CAPÍTULO 2: MODELOS DE SEGURIDAD

Las políticas de seguridad informática son los instrumentos para garantizar que una organización cumpla con su misión tomando conciencia de la sensibilidad de la información y los servicios críticos presentes, lo que exige establecer fallas y deficiencias.

Una política de seguridad se divide en los estados de un sistema autorizado y no autorizado, debe incluir las leyes, normas y prácticas que regulan la manera como una institución gestiona y protege sus recursos, debe tener un carácter general (en relación a todo el negocio) y específico (para la división de las funciones básicas). Asimismo, puede tener un origen externo (impuestas por la legislación, el gobierno o la industria).

Un modelo de capas se puede utilizar para describir cómo se estructuran las políticas, pasando de las políticas de la institución del más alto nivel hasta llegar a las políticas específicas de los usuarios que acceden a los datos, las políticas de encriptación, etc.

Las políticas pueden asociarse a los siguientes tipos de criterios:

a) Sistemas abiertos/cerrados: en un sistema cerrado, nada es accesible a menos que se autorice expresamente; en un sistema abierto o institución todo es accesible a menos que esté explícitamente denegado.
b) Menos privilegio: las personas o cualquier entidad activa debe acceder solo a los recursos computacionales necesarios según su función, suele combinarse con la política de sistemas cerrados.
c) Maximizar el intercambio de información para maximizar su uso
d) Autorización explicita: tanto para el acceso y las condiciones del mismo
e) Obligación: definen qué debe o no debe realizarse en un conjunto de datos
f) Separación de los derechos: las funciones críticas deben ser asignadas a más de una persona o sistema.
g) Auditoria: se debe llevar un registro de que se hizo, quien y en qué momento, para fines de prevención y rendición de cuentas.
h) Control centralizado/descentralizado: en el caso de un sistema descentralizado sus divisiones tienen autoridad para definir sus propias políticas siempre que no violen las políticas globales.
i) Propiedad y administración: para evitar que el usuario considere algunos datos como su propiedad y por lo tanto tendría los derechos sobre ellos. Asimismo, una política administrativa separa la administración de los datos de su uso.
j) Rendición de cuentas individuales: todas las personas o los procesos deben ser identificados y sus acciones registradas y revisadas.
k) Roles: para asignar un grupo de derechos que se les da a los usuarios de acuerdo a sus funciones.
l) Nombres o identificadores para el control de acceso: el acceso de control está designado por su número o por las clases incluidas en sus instancias.
m) Contenido según el control de acceso: el acceso a los datos depende de los requerimientos de los archivos específicos.

2.1 MODELOS DE SEGURIDAD Y PROTECCIÓN

Los modelos de seguridad son más precisos y detallados que las políticas, se podría decir que son su instanciación, por lo que se utilizan como directrices para crear y evaluar sistemas; pueden describirse de manera formal o semiformal. En general los modelos pueden ser de carácter obligatorio o discrecional. En el primer caso, cuando el modelo es obligatorio sólo determinados roles o actores están autorizados a conceder derechos y los usuarios que los reciben no pueden transferirlos; mientras que, en el caso de un modelo discrecional, los titulares de derechos podrían estar autorizados a transferir los derechos según su discreción.

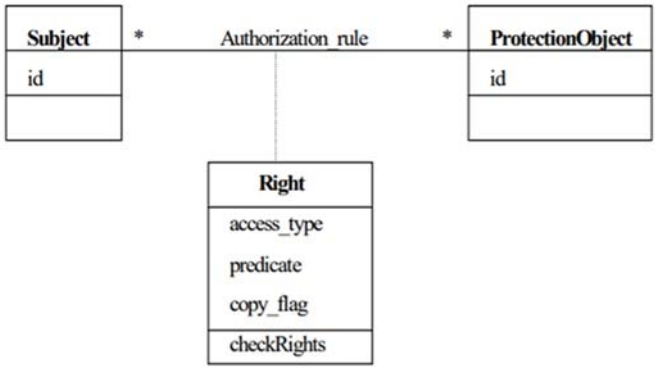
Hay diferentes criterios para clasificar y describir los modelos, pero la mayoría de ellos hacen su descripción usando alguna de las siguientes herramientas:

- matriz de acceso
- acceso basado en funciones de control
- modelos multinivel

Los dos primeros son modelos de control de acceso y el último es un control de flujo de información.

a) Matriz de acceso (AM)

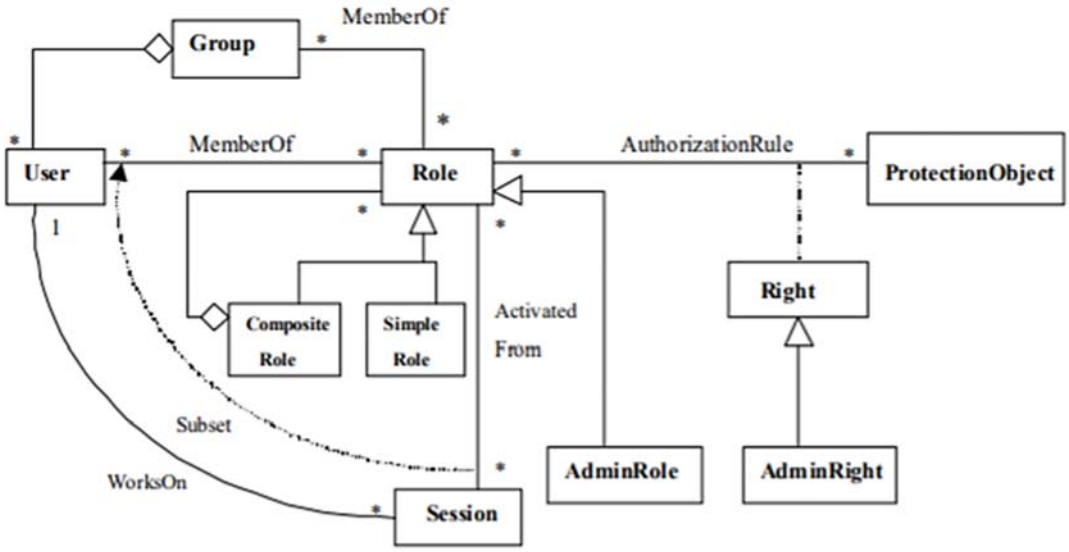
El modelo considera un conjunto de: sujetos S (entidades), objetos protegidos O (que son solicitados por las entidades), y tipos de acceso T (la forma en que el objeto se accede). Las normas de autorización serían:



El predicado define limitaciones en el acceso, la condición establece una condición que debe ser cierto en el caso de la norma a aplicar, si la copia bandera autoriza al objeto de la norma de conceder el derecho a otros usuarios, y el autorizador indicó que ha realizado esta autorización. Ejemplos de estos modelos son los de Lampson, el modelo de Dependencia de los Derechos Humanos,

b) Control de Acceso basado en funciones - RBAC (Role Based Access Control)

Es una variación de la matriz de acceso, donde los sujetos son funciones. Un rol correspondería a un puesto o funciones dentro de un puesto de trabajo y los derechos se asignan a las funciones. Si los usuarios se asignan a las funciones y los derechos sólo los da un administrador entonces este modelo es de carácter obligatorio. Suele aplicar políticas de mínimos privilegios y la separación de funciones. Un patrón para RBAC sería



