EXOR I - tutti "1" O - tutti "0"

$$P \oplus I = \overline{P} \quad \rightarrow \quad P \oplus \overline{P} = I$$

$$P \oplus O = P \quad \rightarrow \quad P \oplus P = O$$



S-BOX P-BOX

SUBSTITUTION-BOX
PERMUTATION-BOX

se si cambia un carattere di P molti caratteri di C cambiano e viceversa — confusion

ogni carattere di C dipende da vari bit della chiave — diffusion

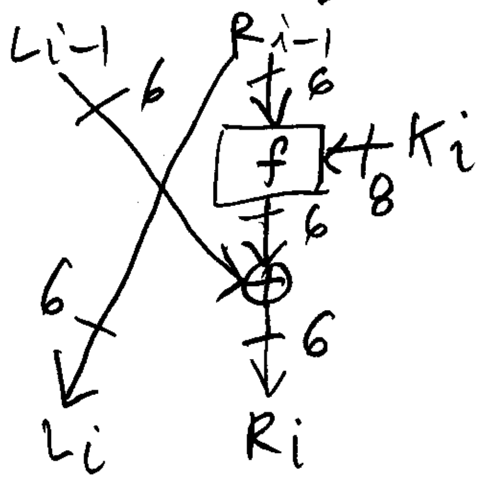
— non-linearity

ad es. {sostituzione non lineare, inverso moltiplicativo}

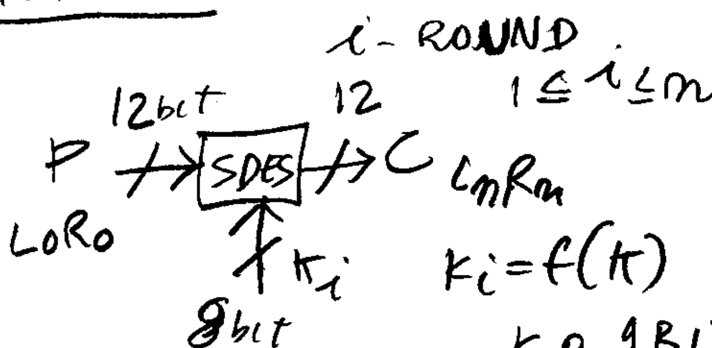
attacchi chosen plaintext

- crittoanalisi differenziale
- crittoanalisi lineare (known plaintext)

ESEMPIO DES SEMPLIFICATO



$f(R_{i-1}, K_i)$



$1 \le i \le n$

$K_i = f(K)$

K a 9 BIT

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \end{cases}$$

cifratura

$$\begin{cases} L_{i-1} = R_i \oplus f(R_{i-1}, K_i) \\ R_{i-1} = L_i \end{cases}$$

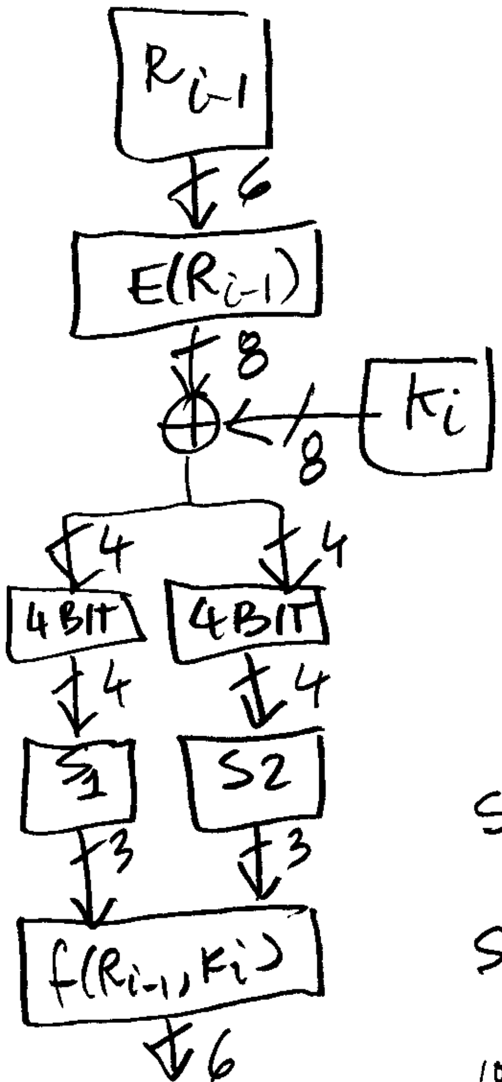
Decifratura

scambio

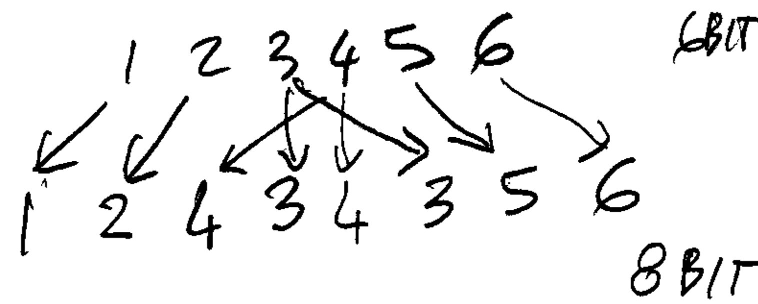
$C \to L_n R_n \to \underline{R_n L_n}$

$K_n \div K_1$ chiavi in ordine inverso

$$\overbrace{K_n, K_{n-1} \dots K_2, K_1}^{n \text{ round}}$$



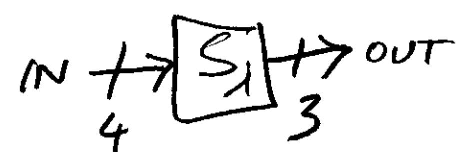
$E(R_{i-1})$



$$S_1 = \begin{bmatrix} 101 & 010 & 001 & 110 & 011 & 100 & 111 & 000 \\ 001 & 100 & 110 & 010 & 000 & 111 & 101 & 011 \end{bmatrix}$$

$$S_2 = \begin{bmatrix} 100 & 000 & 110 & 101 & 111 & 001 & 011 & 010 \\ 101 & 011 & 000 & 111 & 110 & 010 & 001 & 100 \end{bmatrix}$$

1° bit specifica la <u>riga</u>, 2°, 3°, 4° bit la <u>colonna</u>



e l'entry di 3 bit è l'uscita.

