Network Security

Elements of Applied Cryptography

The Data Encryption Standard

(FIPS 46, January 15, 1977)

History

- On **May 15, 1973**, **National Bureau of Standards** published a solicitation for cryptosystems in the Federal Register
- **DES** was published in the Federal Register of **March 17, 1975**
  - DES was developed by **IBM** as a modification of **LUCIFER**
- DES was considered a standard for **"unclassified" applications** on **January 15, 1977** after much public discussion
- DES has been reviewed every 5 years
- The most recent review was January 1994
- It is not a standard since 1998.

Criteri alla base di un cifrario

- I principali **criteri** alla base di un cifrario sono (Shannon 1940):
- **Diffusione**
  - alterare la struttura del testo in chiaro "*spargendone*" i caratteri su tutto il testo cifrato
- **Confusione**
  - combinare in modo "*complesso*" il messaggio e la chiave per non permettere al crittoanalista di separare queste due sequenze mediante un'analisi del crittogramma

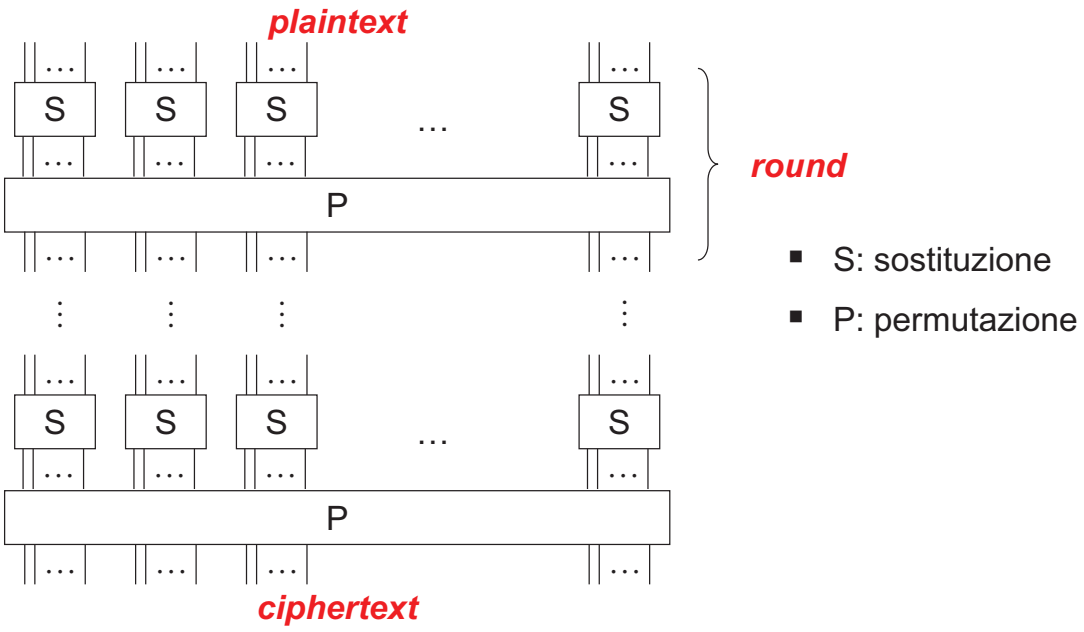
Diffusione

- **Obiettivo: diffusione**
  - Alterare la struttura del testo in chiaro "*spargendone*" i caratteri su tutto il testo cifrato
- **Meccanismi (intuizione)**
  1. **Permutazione** — *rimane immutata la frequenza delle singole lettere ma si perde l'informazione sulla frequenza dei **q**-grammi*
  2. **Combinazione** — *combinare i caratteri del testo in chiaro tra loro in modo che ciascun carattere del crittogramma venga a dipendere da molti di essi. Così facendo si perde l'informazione sulla frequenza delle singole lettere oltre che dei **q**-grammi*

