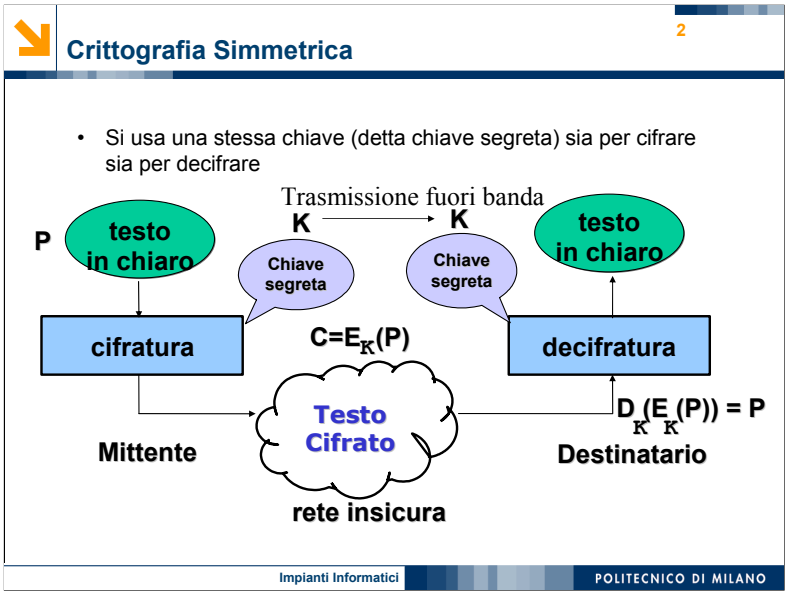
Paolo Cremonesi

Impianti Informatici

POLITECNICO DI MILANO

Sicurezza:
La crittografia simmetrica



La diffusione del Web ha portato alla nascita di una nuova categoria di applicazioni, denominata appunto Web Application.

1. Una Web application è una qualsiasi applicazione basata sul paradigma client/server, e che utilizzi
2. il protocollo applicativo HTTP per la comunicazione tra client e server. Questo significa che i due componenti si scambiano dati effettuando
3. richieste HTTP, quindi usando metodi come GET o POST, e ricevendo
4. delle risposte HTTP. Il client di una Web Application
5. è quindi generalmente un browser, dato che utilizza nativamente il protocollo HTTP per la comunicazione. In ogni caso è possibile che venga implementato un qualsiasi altro client, che si appoggi però allo stesso standard.
6. Uno dei classici impieghi di una web application è l'accesso ad una base di dati, operando così da interfaccia per l'utente.

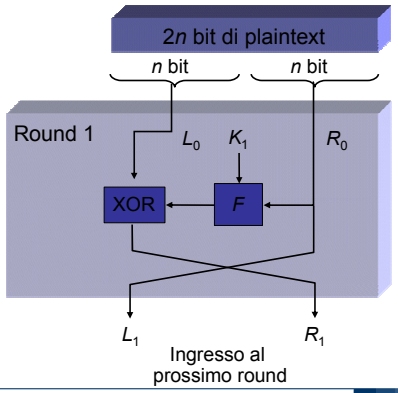
Cifrari simmetrici a blocco

- Processano il plaintext a blocchi di dimensione fissa
  - Può essere necessario aggiungere padding
- Cifrano ogni blocco separatamente (ECB) o congiuntamente al blocco precedente (CBC)
  - CBC è più sicuro, blocchi uguali diventano diversi
- Esempi: DES, RC2, Blowfish, AES

Cifrari simmetrici a flusso

- Processano il plaintext bit per bit
- Usano la chiave per generare un flusso pseudocasuale di dati che viene XORato con il plaintext
  - XOR (indicato con $\oplus$): $0 \oplus 0=1 \oplus 1=0$; $1 \oplus 0=0 \oplus 1=1$
  - Somma modulo 2
  - Lo XOR è invertibile: $(x \oplus y) \oplus y=x$
- Esempi: RC4, SNOW 2.0

Cifrari a blocco “di Feistel”



F: round function

Cambiando la round function si possono costruire infiniti algoritmi diversi

K_1: round subkey, derivata da *K* mediante una *funzione di scheduling*

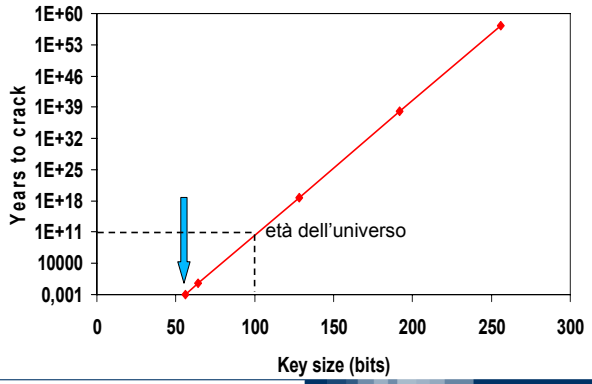
Decifratura: stesso schema applicato in ordine inverso