$K \equiv 9$ BIT

K_i è ottenuta usando 8 bit di K, <u>iniziando con l'i-esimo bit</u> e

$K = 010011001$

e.g. $K_4 = 01100101$

$$K_i \begin{cases} i = 1 \\ \vdots \\ i = n \end{cases}$$

n-round

se $R_{i-1} = 100110$ $\quad K_i = 01100101$

$$E(100110) \oplus K_i = 10101010 \oplus 01100101 =$$

$$= \underbrace{1100}_{S_1 \to 000} \; \underbrace{1111}_{S_2 \to 100}$$

$$f(R_{i-1}, K_i) = 000100$$

es. $L_{i-1} R_{i-1} = 011100 | 100110$

$K_i = 01100101$

$f(R_{i-1}, K_i) = 000100 \quad \oplus$

$\phantom{f(R_{i-1}, K_i) = } 011100 \quad L_{i-1}$

$R_i = 011000 \rightarrow L_i = R_{i-1}$

$L_i R_i = \underbrace{100110}_{L_i} | \underbrace{011000}_{R_i}$

DIFFERENTIAL CRYPTOANALYSIS $\quad$ BIHAM-SHAMIR 1990

ATTACCO CHOSEN PLAINTEXT

$\left\{ \begin{array}{l} P_1 \\ P_2 \end{array} \right. \rightarrow \boxed{E_{DES}} \rightarrow \begin{array}{l} C_1 \\ C_2 \end{array}$ $\oplus$ calcolo delle differenze XOR sui ciphertext per scelti plaintext

TRE RIPRESE

3 ROUND

partiamo da $\boxed{L_1 R_1}$ $\leftarrow$ scelti plaintext

per arrivare a $\boxed{L_4 R_4}$ $\leftarrow$ corrispondenti ciphertext l'attacco si può estendere a $n > 3$ round

le tecniche di analisi differenziale sono molto più efficienti di quelle di forza bruta fino a un certo valore di n. Per la scelta di DES si suppone che $n = 15$ sia la soglia

complessità crittoanalisi differenziale $< 2^{56}$ ⊗ complessità attacchi forza bruta 2^{56}

$n = 15$

per DES si scelsero infatti 16 round.

Se appunto DES a una funzione lineare

$C = f_{DES}(P)$ funzione lineare

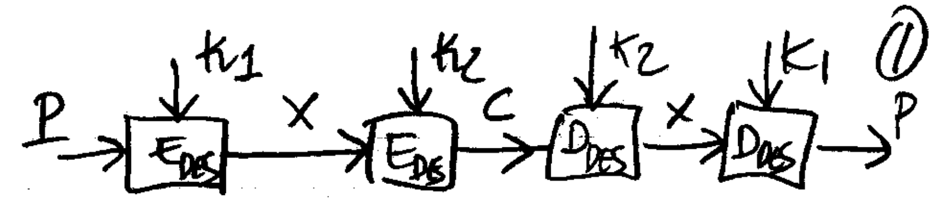
è più veloce della ricerca esaustiva

CRITTOANALISI LINEARE

richiede 2^{43} coppie $P \leftrightarrow C$ per individuare la chiave

attacco known plaintext

2^{43} coppie known $P \& C$



Double DES

$$C = E_{K_2}(E_{K_1}(P))$$

$$P_1 = D_{K_1}(D_{K_2}(C))$$

N.B.

Nell'affine
$C = aP + b \pmod n$
in RSA
$C = P^e \pmod n$

due cifrature in cascata equivalgono a una cifratura con chiave
Affine: $a = a_1 a_2$; $b = a_1 b_2 + b_1$ $\{$ a e b equivalenti
RSA: $e = e_1 \cdot e_2$ $\{$ esponenti di cifratura equivalenti

---

In DES no, ma la sicurezza è la stessa di quella di una sola cifratura.
Attacco Meet-in-The-Middle

Basta una coppia Known Plaintext → Ciphertext (P_1, C_1) ✓ per ridurre la complessità dell'attacco a quello di forza bruta su una sola chiave.
È simile all'attacco del compleanno, il numero di tentativi esaustivi è $2^{\frac{n}{2}}$ se n è la lunghezza in bit delle due chiavi K_1 e K_2: in DES 112 bit cioè 2^{56} tentativi come nell'attacco a una chiave DES di 56 bit. Si fa una doppia lista

$E_{K_1}(P_1)$ per $1 \leq K_1 < 2^{56} - 1$ $\qquad$ $D_{K_2}(C_1)$ per $1 \leq K_2 < 2^{56} - 1$

e si controlla se esistono una o più uguaglianze per cui

per $K_1 = K_1^*$, $K_2 = K_2^*$ $\quad (1)\ E_{K_1^*}(P_1) = D_{K_2^*}(C_1)$ che individuano la coppia di chiavi (K_1^*, K_2^*)

è come l'attacco del compleanno, ma è deterministico

Se c'è un solo match (1) OK la coppia (K_1^*, K_2^*) è la chiave. Se ci sono n coppie (K_1^*, K_2^*) allora bisogna avere a disposizione al massimo altri $(n-1)$ known plaintext del tipo (P_i, C_i) per $2 \le i \le n$, per identificare la coppia di chiavi corretta. Generalmente con due known plaintext si trova la coppia (K_1, K_2).

