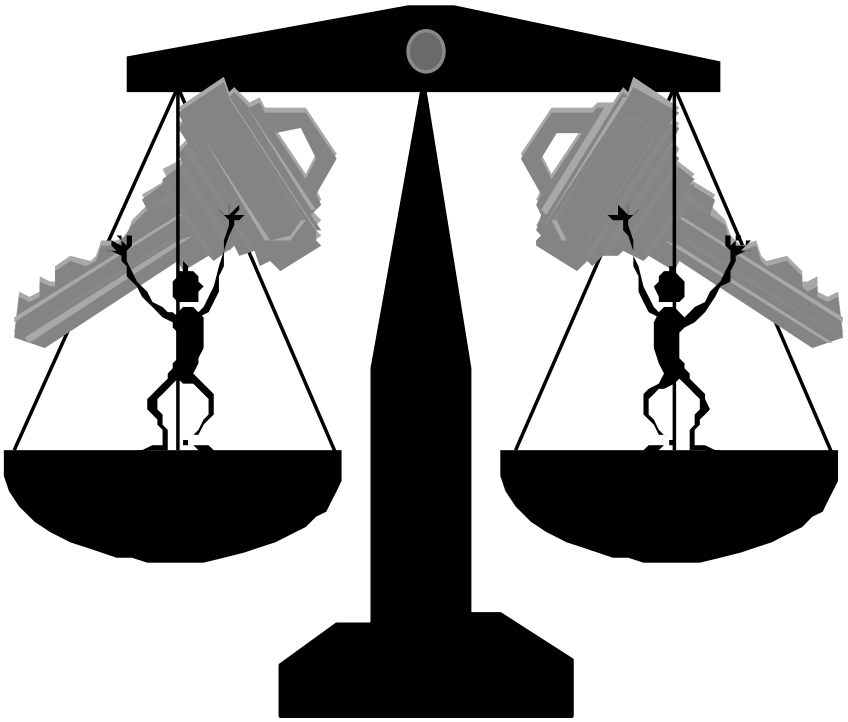
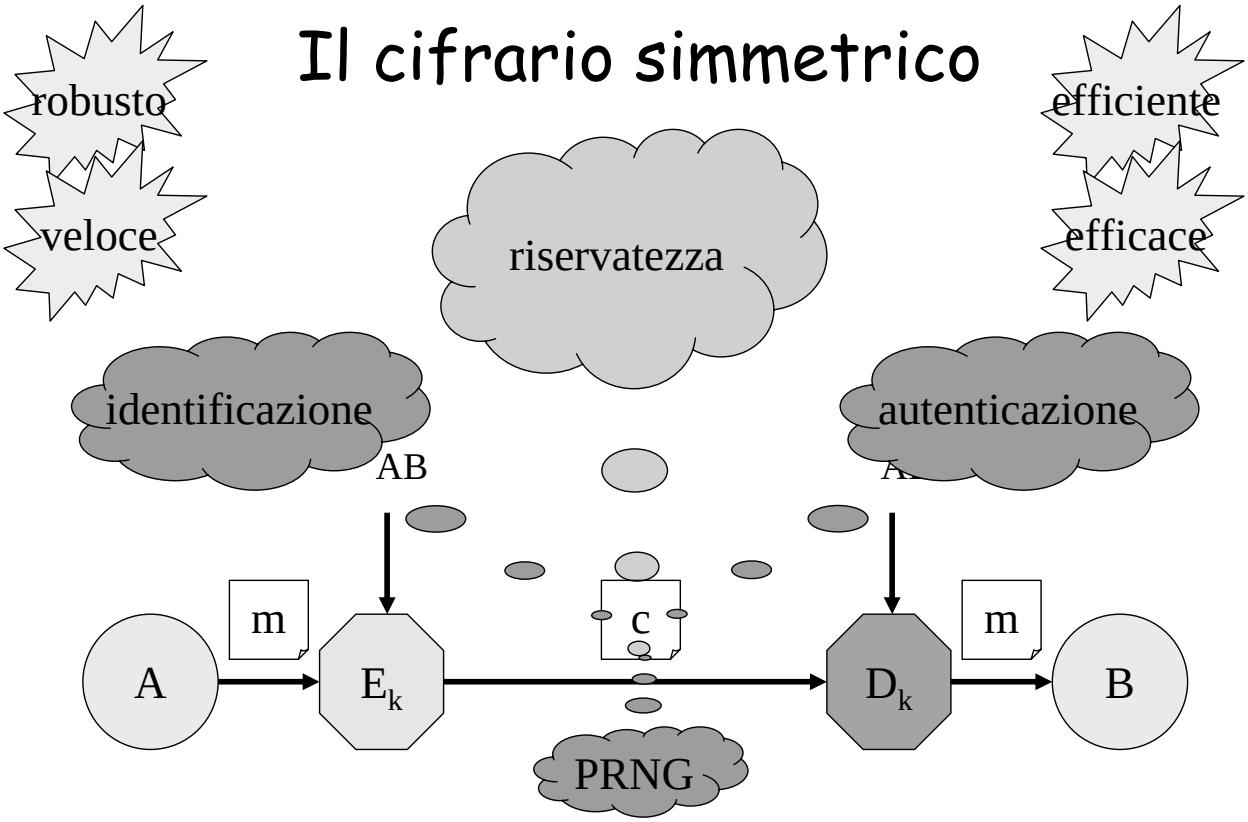
Meccanismi simmetrici



Il cifrario simmetrico



$m_1, m_2, .., m_N$
$c_1, c_2, .., c_N$

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

+ veloce

Cifrario a flusso (stream cipher): trasforma, **con una regola variabile al progredire del testo**, uno o pochi bit alla volta del testo da cifrare e da decifrare.

Protezione dei singoli bit di una trasmissione seriale — WEP, GSM

Cifrario poligrafico
Cifrario composto

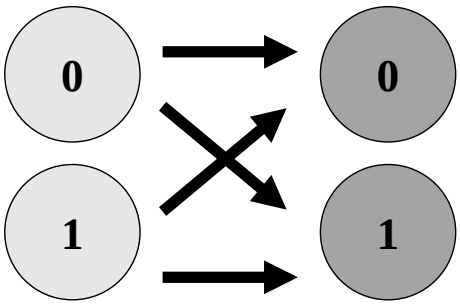
+ sicuro

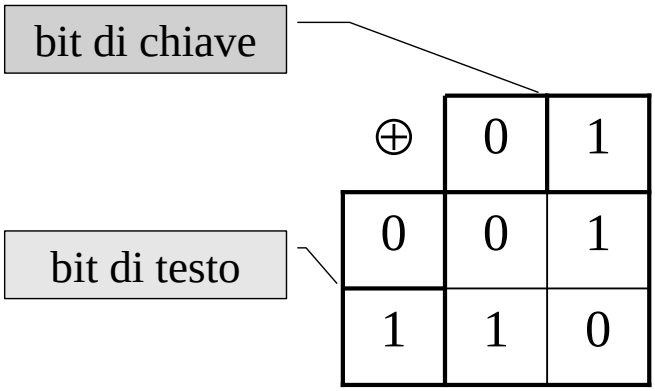
Cifrario a blocchi (block cipher): trasforma, **con una regola fissa** ed uno alla volta, blocchi di messaggio formati da molti bit.

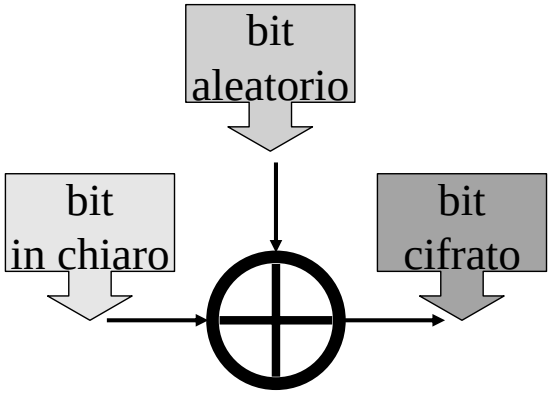
Protezione di pacchetti, di file e di strutture di dati — IPSec, SFS

Cifrari a flusso

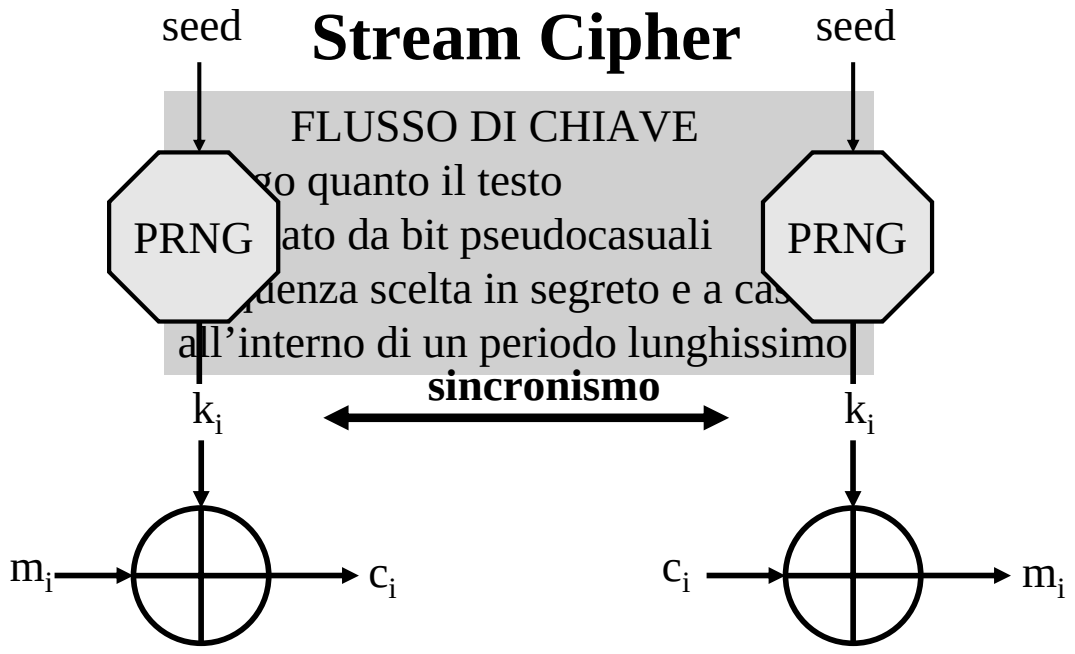
Il meccanismo per la sostituzione di un bit







Stream Cipher



CIFRATURA

$c_i = m_i \oplus k_i$

i= 1, 2, 3, ..

