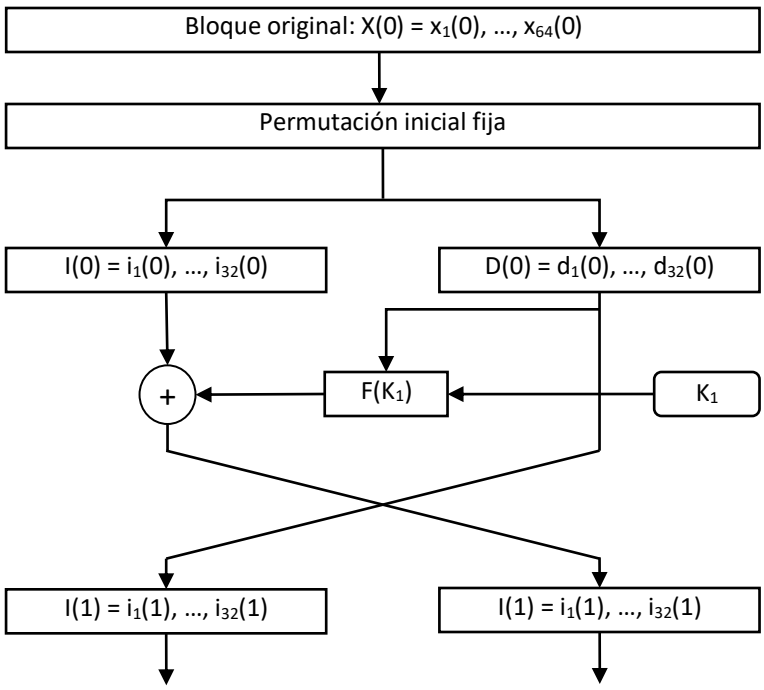
ANEXO A. FUNCIONAMIENTO DEL DES

DES emplea un bloque original de 64 bits, el cual sufre una permutación fija inicial sin valor criptográfico, luego se divide en dos bloques de 32 bits cada uno y se nombra como bloque de la izquierda y bloque de la derecha. A continuación se realiza una suma modulo 2 de la parte izquierda con una función de la parte derecha **F(K_i)** dependiente de una clave **K_i** de 48 bits que a su vez depende de la clave inicial de 56 bits. El proceso de creación de claves se explicará más adelante. A continuación se intercambian las partes derecha e izquierda. En la última vuelta no se realiza el intercambio, en su lugar se hace una permutación que es la inversa a la permutación inicial y de este modo termina el algoritmo. La figura 2.1 muestra el inicio y primera vuelta de la estructura del DES [3].

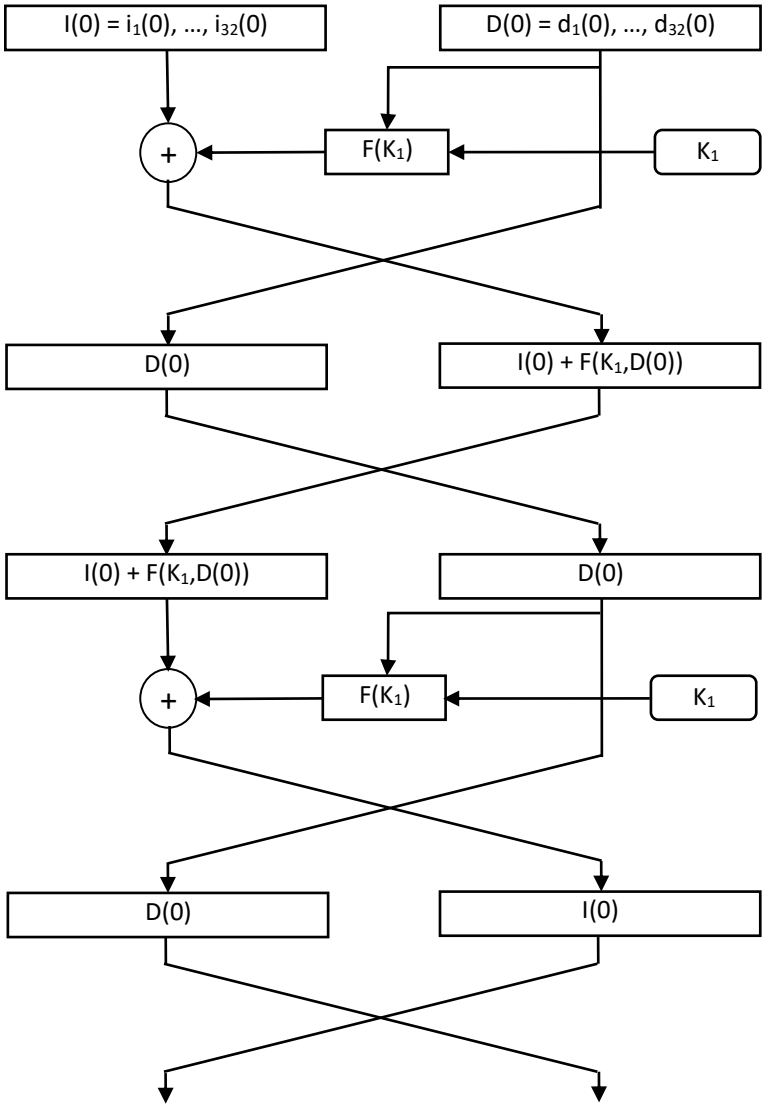
Figura A.1 Inicio y primera vuelta de la estructura del DES [3].