Este modelo utiliza el concepto de período de sesiones para limitar los derechos utilizados en un momento dado y para hacer cumplir la separación de servicio. La definición del modelo puede hacerse utilizando casos de uso y admite herencia.

c) Modelos multinivel

En este tipo de modelos, los datos se clasifican en niveles de sensibilidad y los usuarios tienen acceso de acuerdo con sus autorizaciones. Debido a la forma del control de seguridad también se denominan modelos de flujo de datos, porque controlan el flujo de datos entre los niveles. Admiten tres formas diferentes:

- Modelo de La Bell-Padula: controlan las fugas de información entre los niveles.
- Modelo de Biba: controlan la integridad de los datos.
- Modelo de celosía: con niveles parcialmente ordenados de los modelos anteriores mediante la matemática de celosías

Trabajo de investigación formativa 3:

En grupos de tres alumnos realizar por asignación una investigación sobre los siguientes modelos de seguridad

- Modelos de protección de la memoria
- Modelo de control de acceso obligatorio
- Modelo de control a discreción
- Modelo de control por el origen
- Modelo de control basado en el rol
- Modelos de control de acceso (Harrison-Russo-Ullman)
- Modelos de confidencialidad (Bell-LaPadula)
- Modelos de integridad (Biba, Clark-Wilson)

TERCERA UNIDAD
CRIPTOGRAFÍA

3.1 CRIPTOGRAFIA

La palabra Criptografía proviene del griego "kryptos" que significa oculto, y "graphia", que significa escritura, y su definición según el diccionario es "Arte de escribir con clave secreta o de un modo enigmático". La Criptografía es el conjunto de técnicas (Teoría de la Información, Algorítmica y Teoría de números o Matemática Discreta) para la protección o el ocultamiento de la información frente a observadores no autorizados.

La **criptografía** debe proteger la información contra accesos no autorizado, interceptación, modificación o inserción de información, prevenir acceso y uso no autorizado de los recursos, prevenir la denegación de servicios a los que sí están permitidos. En la actualidad se centra su aplicación sobre redes telemáticas (identificación, autenticación, control de acceso a recursos, confidencialidad e integridad de mensajes transmitidos y su no rechazo).

La **encriptación** es la tecnología hardware o software, para cifrar mensajes de correo electrónico, información de base de datos y otros datos, con el fin de mantenerlos confidenciales.

El **encriptamiento** es el conjunto de procesos que mantiene la seguridad en los sistemas distribuidos, cuando dos entidades se comunican, deben establecer una clave de comunicación para la autentificación, con ella se convierte un texto a un texto encriptado a partir de un conjunto de transformaciones en las que se aplican diversos algoritmos a un conjunto de parámetros de entrada. Con ello se implementa la codificación de información antes de ser transmitida.

La **estenografía** es ocultar en el interior de una información inocua, otro tipo de información que puede estar cifrada o no, lo que permite burlar el control.

El **criptoanálisis** es el conjunto de técnicas usadas para romper los códigos que encriptan la información, finalmente, la criptología, agrupa tanto la criptografía como el criptoanálisis.

Las **funciones o servicios de seguridad** propios de la criptografía son:

- Confidencialidad: solamente usuarios autorizados tienen acceso a la información o servicio.
- Integridad de la información: garantía a los usuarios de que la información original no será alterada, ni intencional ni accidentalmente.
- Autenticación de usuario: proceso que permite al sistema verificar si el usuario que pretende acceder o hacer uso del sistema es quien dice ser.
- Autenticación de remitente: proceso que permite a un usuario certificar que el mensaje recibido fue enviado por el remitente y no por un suplantador.
- Autenticación del destinatario: proceso que garantiza la identidad del usuario destinatario.
- No repudio en origen: que cuando se reciba un mensaje, el remitente no pueda negar haber enviado dicho mensaje.
- No repudio en destino: que cuando se envía un mensaje, el destinatario no pueda negar haberlo recibido cuando le llegue.

- Autenticación de actualidad (no replay): consiste en probar que el mensaje es actual, y que no se trata de un mensaje antiguo reenviado.

Existen dos **tipos de criptosistemas:**

a) *Criptosistema simétricos o de clave privada*: son aquellos que emplean la misma clave k tanto para cifrar como para descifrar, entonces emisor y receptor deben conocer la clave k, lo que genera el problema adicional de transmitir la clave de forma segura.
b) *Criptosistema asimétricos o de llave pública*, emplean una doble clave (kp, kP). Kp es la clave privada y kP la clave pública. Una de ellas se usa para la transformación de cifrado y la otra para la transformación de descifrado. A veces son intercambiables y se debe cumplir que el conocimiento de la clave pública kP no permita calcular la clave privada kp. En estos sistemas se pueden establecer comunicaciones seguras por canales inseguros. Este tipo de sistemas se dividen en dos ramas:

   - *Cifrado de clave pública*: un mensaje cifrado con la clave pública de un destinatario no puede ser descifrado por nadie (ni siquiera el que lo cifró), excepto el poseedor de la clave privada correspondiente, se utilizan para confidencialidad.
   - *Firmas digitales*: el mensaje se firma con la clave privada del remitente y puede ser verificado por cualquier persona que tenga acceso a la clave pública del remitente, se utilizan para la autenticidad.

Dentro de las principales **tecnologías de encriptación** tenemos:

- Virtual PrivateNetworking(VPN): usado para asegurar datos en Internet.
- SecuresocketsLayer(SSL): para asegurar transacciones web cliente–servidor
- S-MIME: para asegurar transacciones de e-mail
- Protocolo WPA: para asegurar transacciones inalámbricas.
- Key Hopping: nueva tecnología para redes WLAN 802.11a y 802.11b, basada en MD5, tecnología usada en la autentificación de tarjetas de crédito. La tecnología utiliza un sistema gestor de claves que permiten transmitir por ondas de radio claves seguras saltando de frecuencia, lo que impide a los intrusos interceptar las claves y romper la encriptación.

Trabajo de Investigación formativa 3
Investigar sobre las tecnologías de encriptación indicadas, definiendo claramente su principio de funcionamiento, aplicación y amenazas o exploits encontrados

3.1.1 Cifrados y códigos

Hay dos métodos de alterar las representaciones de los mensajes para hacerlos ininteligibles a intrusos:

- Usando códigos: consiste en sustituir unidades textuales semánticas más o menos largas o complejas, habitualmente palabras o frases, para ocultar el mensaje; por ejemplo, "cielo azul" podría significar «atacar al amanecer». En la segunda guerra mundial se usaron códigos en lengua navaja para identificar mensajes militares. Por ejemplo, chai-da-gahy-nail-tsaidi (asesino de tortugas) quería decir “armas antitanque”. Esta técnica requiere recopilar la información secreta en un diccionario o libro de códigos (codebook).

- Por cifrado: es una transformación carácter por carácter o bit por bit, sin importar la estructura lingüística del mensaje. Para descifrar se utiliza otro algoritmo que permite obtener la cadena original. Estos sistemas están controlados por claves que son entradas a los algoritmos usados. Si la clave de cifrado es igual que la de descifrado se dice que es un cifrado simétrico. Si son distintas se dice que es un cifrado asimétrico. Es necesario considerar el Principio de Kerckhoffs, llamado de seguridad por oscuridad, que define que la seguridad de un sistema de cifrado debe estar en el secreto de las claves y no en el secreto del algoritmo. La difusión del algoritmo permite que los especialistas evalúen la seguridad del algoritmo.

