Introduzione alla crittografia e schemi di cifratura simmetrici

Rocco DE NICOLA
IMT Lucca
Rocco.DeNicola@imtlucca.it

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

Indice

- Introduzione
- Schemi a chiave simmetrica
- Tipologie di attacchi
- Tecniche di Cifratura
  - Sostituzione e Trasposizione
  - Cifrari Classici
  - Data Encryption Standard (DES)
  - Dopo DES

Introduzione

- La crittografia è la pratica e lo studio di tecniche per la comunicazione sicura (segreta) in presenza di terzi chiamati avversari.
- Più in generale, la crittografia riguarda la costruzione e l'analisi di protocolli che impediscono a terzi di leggere o alterare messaggi non destinati a loro.
- Riservatezza, integrità dei dati, autenticazione, non ripudio, sono proprietà alla garanzia delle quali può la crittografia.

La crittografia è onnipresente

- Transazioni sicure su Internet
- WiFi criptato
- Cifratura del contenuto delle memorie secondarie
- Firma digitale
- Aggiornamenti software
- Hashing delle password
- Monete Elettroniche
- …

Crittografia, Crittoanalisi, ecc…

Alcuni termini chiave:

- **Algoritmo di cifratura**: trasforma un testo in chiaro (**plaintext**, comprensibile a un umano o a una macchina) in un testo cifrato (**ciphertext**, incomprensibile).
- **Algoritmo di decifratura**: prende il *ciphertext* e ritorna il *plaintext*.
- A ogni algoritmo di cifratura deve corrisponderne uno «inverso» di decifratura.
- Un coppia di algoritmo di cifratura/decifratura viene anche chiamata **schema crittografico**.

Chiavi crittografiche

- L'algoritmo di cifratura di solito prende in ingresso una o più *chiavi crittografiche*.
- Una chiave crittografica:
  - è un'informazione (un parametro) che determina l'output funzionale di un algoritmo di cifratura/decifratura.
  - specifica la trasformazione del testo in chiaro in testo cifrato e del testo cifrato in testo in chiaro.
  - La sicurezza di uno schema dipende strettamente dalla segretezza di almeno una delle chiavi usate.

Chiavi Crittografiche

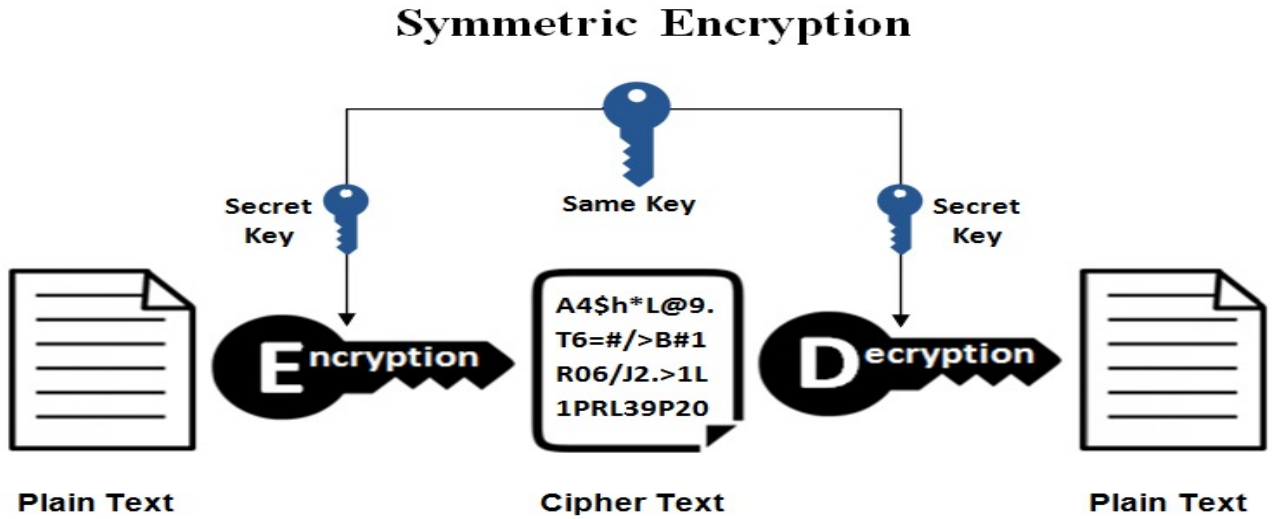
- Due principali metodi:
  - *A chiave simmetrica* – Unica chiave
  - *A doppia chiave* – Due chiavi: una pubblica e una privata

Crittografia a chiave simmetrica

- Chiamata anche *crittografia convenzionale* o *crittografia a chiave singola.*
- Tecnica universale per garantire la riservatezza dei dati trasmessi o memorizzati
- L'unico tipo di cifratura in uso prima della introduzione della cifratura a chiave pubblica (fine anni '70)
- Rimane il più diffuso tra i due tipi di crittografia

Crittografia a chiave simmetrica

Si riferisce a metodi in cui sia il mittente sia il destinatario condividono la stessa chiave.



