SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

4.1.2.MF0489_3. Capítulo 1
Parte 2
Criptografía

JOSÉ PABLO HERNÁNDEZ

5. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA

Principio de Kerchkoff:

“Solo el secreto de la clave proporciona un cifrado seguro”

5. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA

Se distinguen dos tipos de criptografía:

- **criptografía de clave privada**
- **criptografía de clave pública**

5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

Según la cantidad de elementos que se vayan a cifrar, se distinguen dos familias de sistemas de clave privada:

- **cifradores de flujo**
- **cifradores de bloque**

5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

Cifradores de flujo

Permiten el cifrado de uno o pocos símbolos.

Por un lado, la información a cifrar se divide en caracteres o bits.

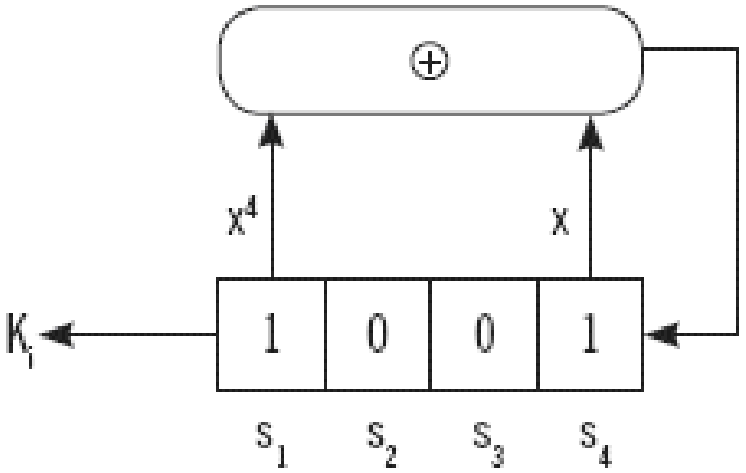
Por otro lado, tanto el emisor como el receptor comparten una clave, denominada serie cifrante, que se corresponde con un conjunto de caracteres o bits aleatorios.

5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

Cifradores de flujo

Ejemplo de generador LFSR

Bits K	Registro	Bits realimentación
	1001	$1 \oplus 1 = 0$
1	0010	$0 \oplus 0 = 0$
0	0100	$0 \oplus 0 = 0$
0	1000	$0 \oplus 1 = 1$
...	...	...
	1001 ⟶	semilla