3.1.2 **Evolución**

- La criptografía surge en el antiguo Egipto, romanos y griegos para las órdenes militares. Los espartanos utilizaron (400 A.C.) la Escitala, que usa transposición (alterar el orden) se escribia en una tela sobre una vara, el mensaje sólo podía leerse si se enrollaba la tela sobre un bastón del mismo grosor.

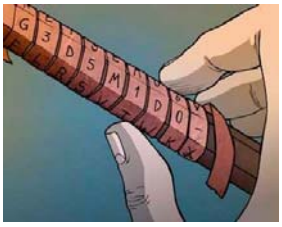


Figura 3.1.- La escitala

- Julio César se basó en la sustitución de cada letra por la situada tres puestos después en el alfabeto latino (cifrado César).
- En la Edad Media por usos papales surgen los sistemas por sustitución polialfabética, que emplea varios abecedarios, saltando de uno a otro cada tres o cuatro palabras. El emisor y el destinatario han de ponerse de acuerdo para fijar la posición relativa de dos círculos concéntricos, que determinará la correspondencia de los signos.

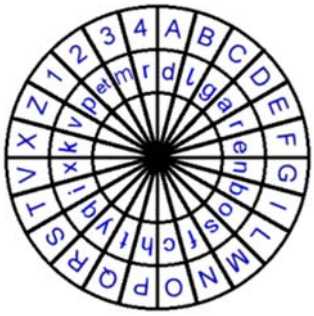


Figura 3.2.- Discos de Alberti

- Un siglo después, aparecen las claves, formada por una palabra o una frase, debe transcribirse letra a letra sobre el texto original. Cada letra del texto se cambia por la correspondiente en el alfabeto que comienza en la letra clave, Cifrado Vigenère (Blaise de Vigenère, S. XVI). Débil por razones estadísticas.
- En el siglo XX apareces teletipos con rotores móviles que giraban con cada tecla generando un código polialfabético complejo (traductores mecánicos, Rueda de Jefferson)

- La primera patente data de 1919, y es obra del holandés Alexander Koch, que comparte honores con el alemán Arthur Scherbius, el inventor de Enigma una máquina criptográfica a rotor que los nazis creyeron inviolable (“hackeada” por Turing)

Figura 3.3.- Rueda de Jefferson y Enigma

- Surgen luego los algoritmos modernos basados en tecnologías electrónicas y digitales
    - DES (IBM)
    - sistemas de cifrado asimétrico o de clave pública (como RSA)
    - sistemas de cifrado simétricos o de clave privada
    - la firma digital como aplicación del cifrado asimétrico

- El desarrollo de la teoría criptográfica actual, se sustenta en los trabajos de Claude Shannon “A Mathematical Theory of Communication" (1948) y "Communication Theory of Secrecy Systems" (1949) y Whitfield Diffie, Martin Hellman "New directions in Cryptography" (1976). Con la publicación del algoritmo **RSA** en 1977 por parte de los matemáticos Ron Rivest, Adi Shamir y Len Adleman la criptografía de clave pública se consolida.

3.2 CRIPTOGRAFÍA SIMÉTRICA

Son sistemas de cifrado, definidos formalmente como una quíntupla (**X, Y, K, E, D**), donde:

- **X** conjunto de todos los mensajes sin cifrar (texto plano o plaintext) que pueden ser enviados.
- **Y** conjunto de todos los posibles mensajes cifrados, o criptogramas.
- **K** conjunto de claves que se pueden emplear en el criptosistema.
- **E** conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de **X** para obtener un elemento de **Y**. Existe una transformación diferente $\mathbf{E_k}$ para cada valor posible de la clave **k**.
- **D** conjunto de transformaciones de descifrado, análogo a **E**.

Todo criptosistema funciona a partir de la siguiente relación si $\mathbf{Y = E_k (X)}$:

$$\mathbf{D_k (Y) = D_k (E_k (X)) = X}$$

Es claro entonces que el esquema de cifrado simétrico tiene cinco componentes:

- Texto plano o Plaintext: es el mensaje o dato inteligibles originales que se introduce en el algoritmo como entrada.
- Algoritmo de cifrado: algoritmo que realiza sustituciones y transformaciones en el texto plano.

- Clave secreta: también se introduce en el algoritmo de cifrado, es un valor independiente del texto sin formato y del algoritmo. El algoritmo producirá una salida diferente dependiendo de la clave específica que se esté utilizando en ese momento, las sustituciones y transformaciones exactas realizadas por el algoritmo dependen de la clave.
- Texto cifrado: mensaje codificado producido a la salida. Depende del texto plano y de la clave secreta. Para un texto plano, dos claves diferentes producirán dos textos cifrados diferentes. El texto cifrado debe ser ininteligible.
- Algoritmo de descifrado: es esencialmente el algoritmo de cifrado ejecutado en sentido inverso, toma el texto cifrado y la clave secreta y produce el texto plano original.

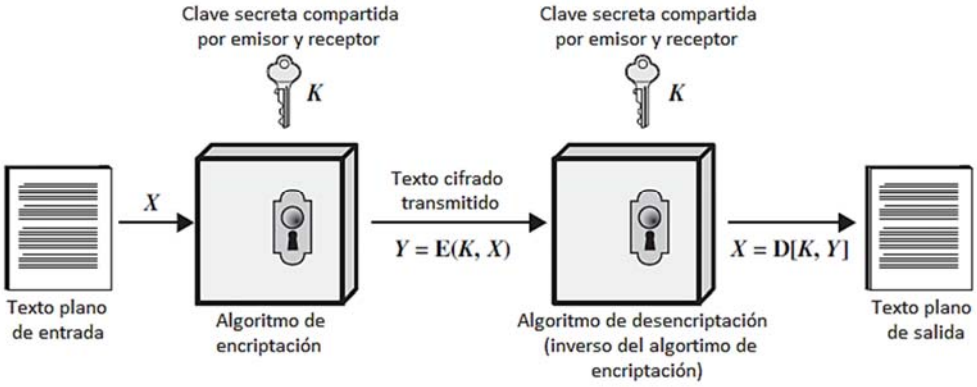


Figura 3.4 Modelo simplificado de la encriptación simétrica

Los requerimientos de seguridad son:

1. Un algoritmo de encriptación fuerte, de tal forma que, si una persona externa que conoce e algoritmo y accede a un texto cifrado, no podrá desencriptarlo sin la clave o descubrir la clave aun cuando posea varios textos encriptados y los textos planos originales.
2. El remitente y el receptor deberán obtener copias de la clave secreta de una manera segura y deben mantener la llave segura.