Sistemi crittografici simmetrici

Gli schemi crittografici si differenziano per:

- **Il tipo di operazione** per trasformate il plaintext (P) nel ciphertext (C):
  - **Sostituzioni:** ogni elemento di P viene sostituito con un elemento di C
  - **Trasposizioni:** vengono effettuati spostamenti tra elementi di P.
- **Il modo di «elaborare» P:**
  - Cifrari a **blocchi:** P è diviso in blocchi ed elaborato dall'algoritmo di cifratura «un blocco alla volta»
  - Cifrari a **flusso**: P è elaborato considerando un elemento per volta.

Critto analisi

Uno schema di cifratura simmetrica è sicuro se:

- L'algoritmo di cifratura è **robusto** e cioè un attaccante in possesso di un certo numero di ciphertext ma non della chiave non è in grado di inferire i plaintext o la chiave.
- Il mittente e il ricevente **ricevono e mantengono la chiave in maniera sicura** (nessun attaccante deve intercettare chiave).

Si assume che l'algoritmo sia noto e che sia impraticabile decifrare dei messaggi avendo solo ciphertext.

Crittoanalisi

La crittoanalisi è un insieme di tecniche per testare la robustezza dell'algoritmo e della chiave provando a capire la chiave a partire dai ciphertext disponibili.

Tecniche di crittoanalisi possono essere applicate a partire da «ipotesi» diverse sulle informazioni possedute dall'attaccante:

- non conoscere niente, nemmeno l'algoritmo
- Conoscere alcuni ciphertext e l'algoritmo
- Conoscere anche alcuni plaintext.

Tipi di Attacco

- Attacchi Criptonalitici
- Attacchi di forza bruta

Attacchi Criptonalitici

- L’attaccante:
  - Sfrutta la conoscenza dell'algoritmo, quella delle caratteristiche generali del testo in chiaro ed eventualmente alcune coppie campione

    <testo_in_chiaro – testo_cifrato>.
  - Prova a dedurre la chiave utilizzata, in modo da compromettere tutti i messaggi futuri e passati criptati con quella chiave.

Attacchi di forza bruta

- L'attaccante:
  - Prova tutte le chiavi possibili su qualche testo cifrato fino a ottenere una traduzione comprensibile in chiaro.
  - In media, deve provare la metà di tutte le chiavi possibili prima di avere successo
  - Deve possedere:
    - Un certo grado di conoscenza del testo in chiaro atteso
    - Strumenti per distinguere il testo in chiaro da quello cifrato.

Crittoanalisi e attacchi a forza bruta

μs = milionesimo di secondo

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

Tecniche di cifratura

- Meccanismi di base da applicare ai plaintext per ottenere i ciphertext:
  - la sostituzione
  - la trasposizione.
- La composizione di queste due tecniche è alla base di tutti gli algoritmi di cifratura/decifratura a chiave simmetrica.

Tecniche di Sostituzione

- Una tecnica di sostituzione si basa sulla sostituzione di ogni elemento del plaintext con un altro elemento dello stesso alfabeto.
- Le sostituzioni devono essere reversibili, ovvero si deve poter tornare indietro.
- Dato un elemento nel plaintext, la scelta di quale elemento usare per sostituirlo nel corrispondente ciphertext dipende dalla chiave.

Il Cifrario di Cesare

Un cifrario a sostituzione è quello di Giulio Cesare che prevede di sostituire ogni lettera con la corrispondente lettera dell'alfabeto che sta «*tre spazi*» più in là (quando l'alfabeto finisce ricomincia da capo).