Confusione

- **Obiettivo: confusione**
  - **Combinare** *in modo* ***"complesso"*** *il messaggio e la chiave per non permettere al crittoanalista di separare queste due sequenze mediante un'analisi del crittogramma*
- **Meccanismi**
  - Il crittogramma è una funzione *non-lineare* del messaggio e della chiave

SP-network

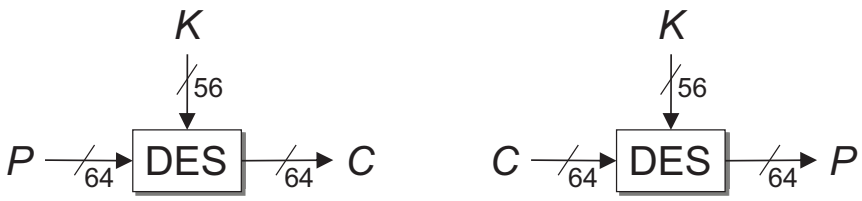


- S: sostituzione
- P: permutazione

Data Encryption Standard (DES)

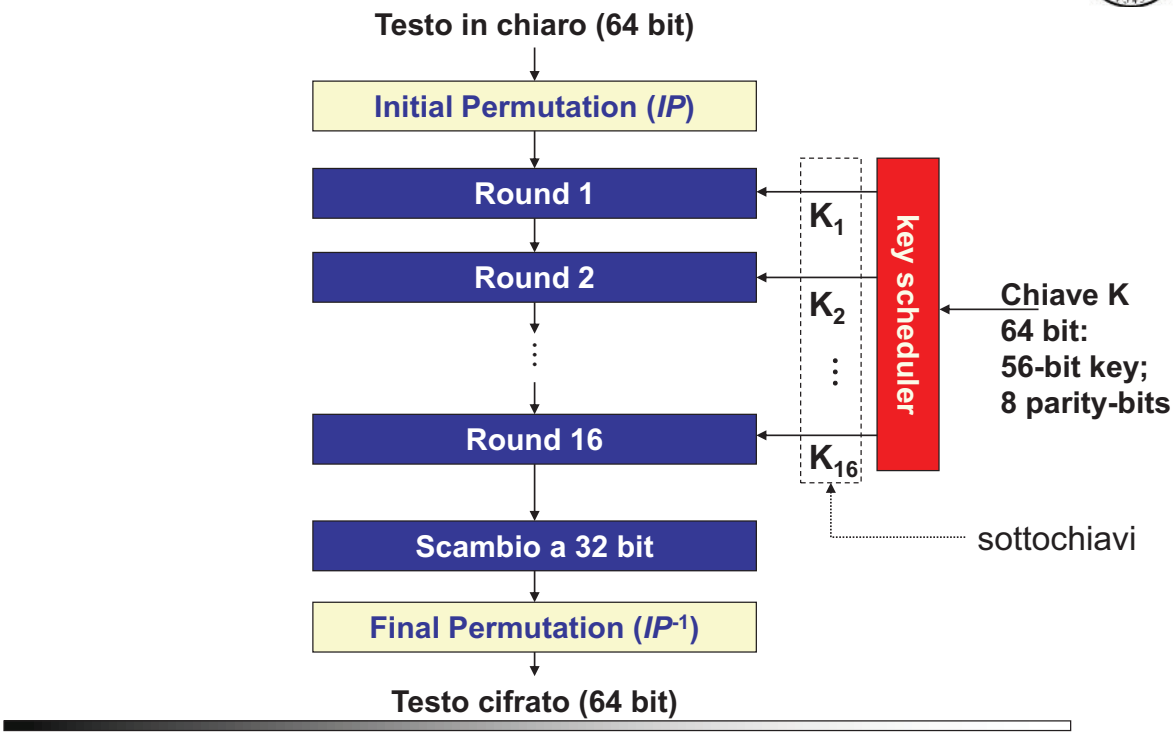
- Le elaborazioni interne di DES garantiscono che **ciascun bit del crittogramma dipenda da tutti i bit della chiave e da tutti i bit del messaggio**
  - **Diffusione**: permutazioni ed espansioni dei bit
  - **Confusione**: sostituzione e successiva compressione dei bit del messaggio e della chiave
- *Le idee alla base del DES sono rimaste immutate e sono quelle che si trovano in AES*