L'algoritmo DES

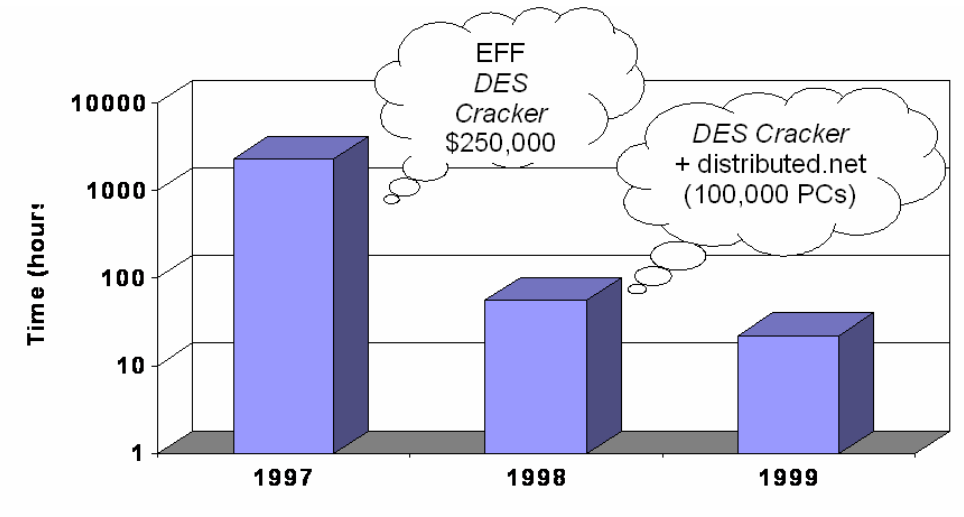
- Nato nel 1970, progetto IBM
- 1977: standard del governo americano
- Algoritmo simmetrico a blocco (blocchi di 64 bit, chiavi di 56 bit)
  - Originariamente: chiavi da 64 bit, ma poi NSA...
- 16 iterazioni (round) di Feistel su ogni blocco, con F costituita da delle S-box (tabelle di sostituzione)
  - S-Box ritoccate da NSA...
- Si può implementare sia in software che in hardware in modo efficiente
- Problemi
  - Vulnerabile alla crittanalisi differenziale
  - Chiave troppo corta

Tempi di bruteforcing

(si ipotizzano 10^6 decriptazioni per µs)



Cracking DES

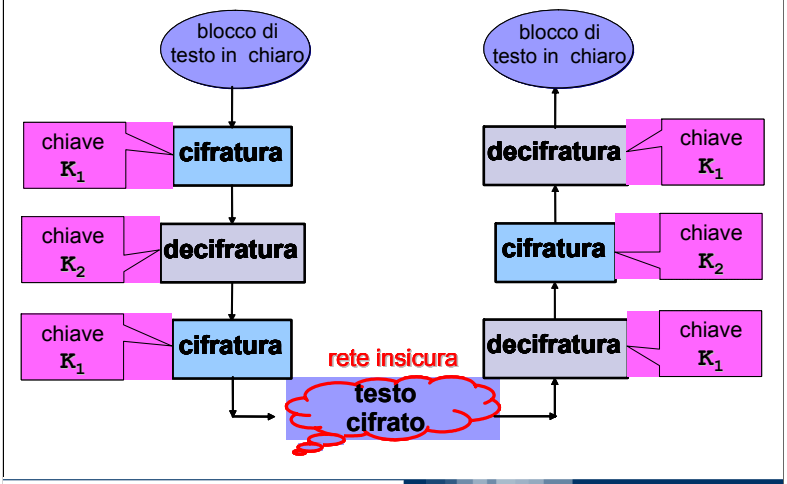


1997: 96 days

1998: < 3 days (56 hours)

1999: 22 hr 15 min – 245 billion keys tried per sec!

TripleDES (3DES)



AES (Advanced Encryption Standard)

- 1997: NIST, gara per sostituire il DES con un nuovo algoritmo
- viene scelto Rijndael (di J.Daemen e V.Rijmen)
- È un cifrario “non-Feistel”
- Input/output: blocchi da 128, 192 o 256 bit
- Chiavi: 128, 192 o 256 bit (non necessariamente come il blocco)
  - 256 bit è molto più che sufficiente !
- Benefici secondari: efficiente in hardware e in software, libero da brevetti, distribuibile liberamente in tutto il mondo