La memoria richiesta da una lista completa è circa

$2^{56} \times (56+64)$ bit (K_1 è lungo 56 bit e $E_{K_1}(P_1)$ 64 bit)

quindi per le due liste (usando 64 bit per immagazzinare le chiavi da 56) servono circa

$2^{56} \times 256 \text{(bit)} = 2^{61}$ byte $\gtrsim 10^{18}$ byte

che rappresenta una quantità di un milione di Terabyte (10^{12} byte) o mille Petabyte (10^{15} byte) assolutamente proibitiva nel 2007. (o 1 Exabyte (10^{18} byte)

Si stima che nell'anno 2007 sono stati prodotti nel pianeta terra circa 20 Exabyte (carta - film - dischi ottici - memorie solide - memorie magnetiche - ecc)

Inoltre il tempo di analisi è comunque molto elevato. Se si assume una frequenza di lettura di ciascun entry delle liste in 1 ns (10^{-9} s) e considerando 2^{56} entry e una lettura di forza bruta con m macchine in parallelo:

RSA 10K\$ # 96 days $\gtrsim$ 100 days $\gtrsim 10^7$ secondi (oggi < 1 gg)

computing power 1997 # 70.000 machines in parallel } 1 ns per scansione entry due liste

$\frac{1}{4}$ of key space analyzed before cracking the key $\quad \frac{2^{56}}{4} = 2^{54} \rightarrow \frac{2^{54}}{4} \gtrsim 10^{16} \rightarrow \frac{10^{16}}{10^7} = 10^9$ scan/secondo

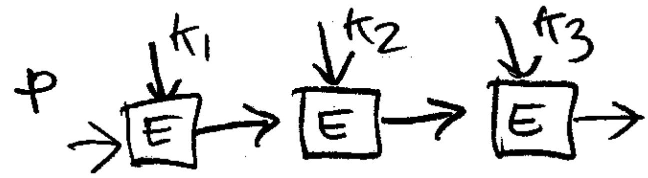
2007 $= \frac{\$}{2^7} \approx 100\$$

RSA CHALLENGE 1997 ||

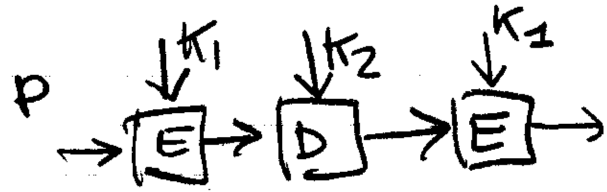
TRIPLE DES

56+56=112-bit

56×3=168-bit



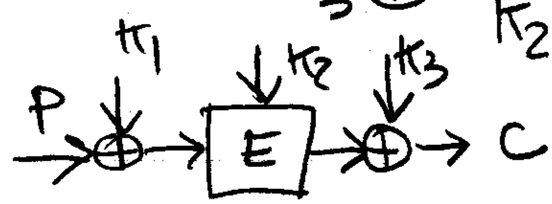
$C = E_{K_1}(E_{K_2}(E_{K_3}(P)))$



$C = E_{K_1}(D_{K_2}(E_{K_1}(P)))$ (*)