PLAINTEXT	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
CIPHERTEXT	D	E	F	G	H	I	J	K	L	M	N	O	P
PLAINTEXT	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
CIPHERTEXT	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

`Attack` diventa `dwwdfn`

Cifrario di Cesare

- Un altro esempio:

```
Plaintext:  meet me after the toga party
Ciphertext: PHHW PH DIWHU WKH WRJD SDUWB
```

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Con l'associazione lettere-numeri a destra, la codifica numerica del ciphertext C corrispondente al numero p è data da:

$$C = E(3,P) = (P+3) \bmod 26.$$

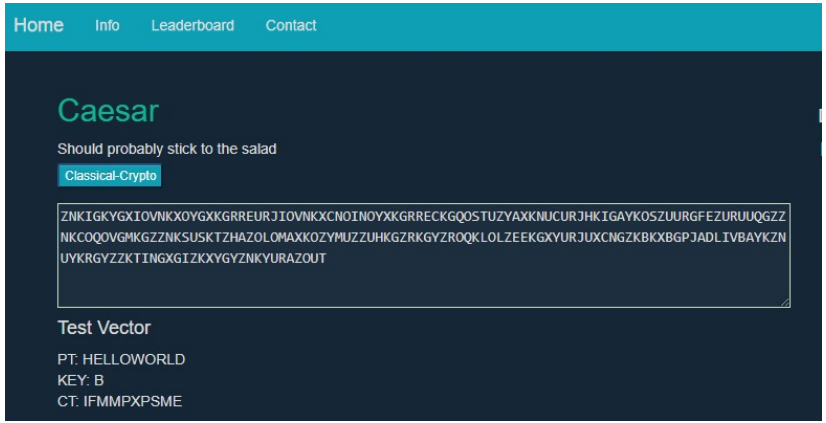
Limiti del Cifrario di Cesare

Cifrario di Cesare

Dal punto di vista della crittoanalisi, il cifrario di Cesare è debole per tre motivi:

1. L'algoritmo di cifratura è noto (ma quasi sempre è così)
2. Ci sono solo 25 chiavi possibili da provare
3. Il linguaggio in chiaro è facilmente riconoscibile (è molto semplice accorgersi quando la chiave è giusta).

Cifrario di Cesare – Esempio di attacco



https://id0-rsa.pub/problem/32/

https://www.dcode.fr/caesar-cipher

Cifrario Monoalfabetico

- Un cifrario può essere rinforzato permettendo *sostituzioni arbitrarie ad esempio* introducendo la possibilità di permutare arbitrariamente le lettere.
- Per un insieme di n elementi, abbiamo n! possibile permutazioni. Se S= {a,b,c} ci sono 6 (3!) permutazioni di S: *abc, acb, bac, bca, cab, cba*.
- Nel cifrario di Cesare, (S = 26 - caratteri alfabeto) si usa sempre una specifica permutazione: quella che sposta di 3 ogni carattere.
- Quando un messaggio viene cifrato cambiando il plaintext utilizzando una delle 26! possibili permutazioni, diventa (molto) più difficile portare attacchi di forza bruta.

Cifrario monoalfabetico - Permutazioni

Consideriamo la seguente permutazione delle 26 lettere (che poi è la chiave!):

- `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
- `DXUTNAVWKZFQGSIOYJBPLHCERM`

Con questa permutazione il plaintext «arrivano rinforzi» diventa:

- `ARRIVANORINFORZI`
- `DJJKHDSIJKSAIJMK`

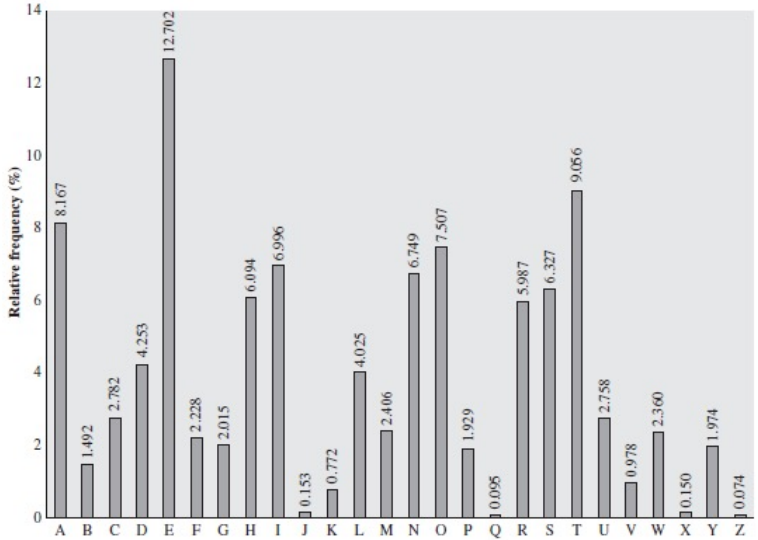
Un attacco a forza bruta richiederebbe di provare, nel caso peggiore, **26!** chiavi, invece che 25 chiavi come nel caso del cifrario di Cesare.