Data Encryption Standard (DES)

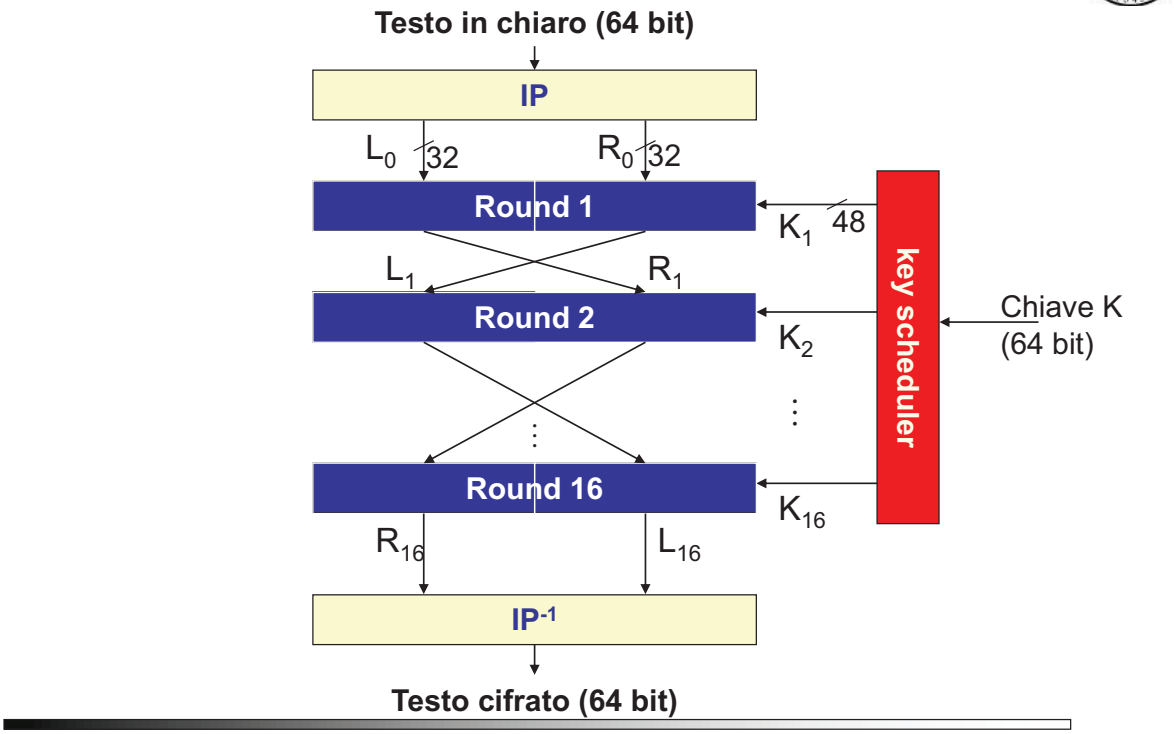


- The input key *K* is actually specified as a 64-bit key, 8 bits of which (bits 8; 16, …, 64) may be used as parity bits.
- The 2^{56} keys implement (at most) 2^{56} of the 2^{64}! possible bijections on 64-bit blocks.

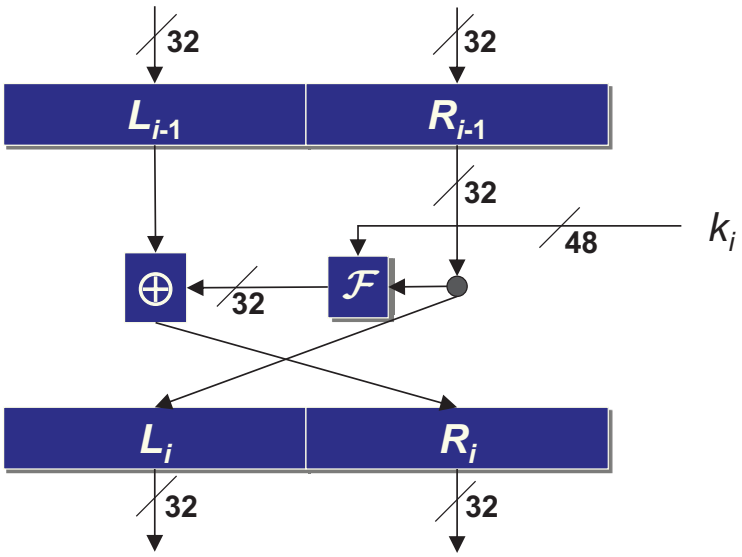
Data Encryption Standard (DES)