Rivest 3-DES scegli tre chiavi K_1, K_2 e K_3 e fai

$$K_3 \oplus E_{K_2}(K_1 \oplus P)$$

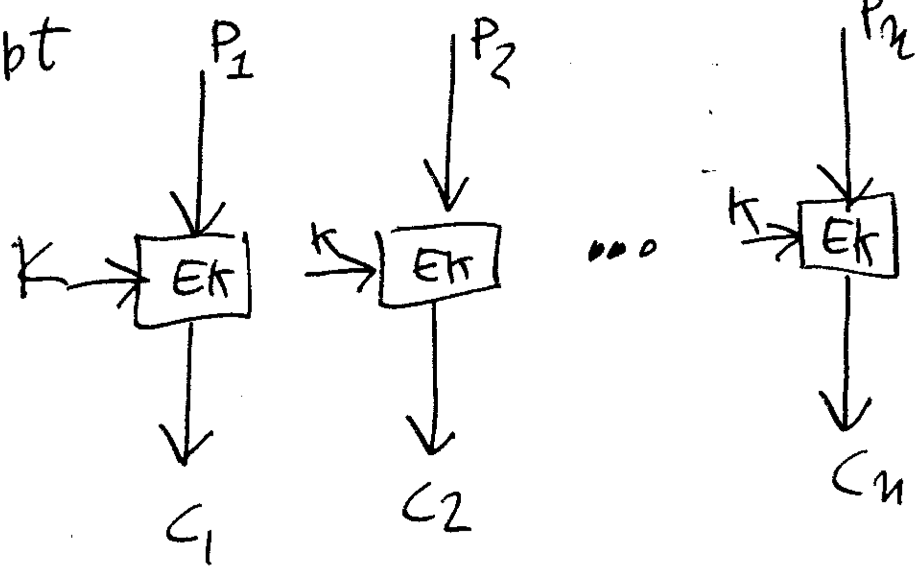


(*) soggetto all'attacco di Merkle-Hellman

AES 128-192-256 bit

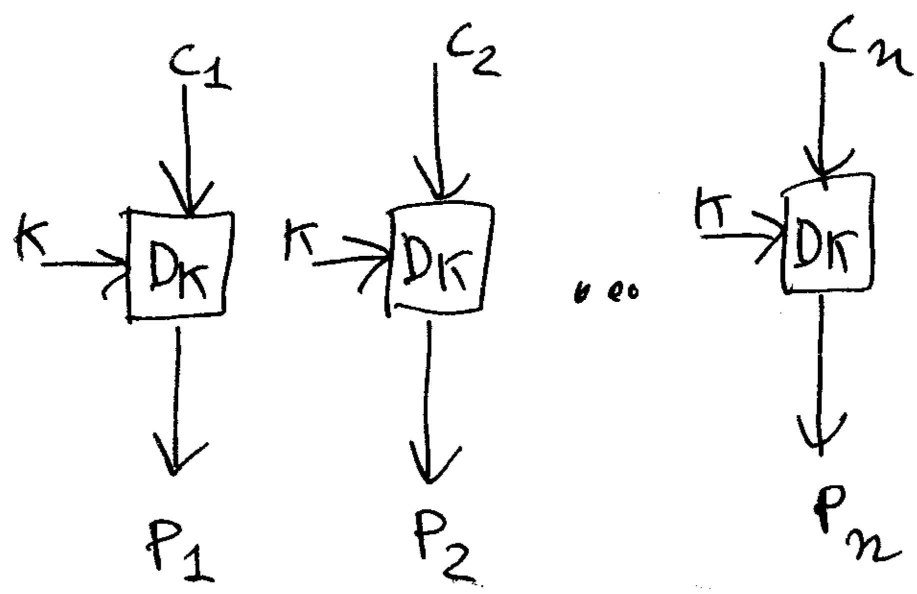
Electronic Code Book - ECB

encrypt



$$C_i = E_K(P_i), \quad 1 \le i \le n$$

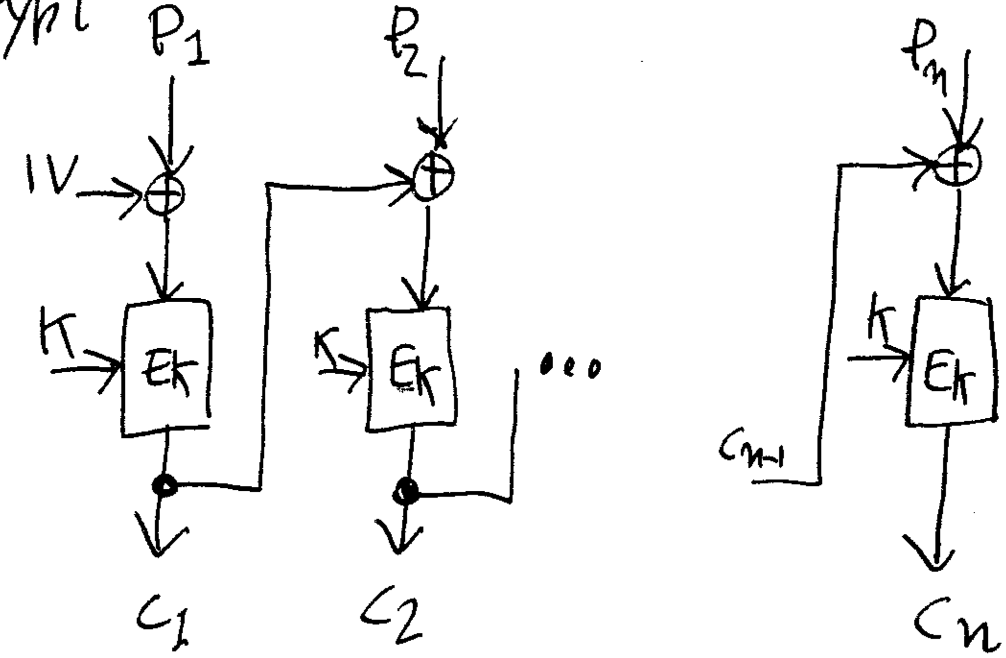
decrypt



$$P_i = D_K(C_i), \quad 1 \le i \le n$$

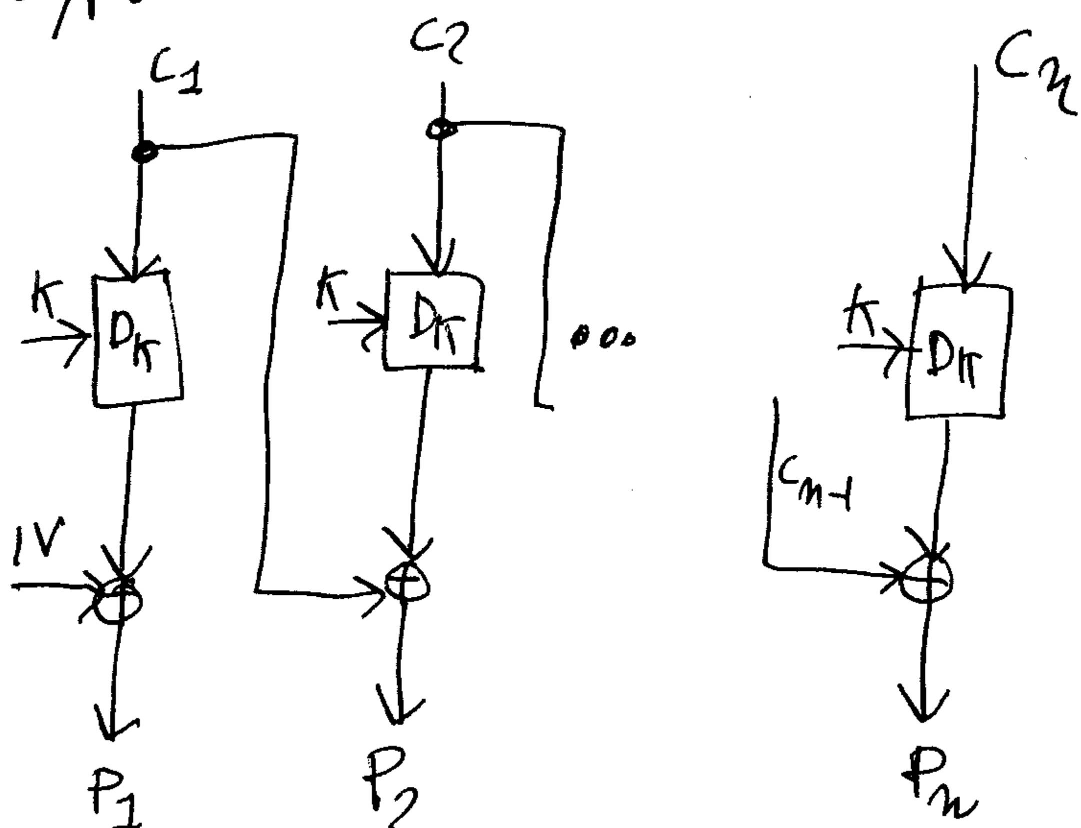
Cipher Block Chaining - CBC

encrypt