Involución en el DES

La involución consiste en aplicar dos veces una misma función para de esta manera llegar a los datos iníciales, de esta manera no es necesario invertir la función ***F*** sino repetirla permitiendo que dicha transformación sea una función en un solo sentido empleando operaciones no lineales.

Figura A.2 Involución en el DES [3]



Manipulaciones en el DES

La función ***F*** es un conjunto de operaciones que se describe en la figura A.2.

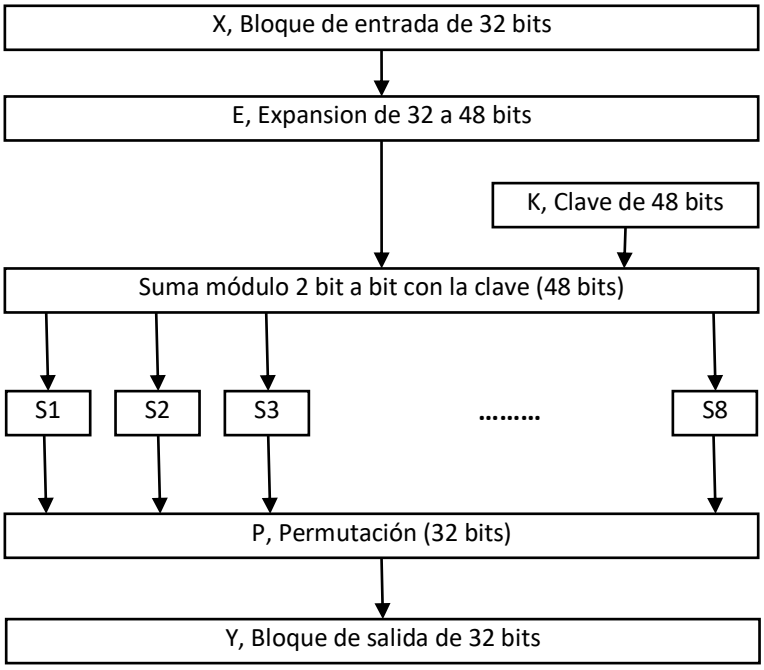
La primera manipulación consiste en utilizar una expansión lineal para conseguir un vector de 48 bits a partir de un bloque inicial de 32 bits. Esta expansión se logra mediante el uso de la tabla que se muestra a continuación.

Tabla A.1 Expansión lineal de 32 a 48 bits

Izquierda	**32**	1	2	3	4	**5**	**4**	5	6	7	8	**9**
Centro izda	**8**	9	10	11	12	**13**	**12**	13	14	15	16	**17**
Centro dcha	**16**	17	18	19	20	**21**	**20**	21	22	23	24	**25**
Derecha	**24**	25	26	27	28	**29**	**28**	29	30	31	32	**1**

Tomada de [3]

Figura A.3 Estructura de la función F



Tomada de [3]

Los bits originales se muestran en los recuadros marcados de la tabla A.1, los bits agregados aparecen en negrita. La presentación de la permutación es por conveniencia, las filas deben tomarse correlativas, es decir, una siguiendo a la otra.

Luego se realiza una suma módulo 2 bit a bit de la clave de 48 bits con el vector expandido dando como resultado otro vector de 48 bits que posteriormente se divide en ocho grupos de 6 bits. Cada grupo conforma lo que se denomina las "*Cajas S*", responsables de la no linealidad del DES.

Cada Caja S tiene una entrada de 6 bits de los cuales salen únicamente 4, los bits sobre los cuales se hace la sustitución son los 4 centrales y dependiendo de los bits laterales hay 4 posibilidades. Los principios para la elección de las Cajas S nunca han sido revelados y es información clasificada como ultra secreta por parte del gobierno de los Estados Unidos.

Por último, la información pasa por una "*Caja P*" la cual es una permutación lineal fija que tiene como objetivo que los bits aparezcan de la manera más difusa posible a lo largo del tamaño del bloque de 32 bits. La permutación se presenta en la tabla A.2. Las filas nuevamente deben considerarse correlativas.

Tabla A.2 Permutación lineal fija de una caja P

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Expansión de claves en el DES

El DES utiliza una clave de 64 bits, de los cuales se extraen 8 bits para paridad y de esta manera se tiene una clave de 56 bits los cuales son reordenados según la tabla A.3. Esta permutación carece de significado criptográfico.

Tabla A.3 Permutación inicial de la clave de 56 bits

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

A continuación se generan las 16 claves de 48 bits necesarias para ser utilizadas en cada vuelta del DES. Primero se divide la clave de 56 bits en dos bloques de 28 bits cada uno y se permutan circularmente, es decir, se rotan uno o dos bits dependiendo de la vuelta. Estas rotaciones se muestran en la tabla A.4.

Tabla A.4 Número de bits rotados en las mitades de las subclaves

Vuelta afectada	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Número de bits	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

El siguiente paso consiste en reunir las mitades teniendo de nuevo 16 grupos de 56 bits cada uno de los cuales se seleccionan los 48 bits que han de componer las 16 subclaves. La tabla A.5 muestra la “permutación con compresión” utilizada en este proceso.

Tabla A.5 Permutación con compresión final de la clave de 56 bits

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32