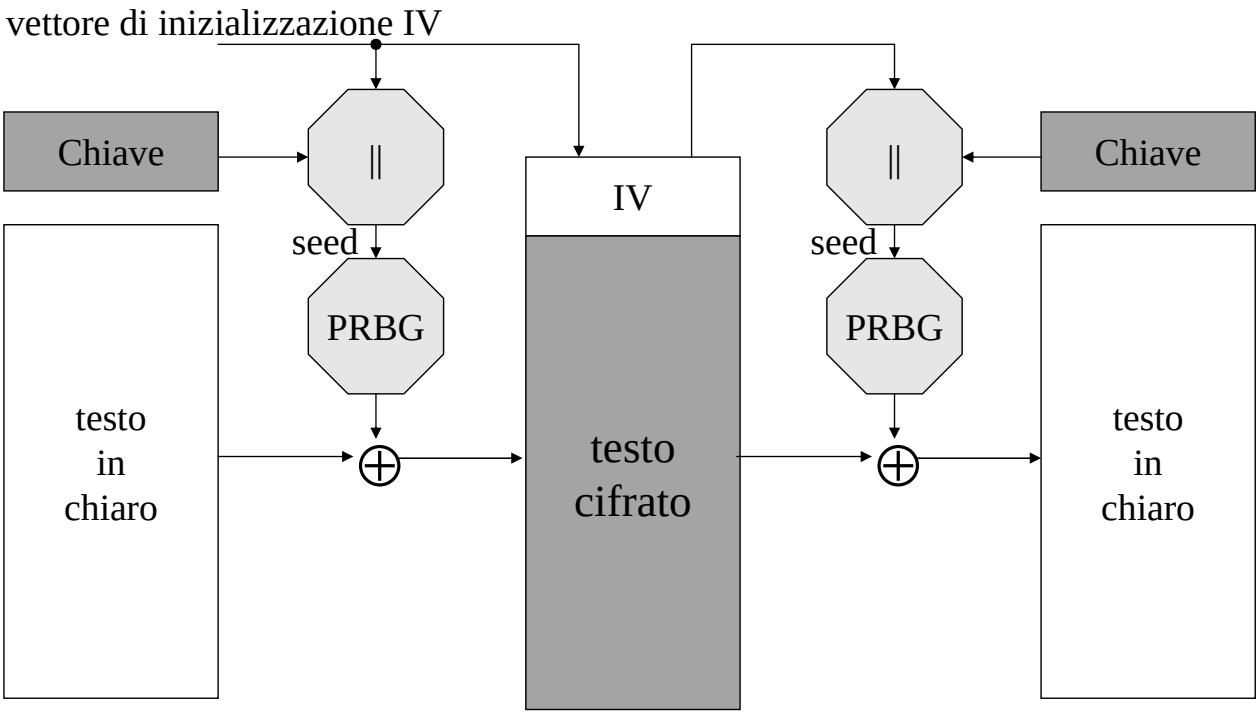
DECIFRAZIONE

$c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i$

$= m_i$

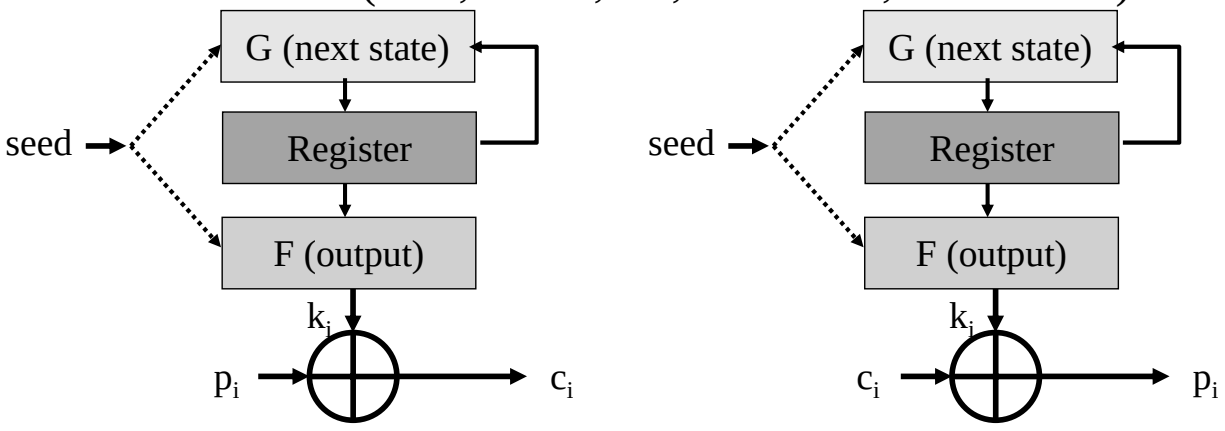
i= 1, 2, 3, ..

Segretezza e variabilità del seme (WEP)

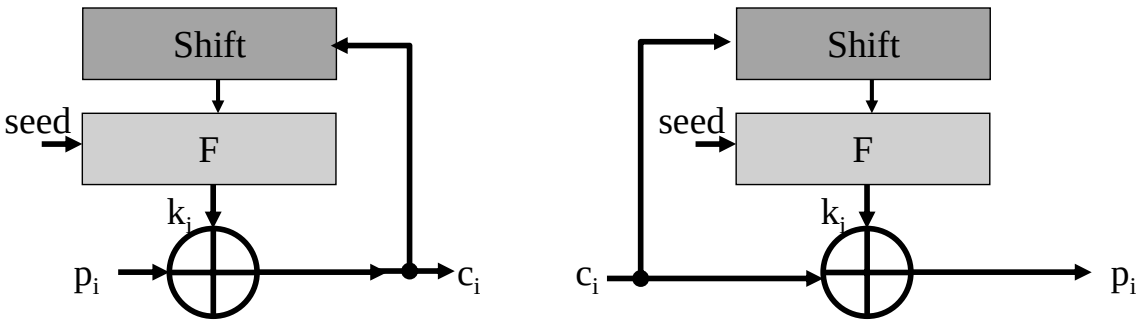


Stream ciphers

- A flusso sincrono (RC4, SEAL, A5, DES-CTR, DES-OFB..)



- Con auto-sincronizzazione (DES-CFB, ..)



Problemi dei Cifrari a flusso

ATTACCHI	FLUSSO SINCRONO	AUTOSINCR.
Cancellazione di bit	perdita di sincronismo	transitorio
Inserzione di bit	perdita di sincronismo	transitorio
Modifica di bit	non propagazione	transitorio

Proprietà del PRNG (Golomb, 1967)

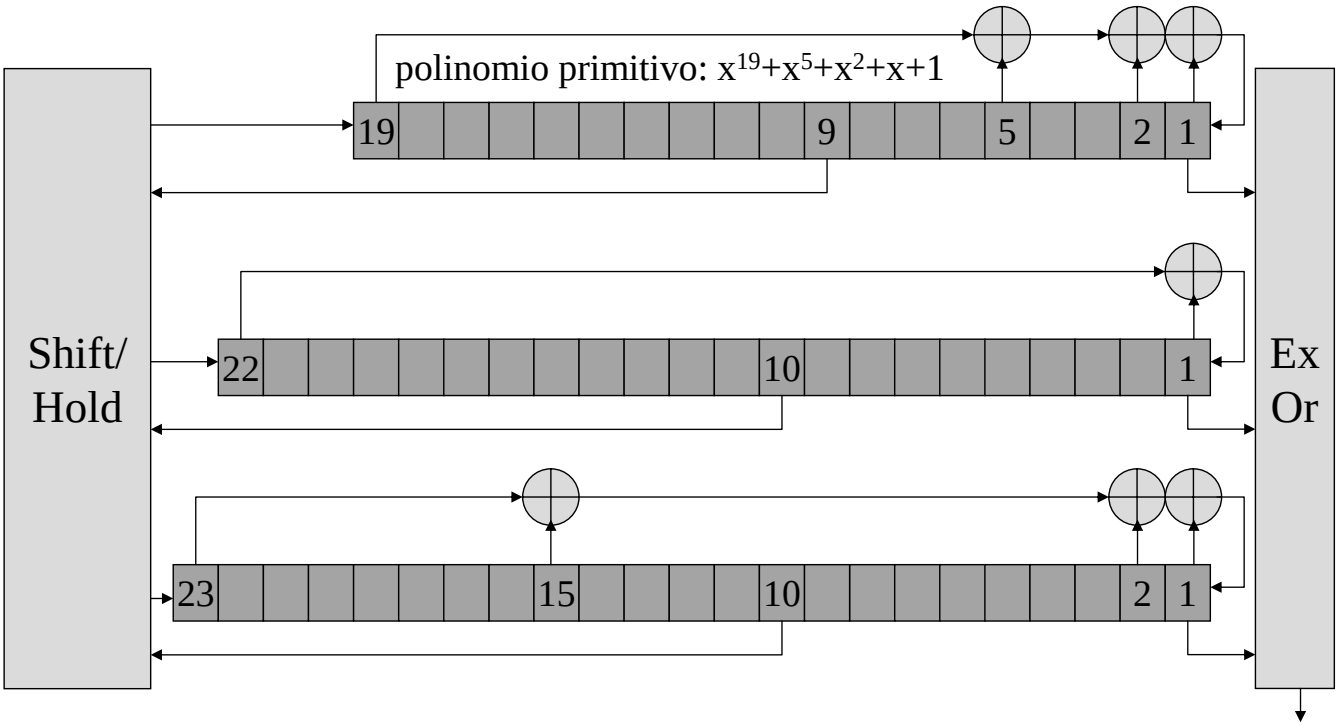
Registri a scorrimento con retroazione

•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**".