$$C_i = E_K(P_i \oplus C_{i-1}), \quad 1 \leq i \leq n$$
$$C_0 = IV$$

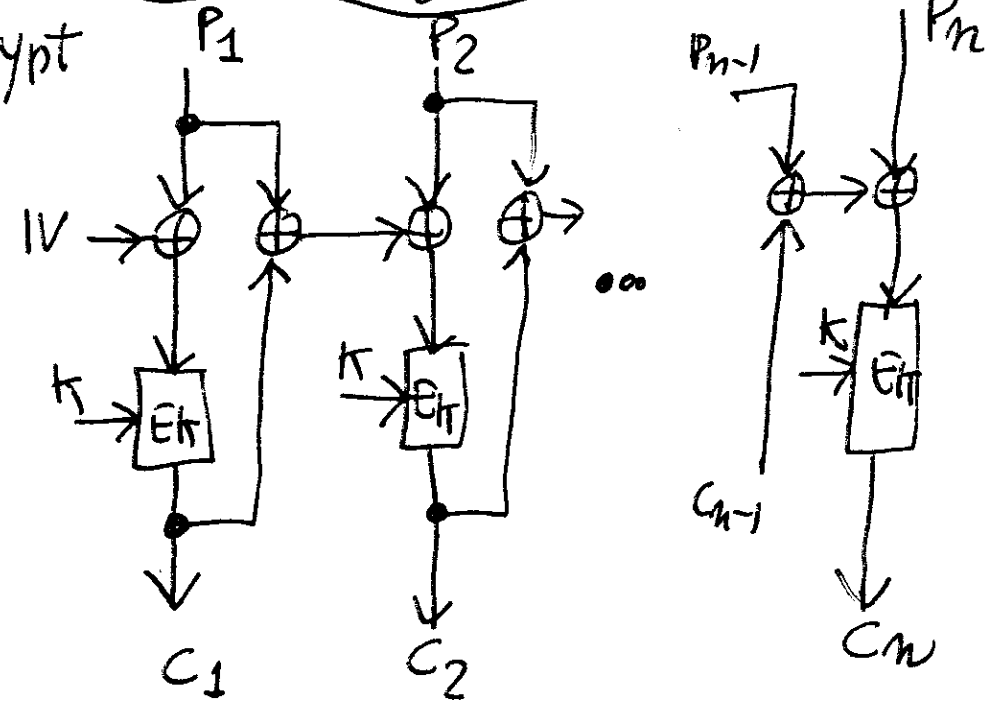
decrypt



$$P_i = C_{i-1} \oplus D_K(C_i), \quad 1 \leq i \leq n$$
$$C_0 = IV$$

Propagating CBC – PCBC

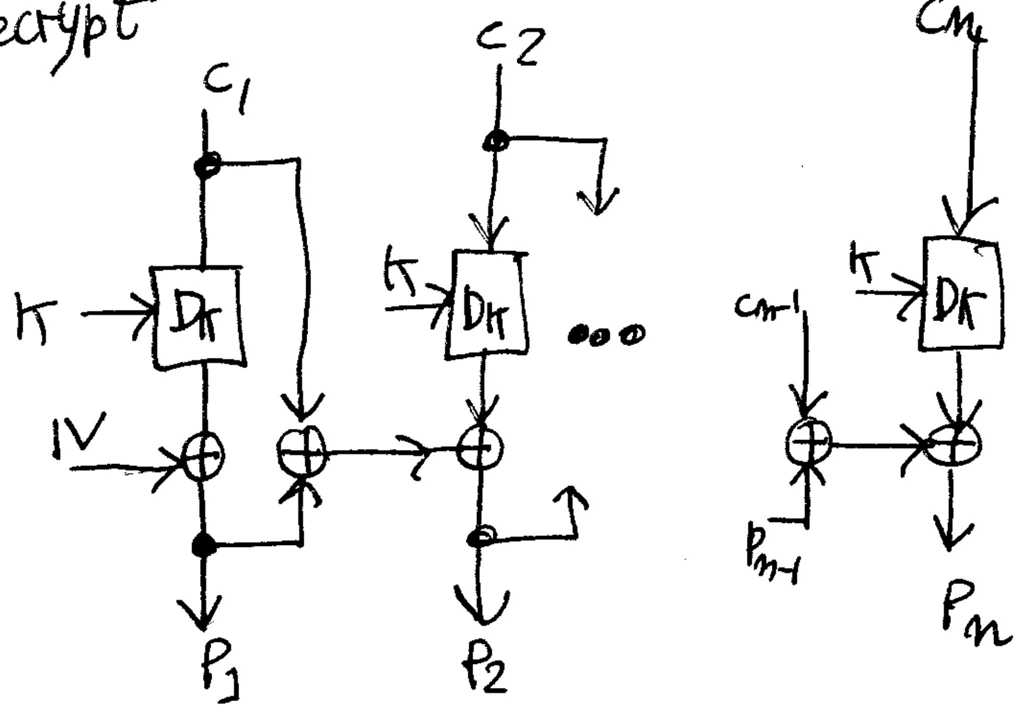
encrypt



$$C_i = E_K(P_i \oplus P_{i-1} \oplus C_{i-1}),\quad 1 \le i \le n$$

$$P_0 \oplus C_0 = IV$$

decrypt

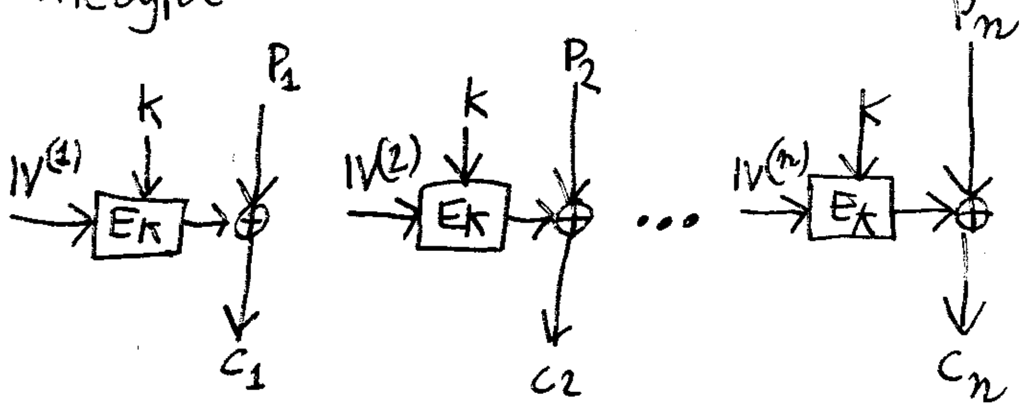


$$P_i = C_{i-1} \oplus P_{i-1} \oplus D_K(C_i),\quad 1 \le i \le n$$