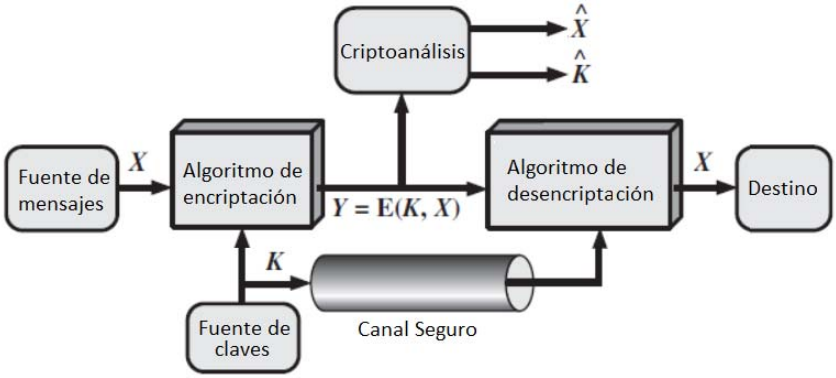


Figura 3.5 Criptosistema Simétrico

Los sistemas criptográficos se definen por:

a) El tipo de operaciones usadas en la transformación de texto plano en texto cifrado, estas operaciones dependen del algoritmo de cifrado, los cuales consideran: la *sustitución* (cada elemento del texto plano -bit, letra, grupo de bits o letras- se mapea en otro elemento, y

la *transposición*, para reordenar los elementos en el texto plano. En estas operaciones no se debe perder información (operaciones reversibles).

b) El número de claves utilizadas, emisor y receptor pueden usar la misma clave (cifrado simétrico o de clave privada) o usar diferentes claves (cifrado asimétrico o de clave pública).

c) La forma en que se procesa el texto sin formato. Un cifrado de bloque procesa la entrada de un bloque de elementos a la vez, produciendo un bloque de salida para cada bloque de entrada. Un cifrado de flujo procesa los elementos de entrada de forma continua, produciendo un elemento de salida a la vez, a medida que avanza.

3.2.1 Ataques

Atacar un sistema de encriptación siempre tiene por objetivo el obtener la clave de encriptación, más que un mensaje particular, para ello existen dos esquemas posibles:

- El criptoanálisis: usando el conocimiento del algoritmo de encriptación y algunos ejemplos disponibles de texto plano y texto cifrado, pueden tener como objetivo la obtención de la clave o la deducción de un texto específico.
- Fuerza bruta: se prueban todas las posibles claves sobre un determinado texto cifrado hasta obtener un posible texto plano. Estadísticamente, se debe probar al menos la mitad de todas las claves posibles para lograr el éxito.

La obtención de la clave quita toda la protección a mensajes pasados, presentes y futuros. Existen varios tipos de ataques criptoanalíticos en función de la información conocida, los ataques más complejos se dan cuando solo se tiene un texto cifrado, pero hay que suponer siempre que el atacante conoce también el algoritmo, si esto es cierto es posible un ataque de fuerza bruta, si este fuera el caso la cantidad de posibles claves o llaves debe ser enorme, en este caso cabría esperar algún análisis estadístico sobre el texto cifrado, para obtener alguna información posible sobre el texto plano (idioma, tipo de archivo, un listado desde Java, etc.).

Un ataque es exitoso si genera una ruptura en el algoritmo, Bruce Schneier define el ataque: "Romper un cifrado simplemente significa encontrar una debilidad en el cifrado que puede ser explotada con una complejidad inferior a la de la fuerza bruta. No importa que la fuerza bruta pudiera requerir 2128cifrados; un ataque que requiera 2110 cifrados se consideraría una ruptura... puesto de una manera simple, una ruptura puede ser tan sólo una debilidad certificacional: una evidencia de que el código no es tan bueno como se publicita" (Schneier, 2000).

3.2.2 Tipos de ataques

a) Según el objetivo del atacante

- Ataques pasivos: no se altera el mensaje, solo se escucha. Usa técnicas de escucha de paquetes (sniffing) y de análisis de tráfico.
- Ataques activos: se modifica la información o se crea información falsa. Hay muchas técnicas que se usan en este tipo de ataques:
    - Suplantación
    - Modificación de mensajes: borrado (dropping attacks), modificado (tagging attack) o reordenado
    - Reactuación: capturar paquetes y retransmitirlo

- Degradación de servicio

b) Según el conocimiento previo: todo ataque se asume presumiendo el conocimiento del algoritmo (Máxima de Shannon "el enemigo conoce el sistema"). Además del algoritmo los ataques podrían conocer:

- Ataque con sólo texto cifrado disponible: sólo se tiene acceso a una colección de textos cifrados o codificados.
- Ataque con texto plano o claro conocido: el atacante tiene un conjunto de textos cifrados de los que conoce el correspondiente texto claro o descifrado.
- Ataque con texto claro escogido (ataque con texto cifrado elegido): el atacante puede obtener los textos cifrados correspondientes a un conjunto arbitrario de textos claros de su elección.
- Ataque adaptativo de texto claro escogido: como el anterior, pero el atacante puede elegir textos claros subsiguientes basándose en la información obtenida de los descifrados anteriormente.
- Ataque de clave relacionada: como un ataque de texto claro escogido, pero el atacante puede obtener texto cifrado utilizando dos claves diferentes. Las claves son desconocidas, pero la relación entre ambas es conocida; por ejemplo, dos claves que difieren en un bit.

c) Clasificación según el objetivo en criptoanálisis: el criptógrafo Lars Knudsen (Knudsen, 1998) clasificó varios tipos de ataque sobre cifrados por bloques de acuerdo con la cantidad y la calidad de la información secreta que pudiera ser descubierta:

- Ruptura total: se deduce la clave secreta.
- Deducción global: se descubre un algoritmo funcionalmente equivalente para el cifrado y descifrado de mensajes, pero no la clave.
- Deducción local (o de instancia): se descubre textos claros o cifrados adicionales a los conocidos previamente.
- Deducción de información: se descubre alguna información en el sentido de Shannon que no era conocida previamente.
- Distinción del algoritmo: distingue información cifrada de una permutación al azar.

d) Clasificación según el coste: según la cantidad de recursos que requieren:

- Tiempo: número de operaciones elementales (suma, XOR, desplazamientos, etc.).
- Memoria: cantidad de almacenamiento.
- Datos: cantidad de textos claros y cifrados necesaria.

Se dice que un sistema de cifrado es *incondicionalmente seguro* si el texto cifrado no contiene suficiente información para determinar de forma exclusiva el texto plano, independientemente de cuánto texto cifrado esté disponible. Prácticamente estos sistemas no existen, así que hay que asegurar el cumplimiento de uno o ambos de los siguientes criterios, con lo que se dice que el sistema *es seguro desde el punto de vista computacional*:

- El costo de romper el cifrado excede el valor de la información cifrada.
- El tiempo necesario para romper el cifrado excede la vida útil de la información.

Tamaño de Clave (bits)	Número de claves posibles	Tiempo requerido si se procesa 1 desencriptación/μs	Tiempo requerido si se procesa 10^6 desencriptaciones/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\mu s = 35.8$ **minutos**	2.15 **milisegundos**
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\mu s = 1142$ **años**	10.01 **horas**
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\mu s = 5.4 \times 10^{24}$ **años**	5.4×10^{18} **años**
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\mu s = 5.9 \times 10^{36}$ **años**	5.9×10^{30} **años**
26 caracteres (permutación)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\mu s = 6.4 \times 10^{12}$ **años**	6.4×10^6 **años**

Figura 3.6 Tiempo promedio para descifrar claves en un ataque de fuerza-bruta

Todos los algoritmos de encriptación simétrica, se basan en dos operaciones elementales: la sustitución y la transposición.