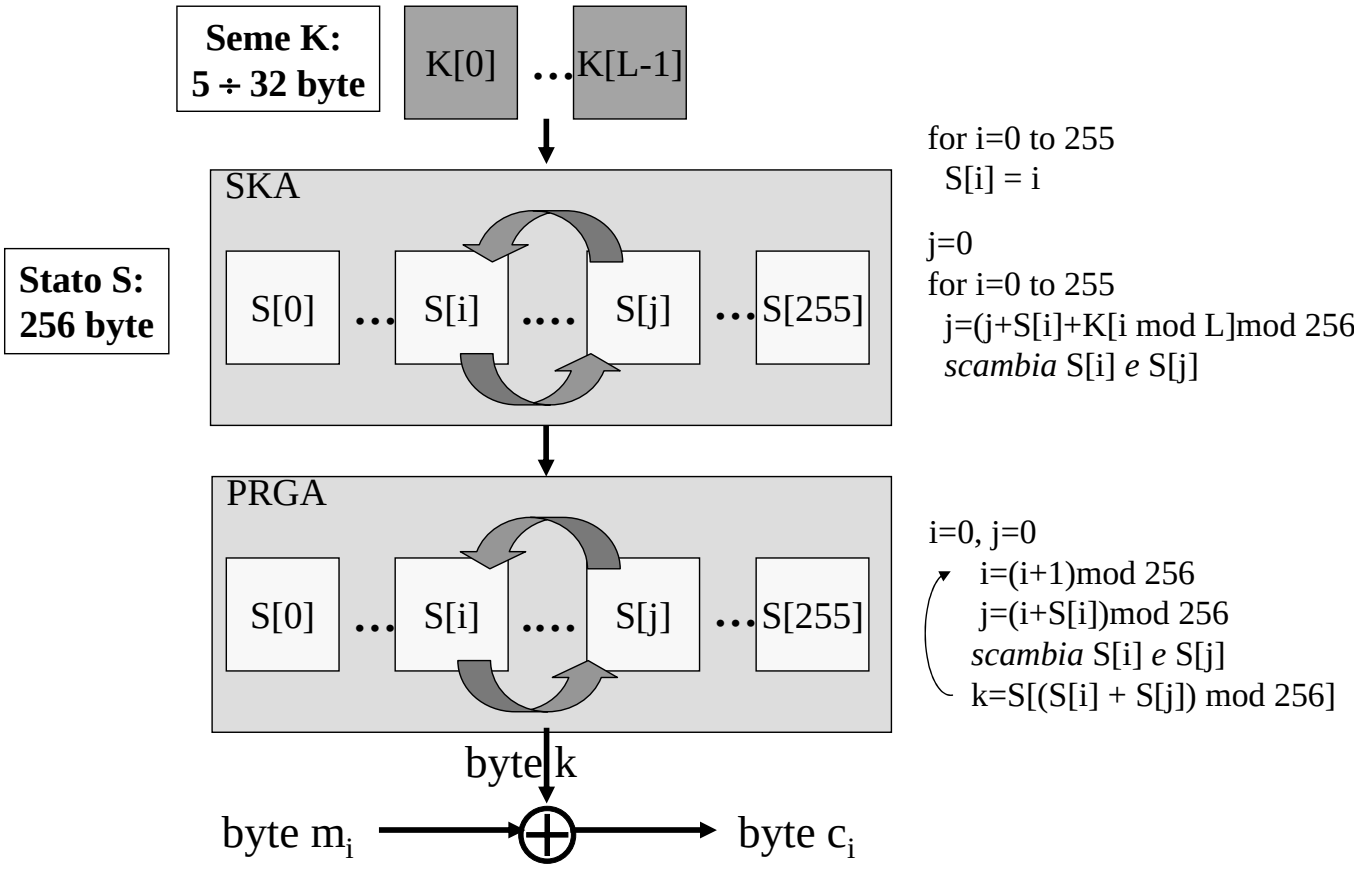
GSM: il generatore di flusso di chiave



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

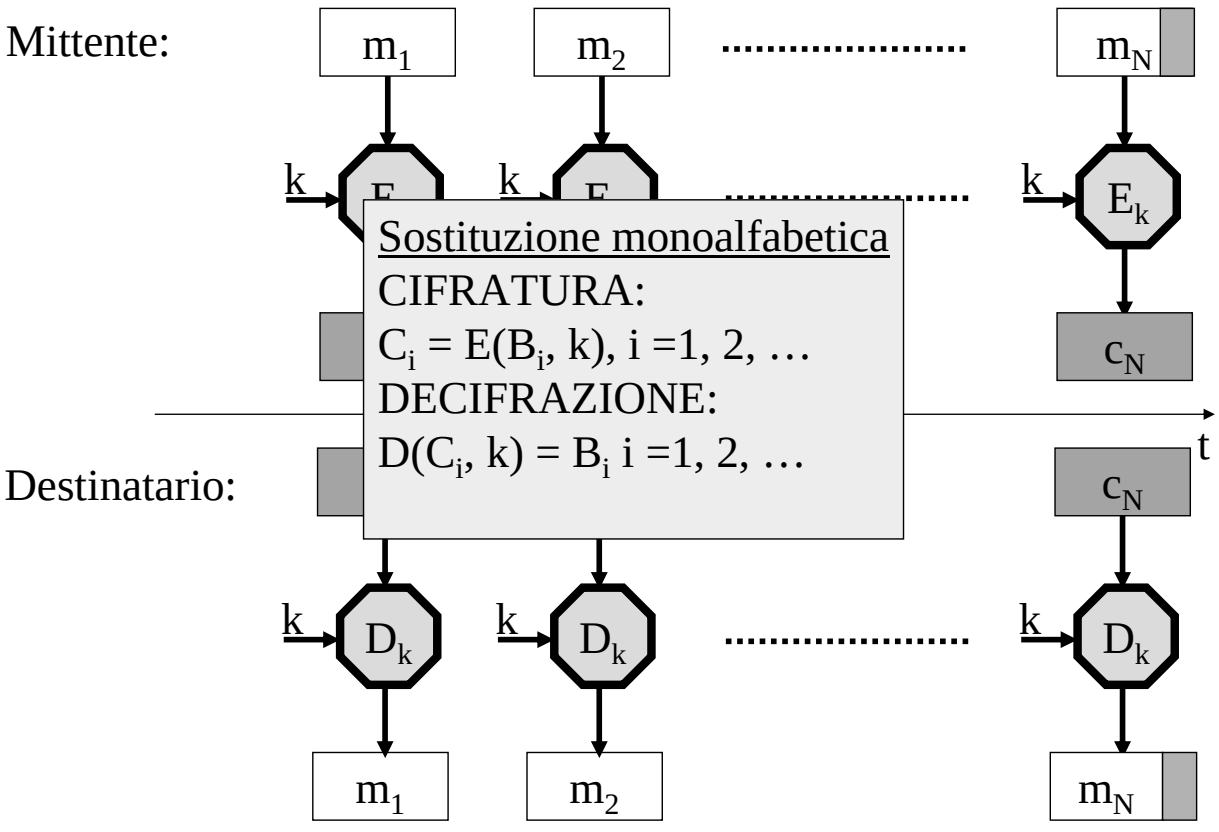
UMTS: Cifrario a blocchi Kasumi

Il Cifrario a flusso RC4 (Rivest, 1984)

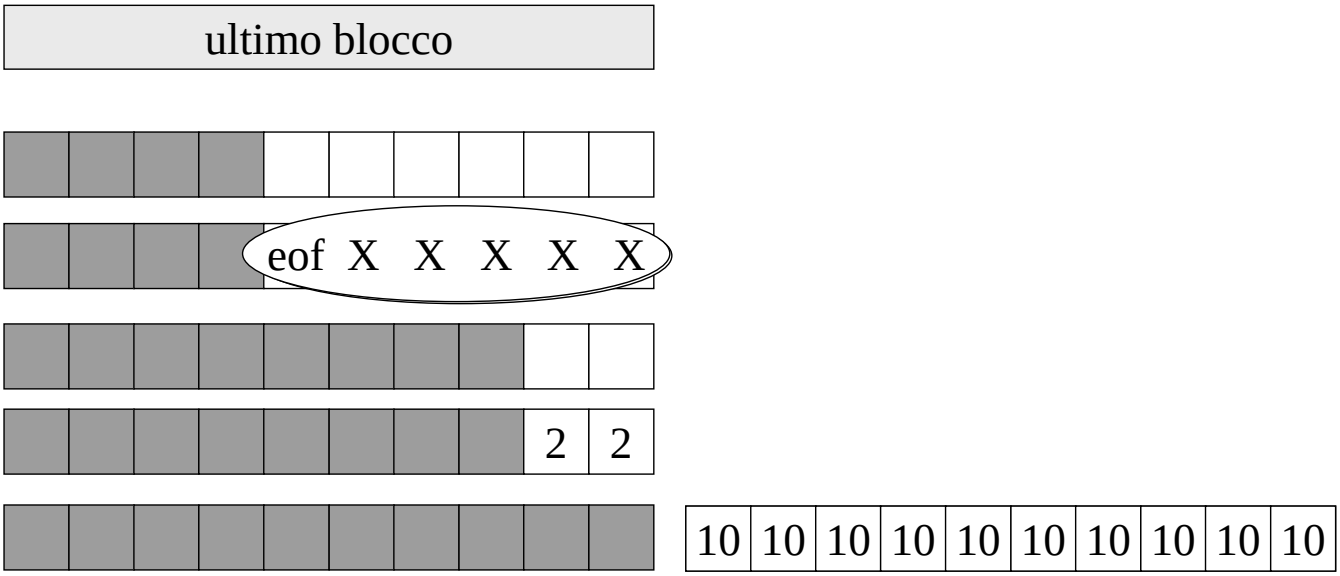


Cifrari a blocchi

Block cipher (modalità ECB)



Padding: standard PKCS#5 e #7



Time to break a code

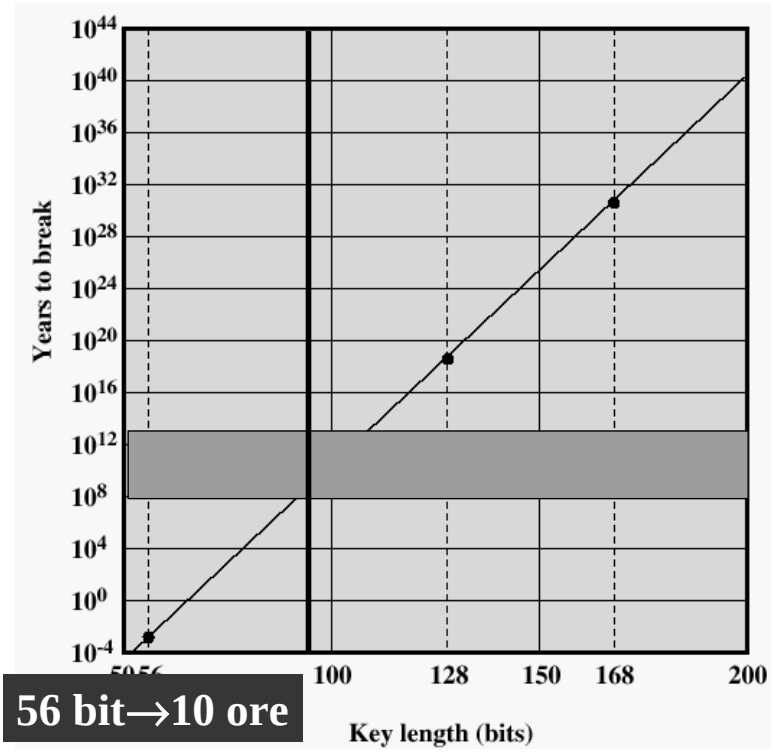
Spazio delle chiavi

N bit	2^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	$2^{192} = 6{,}3 \times 10^{57}$

$p = 2^{-N}$

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

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



56 bit→10 ore

Dimensioni della chiave e del blocco

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)

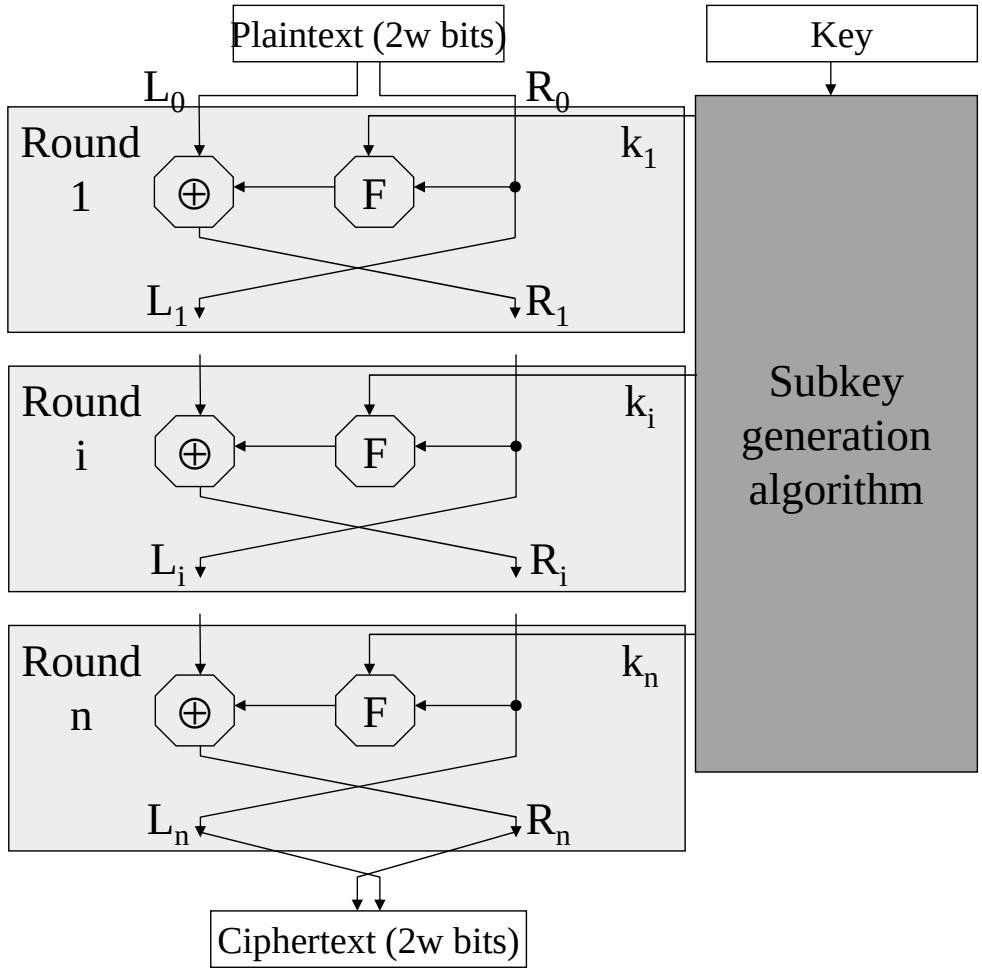
Attacchi con testo noto e scelto: dimensione del blocco

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

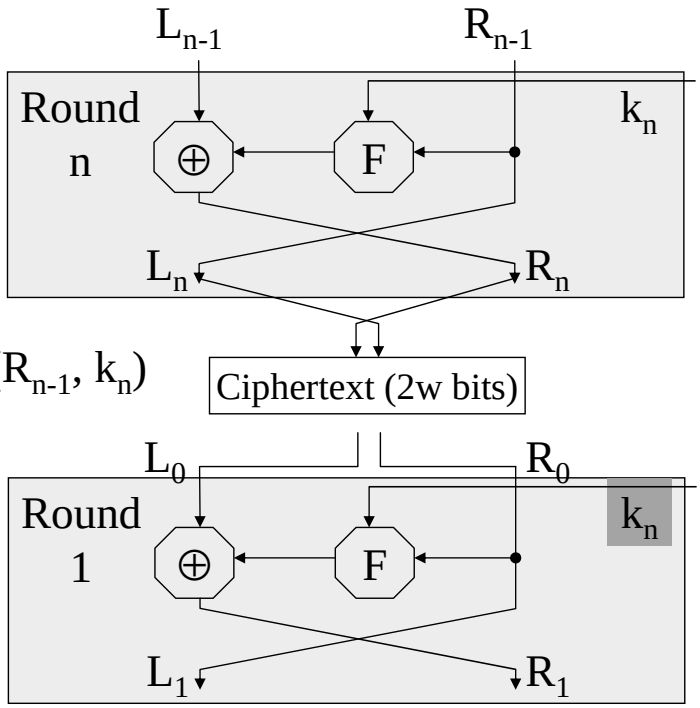
"la chiave segreta deve essere scelta caso (R12) e frequentemente modificata (R24)".