$$P_0 \oplus C_0 = IV$$

Counter mode – CTR

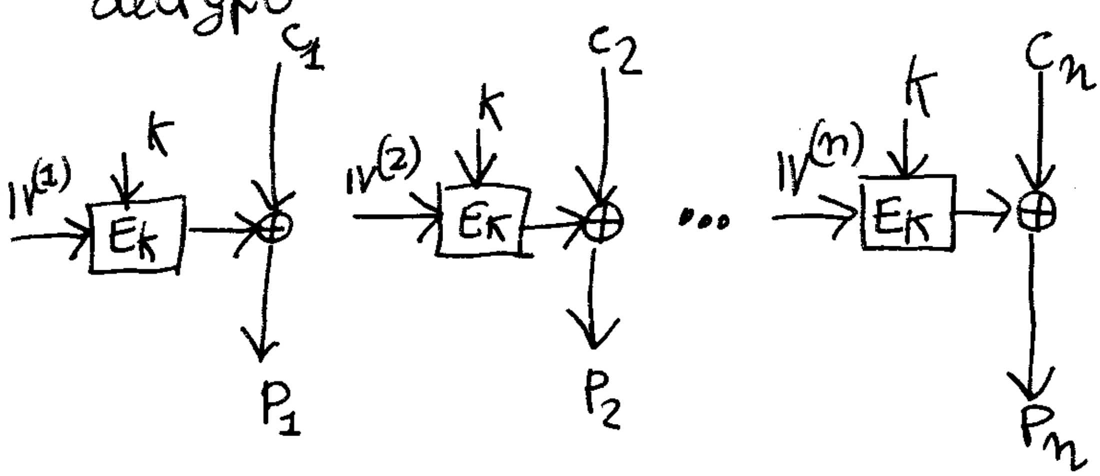
encrypt



$$C_i = P_i \oplus E_K(IV^{(i)}), \quad 1 \le i \le n$$

$$IV^{(i)} = IV^{(0)} + i - 1, \quad 1 \le i \le n$$

decrypt

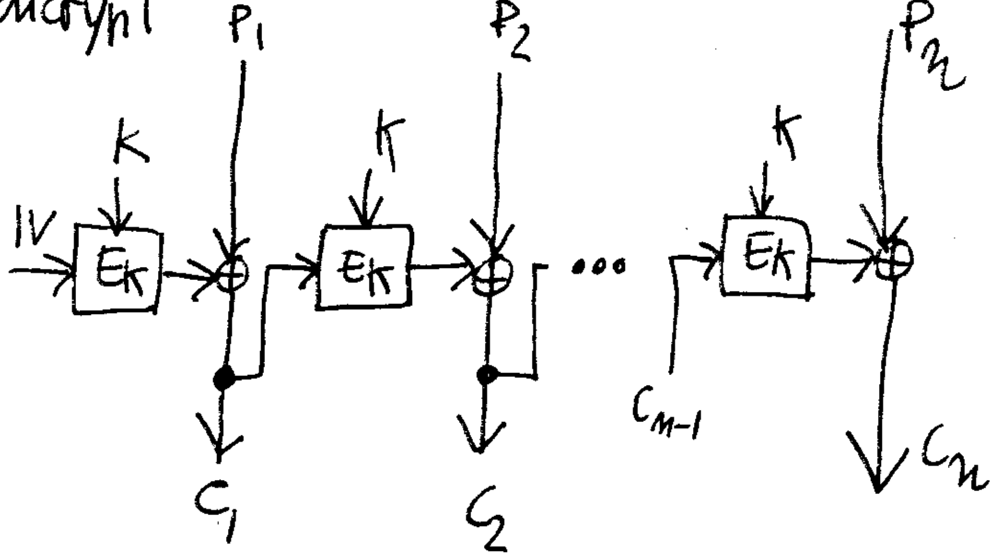


$$P_i = C_i \oplus E_K(IV^{(i)}), \quad 1 \le i \le n$$

$$IV^{(i)} = IV^{(0)} + i - 1, \quad 1 \le i \le n$$

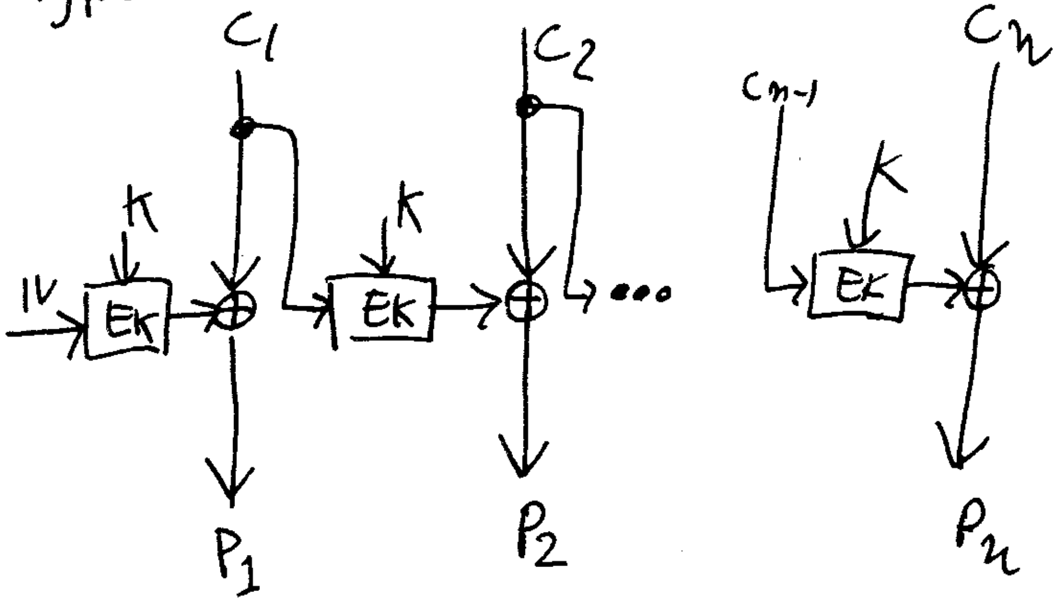
Cipher FeedBack mode - CFB

encrypt



$$c_i = P_i \oplus E_K(c_{i-1}), \quad 1 \le i \le n$$