5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

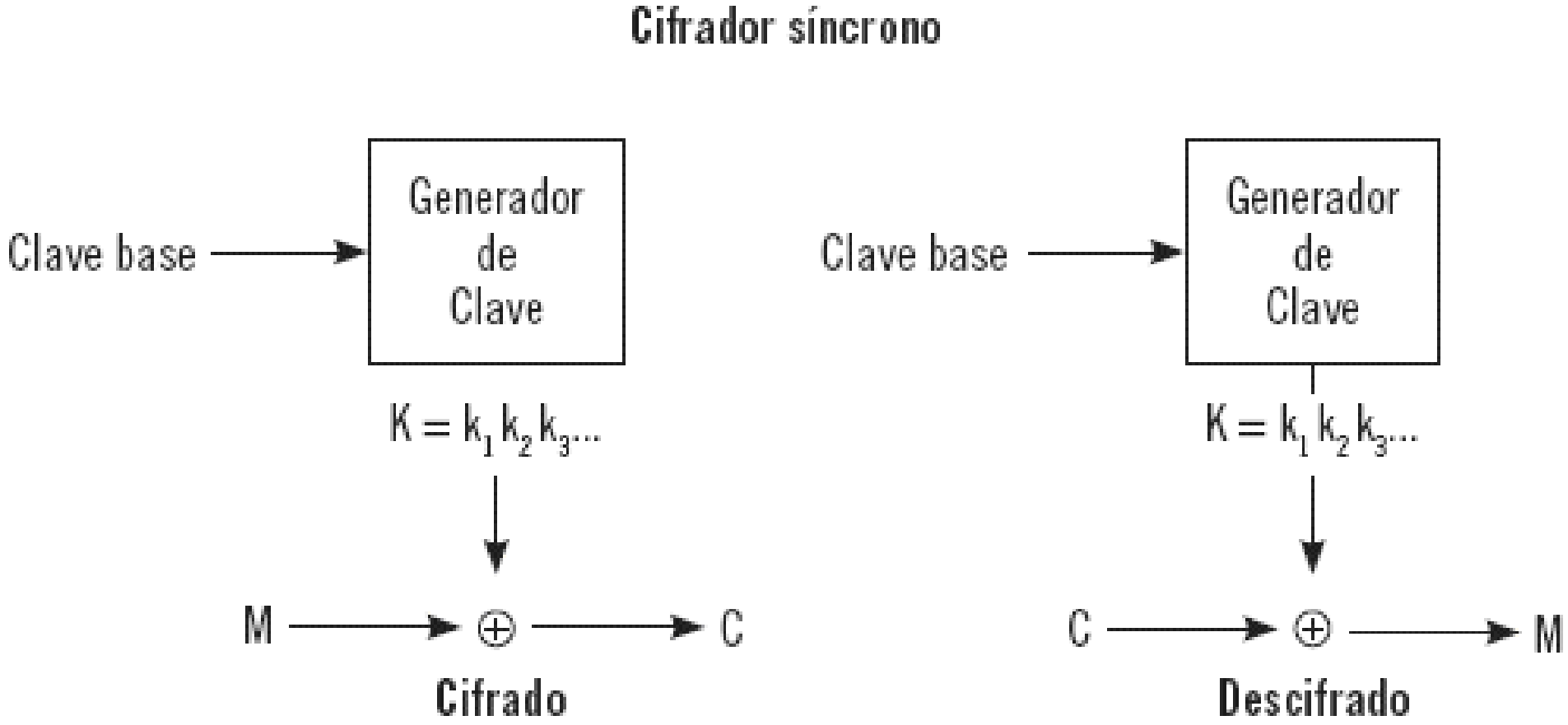
Cifradores de flujo

Se diferencian en:

- **Cifradores síncronos**
- **Cifradores asíncronos**

5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

Cifradores de flujo. Cifradores síncronos



5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

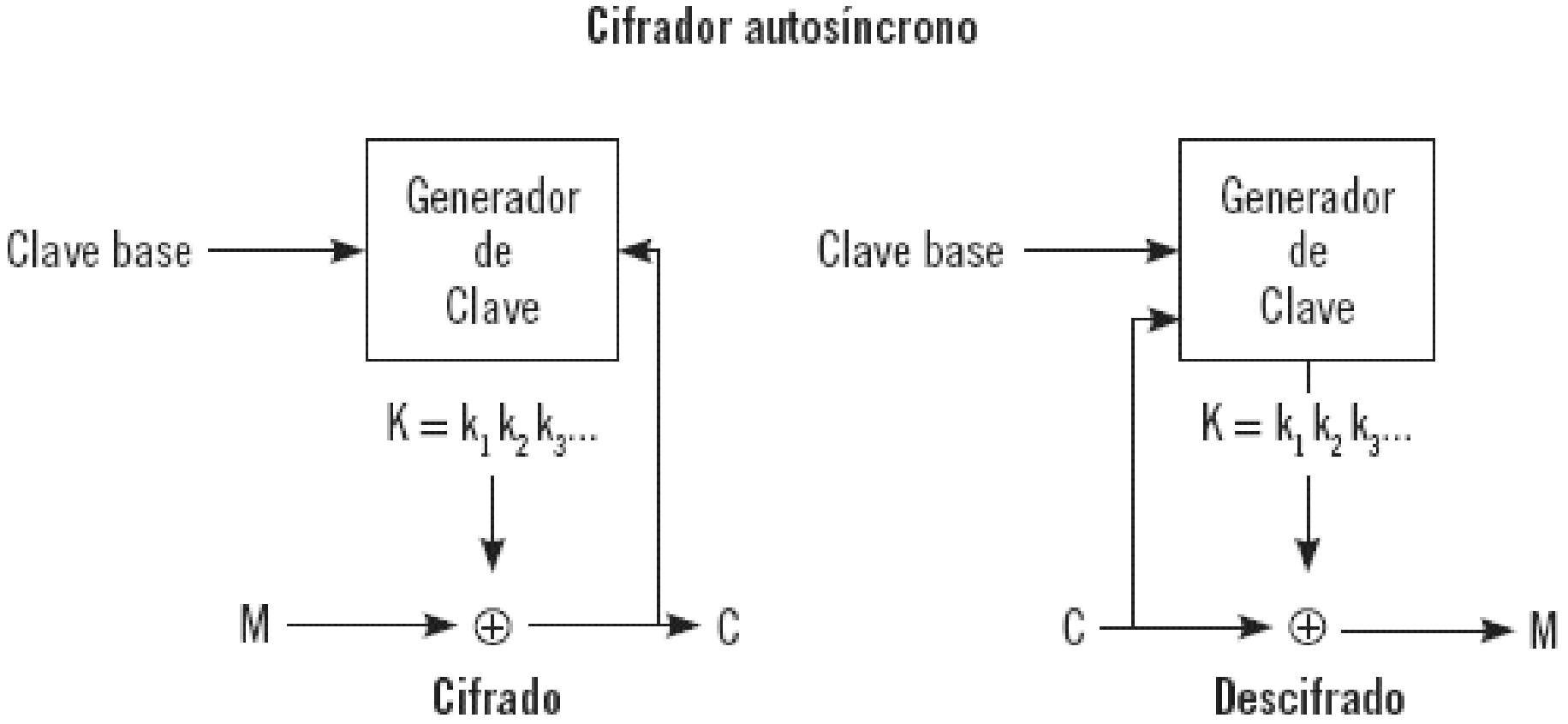
Cifradores de flujo. Cifradores síncronos

Propiedades:

- **Sincronización entre emisor y receptor.**
- **Inexistencia de errores de propagación.**
- **Ataques activos.**

5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

Cifradores de flujo. Cifradores asíncronos



5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

Cifradores de flujo. Cifradores asíncronos

Propiedades:

- **Sincronización automática de emisor y receptor.**
- **Errores limitados de propagación.**
- **Ataques activos.**
- **Difusión estadística en el texto en claro.**

5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

Cifradores de bloque

Permiten el cifrado de un gran conjunto de símbolos. La información a cifrar se divide en bloques de una determinada longitud (tamaños típicos 64, 128 y 256 bits) y cada uno de ellos se cifra con una misma clave.