Cifrario monoalfabetico - Permutazioni

Le permutazioni rendono difficili attacchi a forza bruta, ma per gli attacchi si possono sfruttare *regolarità del linguaggio quali*:

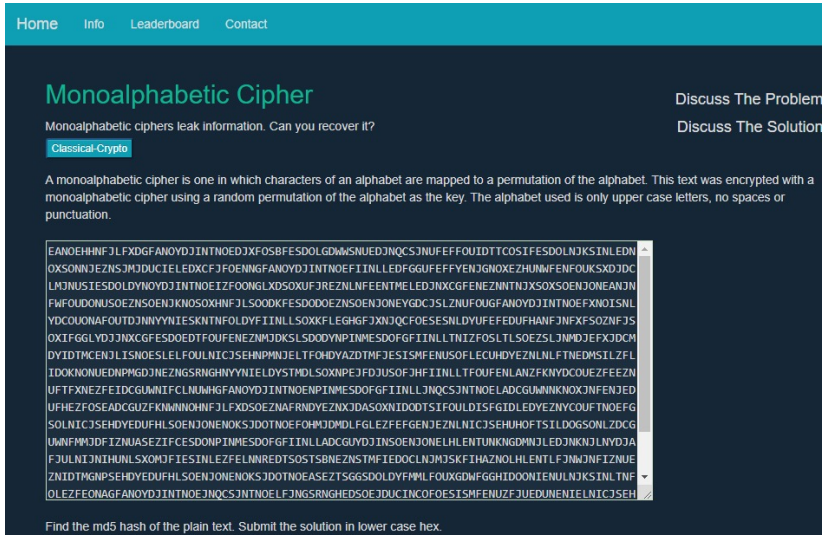
- frequenza di singole lettere cifrate
- coppie di lettere vicine per parole comuni come «of» in inglese

e confrontarle con la frequenza delle lettere o delle coppie nella lingua di riferimento.



Frequenza delle lettere nella lingua inglese

Cifrario monoalfabetico - Esempio di attacco



https://id0-rsa.pub/problem/12/

https://www.guballa.de/substitution-solver

Cifrari polialfabetici

- Cifrari Polialfabetici sono un'alternativa a quelli mono-alfabetici, e si basano su alfabeti di sostituzione multipli.
- Usati per complicare la crittoanalisi basata sulla frequenza delle lettere:
  - Se P è la lettera più frequente in un testo cifrato di un testo in chiaro inglese, si potrebbe ipotizzare che P corrisponda a E,
  - Questo non è possibile quando E viene sostituita con lettere diverse in punti diversi del messaggio.
- Il Cifrario di Vigenère è l'esempio più noto di cifrario polialfabetico.

Il cifrario di Vigenère

- La chiave è ora una stringa, non solo un carattere, e ad ogni carattere viene assegnato un numero in base alla posizione nell'alfabeto (a:0, b:1, c:2, d:3, e:4, f:5, ..., z:25)
- Per cifrare, si sposta ogni carattere in chiaro della quantità dettata dal carattere corrispondente della chiave (si cicla se necessario)
- Per decifrare si inverte il procedimento
- Ha ispirato "macchine a rotore" come Enigma usate nella seconda guerra mondiale

Con la chiave
café abbiamo

```
tellhimaboutme
cafecafecafeca
veqpjiredozxoe
```

Tecniche di Trasposizione

Con la **trasposizione** il ciphertext è ottenuto *modificando l'ordine delle lettere*.

