Requisiti di sicurezza per il sistema:

- **Autenticazione**
  Assicurazione dell'identità dei soggetti coinvolti nella trasmissione
- **Controllo degli accessi**
  I soggetti non autorizzati non possono accedere alle risorse
- **Confidenzialità**
  Nessun soggetto terzo deve accedere ai dati
- **Integrità**
  Assicurazione che i dati non siano stati alterati da soggetti non autorizzati
- **Non ripudiabilità (paternità)**
  Protezione contro la negazione di un soggetto coinvolto nella comunicazione

❖ **Crittografia** → insieme di procedure con lo scopo di nascondere un messaggio
❖ **Testo in chiaro** → messaggio originale
❖ **Testo cifrato** → messaggio che viene trasmesso
❖ **Chiave** → sequenza finita di bit usata come ingresso di un algoritmo crittografico.

I sistemi crittografici sono classificati in base al:

- Tipo di operazioni per cifrare il testo (sostituzione o trasposizione)
- Modo in cui il testo in chiaro è elaborato (crittografia a blocchi o a flusso)
- Numero di chiavi (chiave simmetrica o asimmetrica)

Cifrario di Giulio Cesare con chiave = 5.

Alfabeto non cifrato	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrato (chiave=5)	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Cifrario di Vigenère
Con una chiave lunga 6 cifre: 3-15-2-6-21-8, otteniamo:

Testo in chiaro	O	T	T	O	B	I	T	F	A	N	N	O	U	N	B	Y	T	E
Chiave ripetuta	3	15	2	6	21	8	3	15	2	6	21	8	3	15	2	6	21	8
Testo cifrato	R	I	V	U	W	Q	W	U	C	T	I	W	X	C	D	E	0	M

Cifrario One-Time Pad (OTP)
con chiave di lunghezza variabile e pari alla lunghezza del testo in chiaro;
prevede che la chiave venga utilizzata una sola volta.

Un cifrario è perfetto quando:
LunghezzaChiave ≥ LunghezzaMessaggio

Testo in chiaro	O	T	T	O	B	I	T	F	A	N	N	O	U	N	B	Y	T	E
Chiave NON ripetuta	2	16	3	6	21	2	4	14	1	6	20	8	1	15	7	6	19	5
Testo cifrato	Q	J	W	U	W	K	X	T	B	T	H	W	V	C	I	E	P	J

CRITTOGRAFIA A TRASPOSIZIONE

Cifrario a matrice

gli elementi del testo in chiaro non sono sostituiti, ma riorganizzati.

Chiave	C	I	F	R	A
Testo	O	T	T	O	B
	I	T	F	A	N
	N	O	U	N	B
	Y	T	E	E	D
	U	E	B	Y	T
	E	F	A	N	N
	O	U	N	A	W
	O	R	D	*	*

Il messaggio cifrato da inviare risulta:

BNBDTNW*OINYUEOOTFUEBANDTTOTEFUROANEYNA*

(si prendono le colonne in ordine alfabetico)

IL DES

Confusion → rendere confusa la relazione tra il testo in chiaro e quello cifrato, tipicamente tramite la sostituzione dei caratteri in chiaro con caratteri diversi
Diffusion → alterare la struttura del testo in chiaro spargendo i caratteri su tutto il testo cifrato, tipicamente permutando (trasponendo) i caratteri del testo in chiaro.

Nel DES il messaggio viene diviso in blocchi da 64 bit, si usano chiavi a 64 bit (2^56 possibili combinazioni (8 bit non vengono utilizzati))

L'input viene suddiviso in 2 parti:

- sinistra (L)
- destra (R)

Il round i-esimo genera:

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

La funzione F:

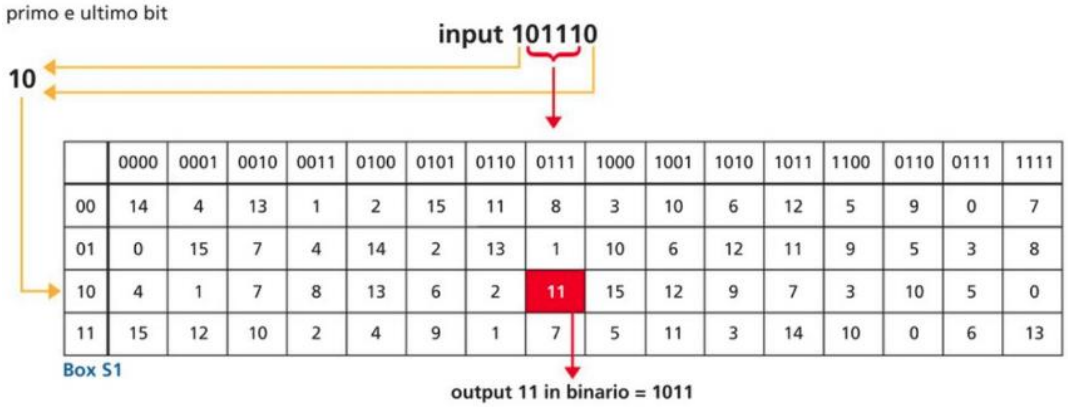
- Espande R a 48 bit mediante una permutazione/espansione
- Effettua lo XOR del risultato con la sottochiave
- Invia il tutto a 8 S-BOX per ottenere un output di 32 bit
- Infine, esegue una permutazione finale dei 32 bit

Le S-BOX:

Ci sono 8 S-Box → funzioni che accettano in ingresso 6 bit e ne producono 4

- Ogni S-Box è una matrice 4x16 contenente numeri interi tra 0 e 15
- I bit 1 e 6 selezionano la riga
- I bit 2-5 selezionano la colonna

- Il risultato è l'espansione binaria dell'elemento selezionato della matrice
- L'output delle S-Box dipende sia dai dati che dalla chiave



	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	0110	0111	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	7	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	10	2	4	9	1	7	5	11	3	14	10	0	6	13

Box S1