La rete di Feistel

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

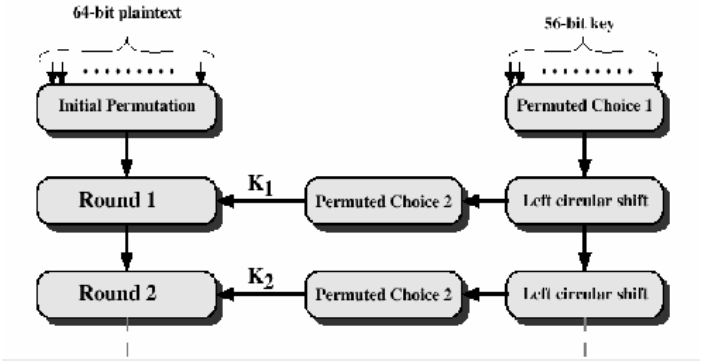


Reti di Feistel: Cifratura/Decifrazione



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

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



VLSI: 120 milioni di byte al secondo
SW: 100 mila byte al secondo

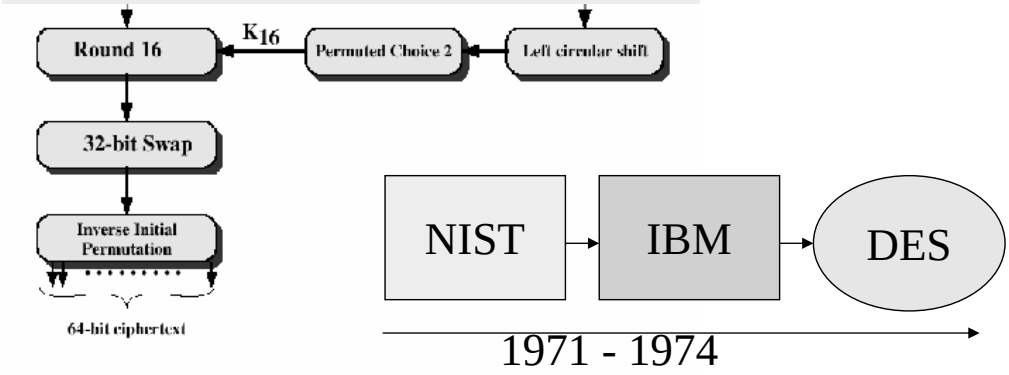


Figure 2.3 General Depiction of DES Encryption Algorithm

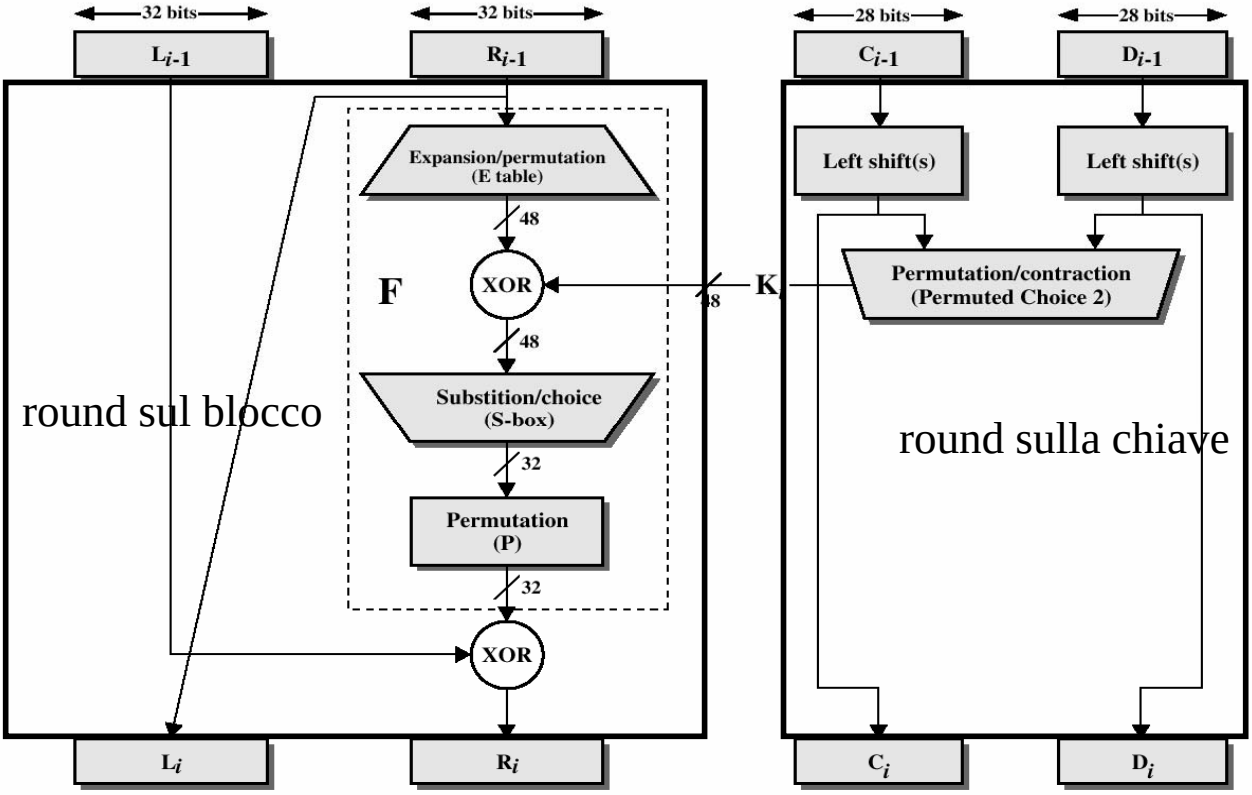


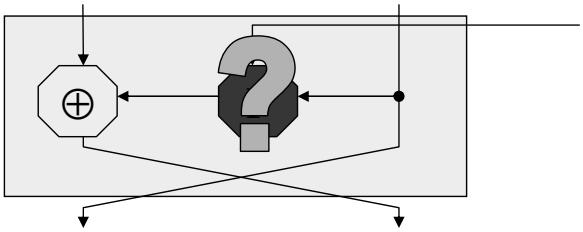
Figure 2.4 Single Round of DES Algorithm

Crittanalisi differenziale e lineare

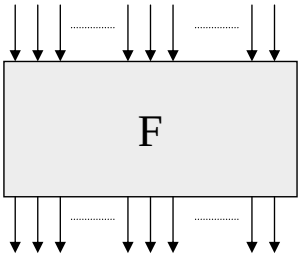
Crittanalisi differenziale: cerca coppie di testo in chiaro scelto la cui differenza si riscontri identica anche sull'uscita della F

Crittanalisi lineare: cerca coppie con testo in chiaro noto con cui costruire una approssimazione lineare della F

FEAL: rotto!



DES: 2^{47} coppie



Invertendo un bit d'ingresso
SAC: i bit d'uscita si modificano con p = 0,5
BIC: si modificano 2 bit d'uscita non prevedibili
GA: si modificano da 2 a 5 bit d'uscita

I successori del DES

Hw → Sw

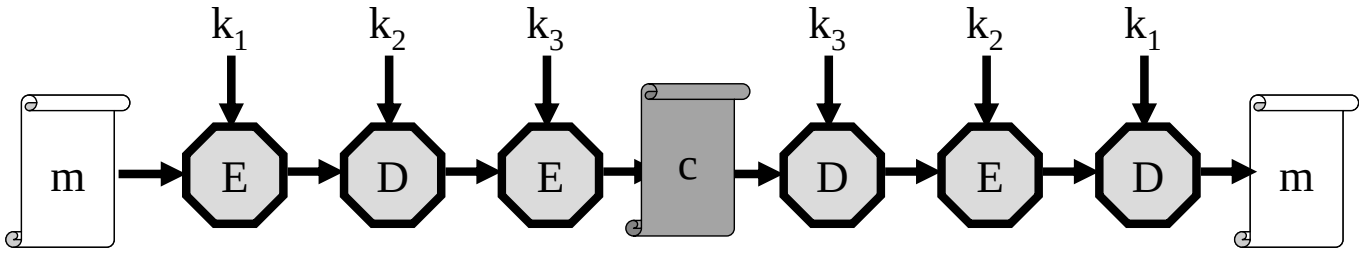
K: 64 → 128+

B: 64 → 128+

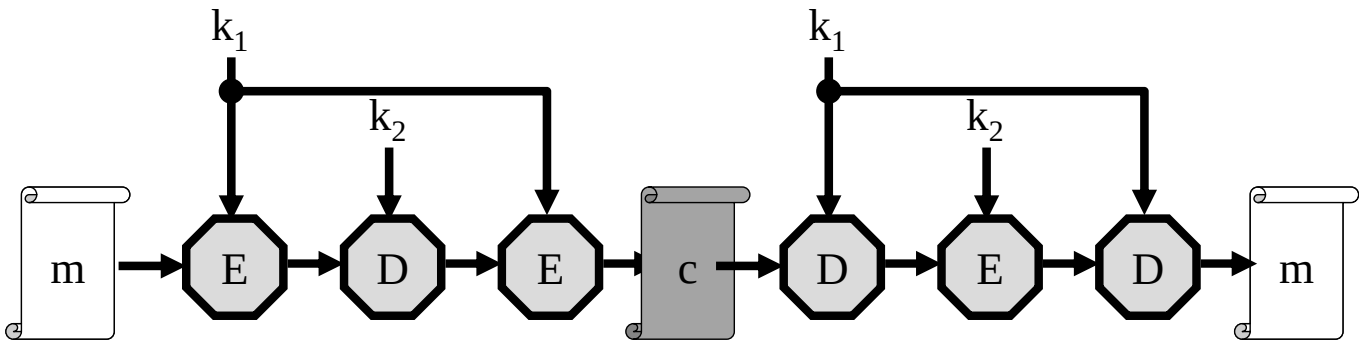
IDEA
TDES
BLOWFISH
CAST-128
ecc.

opera su 3 gruppi:
- Somma modulo 2 su vettori di 16 bit
- Addizione tra interi modulo 2^{16}
- Moltiplicazione tra interi modulo $2^{16}+1$

Il Triplo DES (TDEA, EDE)



La versione con 168 bit di chiave



La versione con 112 bit di chiave

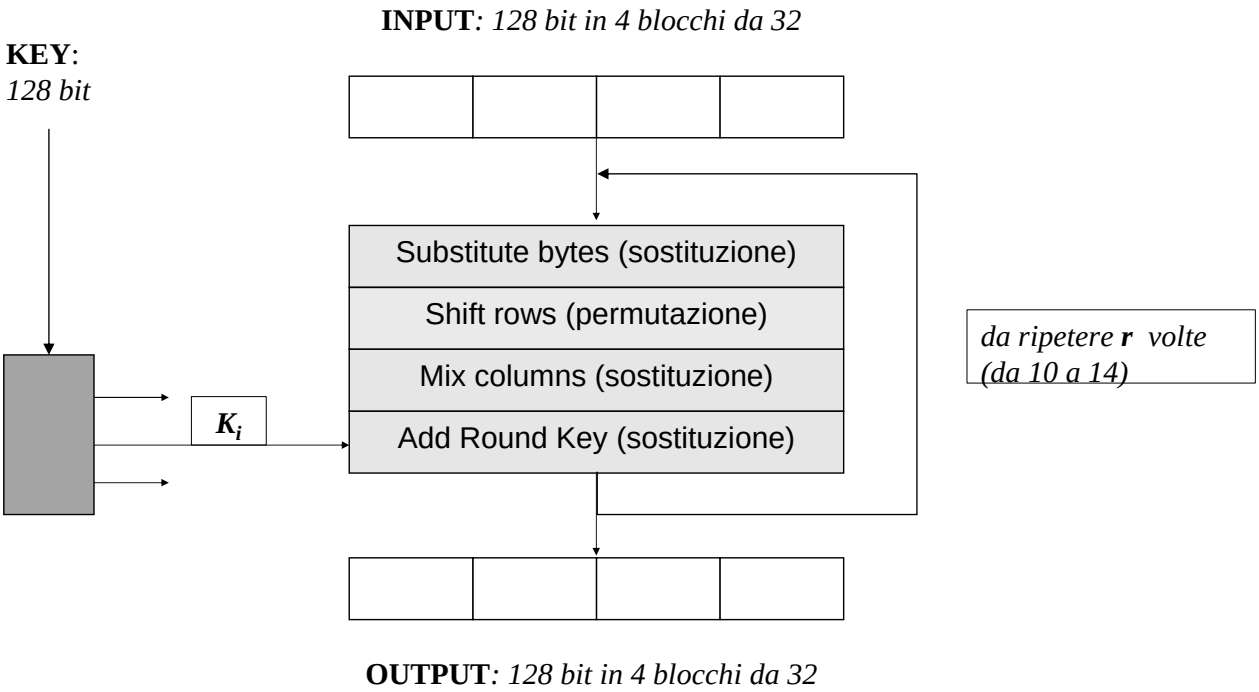
Advanced Encryption Standard

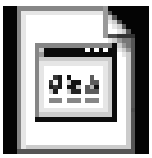
5 finalisti su 16 candidati:
MARS, RC6, Rijndael, Serpent, Twofish

Valutazione di Rijndael

- eccellenti prestazioni su tutte le piattaforme (dai main frame alle smart card),
- buon margine di sicurezza a fronte di ogni attacco conosciuto,
- bassa richiesta di memoria, sia ROM che RAM,
- veloce procedura di key setup,
- buone caratteristiche per l'esecuzione parallela delle istruzioni,
- chiavi e blocchi di lunghezza variabile per multipli di 32 bit.