- Se il plaintext è scritto in sequenze di diagonali e poi trasmesso per righe, il messaggio «meet me after the toga party» diventa:

```
m e m a t r h t g p r  y
 e t e f e t e o a a t
```

  Che letto riga per riga è MEMATRHTGPRYETEFETEOAAT

- Un'alternativa è scrivere in un quadrato il messaggio riga per riga, e trasmetterlo colonna per colonna fissando l'ordine di lettura tra le colonne

```
Key:        4 3 1 2 5 6 7
Plaintext:  a t t a c k p
            o s t p o n e
            d u n t i l t
            w o a m x y z
```

Trasmettendo le colonne nell'ordine imposto dalla chiave abbiamo

TTNAAPTMTSUOAODWCOIXKNLYPETZ

Cifrari a blocco e a flusso

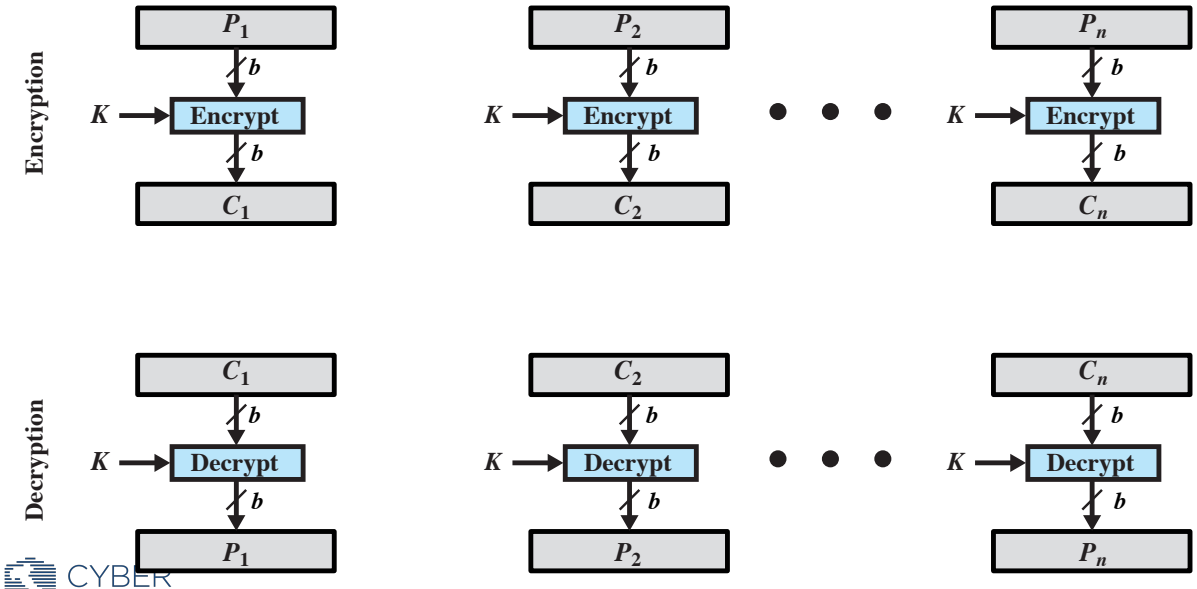
- I Block cipher elaborano i messaggi in blocchi, che vengono cifrati o decifrati separatamente
  - Una tecnica di sostituzione polialfabetica con un set di caratteri molto grande (64 bit o più) abbinata a tecniche di permutazione.
- Gli Stream ciphers elaborano i messaggi un bit o un byte alla volta durante la cifratura o la decifratura
  - Un flusso di bit generato a partire da una chiave è combinato con il flusso del testo in chiaro.
- Molti cifrari attuali sono basati su tecniche di cifratura a blocchi
  - Analizzati meglio e con una più ampia gamma di applicazioni

Cifrari a flusso

- I cifrari a flusso cifrano un flusso di dati digitali un bit o un byte alla volta
- Le cifre in chiaro sono combinate (XOR-ed) con un flusso di cifre pseudorandom (keystream) per ottenere un bit o un byte di testo cifrato
- Il generatore di flusso di bit è una procedura algoritmica utilizzata da entrambi i partner per cifrare e decifrare.
- I due partner, per produrre il keystream, devono solo condividere la chiave per la generazione pseudocasuale.

Cifrari a blocchi

- Un dato plaintext di lunghezza n*b viene diviso in n blocchi di b-bit ciascuno



- Ogni blocco è criptato utilizzando lo stesso algoritmo e la stessa chiave di cifratura
- Viene prodotta una sequenza di n blocchi di b-bit di testo cifrato

Cifrari a blocchi

- Un cifrario a blocchi opera su un blocco di n bit in chiaro per produrre un blocco cifrato di n bit.
- Un blocco di testo in chiaro viene usato nel suo insieme per produrre un blocco di testo cifrato di uguale lunghezza
- Si utilizzano blocchi di dimensioni tipiche di 64 o 128 bit (n = 64 o 128)
- Gli utenti condividono una chiave di crittografia simmetrica
- Ci sono 2^n possibili diversi blocchi di testo in chiaro e, affinché la crittografia sia reversibile, ognuno deve produrre un unico blocco di testo cifrato.