$$c_0 = IV$$

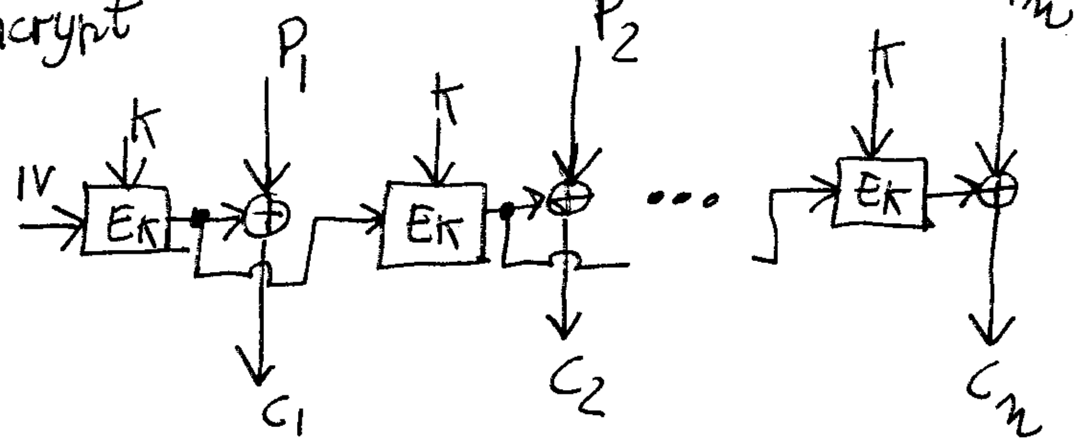
decrypt



$$P_i = c_i \oplus E_K(c_{i-1}), \quad 1 \le i \le n$$
$$c_0 = IV$$

Output FeedBack mode

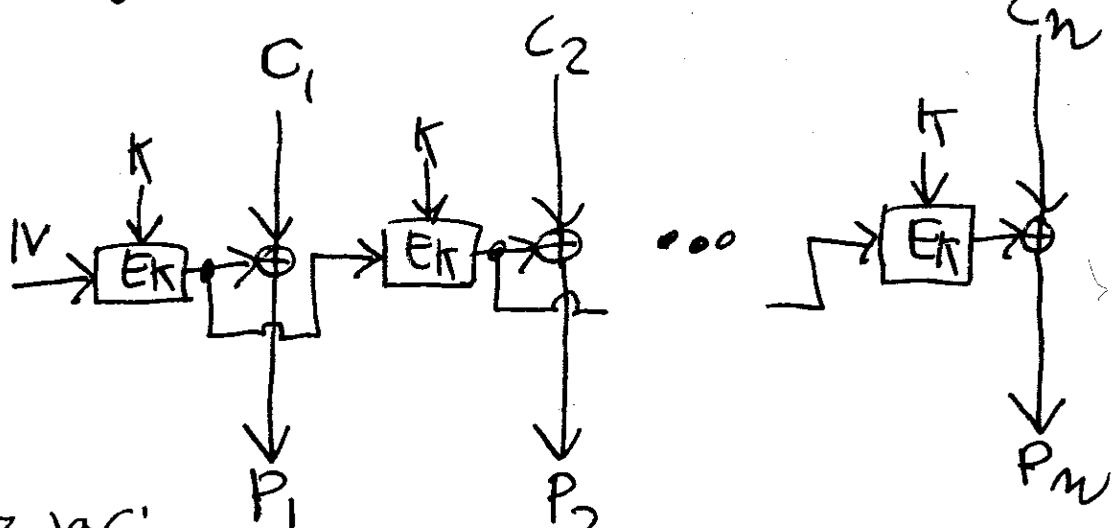
encrypt



$$\begin{cases} Z_i = E_K(Z_{i-1}) \\ C_i = P_i \oplus Z_i \\ \quad 1 \le i \le n \\ \quad Z_0 = IV \end{cases}$$

$$\begin{cases} C_i = P_i \oplus E_K^{(i)}(IV), \quad 1 \le i \le n \\ \text{ove} \quad E_K^{(i)}(IV) = \underbrace{E_K\{E_K[E_K(IV)]\}}_{i\text{-volte}} \end{cases}$$