3.2.3 Técnicas de Substitución

TÉCNICAS DE SUBSTITUCIÓN			
MONOALFABÉTICA		**POLIALFABÉTICA**	
MONOGRÁMICA Caracter a caracter	**POLIGRÁMICA** Por grupo de caracteres	**PERIÓDICA** La clave es periódica	**APERIÓDICA** La clave es aperiódica

a) *Sustitución Monoalfabética*: existe un alfabeto y siempre al texto en claro le va a corresponder el mismo criptograma. Algunos ejemplos:

- Cifrado del César: algoritmo monográmico, sustituye cada letra del texto original por otra situada tres posiciones delante de ella en el alfabeto que se esté utilizando (luego de Z viene A)
  - Ejemplo:
  - MCla: MUCHOS AÑOS DESPUES
  - Cripto: OXFKRV DQRV GHVSXHV

Para el alfabeto en español el valor numérico de cada letra es

a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

El algoritmo de encriptación será:

$$C=E(3,p)=(p+3) \bmod 27$$

Generalizando, k es la clave toma 25 valores posibles

$$C=E(k,p)=(p+k) \bmod 27$$

El algoritmo de desencriptación será:

$$p=D(k,C)=(C-k) \bmod 27$$

Ejemplo de la fuerza-bruta para este cifrado: (algoritmos conocidos, solo 26 claves y el lenguaje es conocido)

k	o	x	f	k	r	v	d	q	r	v	g	h	v	s	x	h	v
1	ñ	w	e	j	q	u	c	p	q	u	f	g	u	r	w	g	u
2	n	v	d	i	p	t	b	o	p	t	e	f	t	q	v	f	t
3	**m**	**u**	**c**	**h**	**o**	**s**	**a**	**ñ**	**o**	**s**	**d**	**e**	**s**	**p**	**u**	**e**	**s**
4	l	t	b	g	ñ	r	z	n	ñ	r	c	d	r	o	t	d	r
5	k	s	a	f	n	q	y	m	n	q	b	c	q	ñ	s	c	q
6	j	r	z	e	m	p	x	l	m	p	a	b	p	n	r	b	p
7	i	q	y	d	l	o	w	k	l	o	z	a	o	m	q	a	o
8	h	p	x	c	k	ñ	v	j	k	ñ	y	z	ñ	l	p	z	ñ
9	g	o	w	b	j	n	u	i	j	n	x	y	n	k	o	y	n
10	f	ñ	v	a	i	m	t	h	i	m	w	x	m	j	ñ	x	m
11	e	n	u	z	h	l	s	g	h	l	v	w	l	i	n	w	l
12	d	m	t	y	g	k	r	f	g	k	u	v	k	h	m	v	k
13	c	l	s	x	f	j	q	e	f	j	t	u	j	g	l	u	j
14	b	k	r	w	e	i	p	d	e	i	s	t	i	f	k	t	i
15	a	j	q	v	d	h	o	c	d	h	r	s	h	e	j	s	h
16	z	i	p	u	c	g	ñ	b	c	g	q	r	g	d	i	r	g
17	y	h	o	t	b	f	n	a	b	f	p	q	f	c	h	q	f
18	x	g	ñ	s	a	e	m	z	a	e	o	p	e	b	g	p	e
19	w	f	n	r	z	d	l	y	z	d	ñ	o	d	a	f	o	d
20	v	e	m	q	y	c	k	x	y	c	n	ñ	c	z	e	ñ	c
21	u	d	l	p	x	b	j	w	x	b	m	n	b	y	d	n	b

- Cifrado Playfair, algoritmo poligrámico (digrámico), un par de letras de un texto claro se convierten en otro par distinto, la clave es una matriz de cifrado de 5x5 (sin ñ y con i=j). Veamos la matriz construida a partir de la palabra MONEDA

M	O	N	E	D
A	B	C	F	G
H	I	K	L	P
Q	R	S	T	U
V	W	X	Y	Z

Reglas:

1. Dos letras repetidas se separan por una x. Ejemplo MALLA sería MA LX LA, si la palabra tiene un número impar de letras se coloca una x al final.
2. Si las dos letras se encuentran en el mismo fila de la matriz, cada una de ellas se sustituye con la letra que esté a su derecha. Por ejemplo, ED se cifra como DM.
3. Si las dos letras se encuentran en la misma columna, cada una de las letras se sustituye por la letra debajo de ella. Por ejemplo, AV se cifra HM
4. En otro caso, la primera letra de la pareja se sustituye por la que este en la intersección de su misma fila y la columna de la segunda letra, la segunda letra se sustituye por la que este en la intersección de su misma fila y la columna de la primera letra. Por ejemplo: BT se cifra FR

COMO ESTAS = CO MO ES TA SX se cifraría como BN NM NT FQ NN

- Cifrado Atbash
- Cifrado de Polybios.

b) ***sustitución polialfabética:*** el criptograma del texto claro puede ser diferentes dependiendo de la clave que se utilice para cifrar, por lo que se dice que existen múltiples alfabetos de cifrado, de ahí el nombre de sustitución polialfabética.

- Cifrado de Alberti

- Cifrado por desplazamiento
- Cifrado de Vigenère
- Cifrado de Vernam
- Cifrado One-Time Pad

3.2.4 Técnicas de Transposición

Una alternativa de cifrado es realizar algún tipo de permutación en las letras de texto plano. Esta técnica se conoce como cifrado de transposición, las unidades que se permutan pueden ser de una letra, pares o trios. (Ejemplo: la escitala). Más que usarlas individualmente se superponen a otras técnicas para mejorar la seguridad. Las 'unidades de texto' pueden ser de una sola letra, pares de letras, tríos de letras o combinaciones de lo anterior, normalmente el algoritmo se basaba en un diseño geométrico o el uso de artilugios mecánicos (Ej escítala). algoritmo y clave son un conjunto indivisible.

- Cifrado por Escritura Inversa
  Se escribe la palabra al revés, por ejemplo, la cadena: *"Hola mi nombre es Pepa"* se cifra como "aloH im erbmon se apeP". Puede emplearse para palabras sueltas o mensajes completos.

- Cifrado por Transposición Columnar Simple
  Este es un cifrado con forma de columna, el mensaje original estará limitado a un rectángulo, de izquierda a derecha y de arriba hacia abajo. Después, se escoge una clave para asignar un número a cada columna del rectángulo para determinar el orden. El número correspondiente a la letra de la clave estará determinado por su posición en el alfabeto, por ejemplo. A es 1, B es 2, C es 3, etc. Por ejemplo, si la clave es CAT y el mensaje es "THE SKY IS BLUE", el proceso sería el siguiente:

C	A	T
3	**1**	**20**
T	H	E
S	K	Y
I	S	B
L	U	E

  Tomando las letras en orden numérico se forma el mensaje, la columna debajo de la A primero, después la columna de C y por último la columna de T, el mensaje cifrado será: HKSUTSILEYBE

- Cifrado por transposición columnar doble
  Considerada, por mucho tiempo, la forma más segura y compleja. Su operación es idéntica a la transposición columnar simple, pero tras una primera transposición, se realizaba una segunda, empleando o no, la misma clave.