5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

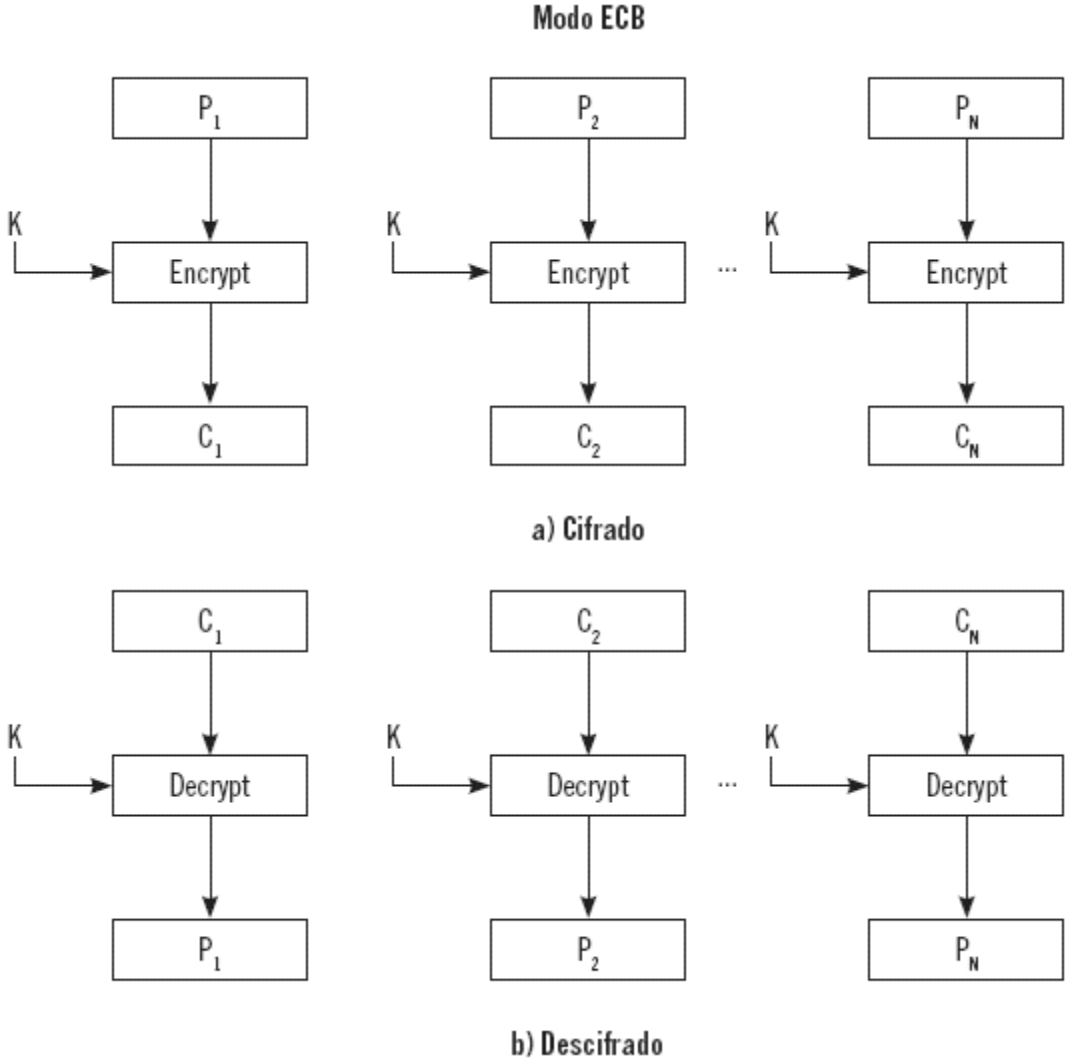
Cifradores de bloque

Se pueden distinguir, entre otros:

- **Electronic Code Book (ECB)**
- **Cipher Block Chaining (CBC)**
- **Cipher Feedback (CFB)**
- **Output Feedback (OFB)**
- **Counter Mode (CTR)**

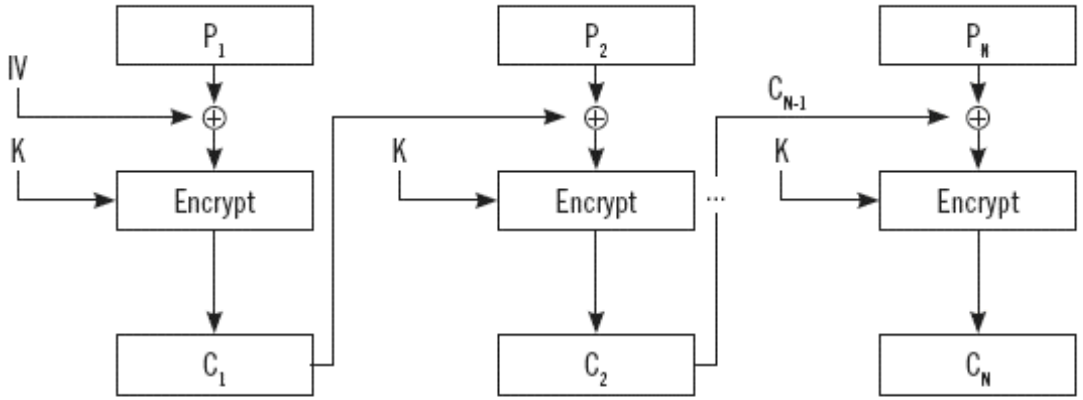
5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

