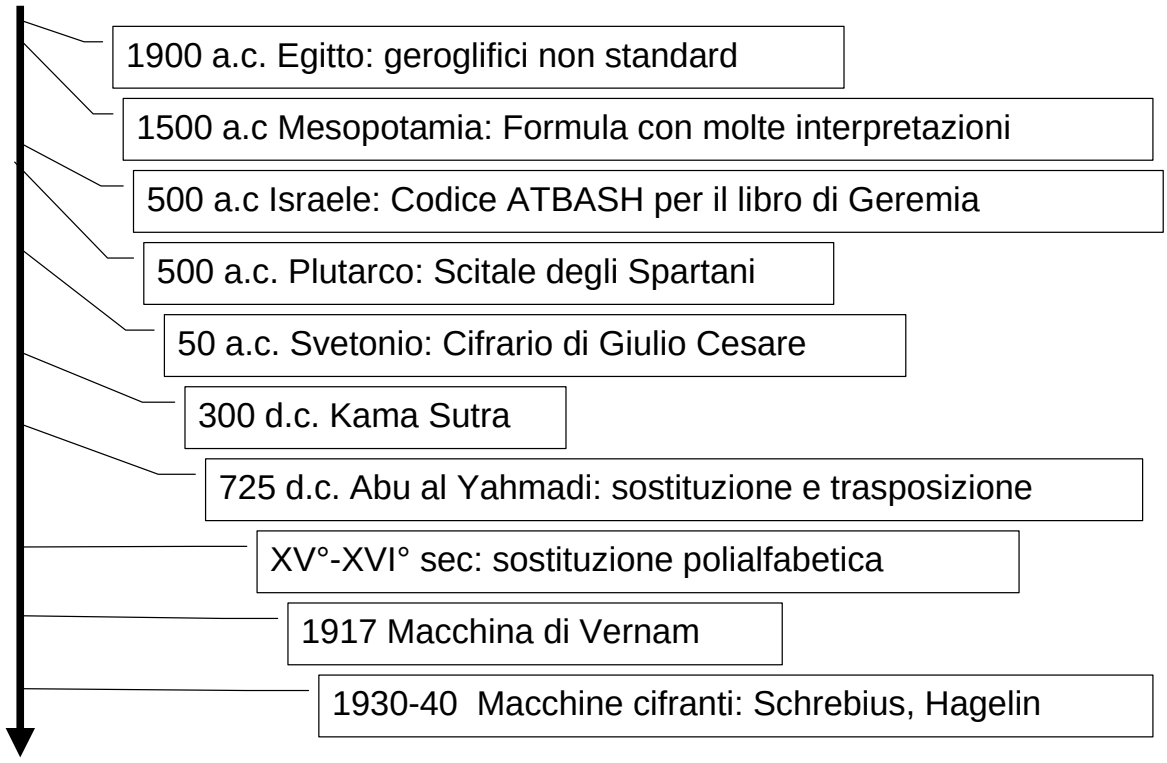
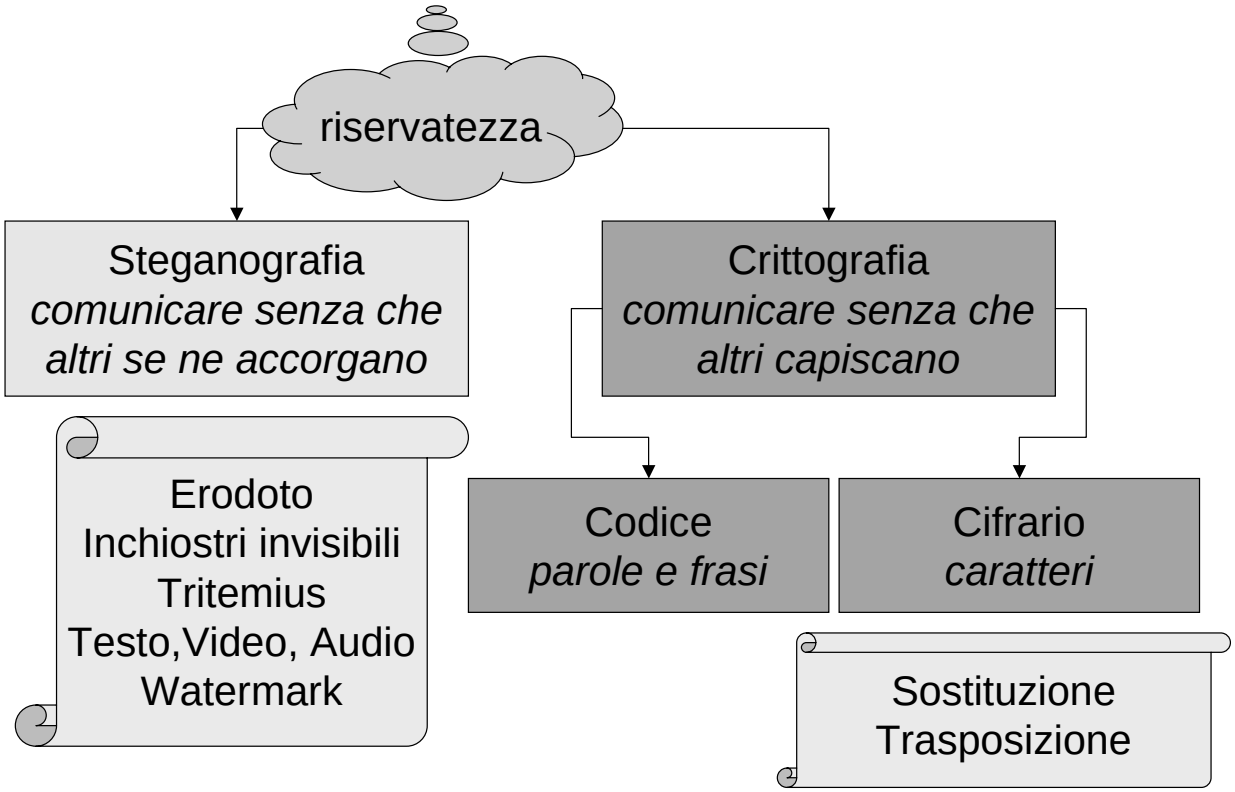
CRITTOGRAFIA CLASSICA



PRINCIPI E CLASSIFICAZIONI



SOSTITUZIONE E TRASPOSIZIONE

SOSTITUZIONE

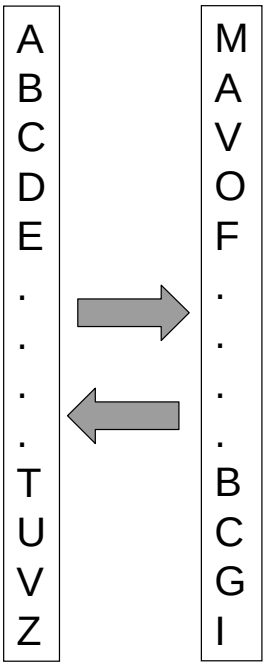
- **l'ordine dei simboli rimane inalterato**
- **quello che cambia sono i singoli simboli:** ogni simbolo è sostituito da un altro, secondo una certa regola.

TRASPOSIZIONE

- **i singoli simboli rimangono inalterati**
- **quello che cambia è l'ordine dei simboli.**

L'OPERAZIONE DI SOSTITUZIONE

I due alfabeti con **n** simboli



Trasformazioni possibili:
n.(n-1). (n-2).(n-3)…

$$|T| = n!$$

n = 21 $\rightarrow$ 5,1 . 10^{19}
n = 26 $\rightarrow$ 4 . 10^{26}

Nessuno uguale a se stesso!

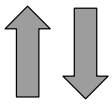
$$|T| = \sum_{j=0}^{n} (-1)^j . \frac{n!}{j!}$$

> (n-1)!

La chiave

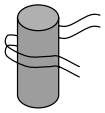
L'OPERAZIONE DI TRASPOSIZIONE

$s_1 s_2 s_3 s_4 s_5 s_6 s_7 s_8 s_9$



$s_3 s_8 s_1 s_2 s_6 s_5 s_9 s_7 s_4$

chiave

Scitala 

Chiave: diametro e lunghezza

n lunghezza della stringa

$$|T| = n!$$

Θεμιστοκλεσ μεν ταυτα ενεγραφε

Θ	τ	σ		α	γ
ε	ο		τ		ρ
μ	κ	μ	α	ε	α
ι	λ	ε	υ	ν	φ
σ	ε	ν	τ	ε	ε

Θτσ αγεο τ ρμκμαεαιλευνφσεντεε

ACCORGIMENTI UTILI

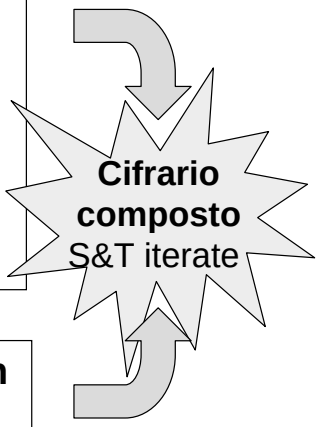
- i simboli della stringa che rappresenta un segreto devono essere **molti** e **scelti a caso**
- **mai archiviare insieme testi cifrati e relativi testi decifrati**
- **mai lasciare incustodite macchine pronte a cifrare/decifrare**
- **ogni simbolo del blocco cifrato deve dipendere da <u>tutti</u> i simboli del blocco in chiaro *(proprietà di DIFFUSIONE)***
- **il blocco cifrato deve dipendere <u>in modo complesso</u> dal valore della chiave *(proprietà di CONFUSIONE)***

CONFUSIONE & DIFFUSIONE (SHANNON)

La **confusione**

- **nasconde la relazione esistente tra testo in chiaro e testo cifrato**
- rende poco efficace lo studio del cifrato basato su statistiche e ridondanze del testo in chiaro.

La **sostituzione** è il mezzo più semplice ed efficace per creare confusione.



La **diffusione nasconde la ridondanza del testo in chiaro spargendola all'interno del testo cifrato.**

La **trasposizione** è il mezzo più semplice ed efficace per ottenere diffusione.

SICUREZZA DI UN CIFRARIO (SHANNON)

SEGRETEZZA PERFETTA

Un Cifrario è detto **PERFETTO**, o **assolutamente sicuro**, se, dopo aver intercettatto un certo testo cifrato **c**, **l'incertezza *a posteriori* sul testo in chiaro m è uguale all'incertezza che si aveva *a priori*,** cioè prima dell'intercettazione.

SICUREZZA

Un Cifrario è detto **sicuro** se, dato un qualsiasi testo cifrato **c**,

per chi non conosce E_k^{-1} e quindi k

è **impossibile** trovare un **m** tale che $\mathbf{E_k(m) = c}$.