- Cifrado por transposición interrumpida
  Diversos puntos de la matriz de cifrado, conocidos por emisor y receptor de la codificación, quedan vacíos, ello altera la serie y distorsiona la lógica de la transposición. Uno de los más conocidos fue propuesto por el general Luigi Sacco que establecía diferentes longitudes para cada una de las líneas a cifrar, extendiéndose hasta encontrar la columna con el número correspondiente a la línea (así la primera línea llega hasta el número 1 y la quinta hasta el 5). Y donde cada columna se leía ignorando los huecos.

Por ejemplo, John Savard propone la clave CONVENIENCE y el texto claro *"Here is a secret message enciphered by transposition"*.

C	**O**	**N**	**V**	**E**	**N**	**I**	**E**	**N**	**C**	**E**
1	**10**	**7**	**11**	**3**	**8**	**6**	**4**	**9**	**2**	**5**
H										
E	R	E	I	S	A	S	E	C	R	
E	T	M	E	S						
S	A	G	E	E	N	C	I			
P	H	E	R	E	D	B	Y	T	R	A
N	S	P	O	S	I	T				
I	O	N								

El texto cifrado será HEESPNI RR SSEES EIY A SCBT EMGEPN ANDI CT RTAHSO IEERO.

- Cifrado AMSCO
  Creado por A. M. Scott, es una transposición columnar en la que los elementos del texto cifrado son escogidos, alternativamente, como letras simples y pares de letras. Así, la palabra MATEMÁTICAMENTE será cifrado con la clave COPLA como sigue:

C	**O**	**P**	**L**	**A**
2	**4**	**5**	**3**	**1**
M	AT	E	MA	T
IC	A	ME	N	TE

El texto cifrado será: TTE MIC MAN ATA EME

- Cifrado por transposición por ruta
  Consisten en repartir el mensaje a cifrar en una figura geométrica, normalmente un paralelepípedo y definir una ruta para leer el mensaje. La complejidad de la ruta determinará la fuerza del cifrado. Pueden establecerse distintas rutas, por ejemplo, para la palabra EUFORICAS se puede ordenar en tres columnas de igual longitud.

E	U	F
O	R	I
C	A	S

Puede leerse como una espiral hacia el centro EUFISACOR, como una espiral desde el centro ROCASIFUE, de modo diagonal ERS UI F C OA, que está inscrito en un cilindro, ERS UIC FOA, la primera columna en descendente, la segunda en ascendente y la tercera en descendente: EOC ARU FIS.

Otros algoritmos de transposición o codificación son:

- Cifrado por permutación de grupos
- Cifrado por permutación por series
- Cifrado por rejillas criptográficas

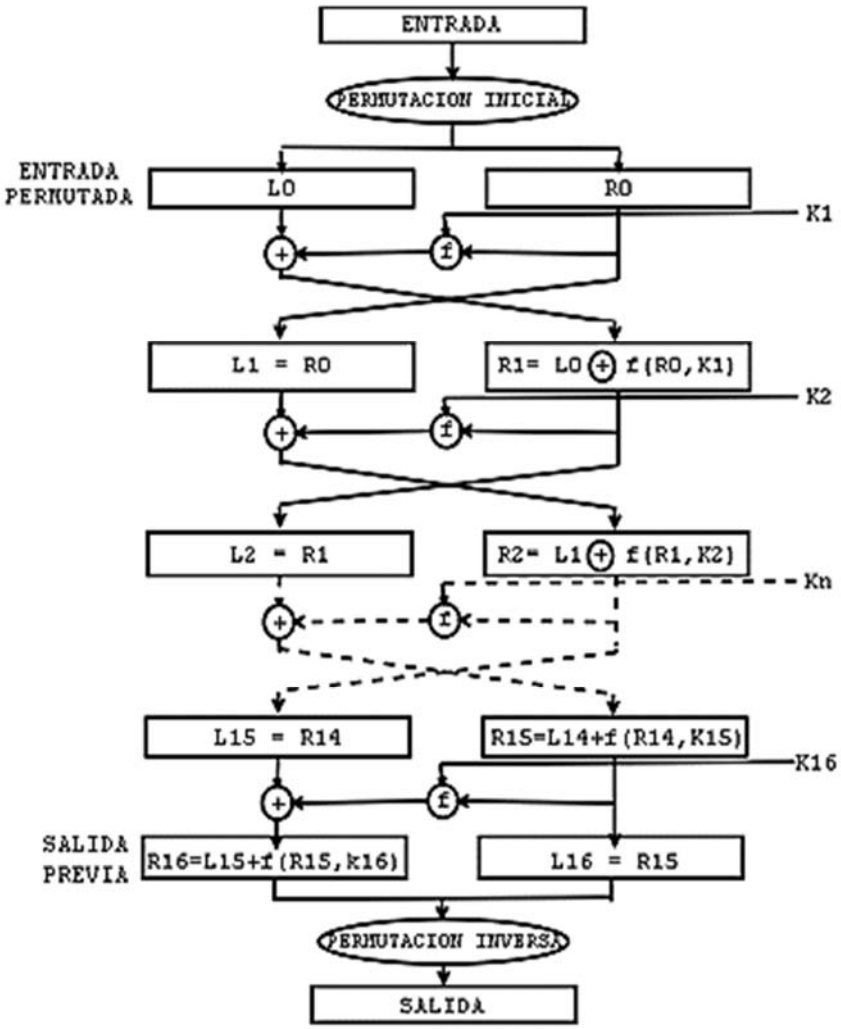
Trabajo de investigación formativa 4:
Según la asignación de grupos implementar los algoritmos de cifrado y descifrado asignados

3.2.5 Algoritmos de Criptografía Simétrica

a) DES (Data Encription Standard o Estándar de Encriptación de Datos) o DEA (Data Encription Algorithm)

Es el algoritmo de cifrado simétrico más empleado, es un algoritmo de cifrado por bloques de 64 bits, con clave de 56 bits (se eliminan 8 bits de paridad), fue diseñado para ser implementado en hardware y es usado en comunicaciones. Emisor y receptor deben conocer la clave secreta, la que se intercambia por algoritmos de clave pública. Se usa para encriptar y desencriptar mensajes, generar y verificar códigos de autentificación de mensajes (MAC) y para encriptación de un sólo usuario (por ejemplo, guardar un archivo en disco), los ataques se realizan con hardware específico que con fuerza bruta descubran una clave en pocos días por el tamaño de la clave. Las fases del algoritmo son las siguientes:

1) fraccionamiento del texto en bloques de 64 bits (8 bytes)
2) permutación inicial de los bloques
3) partición de los bloques en dos partes: izquierda y derecha, *L y R* respectivamente
4) fases de permutación y de sustitución repetidas 16 veces (rondas)
5) reconexión de las partes izquierda y derecha, seguida de la permutación inicial inversa.