Il cifrario di Feistel

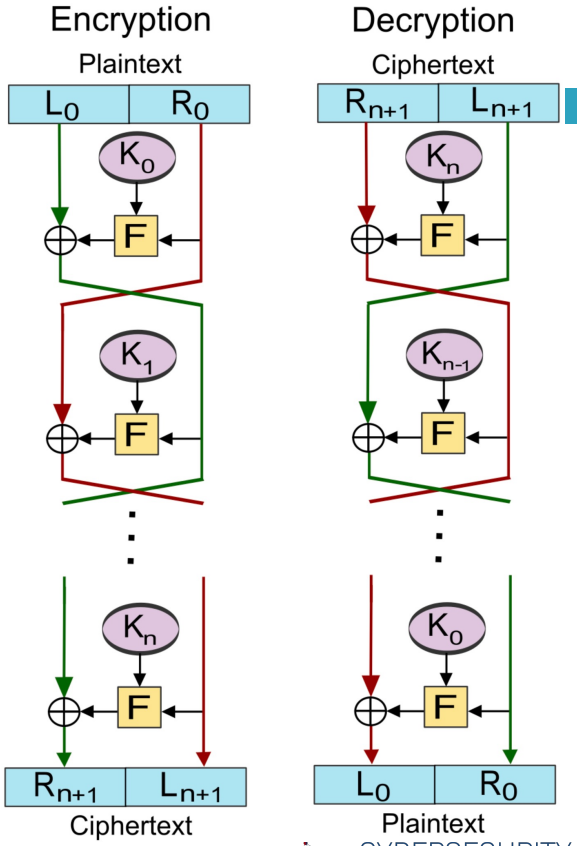
- Usato come base da molti cifrari a blocchi, tra cui il noto Data Encryption Standard (DES).
- Le operazioni di cifratura e decifratura sono simili, in alcuni casi identiche, solo le chiavi vengono utilizzate in ordine inverso.
- Si basa sulla combinazione di semplici trasformazioni come la sostituzione (S-box), la permutazione (P-box) e l'aritmetica modulare.
- Implementa il concetto di "confusion and diffusion" di Shannon attraverso sostituzioni e permutazioni, suddividendo i blocchi di input in due metà ed eseguendo diversi round.

Il cifrario di Feistel: principi

- Tecniche :
  - Sostituzione: Ogni elemento in chiaro è sostituito in modo univoco da un corrispondente elemento cifrato
  - Permutazione: Nessun elemento viene aggiunto, rimosso o sostituito nella sequenza, ma viene cambiato l'ordine in cui gli elementi appaiono.
- Principi di Shannon :
  - Diffusione: dissipa la struttura statistica del testo in chiaro sulla maggior parte del testo cifrato
  - Confusione: ogni bit del testo cifrato dipende da diverse parti della chiave, oscurando le connessioni tra le due.

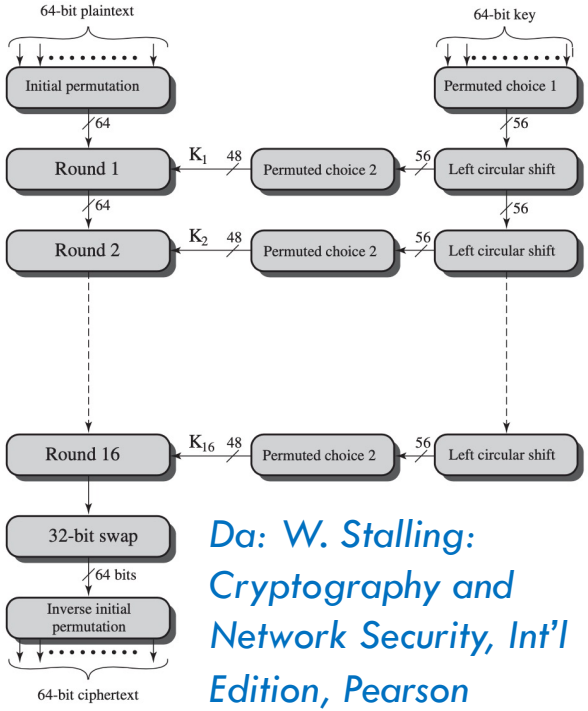
Il cifrario di Feistel

- Il testo cifrato viene calcolato a partire dal testo in chiaro mediante l'applicazione ripetuta della stessa trasformazione.
- Il testo da cifrare è diviso in due. La funzione circolare F viene applicata ad una metà usando una sottochiave e l'output di F è XOR-ed con l'altra metà.
- Le due metà vengono poi scambiate. Ogni round segue lo stesso schema ma nell'ultimo round non c'è scambio
- Cifratura e decifratura sono strutturalmente identiche, ma le sottochiavi sono usate in ordine inverso per cifratura e decifratura.