SICUREZZA COMPUTAZIONALE

Un Cifrario è detto **computazionalmente sicuro** se il calcolare **m** da un **c** è possibile, ma richiede una **potenza di elaborazione *superiore a quella a disposizione dell'attaccante.***

LE BASI DELLA TEORIA dell'incertezza (Shannon)

- **IDEA DI FONDO: considerare un messaggio come una variabile aleatoria e studiare le relative trasformazioni con i mezzi della matematica applicata.**
  - i messaggi sono rappresentati con numeri reali
  - ogni messaggio ha una sua probabilità prefissata di essere scelto

- **POSTULATO: l'informazione *I(m)* fornita dall'arrivo di un messaggio *m* è tanto più grande quanto più piccola è la probabilità del messaggio stesso**
  - per misurare l'informazione è stata scelta la **funzione logaritmo:**

$$I(m) = \log_2 (1/p(m)) = - \log_2 p(m)$$

  - l'unità di misura è lo *shannon (Sh);* un tempo era il bit

- **Per misurare l'incertezza sull'informazione trasportata da un messaggio prima di riceverlo si definisce il concetto di *Entropia* e si costruisce una teoria su esso.**

IL CIFRARIO PERFETTO (1/2)

SEGRETEZZA PERFETTA

Un Cifrario è detto **PERFETTO**, o **assolutamente sicuro**, se, dopo aver intercettatto un certo testo cifrato **c**, **l'incertezza *a posteriori* sul testo in chiaro m è uguale all'incertezza che si aveva *a priori*,** cioè prima dell'intercettazione.

Infatti, in queste condizioni non esistono correlazioni:
- **non serve a niente disporre di un calcolatore con potenza illimitata**
- **si può solo "tirare ad indovinare", ma non si avranno conferme.**

TEOREMA
Condizione necessaria e sufficiente per la **segretezza perfetta** è

$$p(c|m) = p(c)$$ per ogni **m** e **c**

- Conseguenza: **p(c|m)** deve essere **indipendente** da **m**
- e soprattutto: **il numero di chiavi deve essere almeno pari al numero di messaggi.**

IL CIFRARIO PERFETTO (2/2)

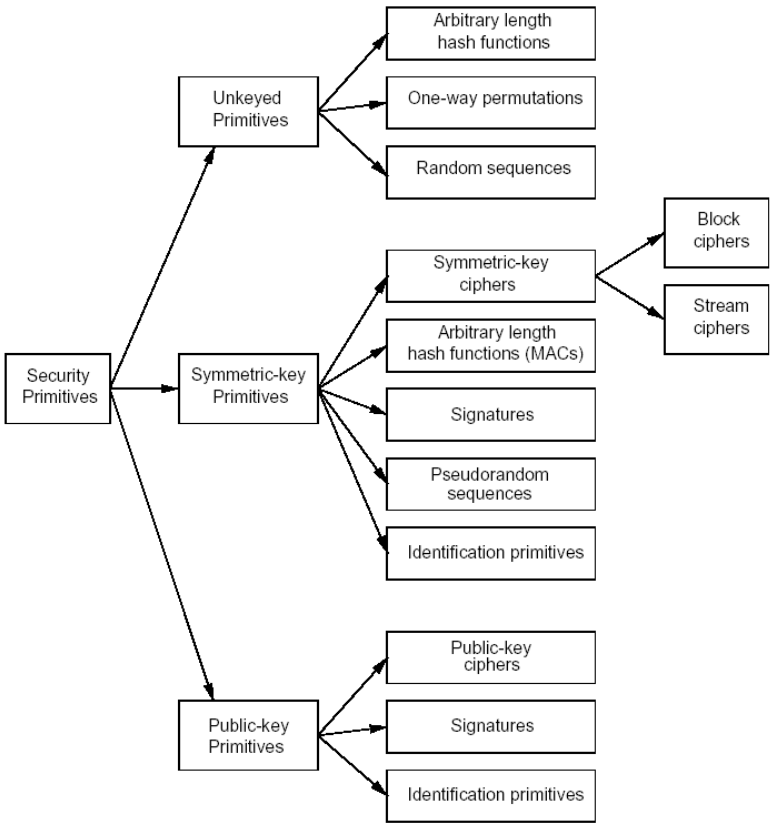
Requisito: il numero di chiavi deve essere almeno pari al numero di messaggi.

Il caso più semplice è che il numero di chiavi sia esattamente uguale al numero di messaggi.

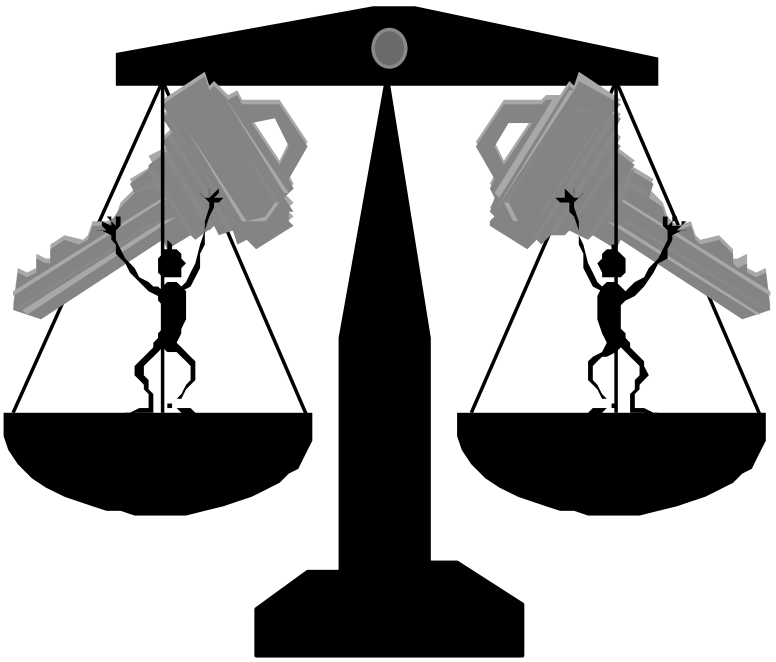
TEOREMA
un Cifrario con **|M| = |K| = |C|** è **PERFETTO se e solo se** c'è **esattamente una chiave** che trasforma ciascun messaggio **m** in ciascun crittogramma **c** e se tutte le chiavi **k** sono **equiprobabili**

È LA CONSACRAZIONE dell' ONE TIME PAD

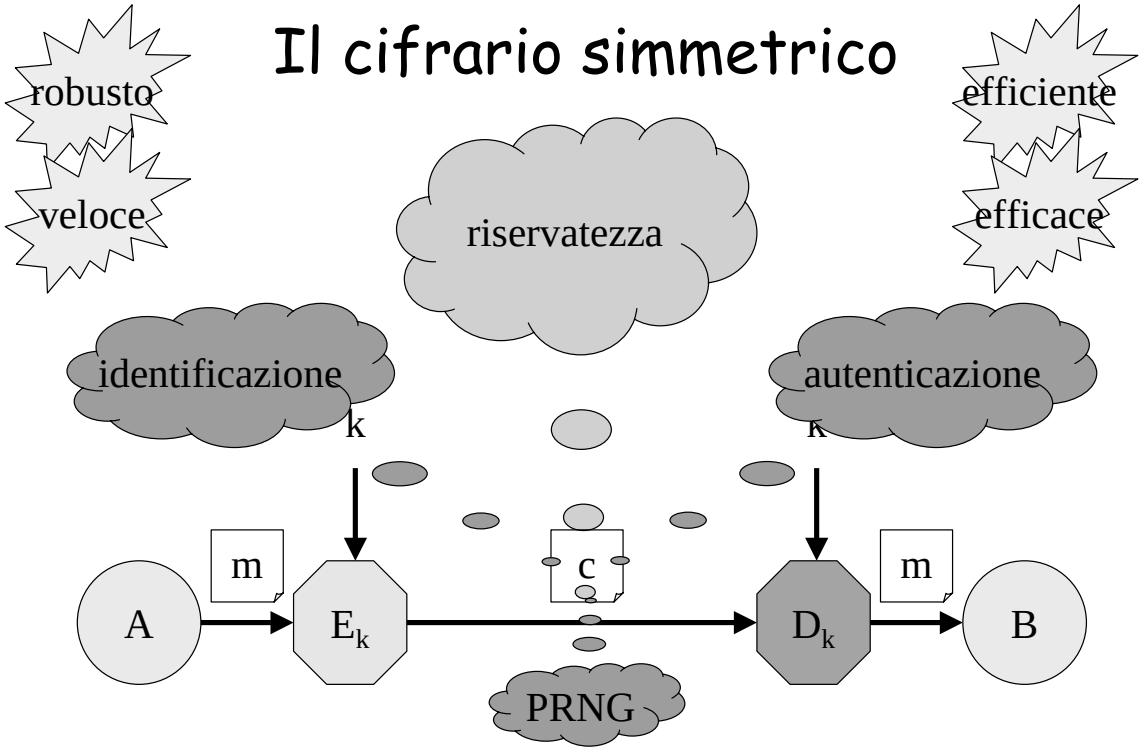
Classificazione delle Primitive Crittografiche



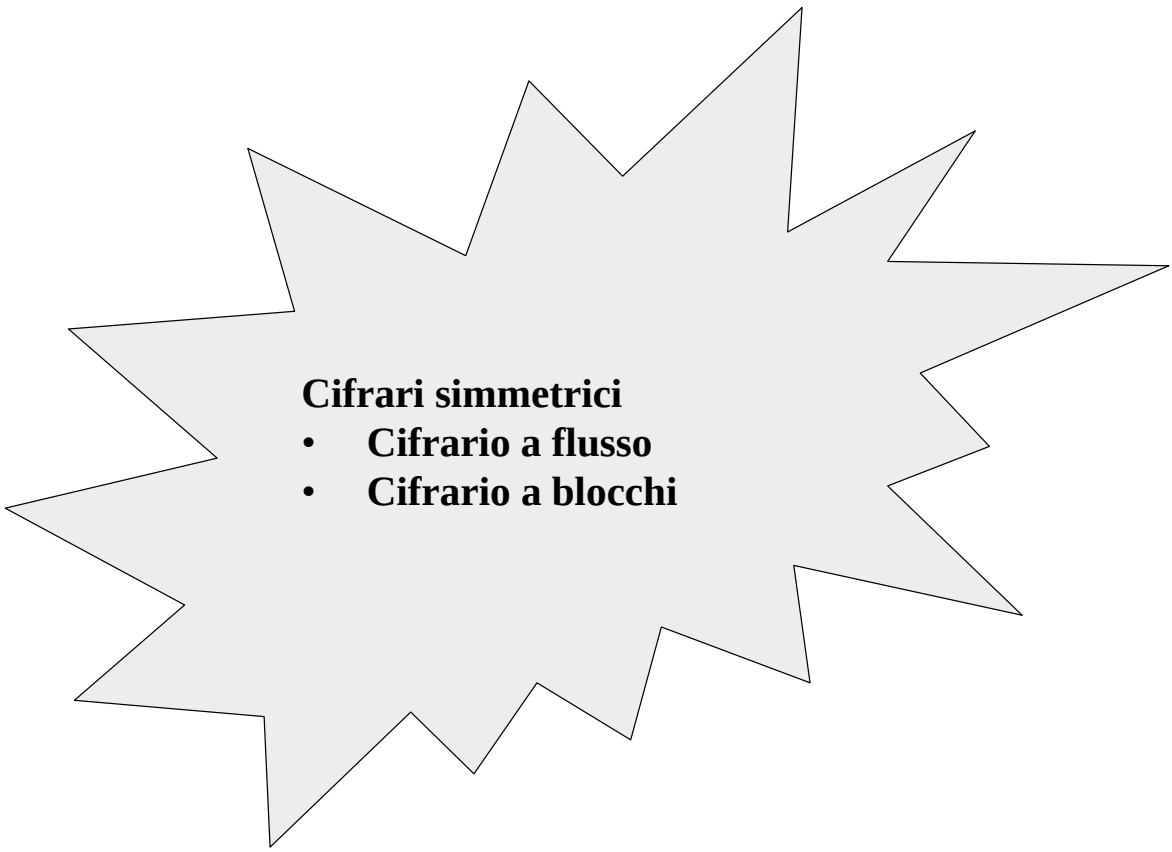
Meccanismi simmetrici



Il cifrario simmetrico



1. A: calcola $c = E_{AB}(m)$ e trasmette c
2. B: calcola $D_{AB}(c) = D_{AB}(E_{AB}(m)) = m$



Cifrari a flusso ed a blocchi

One time pad

Cifrario a flusso (stream cipher): trasforma, uno o pochi alla volta, i bit del testo da cifrare e da decifrare.