- **Permutación inicial** cada bit de un bloque está sujeto a una permutación inicial, representada mediante la siguiente matriz de permutación inicial (PI):

PI								
	58	50	42	34	26	18	10	2
	60	52	44	36	28	20	12	4
	62	54	46	38	30	22	14	6
	64	56	48	40	32	24	16	8
	57	49	41	33	25	17	9	1
	59	51	43	35	27	19	11	3
	61	53	45	37	29	21	13	5
	63	55	47	39	31	23	15	7

- **División en bloques de 32 bits** el bloque de 64 bits se divide en dos bloques de 32 bits llamados L y R por Left y Right. El estado inicial de estos bloques se denomina L_0 y R_0:

L_0								
	58	50	42	34	26	18	10	2
	60	52	44	36	28	20	12	4
	62	54	46	38	30	22	14	6
	64	56	48	40	32	24	16	8

R_0								
	57	49	41	33	25	17	9	1
	59	51	43	35	27	19	11	3
	61	53	45	37	29	21	13	5
	63	55	47	39	31	23	15	7

L_0 contiene los bits en posición par en el mensaje inicial y R_0 contiene los bits en posición impar.

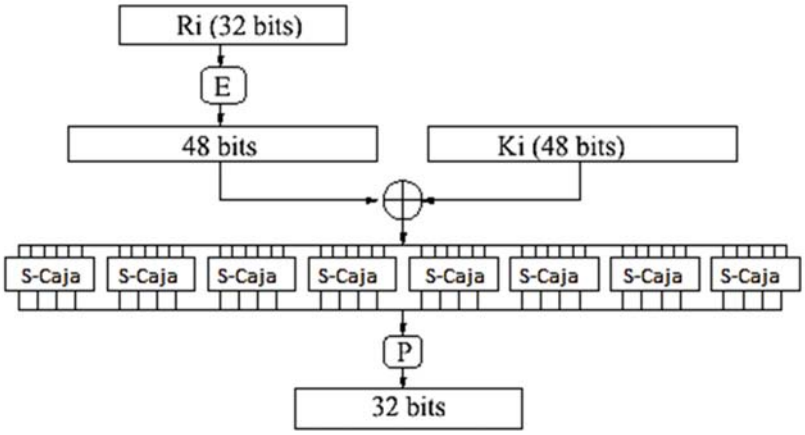
- **Fases de permutación y de sustitución repetidas o 16 rondas** los bloques L_n y R_n sufren transformaciones iterativas llamadas *rondas*, cada una de las 16 iteraciones realiza transformaciones y sustituciones, el resultado de cada iteración T_i, es la concatenación de las partes L_i y R_i, es decir, $Ti = L_i \,.\, R_i$ $(1 \leq i \leq 16)$. Para cada uno de estos pasos se verifica que:

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

K_i es la clave para la iteración *i-ésima*
f es una función de cifrado

K_i es una clave de 48 bits generada en cada ronda por una función generadora de claves definida como $K_i = KS\,(i, K)$ siendo K la clave externa de 64 bits y KS es una función de sustitución generada a partir de la clave externa K y dependiente del número de iteración i, que se explicará más adelante.

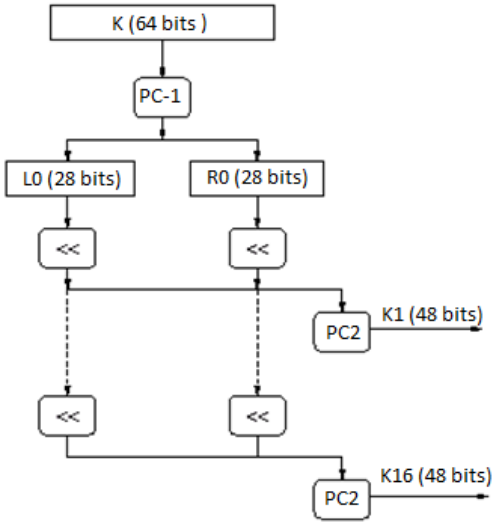
La <u>función de cifrado f</u> transforma los 32 bits del bloque R_{i-1} mediante la subclave Ki, en los 32 bits de $P=f(R_{i-1},K_i)$ según el siguiente esquema:

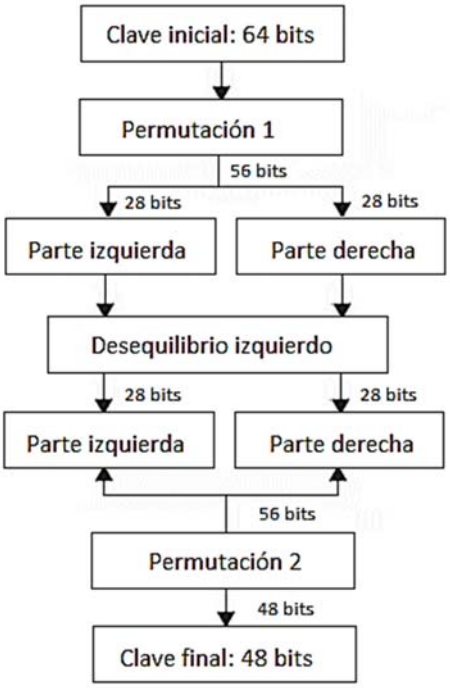


Aquí *E* es una tabla de expansión que transforma R_i de 32 a 48 bits según se muestra:

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

La otra entrada a la función OR-exclusiva es la clave Ki obtenida a partir de una función de generación de claves, en esta función radica toda la seguridad y complejidad del cifrado. El algoritmo que sigue a continuación muestra cómo obtener a partir una clave de 64 bits (compuesta por cualquier de los 64 caracteres alfanuméricos), 16 claves diferentes de 48 bits, cada una de ellas utilizadas en el algoritmo DES:





- En primera instancia, se eliminan los bits de paridad (octavo bit) de cada byte de la clave, para obtener una clave que posea una longitud de 56 bits.

- Se aplica luego una primera permutación llamada Permutación 1 (**PC-1)**, según la siguiente tabla:

PC-1														
	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

- Dividir esta matriz en dos matrices Li y $\mathbf{R}_i$ (izquierda y derecha), cada una de 28 bits:

L_i							
	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

R_i							
	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

- Rotar los dos bloques una posición hacia la izquierda de manera circular, luego los dos bloques de 28 bits se agrupan en un bloque de 56 bits.
- Este bloque pasa por una Permutación 2 (**PC-2)** conformando la clave $\mathbf{K}_i$ de 48 bits

pc-2												
	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

- Iterando el algoritmo se obtienen las 16 claves $\mathbf{K}_1$ a $\mathbf{K}_{16}$ utilizadas en el algoritmo DES.

Una vez obtenido el bloque de 48 bits, se efectúa la operación *or-exclusivo* entre $E(R_{i-1})$ y la clave *i-ésima Ki* y el resultado es dividido en ocho bloques B_j de seis bits.

$$E(R_{i-1}) \oplus K_i = B_1.B_2.B_3.B_4.B_5.B_6.B_7.B_8$$

Cada uno de los bloques B_j se usa como entrada para cada una de las tabla de selección-sustitución S_j (cajas S), dichas cajas realizan una transformación no lineal que da como salida una secuencia de 4 bits, $S_j(B_j)$. Sobre el funcionamiento de cada una de las cajas *S*, que generan $S_j(B_j)$. cada una de estas 8 cajas tiene asociada una matriz de selección definida, por ejemplo, se muestra la matriz de selección S_1 que será aplicada al bloque B_1, en una transformación no lineal:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
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	14	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Sea por ejemplo B_1=101101 se obtendrá $S_1(B_1)$=0001, siguiendo el siguiente procedimiento:

- Con los bits b1=1 y b6=1 se define la fila correspondiente 11.
- Con los bits b2=0, b3=1, b4=1 y b5=0 se define la columna correspondiente 0110=6.
- El elemento seleccionado es el 1, que expresado en binario en 4 bits es $S_1(B_1)$=0001.