Cifradores de bloque. Electronic Code Book (ECB)



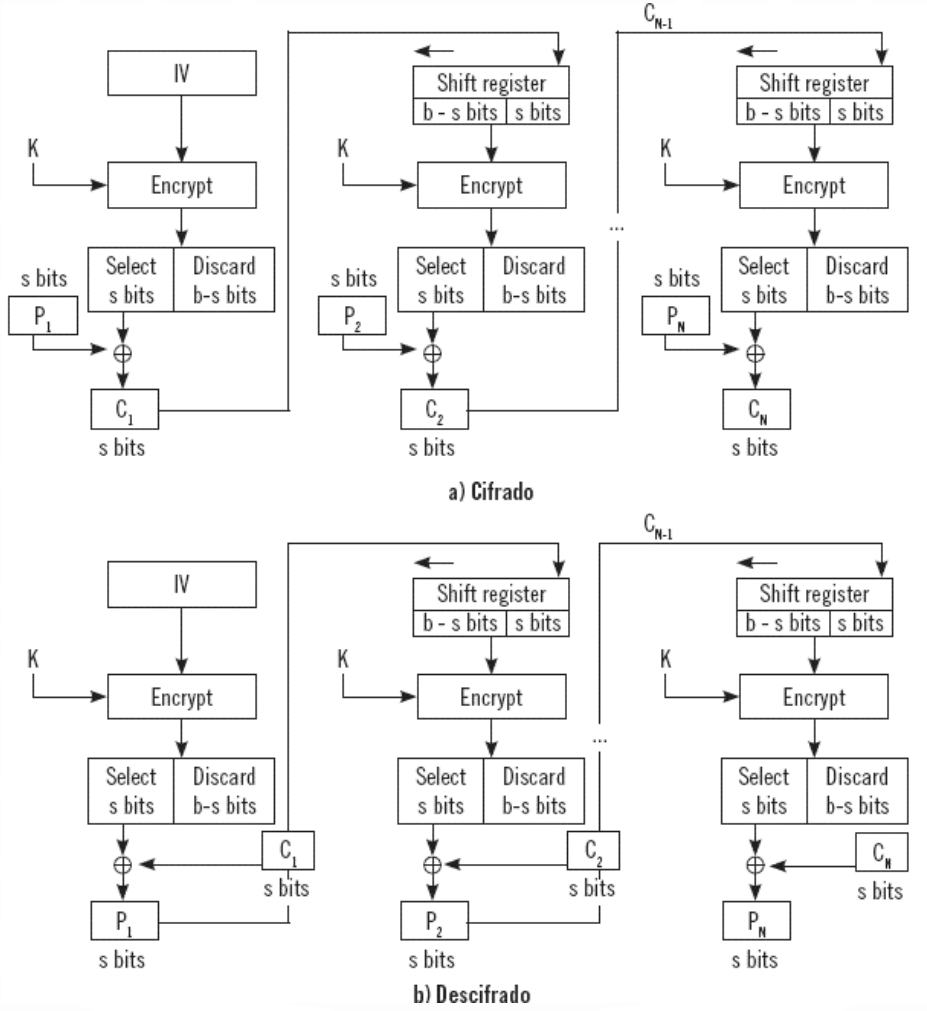
5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

Cifradores de bloque. Cipher Block Chaining (CBC)