Protezione dei singoli bit di una trasmissione seriale

WEP, GSM

Cifrario poligrafico
Cifrario composto

Cifrario a blocchi (block cipher): trasforma, una alla volta, blocchi di messaggio formati da molti bit.

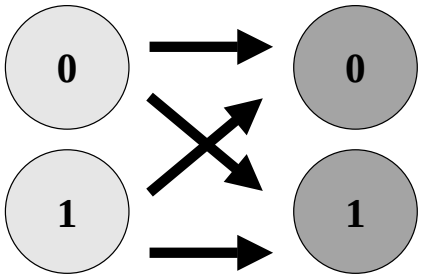
Protezione di pacchetti, di file e di strutture di dati

IPSec, SFS

Cifrari a flusso

- **flusso sincrono**
- **autosincronizzazione**

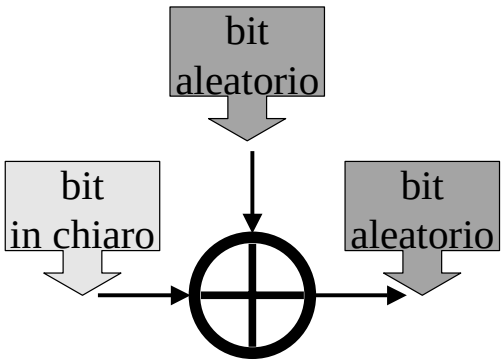
Il meccanismo per la sostituzione di un bit



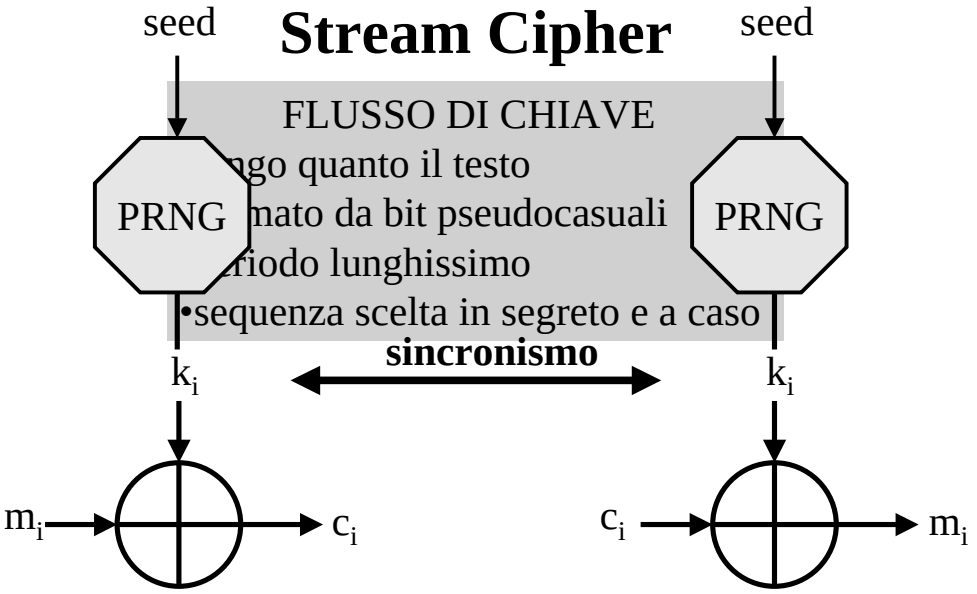
bit di chiave

bit di testo

⊕	0	1
0	0	1
1	1	0



Stream Cipher

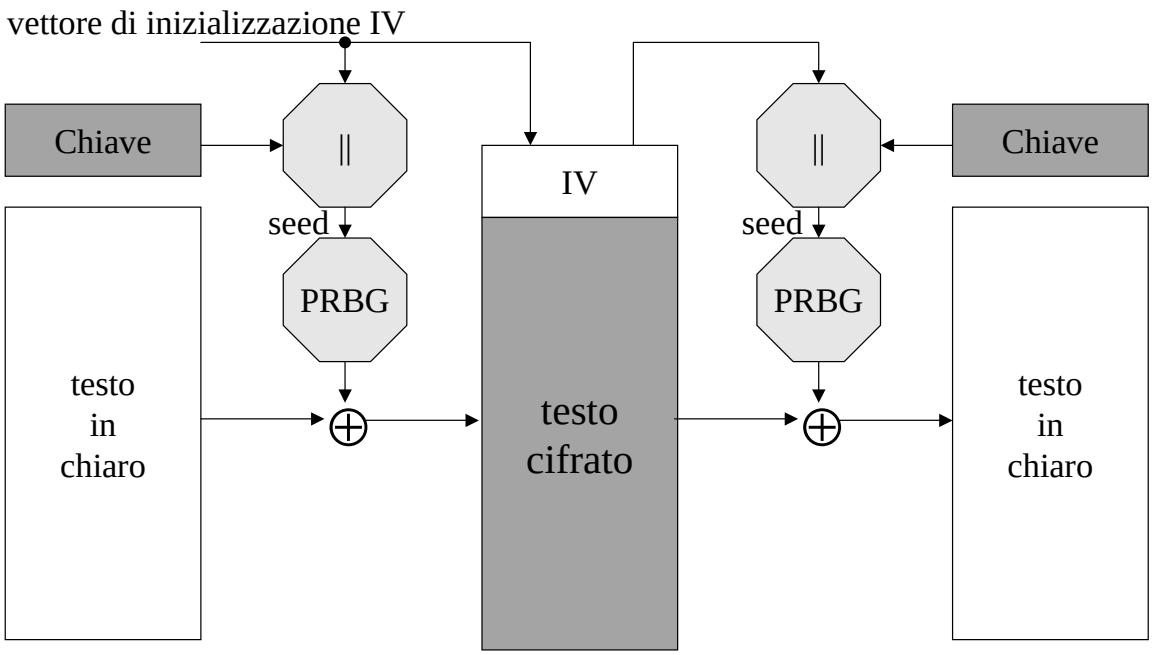


FLUSSO DI CHIAVE
- ngo quanto il testo
- mato da bit pseudocasuali
- riodo lunghissimo
- sequenza scelta in segreto e a caso

CIFRATURA
$c_i = m_i \oplus k_i$
i= 1, 2, 3, ..

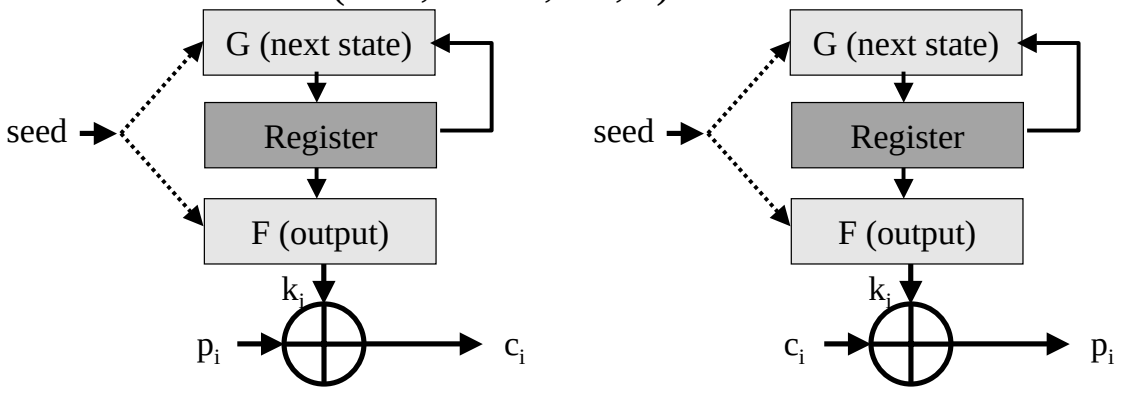
DECIFRAZIONE
$c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i$
$= m_i$
i= 1, 2, 3, ..

Segretezza e variabilità del seme (WEP)

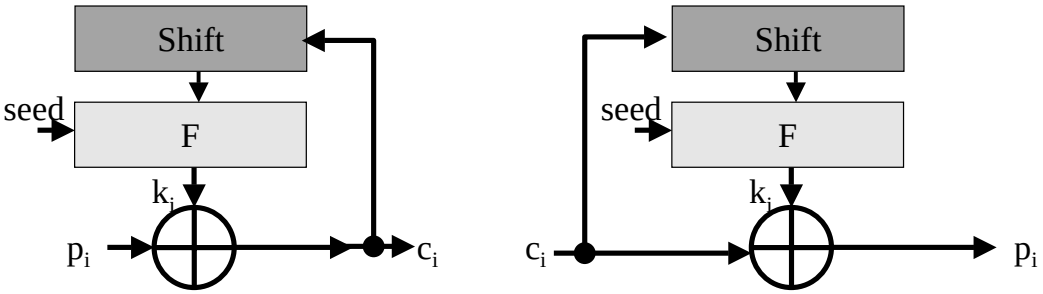


Generatori

- A flusso sincrono (RC4, SEAL, A5, ..)



- Con autosincronizzazione (DES-CFB, ..)