Es decir, los 6 bits $B_j = b_1b_2b_3b_4b_5b_6$ se convierten en 4 bits que es la expresión binaria en 4 bits del valor decimal del elemento de la matriz S_j cuya fila, viene determinada por el valor de los bits b_1b_6 y cuya columna está determinada por el número decimal correspondiente al binario $b_2b_3b_4b_5$ de los bits centrales de B_j. A continuación, se muestran las otras siete matrices de selección:

S_2

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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
1	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
1	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Las salidas $S_j(B_j)$, de cada caja, se concatenan para generar 32 bits que van a ser sometidos a la permutación *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
18	13	30	6
22	11	4	25

La salida será de la forma

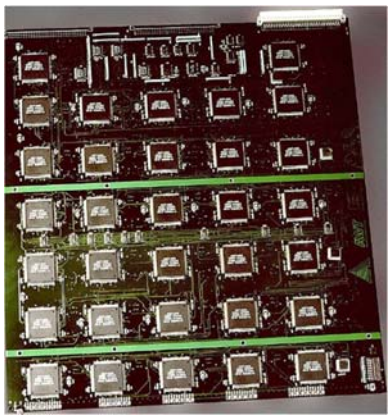
$$P(S_1(B_1).\ S_2(B_2).\ S_3(B_3).\ S_4(B_4).\ S_5(B_5).\ S_6(B_6).\ S_7(B_7).\ S_8(B_8))$$

Hay que notar que esto se itera quince veces, difiriendo en que el resultado de la última ronda se toma como entrada para la permutación inversa.

- Reconexión de bloques izquierdo y derecho o permutación inicial inversa: al final de las iteraciones, los dos bloques $\mathbf{L}_{16}$ y $\mathbf{R}_{16}$ se vuelven a conectar y se someten a una permutación llamada permutación inicial inversa, con la que se obtiene un texto cifrado de 64 bits

IP-1								
	40	8	48	16	56	24	64	32
	39	7	47	15	55	23	63	31
	38	6	46	14	54	22	62	30
	37	5	45	13	53	21	61	29
	36	4	44	12	52	20	60	28
	35	3	43	11	51	19	59	27
	34	2	42	10	50	18	58	26
	33	1	41	9	49	17	57	25

La fuerza bruta sobre estos algoritmos se implementa por hardware, por ejemplo, La máquina de crackeado de DES de la Electronic Frontier Foundation contenía 1,536 chips Deep Crack y podía romper una clave DES por fuerza bruta en días



b) Triple-DES Se encripta tres veces una clave DES. Esto se puede hacer de varias maneras:
- DES-EEE3: Tres encriptaciones DES con tres claves distintas.
- DES-EDE3: Tres operaciones DES con la secuencia encriptar-desencriptar-encriptar con tres claves diferentes.
- DES-EEE2 y DES-EDE2: Igual que los anteriores pero la primera y tercera operación emplean la misma clave.
- Dependiendo del método elegido, el grado de seguridad varía; el método más seguro es el DES-EEE3.

c) AES (Advanced Encription Standard) es un algoritmo de cifrado por bloques que se ha convertido en el estándar.

d) RC2 (Ron's Code o Rivest's Cipher) es un algoritmo de cifrado por bloques de clave de tamaño variable, trabaja con bloques de 64 bits y es tres veces más rápido que el DES en software. Si se elige claves de mayor tamaño es más seguro que el DES ante ataques de fuerza bruta.

e) RC4 es un algoritmo de tamaño de clave variable con operaciones a nivel de byte. Se basa en el uso de una permutación aleatoria y tiene un periodo estimado de más de 10100. Además, es un algoritmo de ejecución rápida en software. Se emplea para encriptación de ficheros y para encriptar la comunicación en protocolos como el SSL (TLS).

f) RC5 es un algoritmo parametrizable con tamaño de bloque variable, tamaño de clave variable y número de rotaciones variable. Los valores más comunes de los parámetros son 64 o 128 bits para el tamaño de bloque, de 0 a 255 rotaciones y claves de 0 a 2048 bits. Fue diseñado en 1994 por Ron Rivest. El RC5 tiene 3 rutinas: expansión de la clave,

encriptación y desencriptación. En la primera rutina la clave proporcionada por el usuario se expande para llenar una tabla de claves cuyo tamaño depende del número de rotaciones. La tabla se emplea en la encriptación y desencriptación. Para la encriptación sólo se emplean tres operaciones: suma de enteros, o-exclusiva de bits y rotación de variables. La mezcla de rotaciones dependientes de los datos y de distintas operaciones lo hace resistente al criptoanálisis lineal y diferencial. El algoritmo RC5 es fácil de implementar y analizar y, de momento, se considera que es seguro.

g) IDEA (International Data Encription Algorithm) es un algoritmo de cifrado por bloques de 64 bits iterativo, la clave es de 128 bits, la encriptación precisa 8 rotaciones complejas. El algoritmo funciona de la misma forma para encriptar que para desencriptar (excepto en el cálculo de las subclaves). El algoritmo es fácilmente implementable en hardware y software, aunque algunas de las operaciones que realiza no son eficientes en software, por lo que su eficiencia es similar a la del DES. El algoritmo es considerado inmune al criptoanálisis diferencial y no se conocen ataques por criptoanálisis lineal ni debilidades algebraicas. La única debilidad conocida es un conjunto de 251 claves débiles, pero dado que el algoritmo tiene 2128 claves posibles no es un problema serio.

h) SAFER (Secure And Fast Encription Routine) es un algoritmo de cifrado por bloques no propietario. Está orientado a bytes y emplea un tamaño de bloque de 64 bits y claves de 64 (SAFER K-64) o 128 bits (SAFER K-128). Tiene un número variable de rotaciones, pero se recomienda un mínimo de seis. El algoritmo original fue considerado inmune al criptoanálisis lineal y diferencial, pero Knudsen descubrió una debilidad en el generador de claves y el algoritmo fue modificado (SAFER SK-64 y SAFER SK-128).

i) Blowfish es un algoritmo de cifrado por bloques de 64 bits desarrollado por Scheiner. Es un algoritmo de tipo Feistel y cada rotación consiste en una permutación que depende de la clave y una sustitución que depende de la clave y los datos. Todas las operaciones se basan en o-exclusivas sobre palabras de 32 bits. La clave tiene tamaño variable (con un máximo de 448 bits) y se emplea para generar varios vectores de subclaves. Este algoritmo está diseñado para 32 bits y es mucho más rápido que el DES. El algoritmo es considerado seguro, aunque se han descubierto algunas claves débiles, un ataque contra una versión del algoritmo con tres rotaciones y un ataque diferencial contra una variante del algoritmo.

Trabajo de investigación formativa 5:
Según asignación investigar en grupo los algoritmos simétricos: DES, TRIPLE-DES, AES, RC2, RC4, RC5, SAFER, IDEA, BLOWFISH, indicando el principio de funcionamiento para la encriptación y desencriptación y las debilidades encontradas en ellos, en cuanto al manejo de claves o ataques por fuerza bruta