Un round di Rijndael

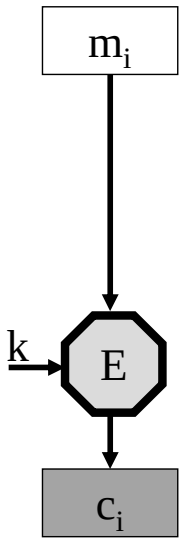




Rijndael_ingles_2004.exe

Modalità di cifratura

Modalità di elaborazione a blocchi



☹ **ECB**: Electronic Code Book — padding

☺ **CBC**: Cipher block Chaining — padding

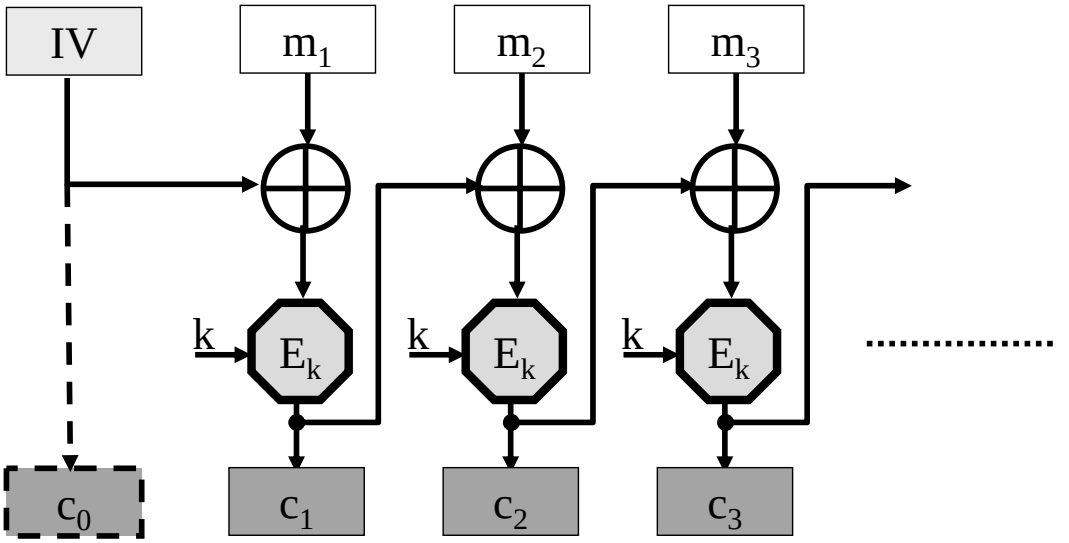
☺ **CFB**: Cipher Feedback, — no padding

☺ **OFB**: Output Feedback — no padding

☺ **CTR**: Counter — no padding

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

Cipher Block Chaining

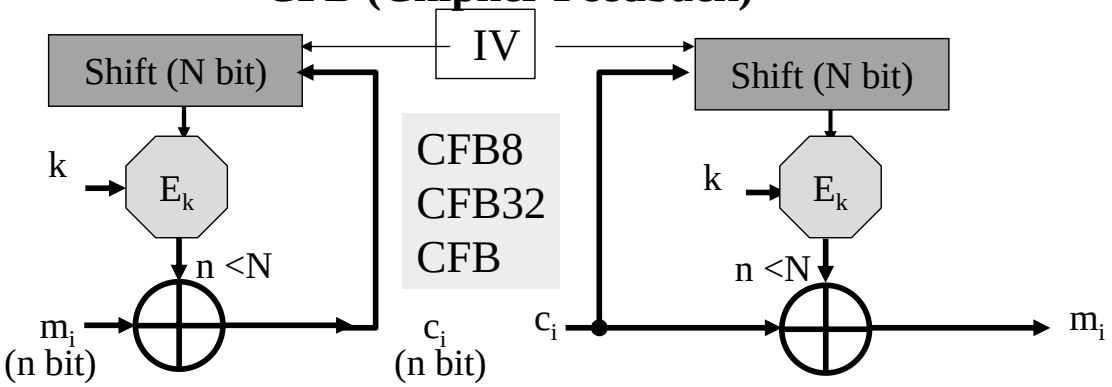


DECIFRAZIONE

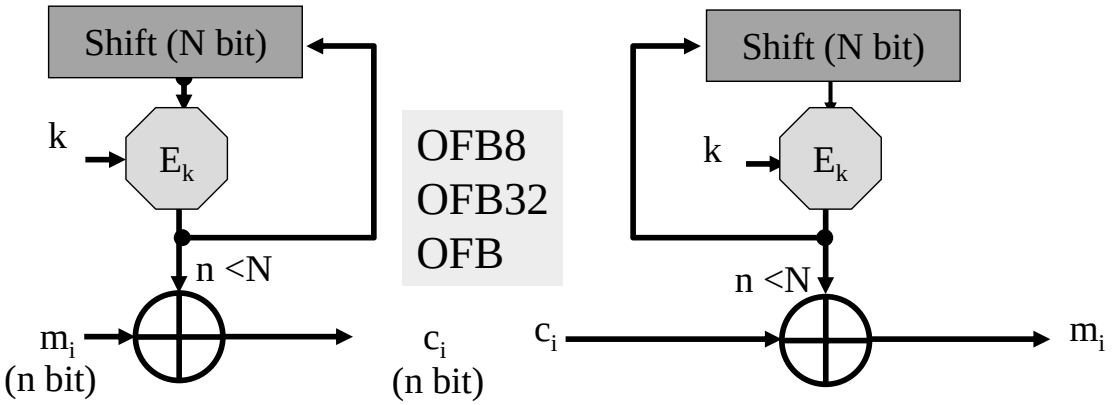
$D(c_i,k) = m_i \oplus c_{i-1}$

$D(c_i,k) \oplus c_{i-1} = m_i \oplus c_{i-1} \oplus c_{i-1} = m_i$

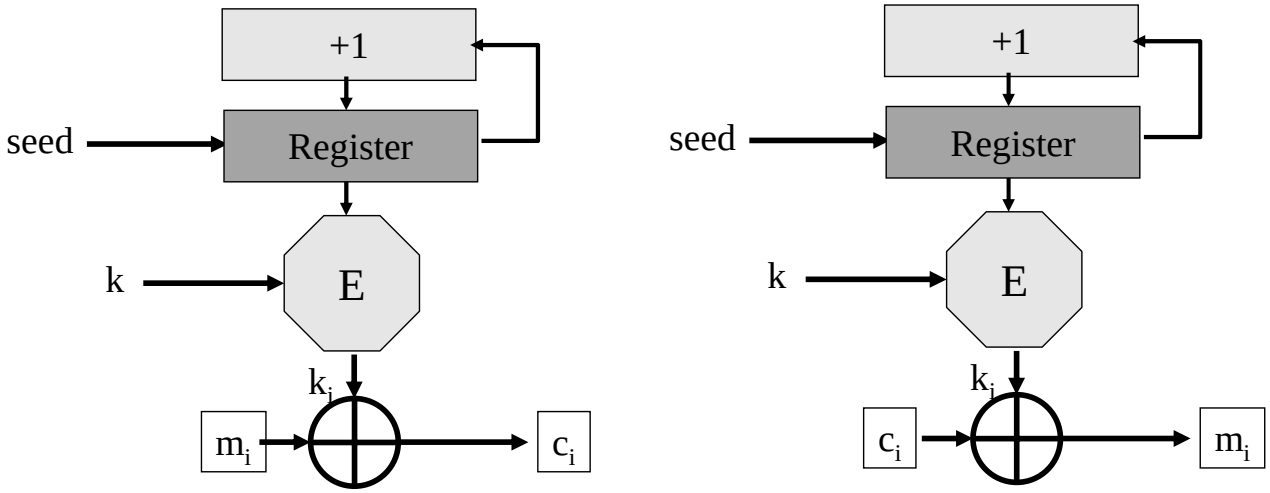
CFB (Chipher Feedback)



OFB (Output Feedback)



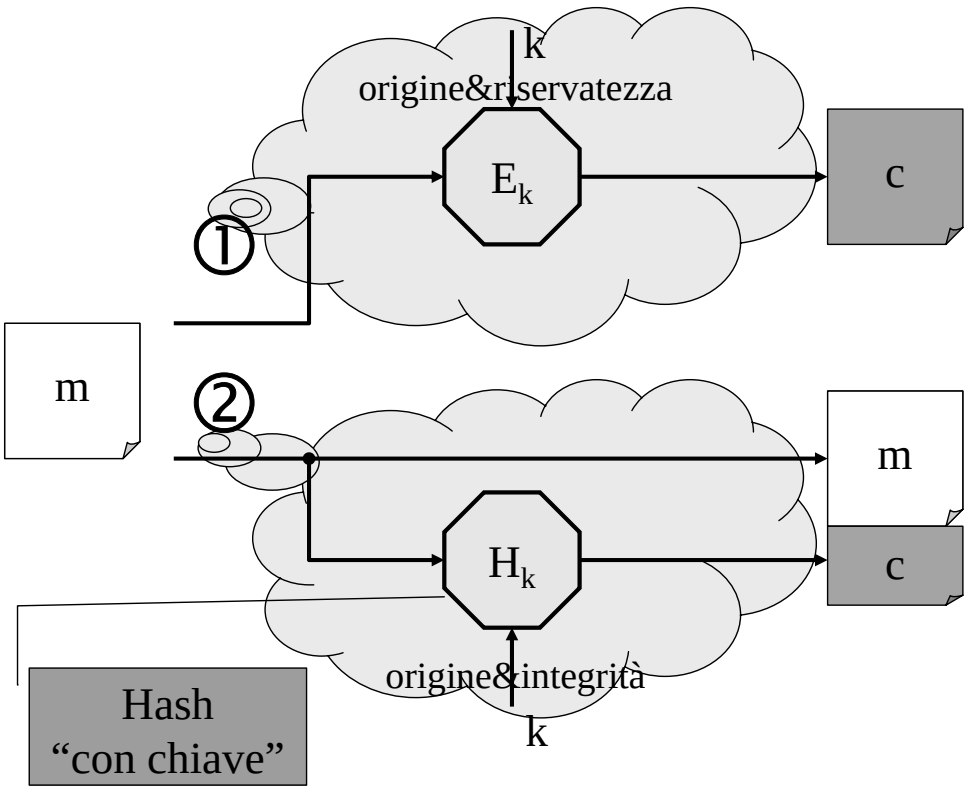
CTR (Counter)