Problemi dei Cifrari simmetrici a flusso

ATTACCHI	FLUSSO SINCRONO	AUTOSINCR.
Cancellazione di bit	propagazione d'errore perdita di sincronizzaz.	transitorio non rilevabile
Inserzione di bit	propagazione d'errore perdita di sincronizzaz.	transitorio non rilevabile
Replica di bit	propagazione d'errore perdita di sincronizzaz.	transitorio non rilevabile
Modifica di bit	non propagazione non rilevabile	transitorio rilevabile

Proprietà del PRNG (Golomb, 1967)

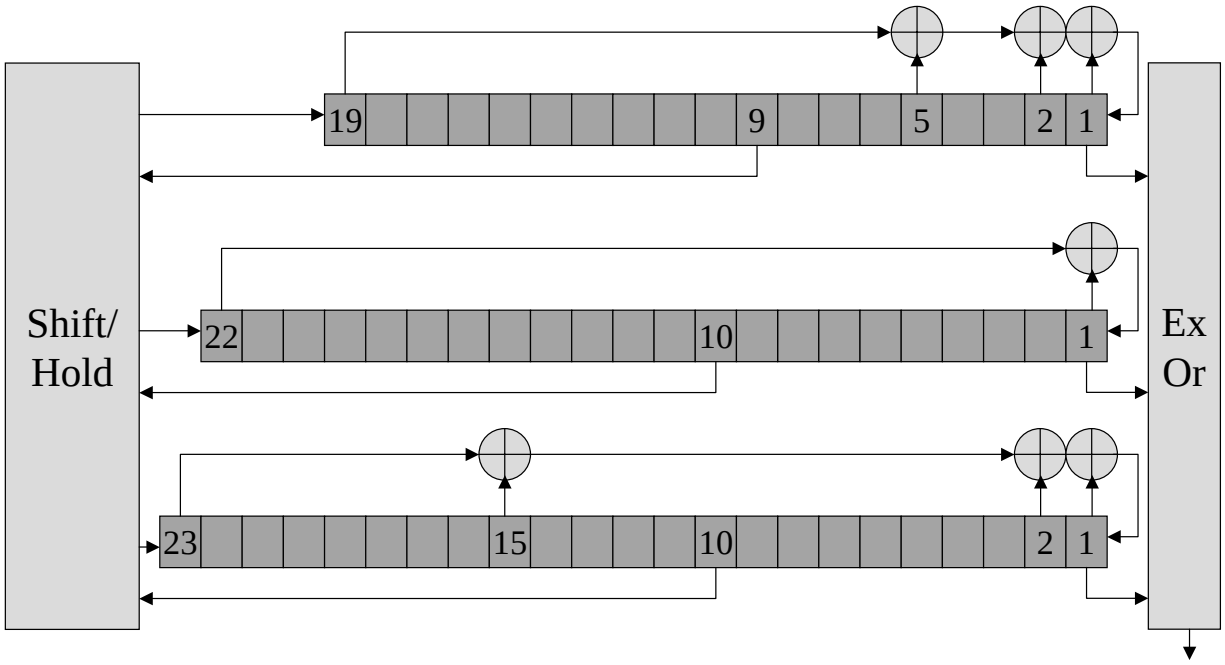
Registri a scorrimento con retroazione

•lineare ☹

•non lineare ☺

MONOBIT e RUN: "In un generatore di bit pseudocasuali di periodo **p**
•il numero complessivo di uni e di zeri deve essere circa uguale a **p/2**;
•il numero complessivo di stringhe di lunghezza l formate da tutti uni (o da tutti zeri),deve essere circa $\mathbf{p/2^l}$.
AUTOCORRELAZIONE: “traslando di **k>p** posizioni verso sinistra la stringa originaria e confrontando le due stringhe, la funzione di **autocorrelazione fuori dalla sequenza** deve avere lo stesso valore per ogni **k** non diviso da **p**".

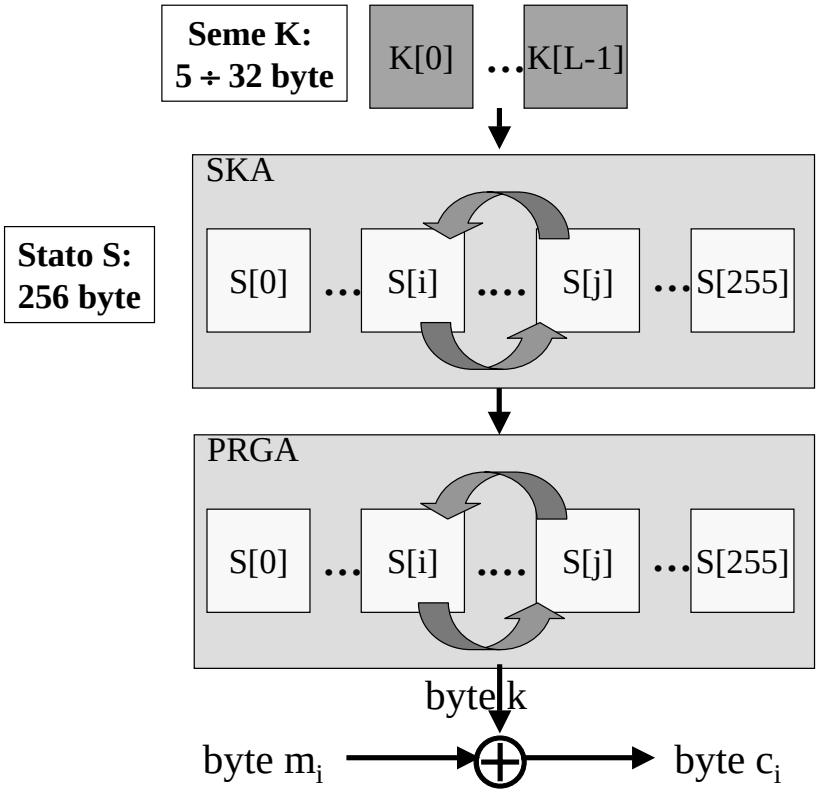
GSM: il generatore di flusso di chiave



Ross Anderson:http://www.chem.leeds.ac.uk/ICAMS/people/jon/a5.html

UMTS: Cifrario a blocchi Kasumi

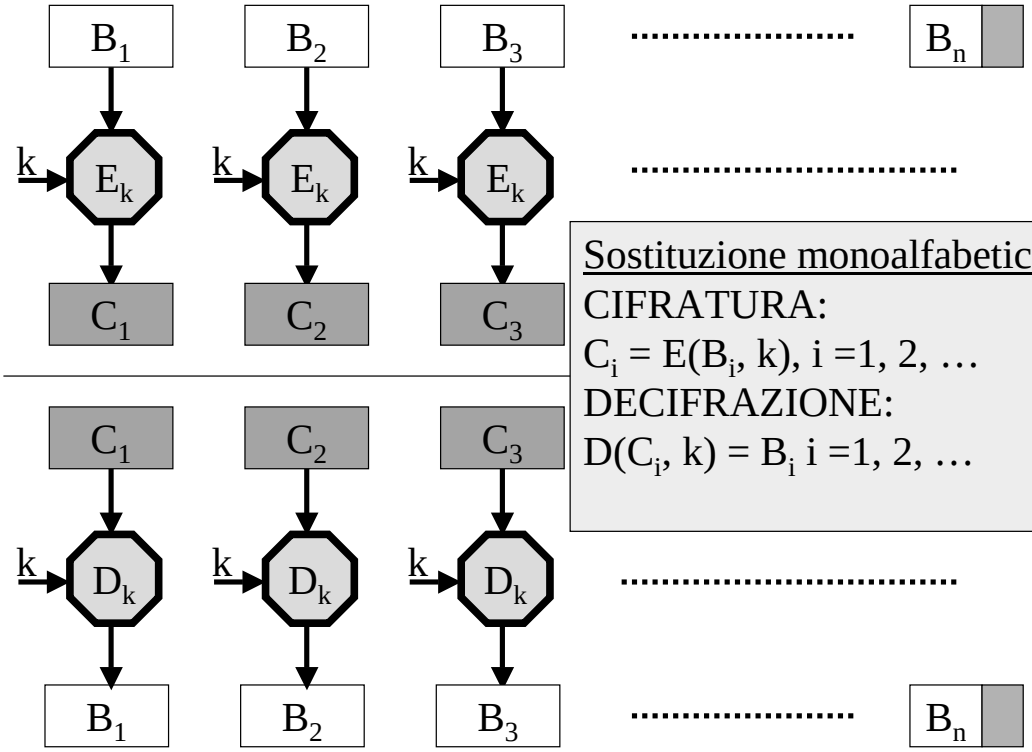
Il Cifrario a flusso RC4



Cifrari a blocchi

- **Rete di Feistel**
- **DES**
- **TDEA**
- **AES-Rijndael**

Block cipher



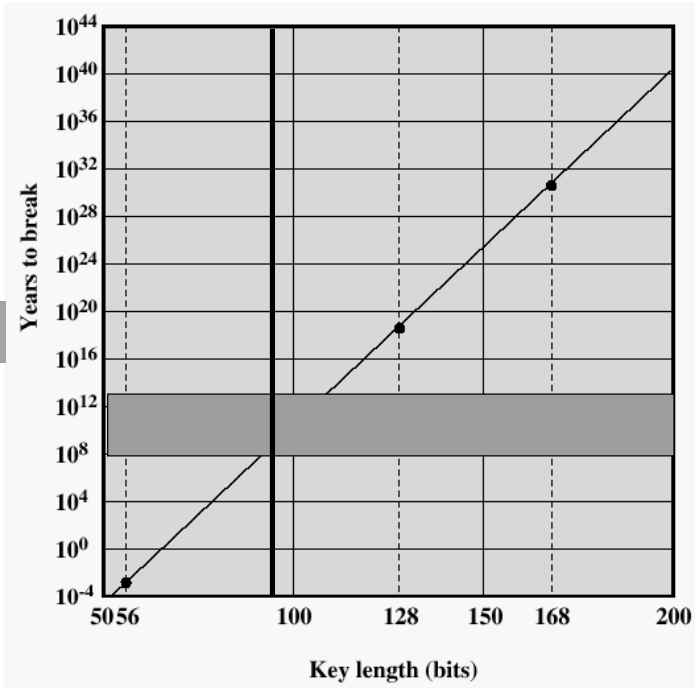
Sostituzione monoalfabetica
CIFRATURA:
$C_i = E(B_i, k)$, i =1, 2, …
DECIFRAZIONE:
$D(C_i, k) = B_i$ i =1, 2, …

Time to break a code (10^6 decryptions/μs)

n bit	N chiavi
32	$2^{32} = 4{,}3 \times 10^9$
56	$2^{56} = 7{,}2 \times 10^{16}$
128	$2^{128} = 3{,}4 \times 10^{38}$
168	$2^{168} = 3{,}7 \times 10^{50}$
192	$2^{192} = 6{,}3 \times 10^{57}$

$p = 2^{-N}$

$T = 2^{N-1}/10^{12}$ s



Valutazione sicurezza
a breve termine (1996)
R28: “75 bit
(6×10^{11} anni MIPS)
+14 bit ogni vent’anni”

Dimensione della chiave

DES Cracker (1998): macchina parallela costata 250.000 $ ha individuato in meno di 3 giorni una chiave di 56 bit.
Con una chiave di 168 bit impiegherebbe 10^{31} anni!