Data Encryption Standard (DES)



DES: round *i*-esimo



$L_i = R_{i-1}$;

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

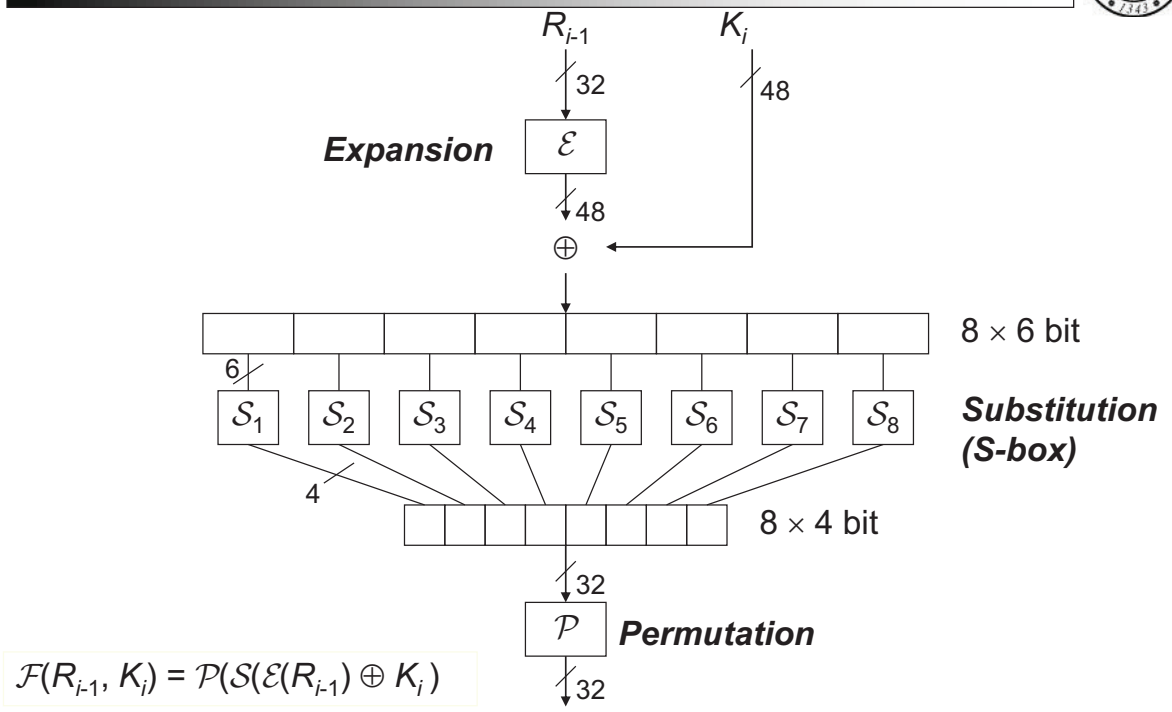
$\mathcal{F}$: ***round function*** **(non-linear)**