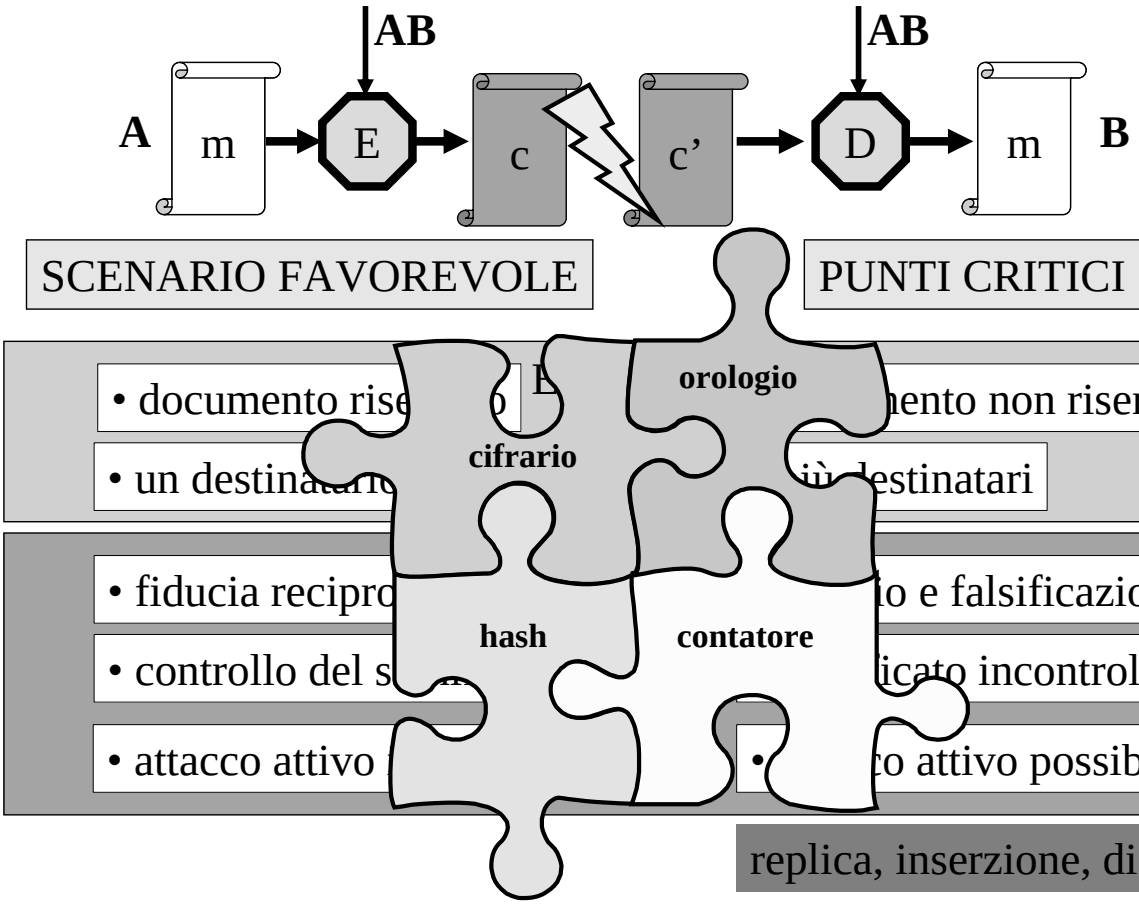
Integrità ed origine di un messaggio

Message Authentication

Ipotesi:Uso della crittografia simmetrica

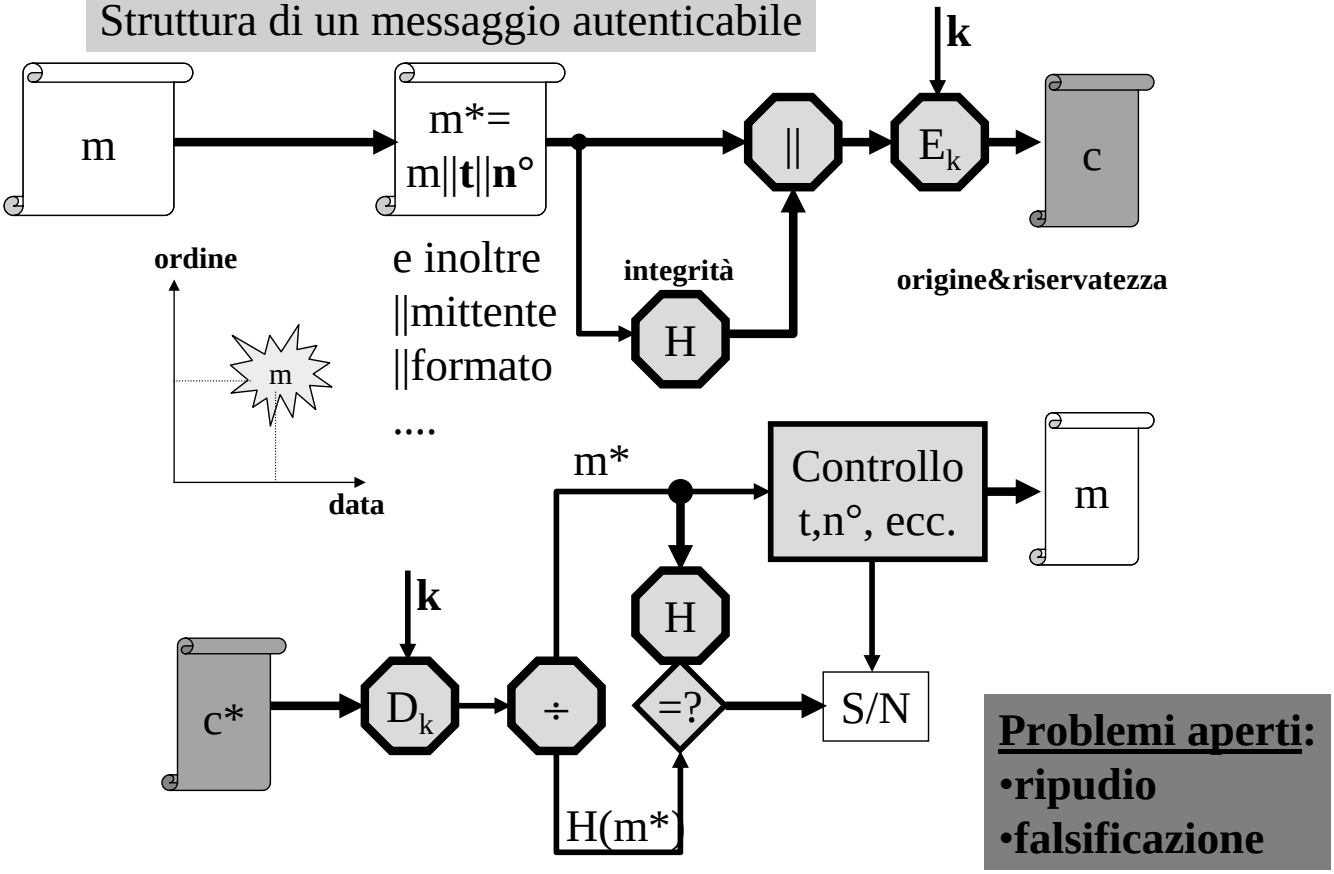


Autenticazione di m con E(m)



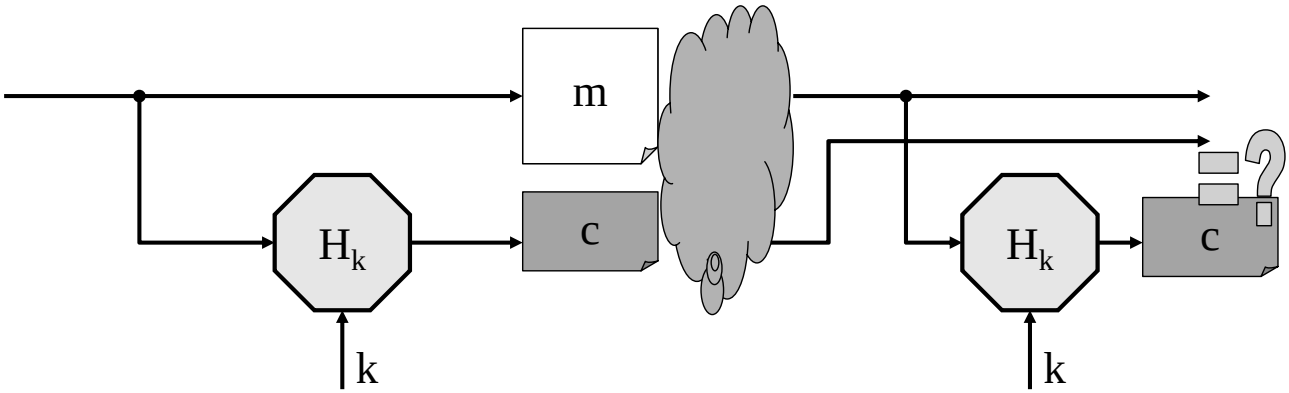
Autenticazione di m con E(m*||H(m*))

Struttura di un messaggio autenticabile



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

Integrità ed origine di un testo in chiaro

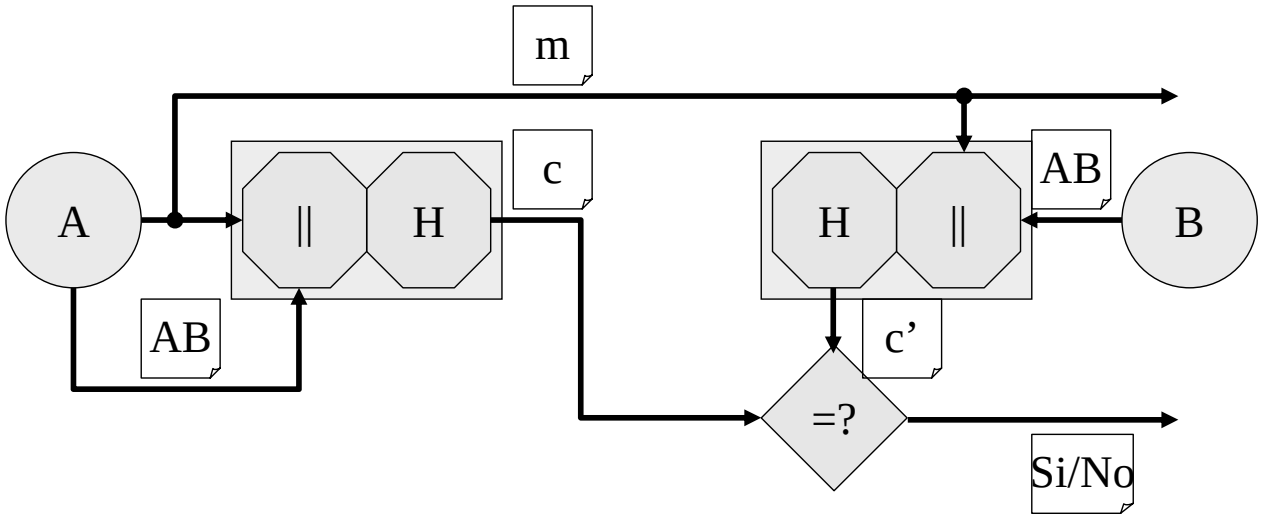


IPOTESI sulla H:
1. impossibilità di inversione
2. impossibilità di individuare collisioni