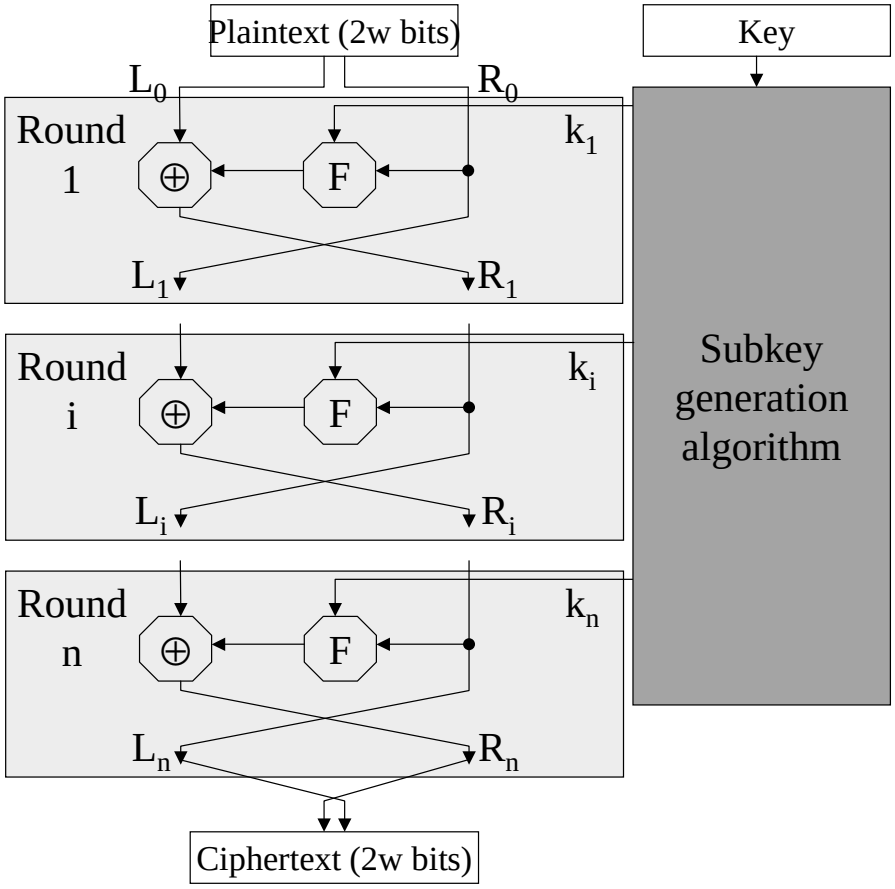
FBI, CIA: esportazione solo di crittografia “debole” (40 bit)

DES (56 bit di chiave e 64 bit di blocco): anni '80 e '90;
TDES (112 o 168 bit di chiave e 64 bit di blocco): anni '90;
AES (da 128 a 256 bit di chiave con blocchi da 128 a 256 bit): Rijndael, prossimi 30 anni

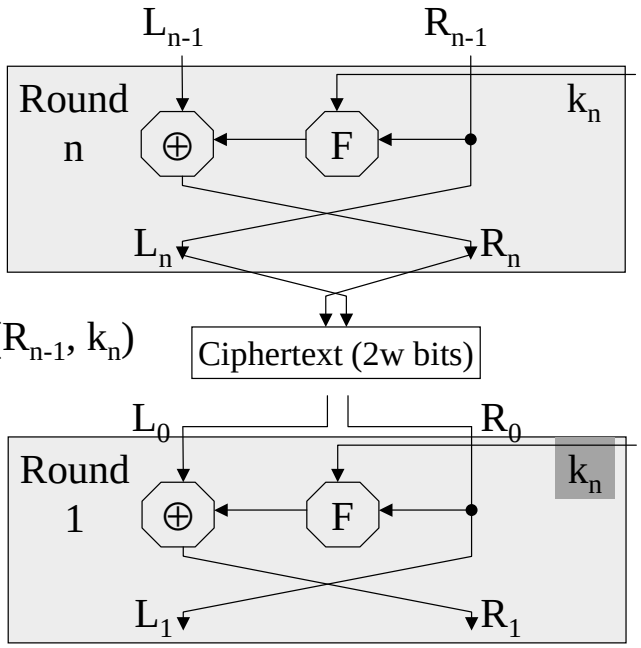
"la chiave segreta deve essere scelta caso (R12) e frequentemente modificata (R24)".

La rete di Feistel

$L_i=R_{i-1}$
$R_i=L_{i-1}\oplus F(R_{i-1}, k_i)$



Reti di Feistel: Cifratura/Decifrazione



$L_0 = R_n = L_{n-1} \oplus F(R_{n-1}, k_n)$
$R_0 = L_n = R_{n-1}$

$L_1 = R_0 = R_{n-1}$
$R_1 = L_0 \oplus F(R_0, k_n) = [L_{n-1} \oplus F(R_{n-1}, k_n)] \oplus F(R_{n-1}, k_n) = L_{n-1}$

Feistel Cipher Structure

- **Block size**: larger block sizes mean greater security
- **Key Size**: larger key size means greater security
- **Number of rounds**: multiple rounds offer increasing security
- **Subkey generation algorithm**: greater complexity will lead to greater difficulty of cryptanalysis.
- **Fast software encryption/decryption**: the speed of execution of the algorithm becomes a concern

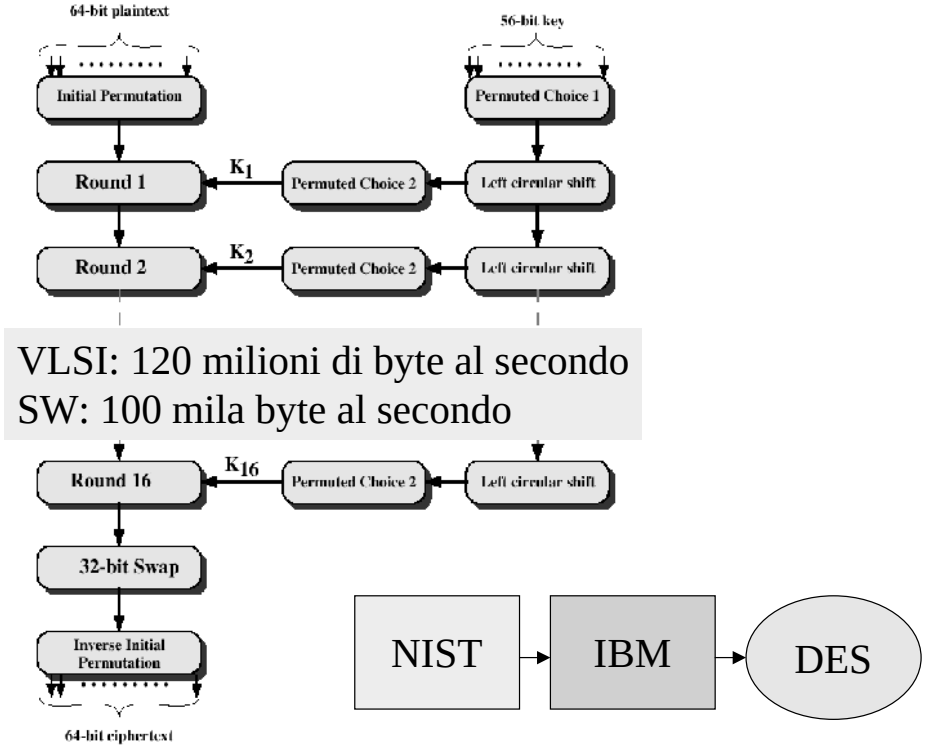


Figure 2.3 General Depiction of DES Encryption Algorithm

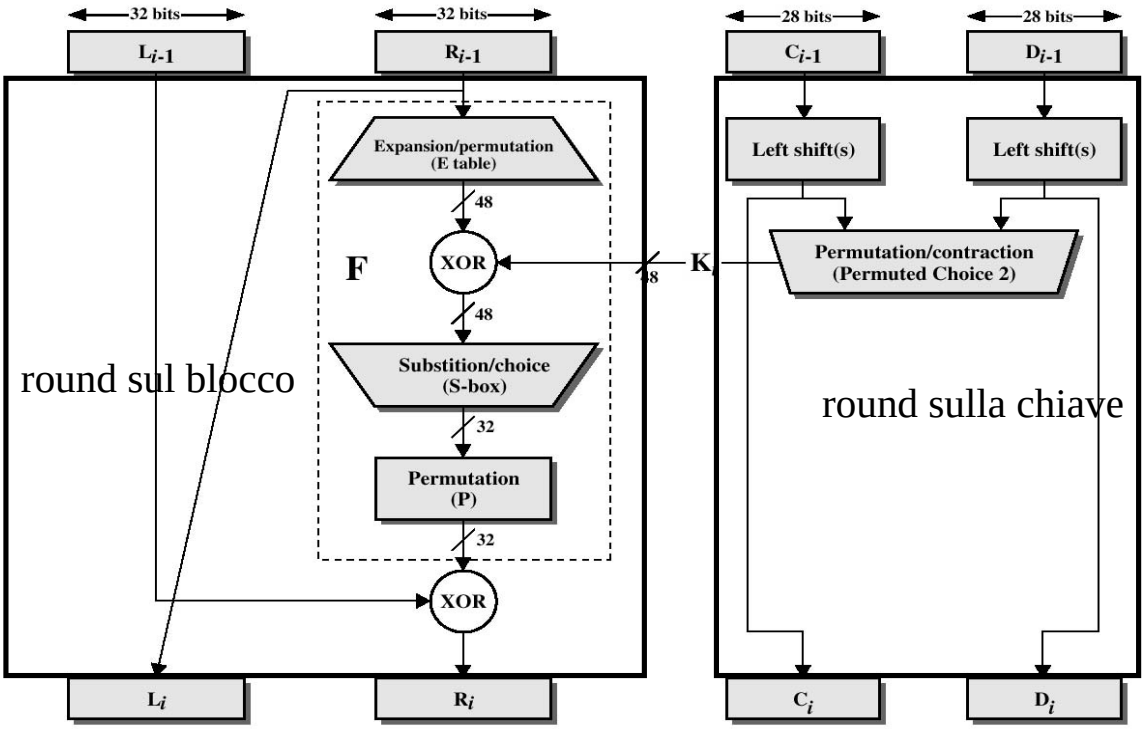


Figure 2.4 Single Round of DES Algorithm

I successori del DES

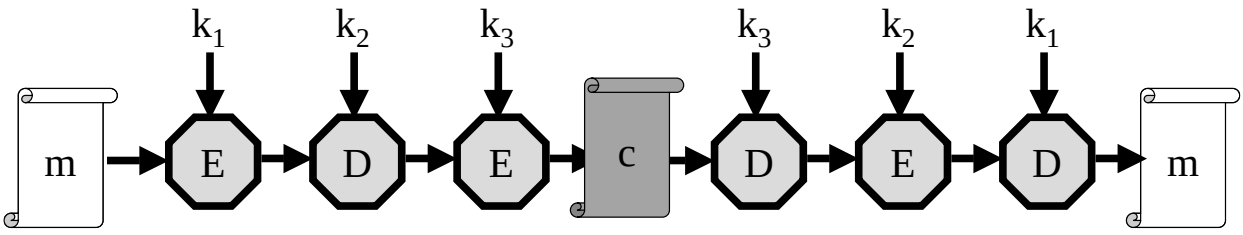
Hw → Sw

K: 64 → 128+

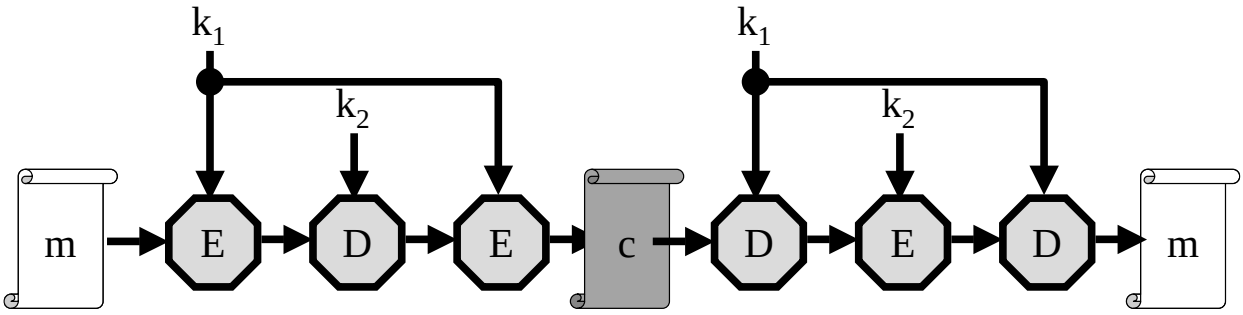
B: 64 → 128+

IDEA
TDES
BLOWFISH
CAST-128
ecc.