DES (Data Encryption Standard)

- Utilizza chiavi di 56 bit, divide il testo in chiaro in blocchi di 64 bit, effettua delle permutazioni iniziali e finali ed un ciclo di 16 iterazioni di permutazioni e xor (Feistel network, tecniche di confusione e diffusione).
- La chiave è in realtà 64 bit, ma ogni 8 bit ce n'è uno per controllo di parità; quindi, solo 56 dei 64 bit sono significativi.
- L'algoritmo originariamente aveva una chiave a 128 bit, ma le dimensioni della chiave sono state ridotte dalla NSA (per qualche ragione)

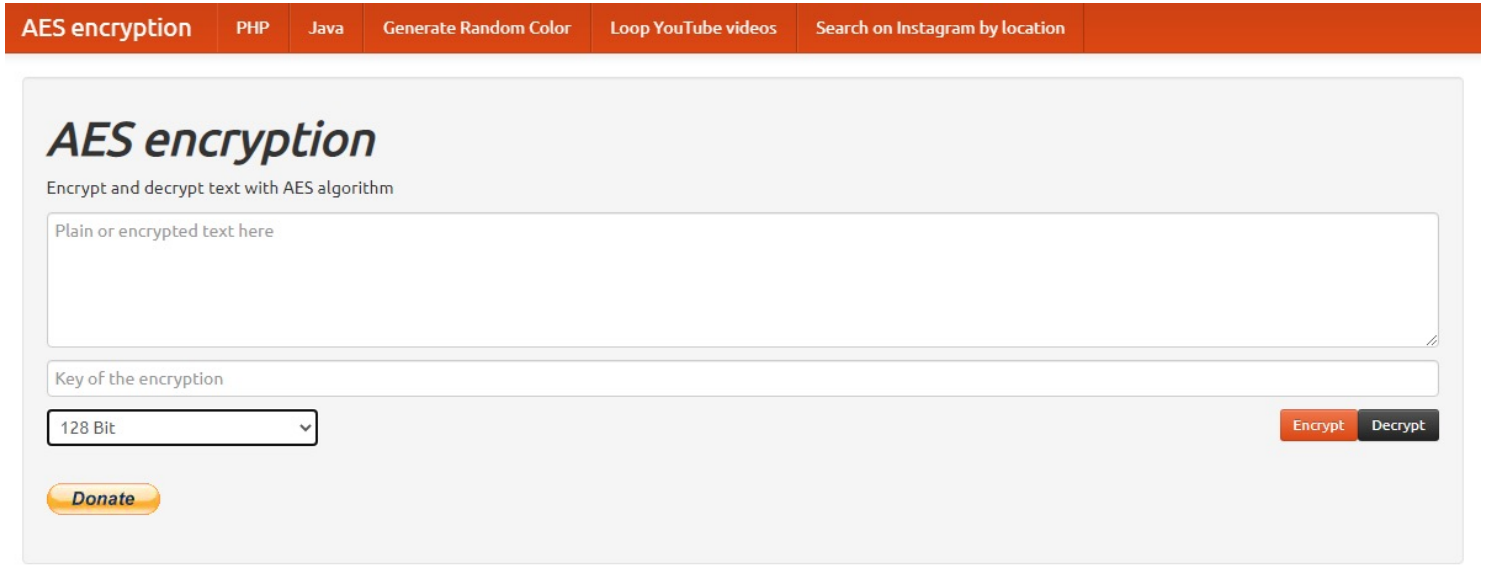


Da: W. Stalling: Cryptography and Network Security, Int'l Edition, Pearson

Debolezze di DES

- DEA l'algoritmo alla base di DES e delle sue varianti successive - Triple DES e Advanced ES - è l'algoritmo di crittografia più studiato
- Nonostante i numerosi tentativi, nessuno ha finora segnalato una debolezza fatale dell'algoritmo
- Però con una chiave di 56 bit, ci sono 2^{56} (circa $7{,}2 * 10^{16}$) possibili chiavi. Con la potenza di calcolo odierna ra sono possibili attacchi di forza bruta -
- La Electronic Frontier Foundation (EFF) ha annunciato nel luglio 1998 di aver rotto una crittografia DES.
- Se l'unica forma di attacco a un algoritmo di cifratura è la forza bruta, allora «utilizzate chiavi più lunghe!» **TRIPLE DES**