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

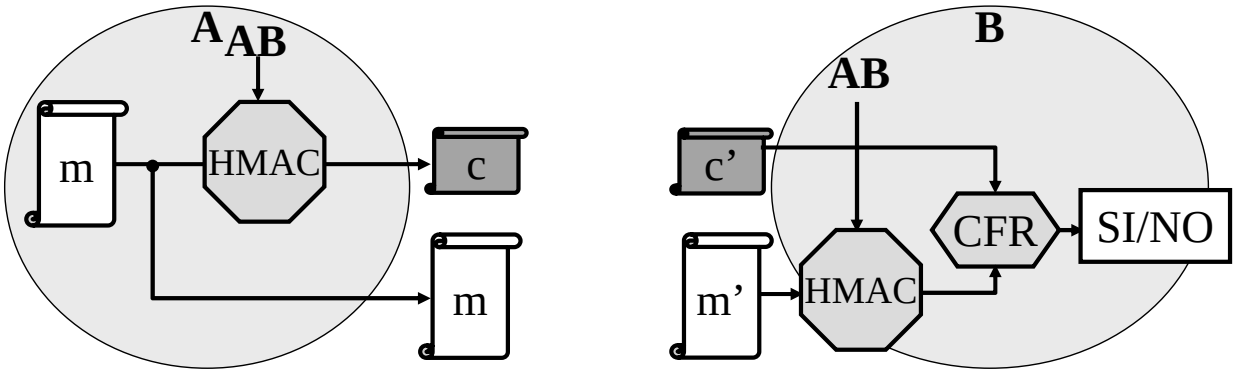
- **MAC** (*hash with CBC encryption*)
- **HMAC** (*hash with key*)

Hash a 2 ingressi o con chiave



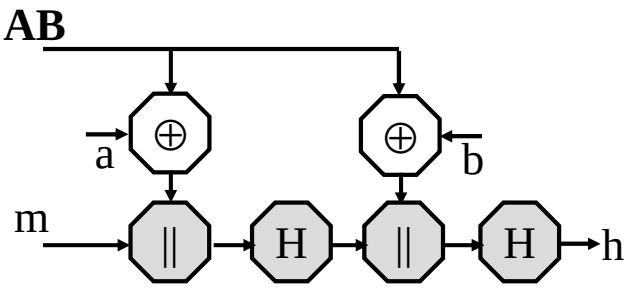
Usando il segreto **AB**, **A** dichiara a **B** di essere l'autore della prova di integrità **c** del messaggio **m**

RFC 2104: HMAC (hash “con chiave”)



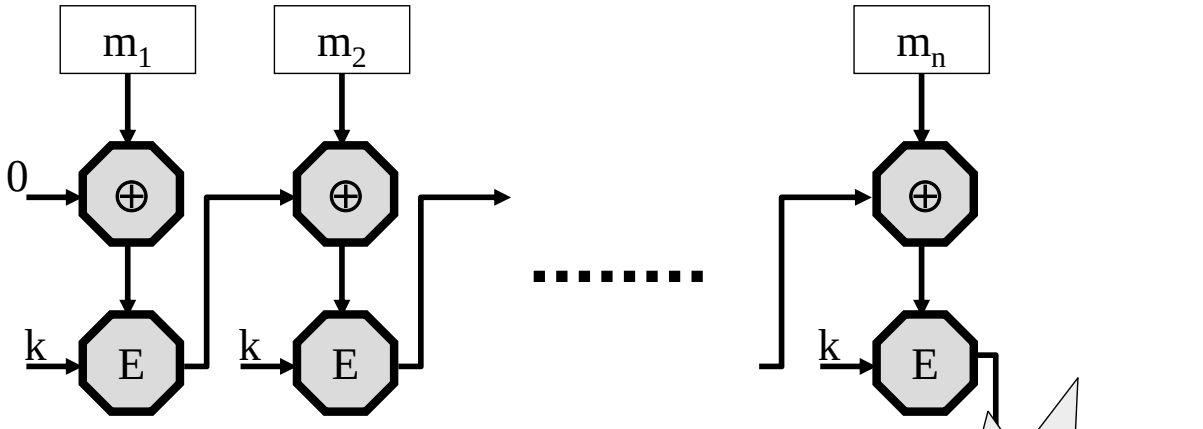
Standard Internet per dare sicurezza al livello **IP**

AB≤64 **byte**, *completato con* 00_H
fino a 512 bit
1. k1 = AB⊕a, a=36_H *per 64 volte*
   k2 = AB⊕b, b=$5C_H$ *per 64 volte*
2. h1 = H(k1||m)
3. **h1’: h1** *completato con* 00_H
4. h = H(k2||h1’) = HMAC(AB, m)

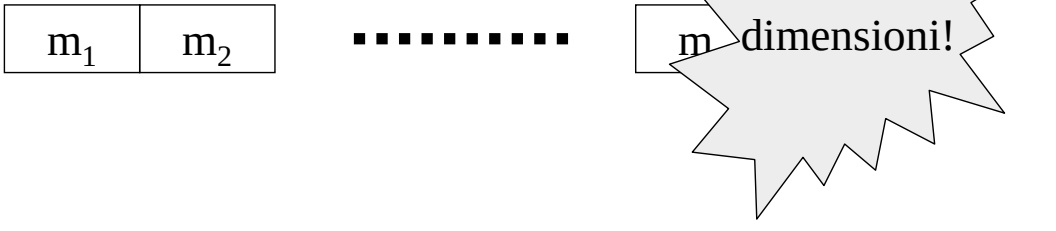


H con compressione iterata

MAC (Message Authentication Code)

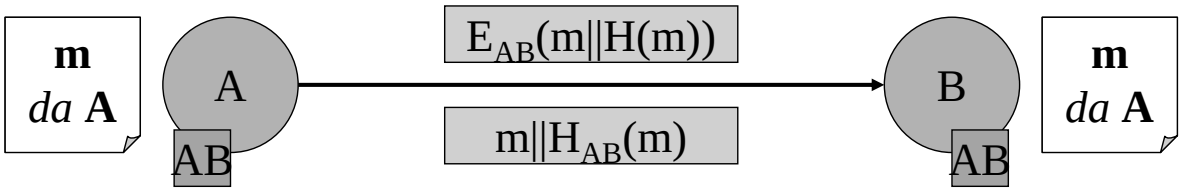


Trasmissione:



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,

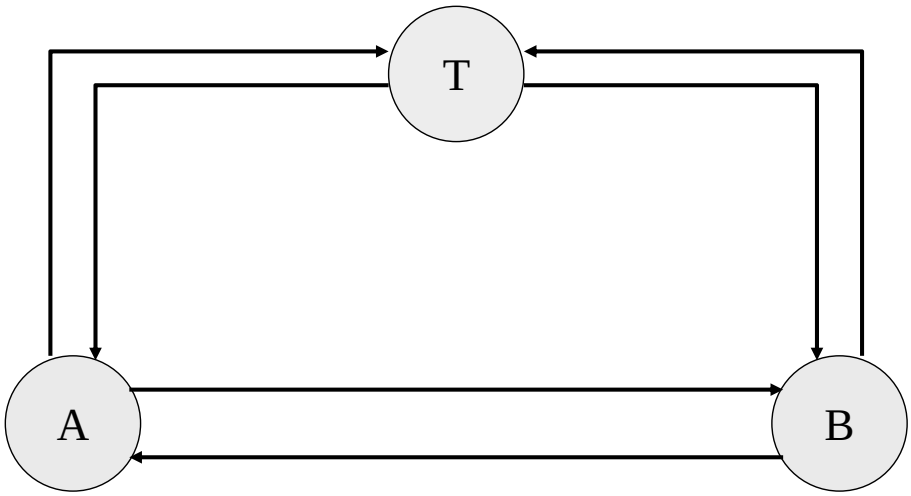
2- non poter essere **imitata** da un impostore,

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

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

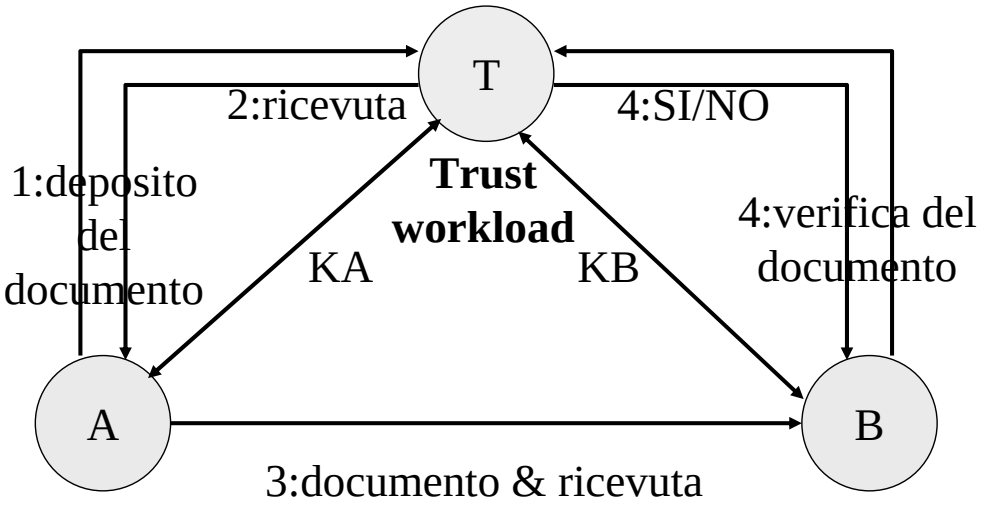
5- rendere **inalterabile** il documento in cui è stata apposta.

Il principio della terza parte fidata

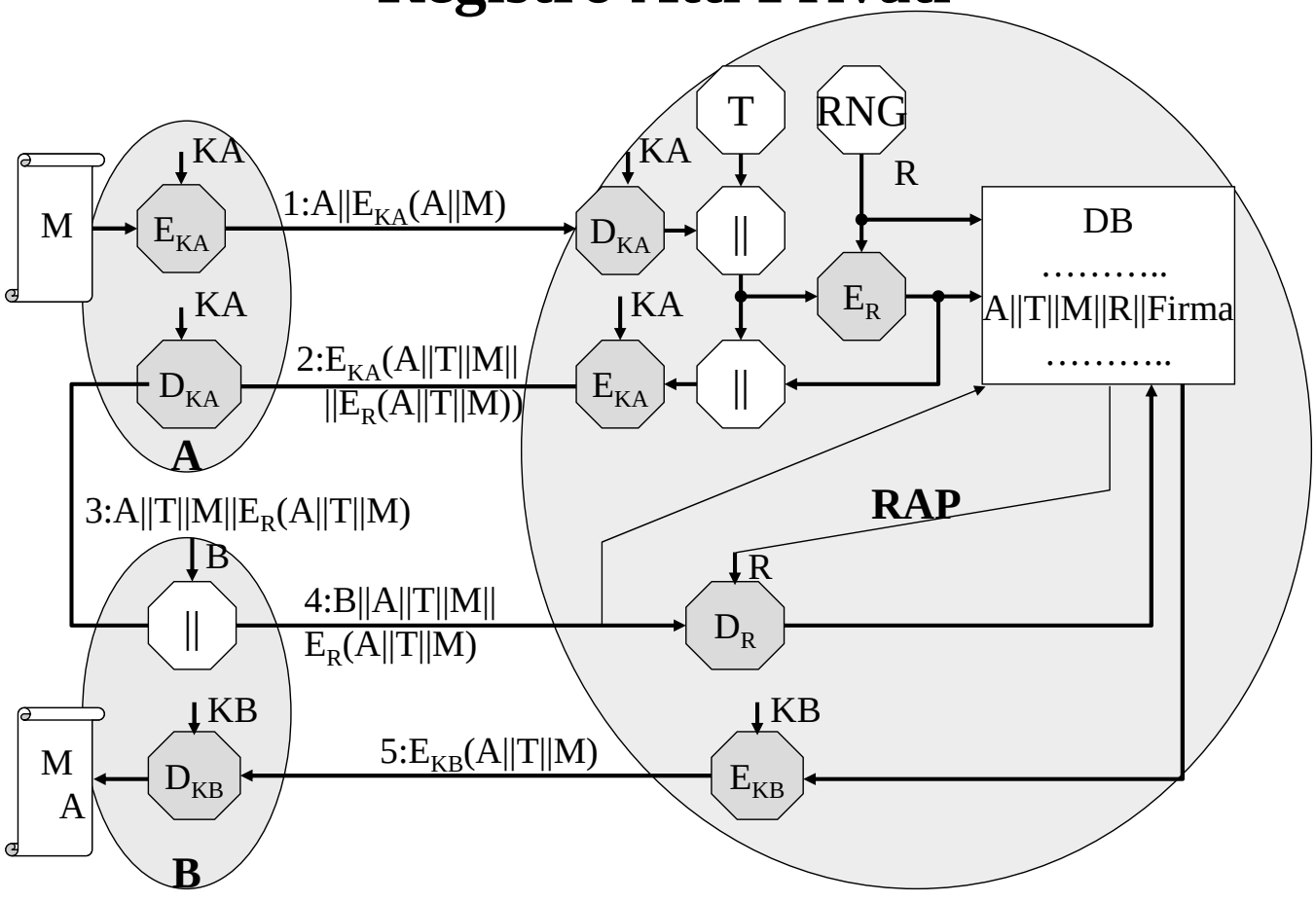


Protocolli resi sicuri dalla partecipazione di una terza parte:
il "notaio" interviene durante lo svolgimento per impedire scorrettezze
il "giudice" interviene al termine per dirimere dispute

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**.