Il Triplo DES



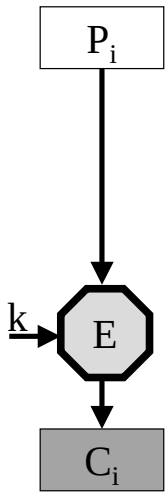
La versione con 168 bit di chiave



La versione con 112 bit di chiave

Modalità di cifratura dei blocchi

Modalità di elaborazione a blocchi

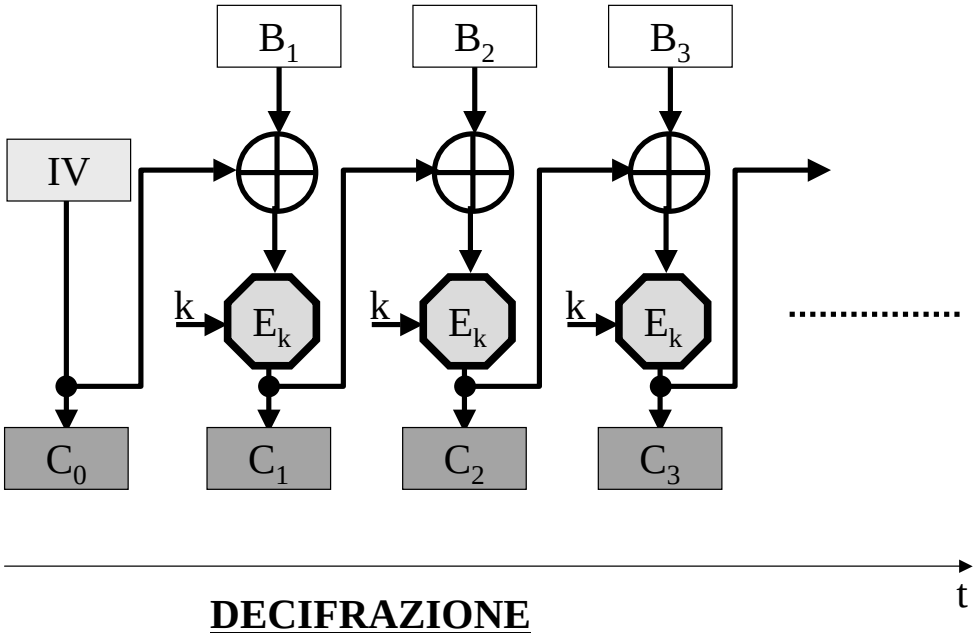


☹ **ECB**: Electronic Code Book

☺
- **CBC**: Cipher block Chaining
- **CFB**: Cipher Feedback,
- **OFB**: Output Feedback
- **CTR**: Counter

blocchi identici di testo in chiaro producono blocchi identici di testo cifrato

Cipher Block Chaining

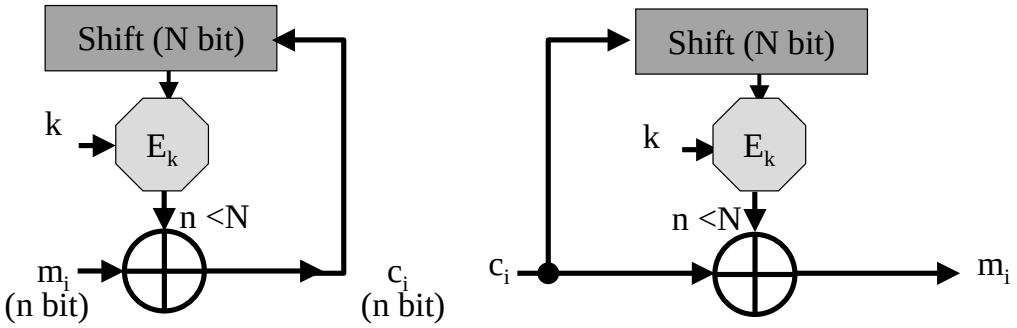


DECIFRAZIONE

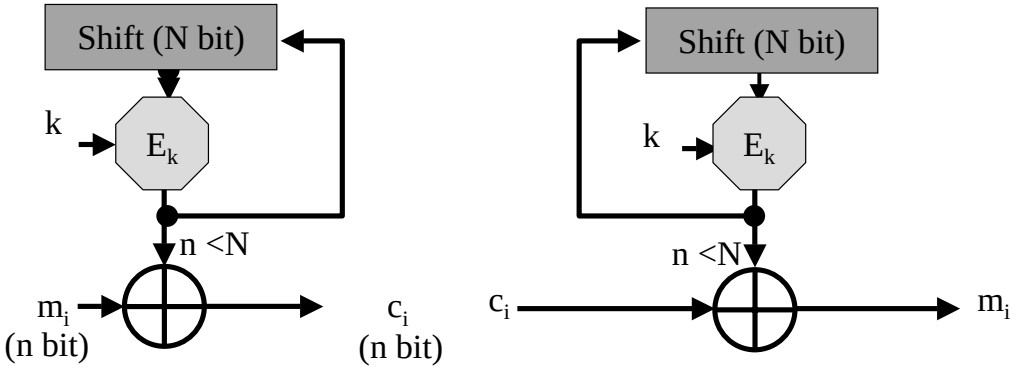
$D(C_i,k) = B_i \oplus C_{i-1}$

$D(C_i,k) \oplus C_{i-1} = B_i \oplus C_{i-1} \oplus C_{i-1} = B_i$

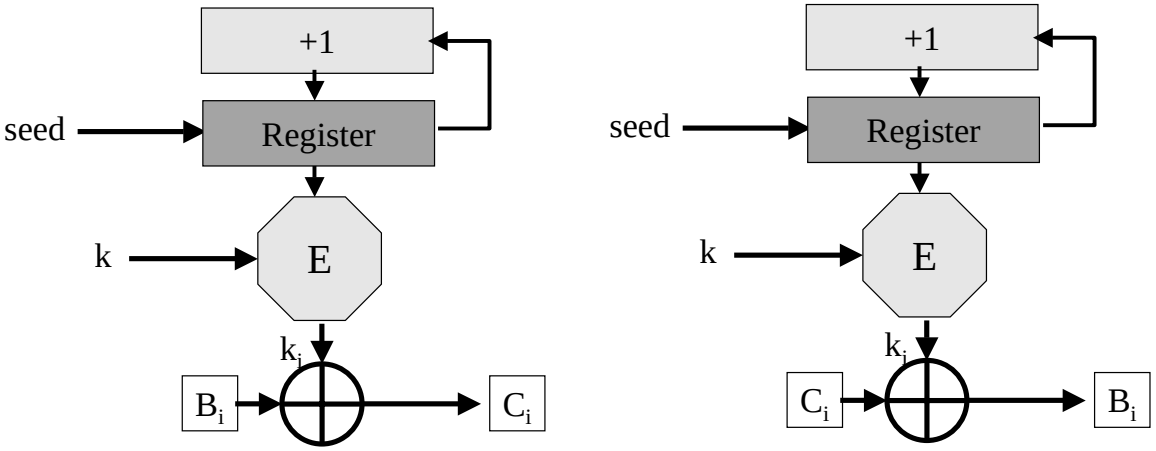
CFB (Chipher Feedback)



OFB (Output Feedback)

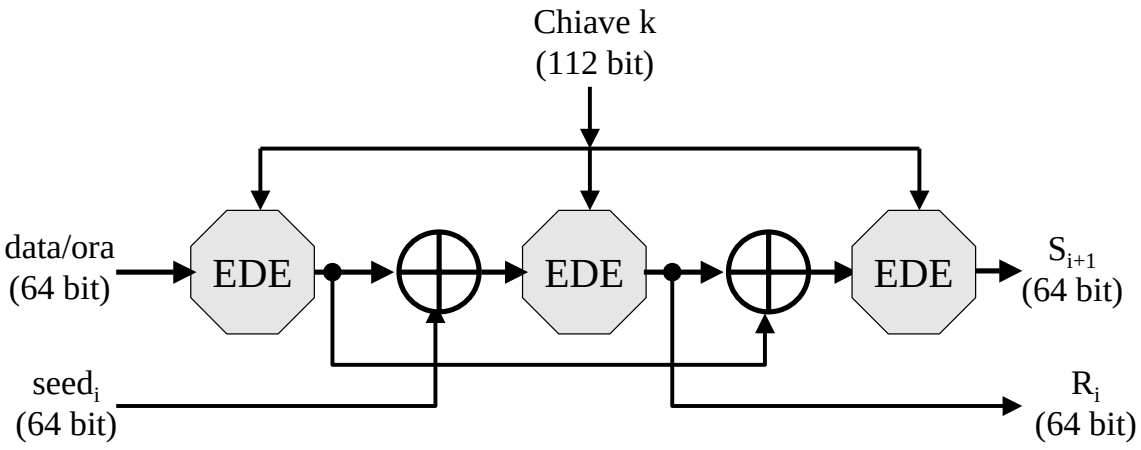


CTR (Counter)



PRNG X9.17

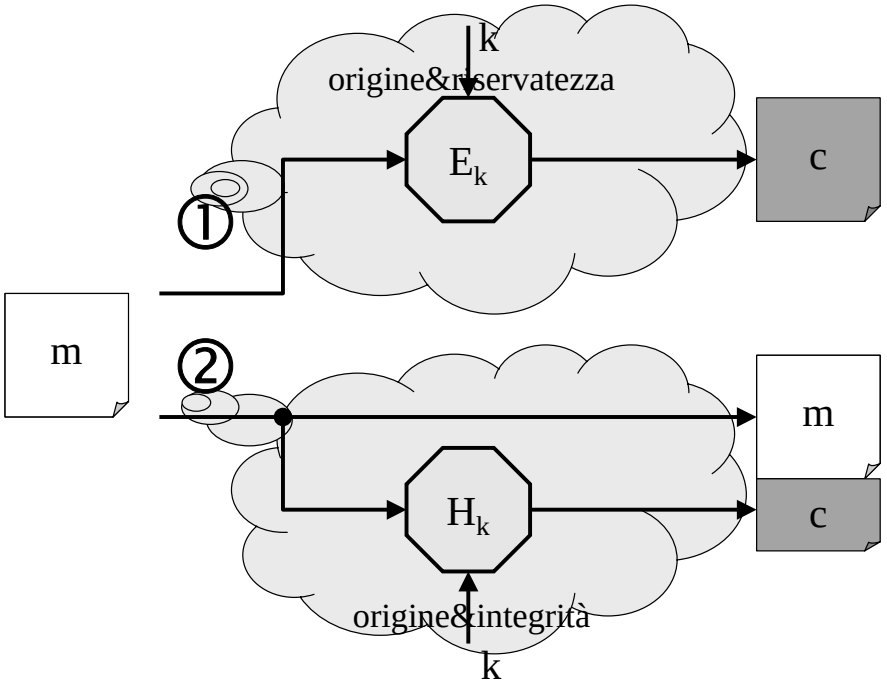
Obiettivo: chiavi e vettori di inizializzazione per il DES
Meccanismo: TDES a due chiavi