decrypt

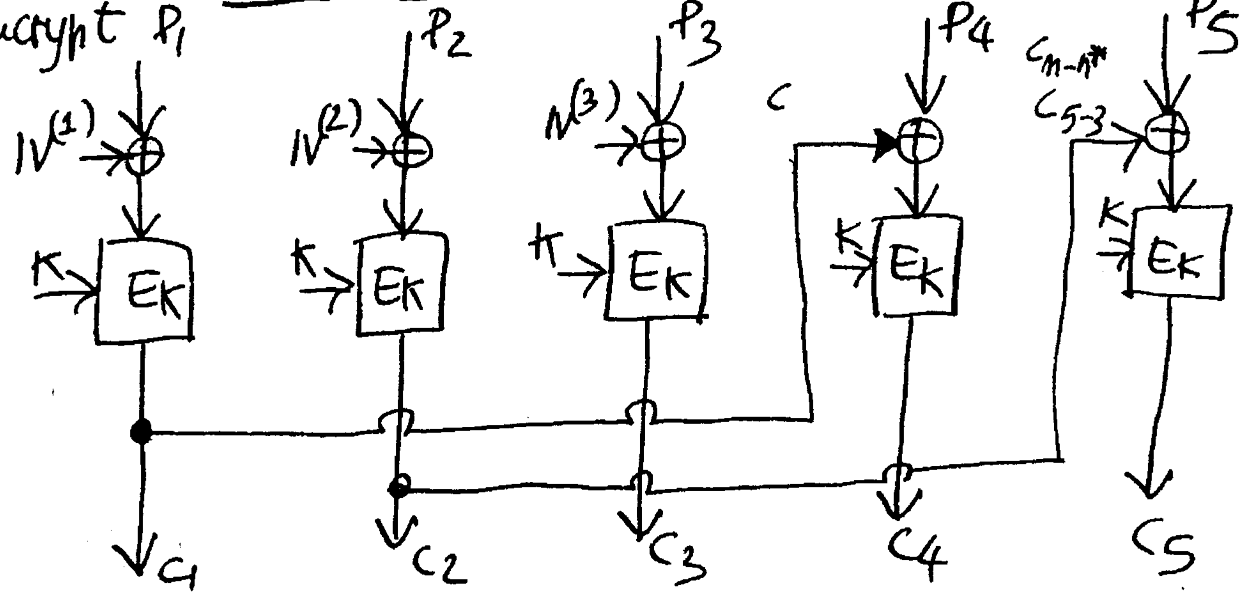


$$\begin{cases} P_i = E_K(Z_{i-1}) \oplus C_i \\ Z_0 = IV \\ \quad 1 \le i \le n \end{cases}$$

$$\begin{cases} P_i = C_i \oplus E_K^{(i)}(IV), \quad 1 \le i \le n \\ \text{ove} \quad E_K^{(i)}(IV) \text{ è la cifratura in cascata per } i\text{-volte del vettore IV.} \end{cases}$$

InTerLeaved - ITL mode

encrypt



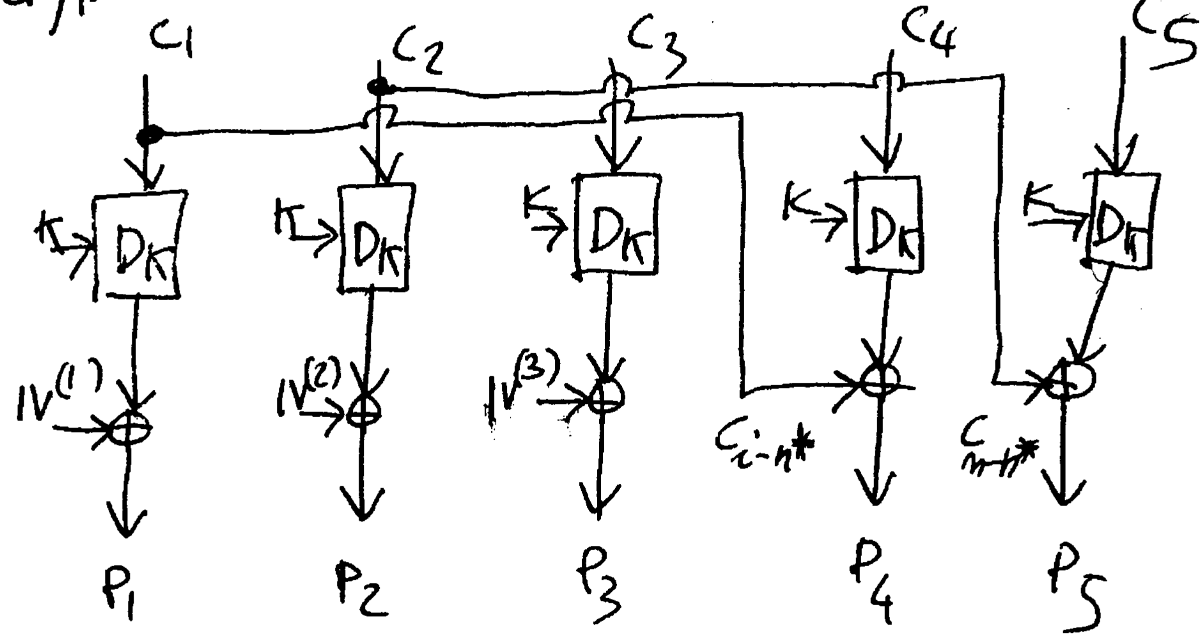
ES. $n=5; n^*=3$

$(n^* < n)$

$IV^{(i)} = IV^{(0)} + i - 1$

$$\begin{cases} c_i = E_K(P_i \oplus IV^{(i)}), & 1 \le i \le n^* \\ c_i = E_K(P_i \oplus C_{i-n^*}), & n^* < i \le n \end{cases}$$

docrypt



$$\begin{cases} P_i = D_K(C_i) \oplus IV^{(i)}, & 1 \le i \le n^*, \quad IV^{(i)} = IV^{(0)} + i - 1 \\ P_i = C_{i-n^*} \oplus D_K(C_i), & n^* < i \le n \end{cases}$$