Decifratura in DES

- L'algoritmo di decifratura con chiave K è uguale all'algoritmo di cifratura con chiave K, dove le chiavi di round K_i applicate in ordine inverso
- **Dimostrazione (solo round 1)**
  - La permutazione IP^{-1} della cifratura è cancellata da IP della decifratura, si ottiene quindi $(L_0^d, R_0^d) \equiv (R_{16}, L_{16})$
  - Round 1 con chiave di round K_{16}
    - $L_1^d = L_{16;} R_1^d = R_{16} \oplus \mathcal{F}(L_{16}, K_{16})$

    essendo $L_{16} = R_{15}$ e $R_{16} = L_{15} \oplus \mathcal{F}(R_{15}, K_{16}) \Rightarrow$
    - $L_1^d = L_{16} = R_{15}$
    - $R_1^d = R_{16} \oplus \mathcal{F}(L_{16}, K_{16}) = L_{15} \oplus \mathcal{F}(R_{15}, K_{16}) \oplus \mathcal{F}(R_{15}, K_{16}) = L_{15}$
  - Il primo round della decifratura produce $(L_1^d, R_1^d) \equiv (R_{15}, L_{15})$, inverte cioè il round 16
  - L'inversione non dipende né da $\mathcal{F}$ né da K_i

Round function $\mathcal{F}$

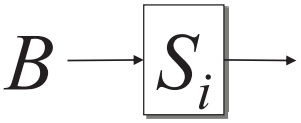


$\mathcal{F}(R_{i-1}, K_i) = \mathcal{P}(\mathcal{S}(\mathcal{E}(R_{i-1}) \oplus K_i))$

Commenti

- Permutazioni iniziale *IP* e finale IP^{-1}
  - Sono l'una l'inversa dell'altra
  - Non sono rilevanti ai fini della sicurezza
  - Alcune implementazioni SW le omettono
- Espansione $\mathcal{E}$
  - Effetto valanga
- Sostituzione $\mathcal{S}$
  - È una funzione **non-lineare** (rispetto a $\oplus$), che maggiormente contribuisce alla sicurezza di DES. È difficile da analizzare
  - È progettata per massimizzare la confusione.
- Permutazione $\mathcal{P}$
  - Aggiunge diffusione

S-box



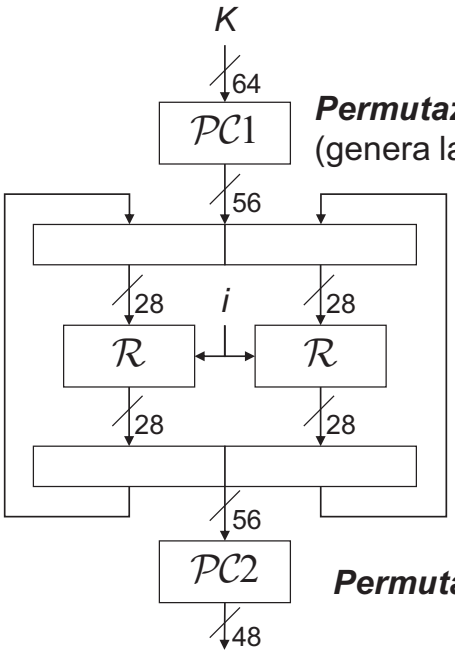
$B = b_1 b_2 b_3 b_4 b_5 b_6$
$row = b_1 b_6$ (outer bits)
column $= b_2 b_3 b_4 b_5$ (inner bits)

ESEMPIO
$S_1(011011) = 5$
$r = 1$
$c = 13$

row	column number															
	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]
S_1																
[0]	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
[1]	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
[2]	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
[3]	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2																
[0]	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
[1]	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
[2]	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
[3]	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																
[0]	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
[1]	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
[2]	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
[3]	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4																
[0]	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
[1]	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
[2]	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
[3]	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5																
[0]	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
[1]	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
[2]	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
[3]	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6																
[0]	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
[1]	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
[2]	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
[3]	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																
[0]	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
[1]	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
[2]	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
[3]	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																
[0]	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
[1]	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
[2]	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
[3]	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Key Scheduling

- $\mathcal{R}$ e $\mathcal{PC}2$ garantiscono che in ogni round venga estratto un diverso sottoinsieme di bit
- Si calcola che ogni bit della chiave originale partecipi in media a 14 round



Permutazione e compressione (genera la prima sottochiave)