Integrità ed origine

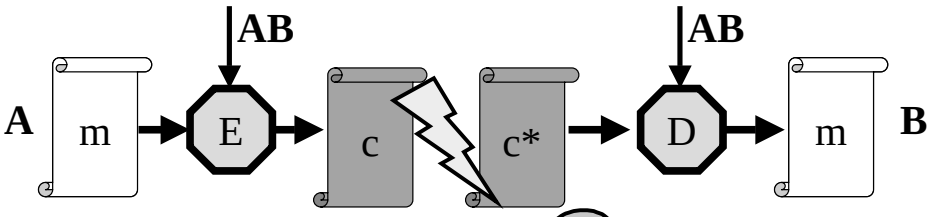
- **MAC**
- **HMAC**

Message Authentication



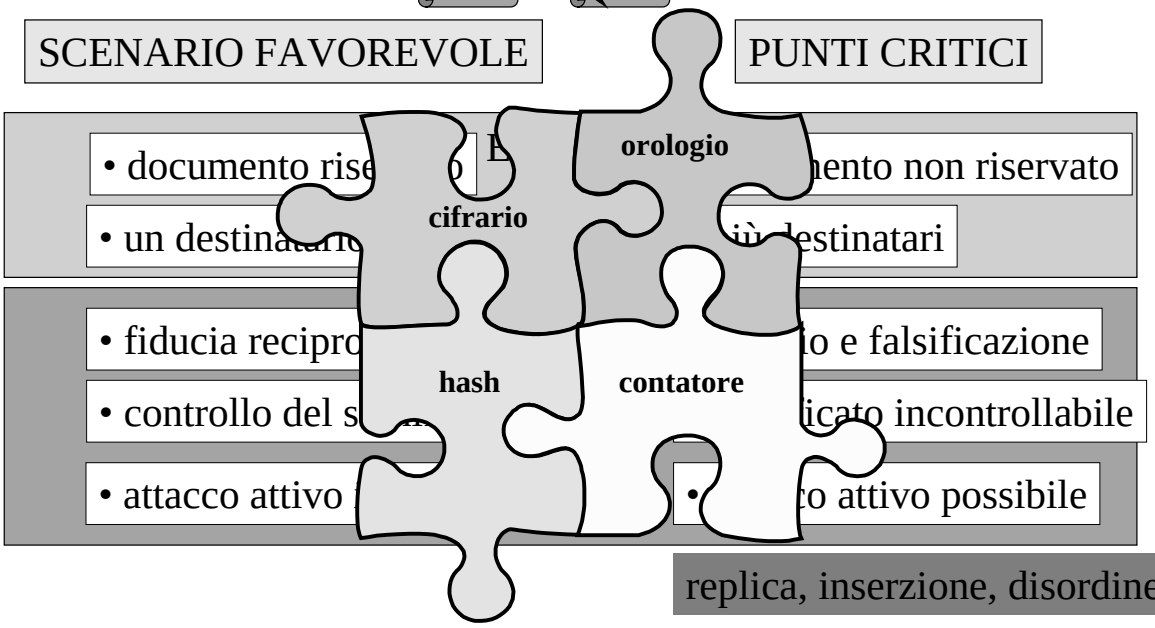
N.B.
La verifica può essere fatta solo da chi condivide il segreto sulla chiave

Autenticazione con E(m)



SCENARIO FAVOREVOLE

PUNTI CRITICI

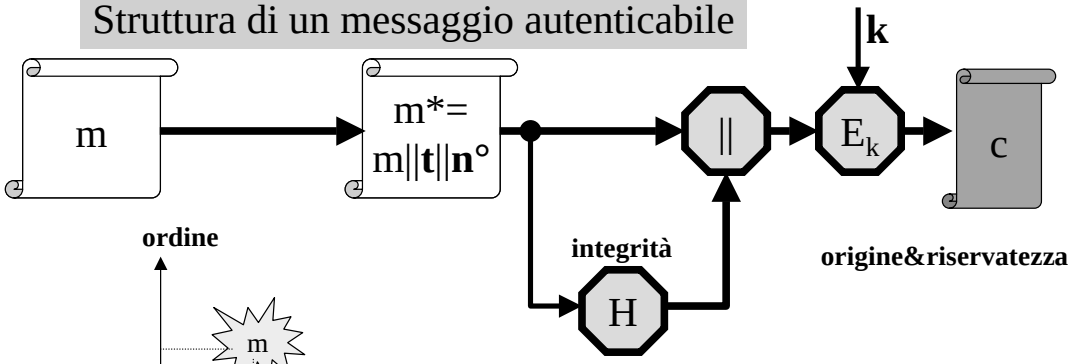


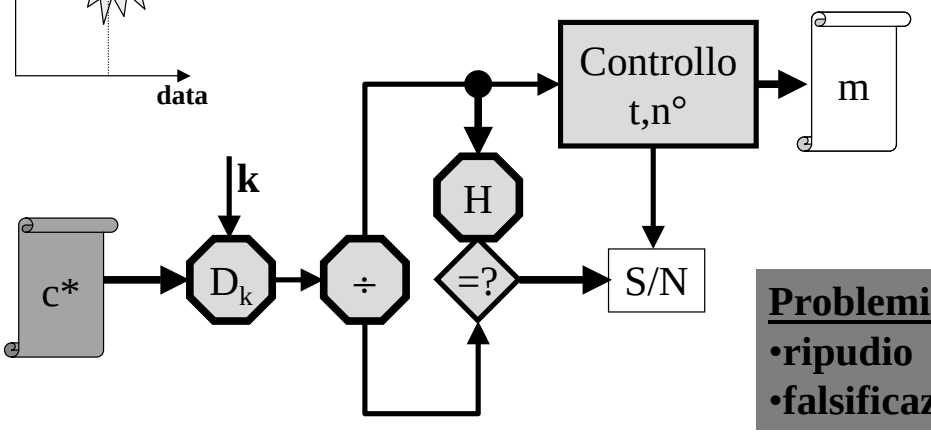
- documento rise… E …mento non riservato
- un destinatario … …destinatari
- fiducia recipro… …o e falsificazione
- controllo del s… …icato incontrollabile
- attacco attivo … • …co attivo possibile

replica, inserzione, disordine

Autenticazione con E(m*||H(m*))

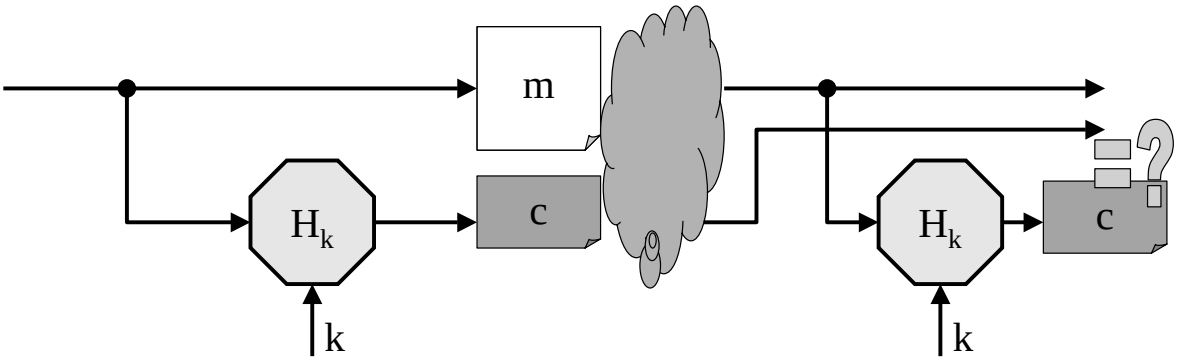
Struttura di un messaggio autenticabile





<u>Problemi aperti</u>:
•ripudio
•falsificazione

Integrità ed origine di un testo in chiaro

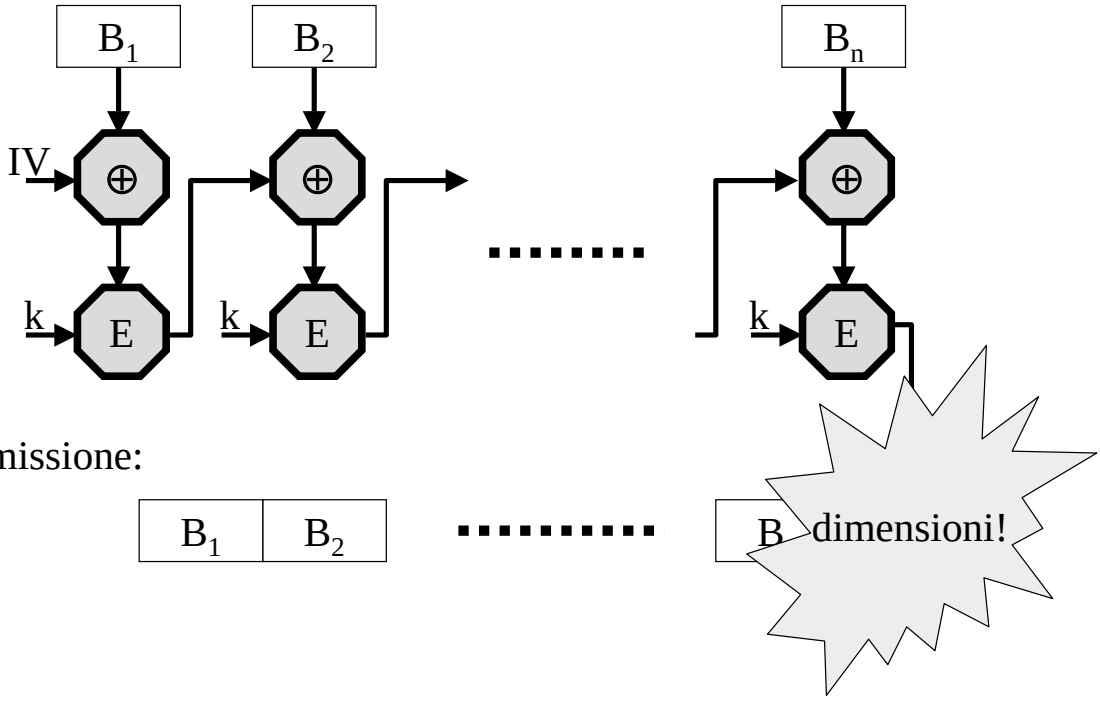


IPOTESI sulla H:
1. impossibilità di inversione
2. impossibilità di individuare collisioni