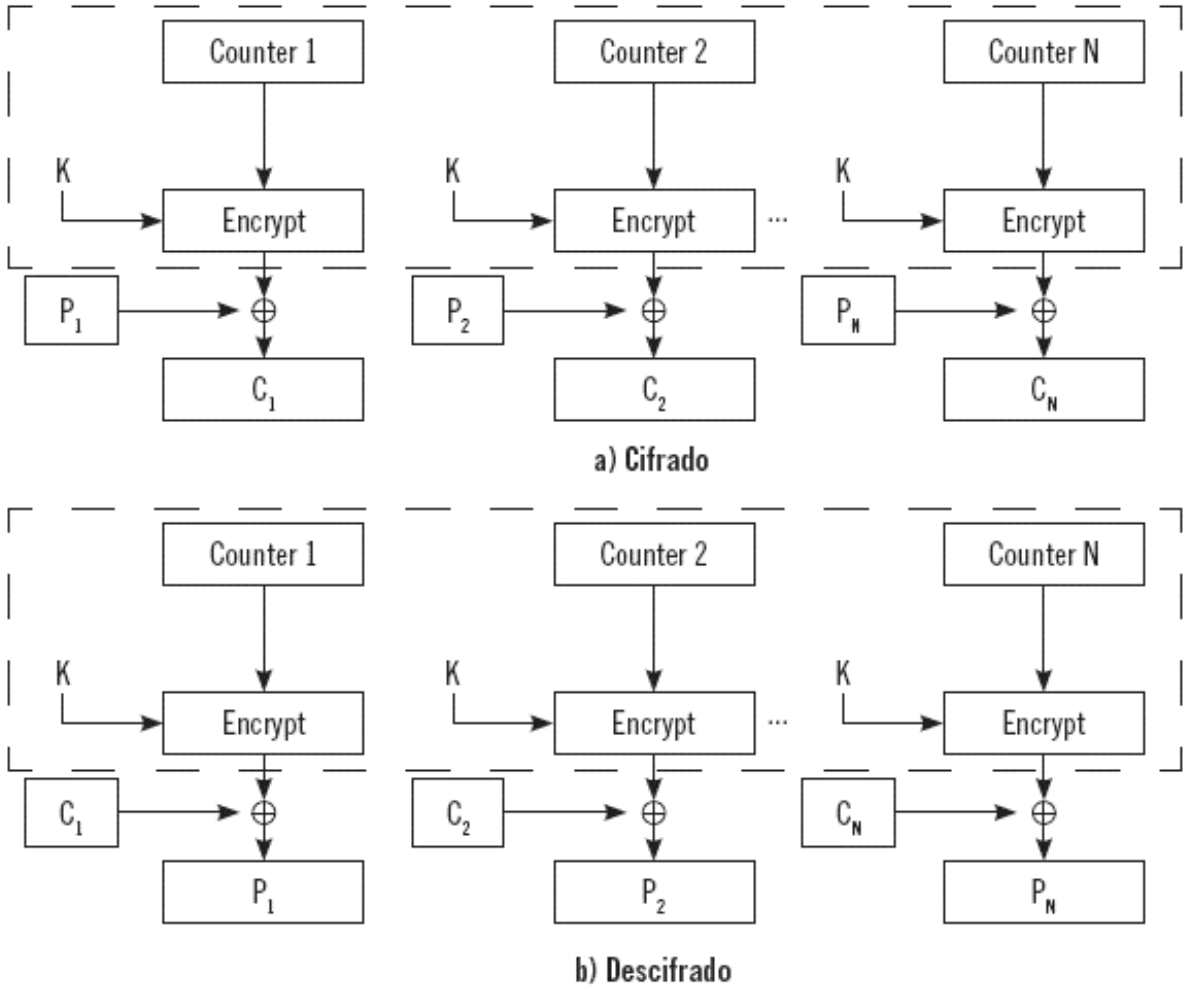
5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

Cifradores de bloque. Cipher Feedback (CFB)