Rotazione sinistra (1 *bit per round = 1, 2, 9, 16; 2 bit altrimenti*)

Permutazione e compressione

DES controversy

- The **S-boxes**, being the only **non-linear** components of the cryptosystem, are vital to security
- The design criteria of S-boxes are **not completely known**
- Some people have suggested that S-boxes contain **trapdoors** which would allow NSA to decrypt messages while maintaining that DES is secure
- It is impossible to disprove such an assertion but no evidence has come to light to indicate that trapdoor in fact exist

DES in practice

- **DES can be efficiently implemented either in hardware or in software**
  - arithmetic operations are exclusive-or
  - ***E***, ***S-boxes***, ***IP***, ***IP*$^{-1}$**, ***key scheduling*** can be done in **constant time** by **table-lookup** (sw) or by **hard-wiring** them into a circuit
- One very important DES application is in banking transactions
- DES is used to encrypt PINs and account transactions carried out at ATM
- DES is also used in government organizations and for inter-bank transactions

Proprietà di DES

Empiricamente, DES raggiunge i seguenti obiettivi:

- Ogni bit del crittogramma dipende da *tutti* i bit della chiave e da tutti bit del messaggio
- Non ci sono relazioni statistiche *evidenti* tra il messaggio ed il crittogramma
- L'alterazione di un bit nel messaggio altera ciascun bit del crittogramma con probabilità 0.5
  - L'alterazione di un bit nel crittogramma causa un cambiamento *imprevedibile* nel messaggio

Anomalie di DES

- **Chiavi deboli**: Una chiave k è debole se $E_K(E_K(x)) = x$, $\forall x \in \mathcal{P}$
- **Chiavi semi-deboli:** Una coppia di chiavi $(K1, K2)$ è semi-debole se $E_{K1}(E_{K2}(x)) = x$, $\forall x \in \mathcal{P}$
- DES ha 4 chiavi deboli e 6 coppie di chiavi semi-deboli
- Le chiavi deboli e semi-deboli sono ben note e vengono scartate quando viene generata la chiave
- Esempio: le chiavi deboli

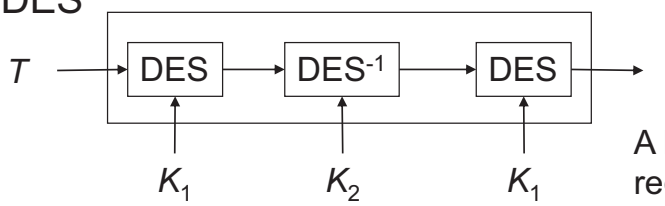
0101 0101 0101 0101	**FEFE FEFE FEFE FEFE**
1F1F 1F1F 1F1F 1F1F	**E0E0 E0E0 E0E0 E0E0**

Anomalie di DES

- **Complementation property**
  - If $u = E_a(e)$ then $\bar{u} = E_{\bar{a}}(\bar{e})$
  - This property makes it possible a chosen-plaintext exhaustive key search in which the key space becomes half the original key space
  - Once a key have been tried, it is not necessary to try the complemented key

DES properties and anomalies

- **DES is not a group**
  - DES is not closed under composition
  - If DES were a group then
    $\forall\ m \in \mathcal{M}, \forall\ K1, K2 \in \mathcal{K}, \exists\ K3 \in \mathcal{K}$ **s.t.**
    $E_{K1}(E_{K2}(m)) = E_{K3}(m)$
  - ***This means that encrypting twice is better than encrypting once***
  - 3DES



A brute-force attack requires 2^{112} attempts

Strength of DES

attack method	data complexity		storage complexity	processing complexity
exhaustive precomputation	—	1	2^{56}	1 (table lookup)
exhaustive search	1	—	negligible	2^{55}
linear cryptanalysis	2^{43} (85%)	—	for texts	2^{43}
	2^{38} (10%)	—	for texts	2^{50}
differential cryptanalys	—	2^{47}	for texts	2^{47}
	2^{55}	—	for texts	2^{55}