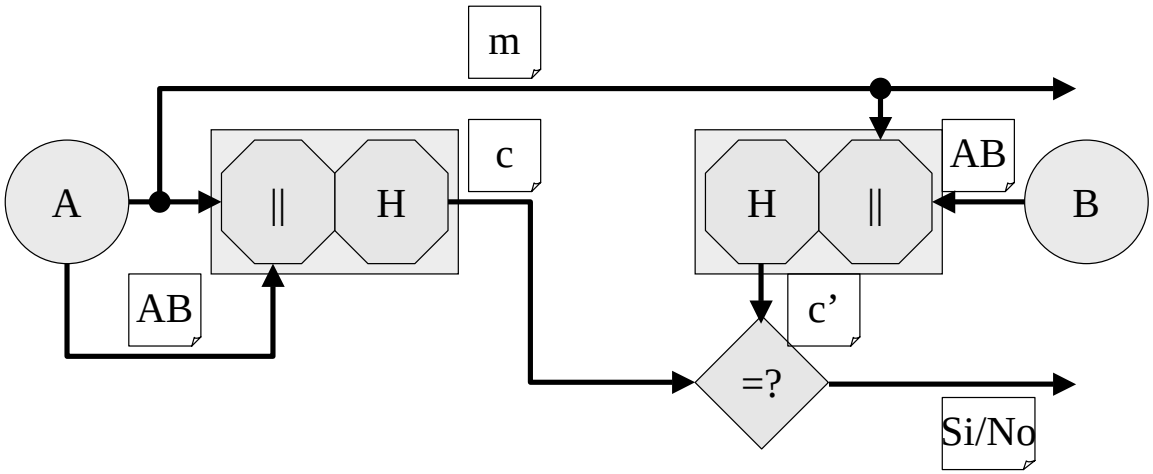
Problemi aperti:
- **ripudio**
- **falsificazione**

- **MAC** (*hash with CBC encryption*)
- **HMAC** (*hash with key*)

MAC (Message Authentication Code)

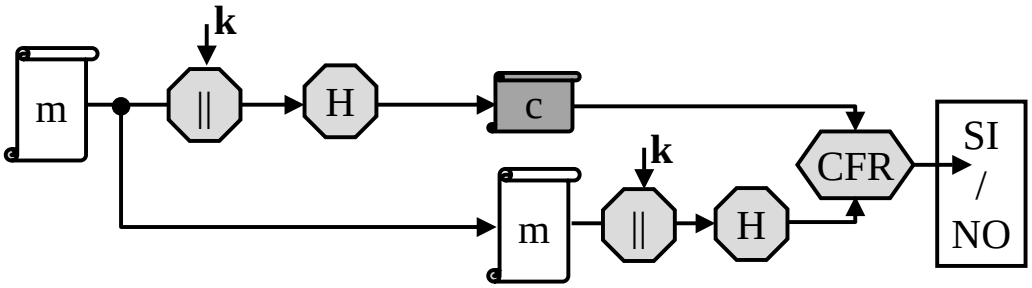


Hash a 2 ingressi o con chiave



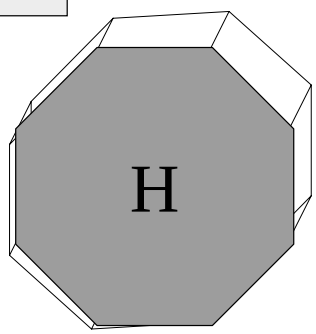
Usando il segreto **AB**, **A** dichiara a **B** di essere l'autore della prova di integrità **c** del messaggio **m**

HMAC



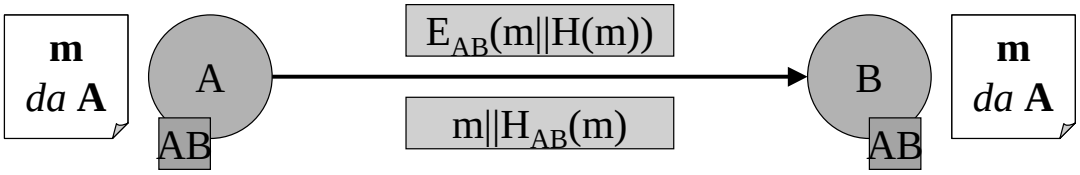
Standard Internet (RFC 2104)
per dare sicurezza al livello **IP**

1: k = k1||k2
2: h1 = H(k1||m)
3: h = H(k2||h1)
= HMAC(k||m)
= $HMAC_k(m)$
Funzione hash "con chiave"



Integrità
&
Origine
&
Non ripudio

Ripudio e Falsificazione



La condivisione del segreto: problemi di sicurezza
1: A **ripudia m**, affermando che B l'ha alterato o forgiato
2: B **altera** o **forgia m**, affermando che l'ha fatto A

Firma digitale nel contesto della Crittografia simmetrica

Firma digitale

La firma digitale di un documento informatico deve:

1- consentire a **chiunque** di identificare **univocamente** il firmatario,

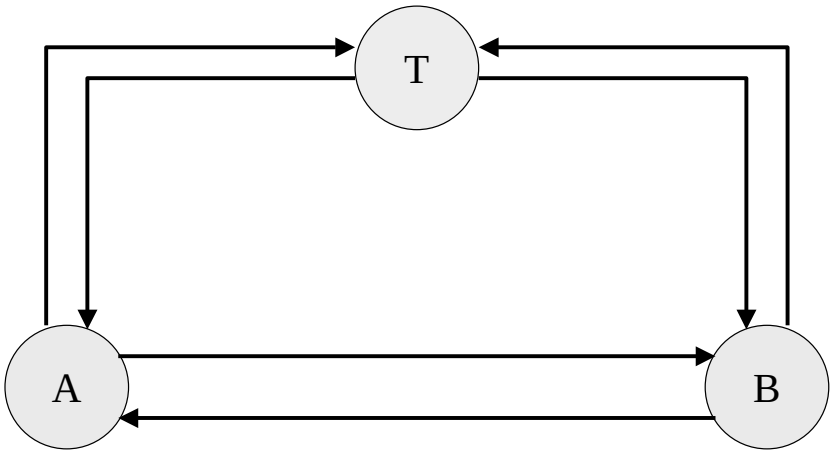
2- non poter essere **imitata** da un impostore,

3- non poter essere **trasportata** da un documento ad un altro,

4- non poter essere **ripudiata** dall'autore,

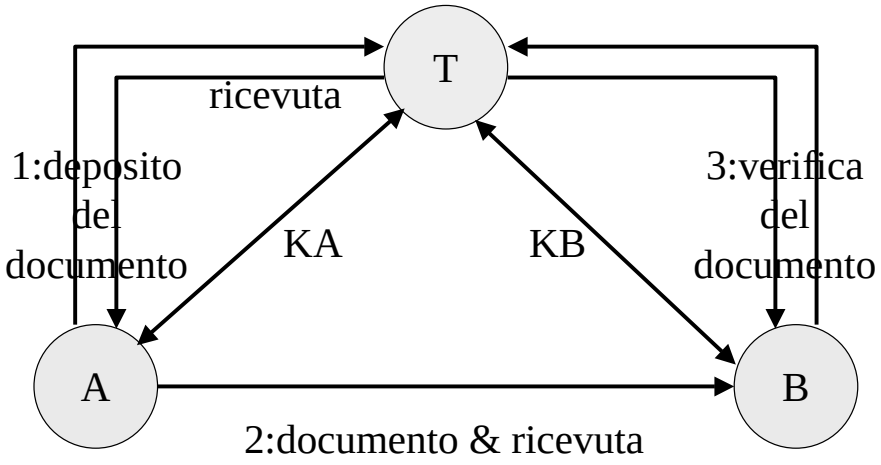
5- rendere **inalterabile** il documento in cui è stata apposta.

Il principio della terza parte fidata

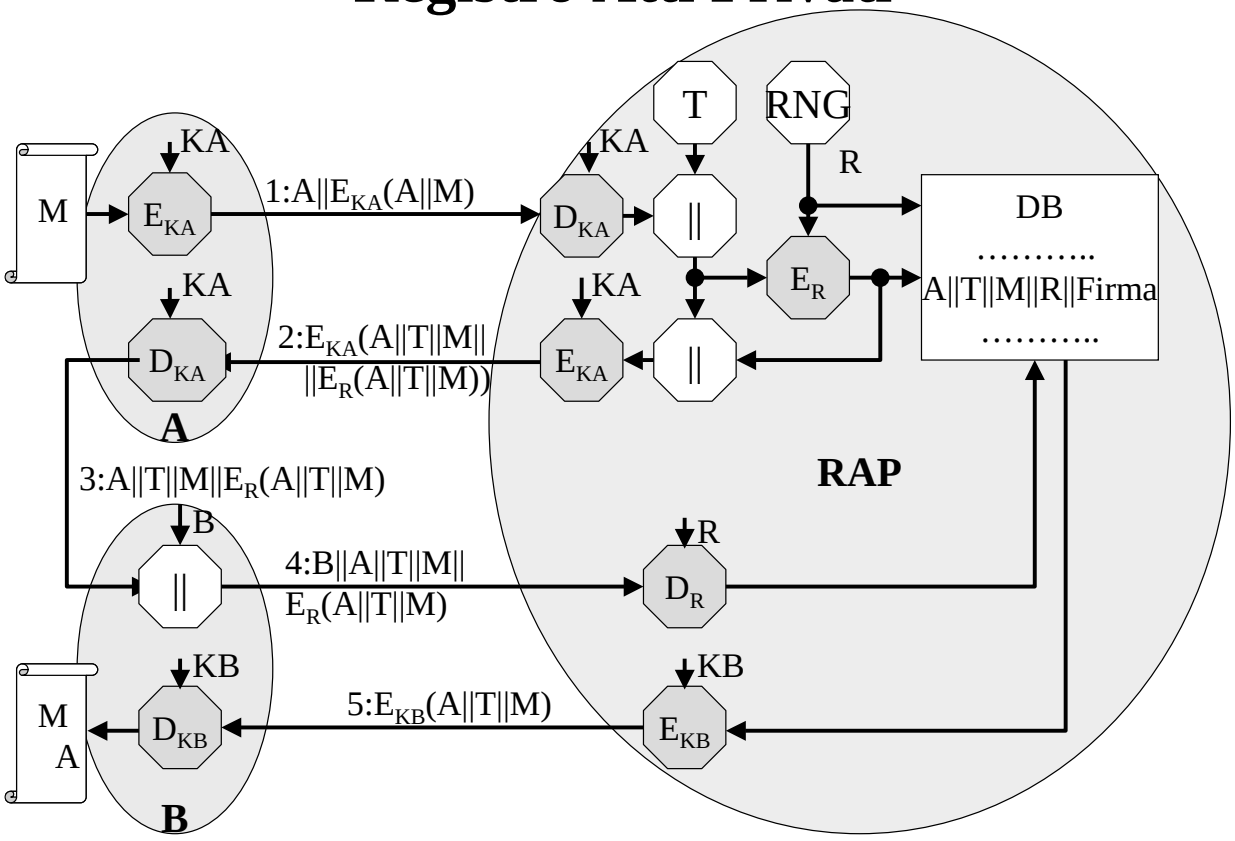


Protocolli resi sicuri dalla partecipazione di una terza parte:
il “notaio” interviene durante lo svolgimento per impedire scorrettezze
il “giudice” interviene al termine per dirimere dispute

Firma digitale
con un Cifrario simmetrico



Registro Atti Privati



Problemi risolti e nuovi problemi

- Ripudio
- Falsificazione

- L'Autorità deve essere sempre **on-line**.
- L'Autorità non deve costituire un **collo di bottiglia**.
- L'Autorità non deve creare **documenti falsi**.
- L'Autorità deve tenere le chiavi in una **memoria sicura**.