Esempio di cifratura usando AES



https://aesencryption.net/

Advanced Encryption Standard (AES)

Necessaria un'alternative a 3DES

- Non ragionevole per un uso duraturo

Nel 1997 NIST ha fatto un bando per estendere DES chiedendo

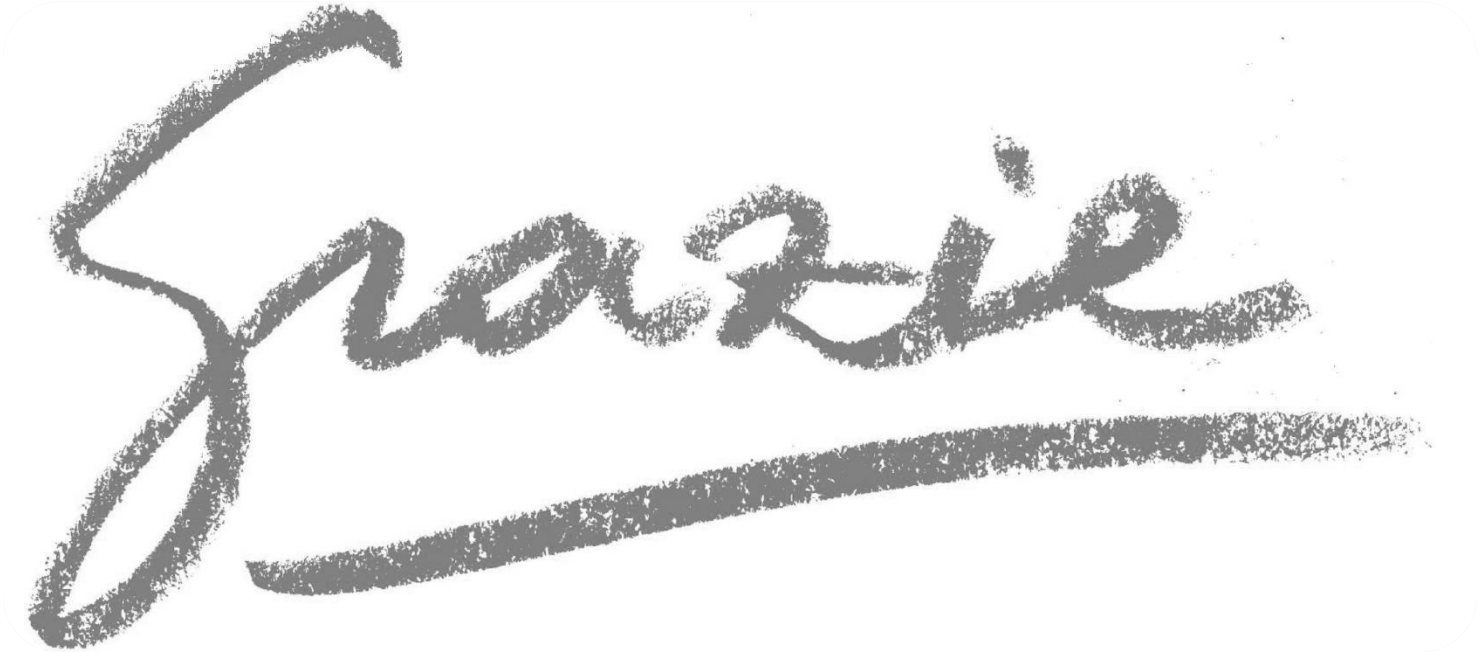
- Più robusto
- Molto più efficiente
- Symmetric block cipher
- Blocchi da 128 e chiavi da 128/192/256 bit

Nel Novembre 2001è stato scelto Rijndael

- Primo giro scelti 15 algoritmi
- Secondo giro ridotti a 5
- Publicato come FIPS 197

Tempi per gli attacchi

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/sec Personal Computer	Time Required at 10^{13} decryptions/sec Super Computer
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years



Introduzione alla crittografia e schemi di cifratura simmetrici

Rocco DE NICOLA
IMT Lucca
Rocco.DeNicola@imtlucca.it

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it