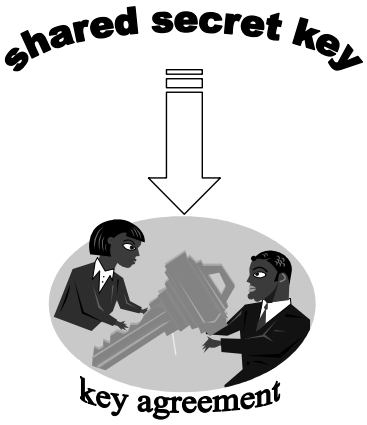
Accordo sulla chiave segreta

“uno a uno”

Incontro
Corriere

“molti a molti”

Internet



“modifica frequente”

Session key
One-time key

chiave che cifra chiavi

CON PRECEDENTE KA

Chiave in uso

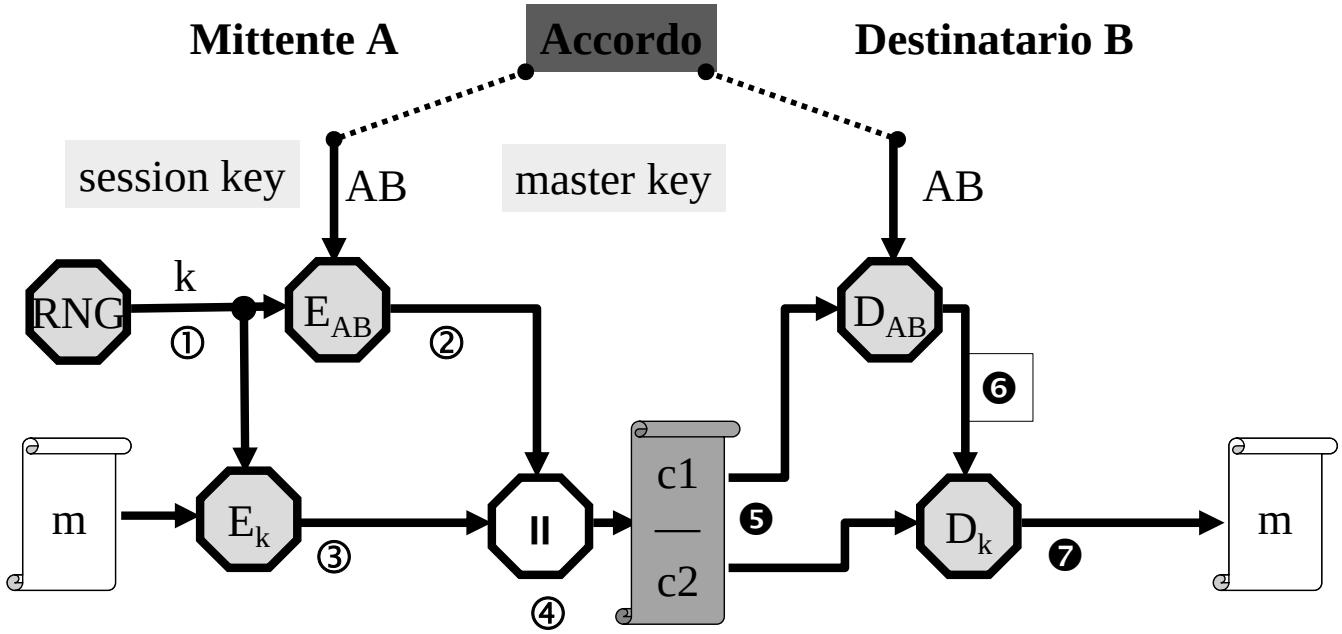
- ***Master key***
- ***KDC***

SENZA PRECEDENTE KA

- ***Scambio di Diffie-Hellman***
- ***Cifrario asimmetrico***

Master key

La master key

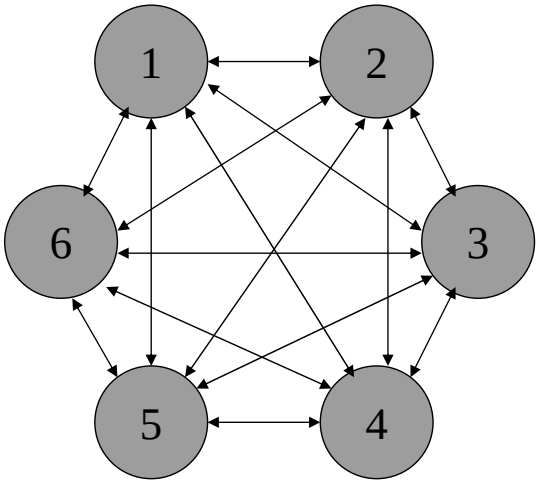


La chiave AB cifra solo le chiavi k e può avere una vita “lunga”
La chiave k cifra messaggi anche “lunghi” ed è usata una volta sola

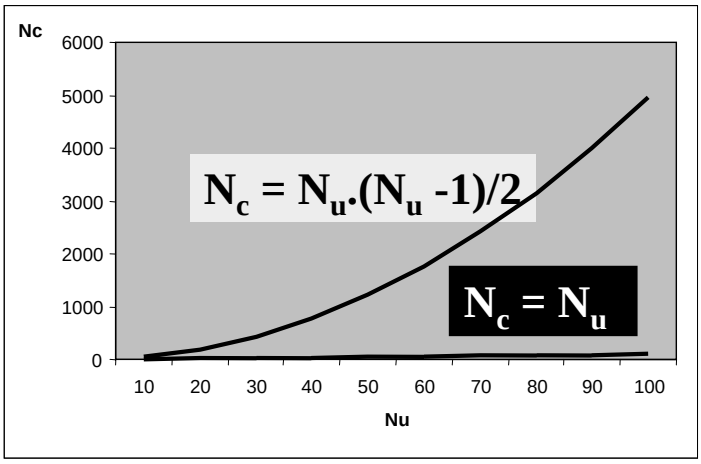
Key Distribution Center

Numero di chiavi in circolazione

Comunità di utenti



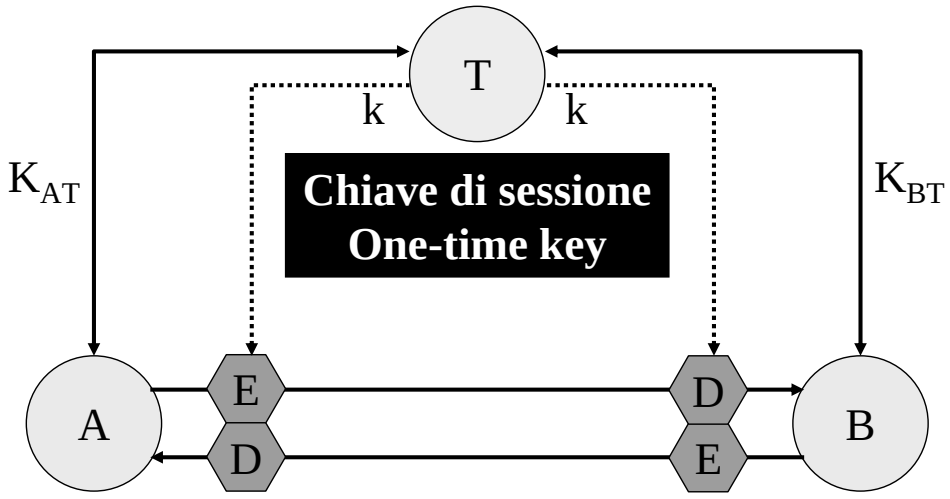
Non è scalabile!



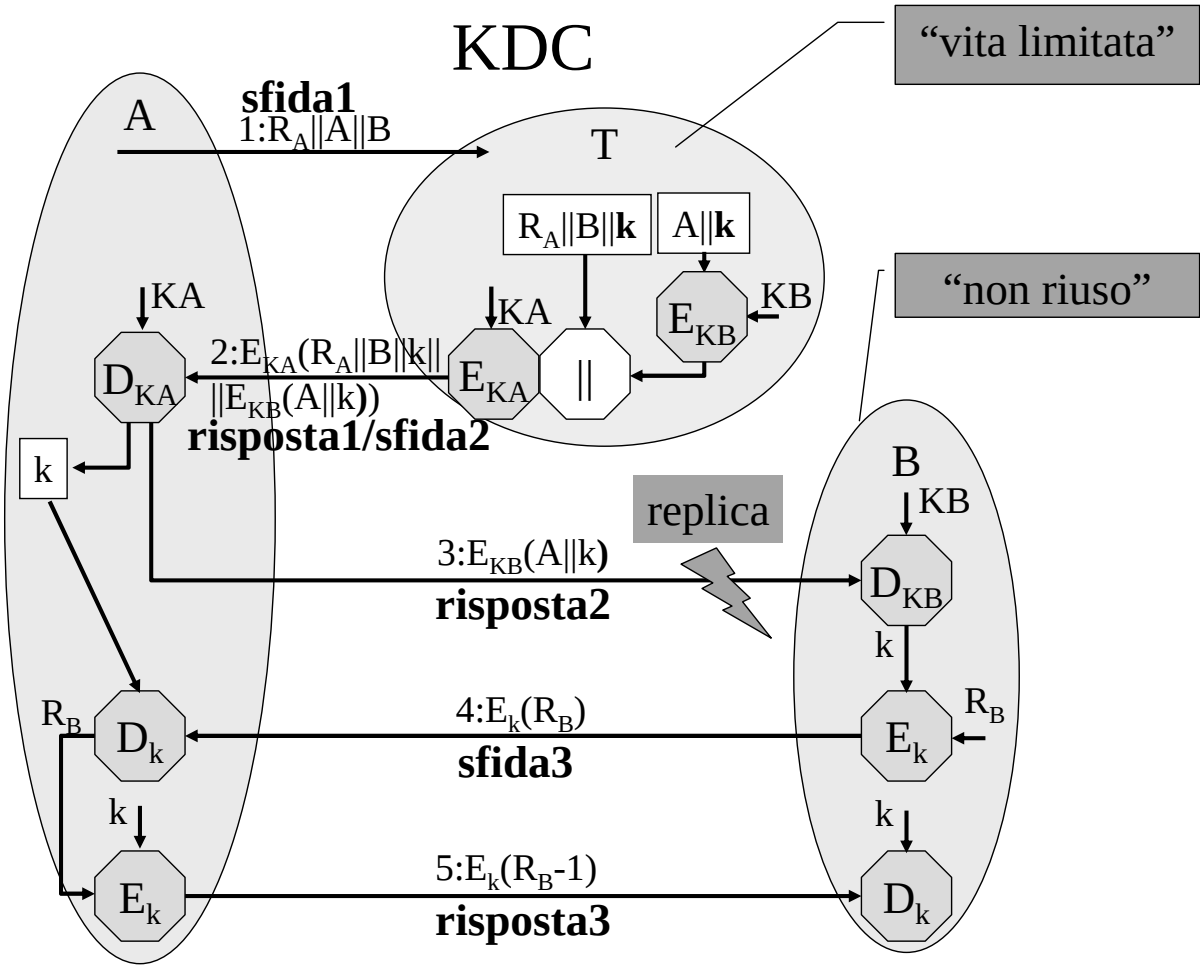
Obiettivo da perseguire: "una chiave per utente"

Soluzione: ogni utente concorda la sua chiave con una terza parte

L'Autorità per la distribuzione chiavi



$N_c = N_u$



Problemi di KDC

- On-line
- Collo di bottiglia (n° max di utenti)
- Memoria sicura
- Ente degno di fiducia

KryptoKnight,
Kerberos,
Distributed Computing Environment,
Windows 2000