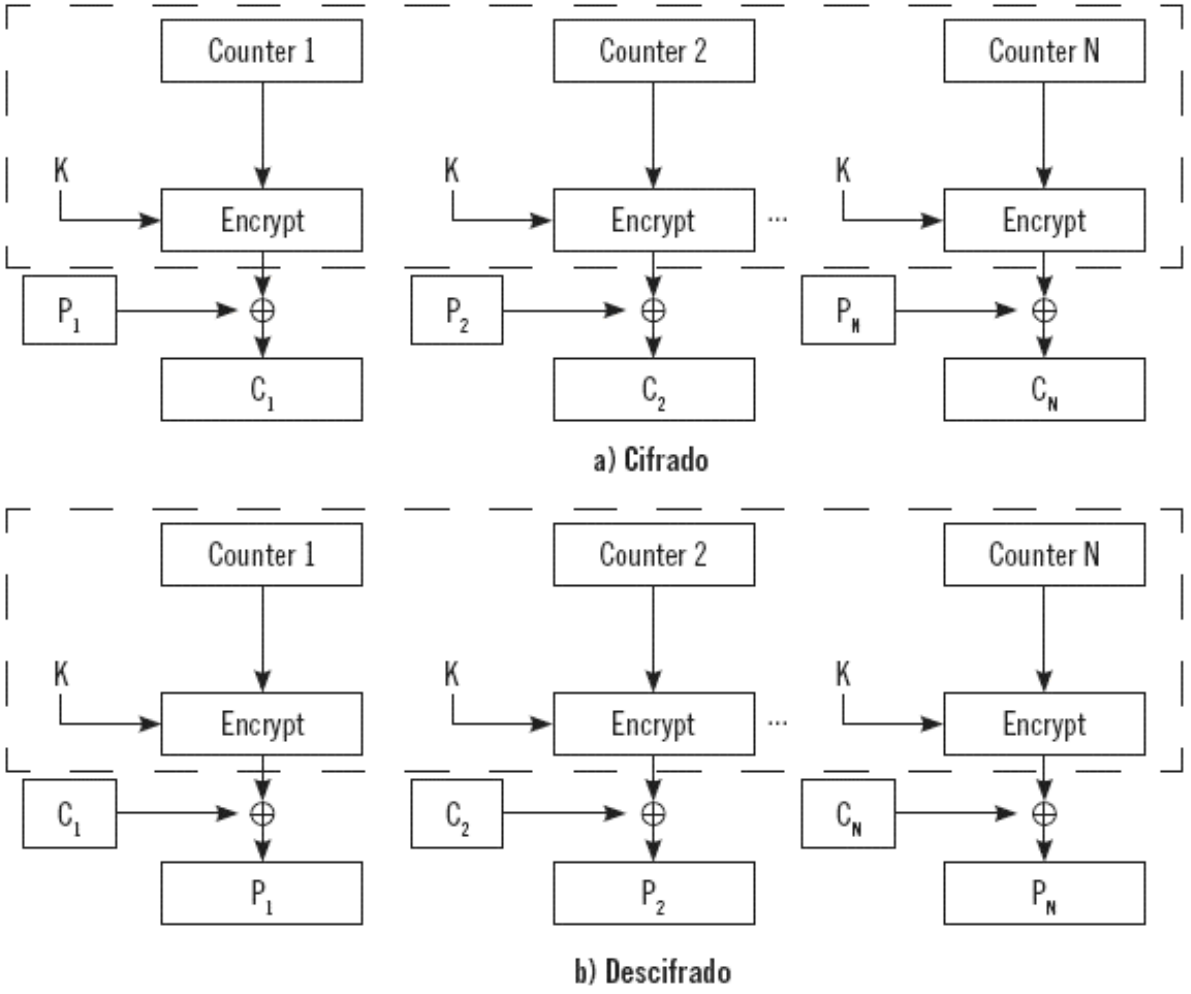
5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

Cifradores de bloque. Cipher Feedback (OFB)



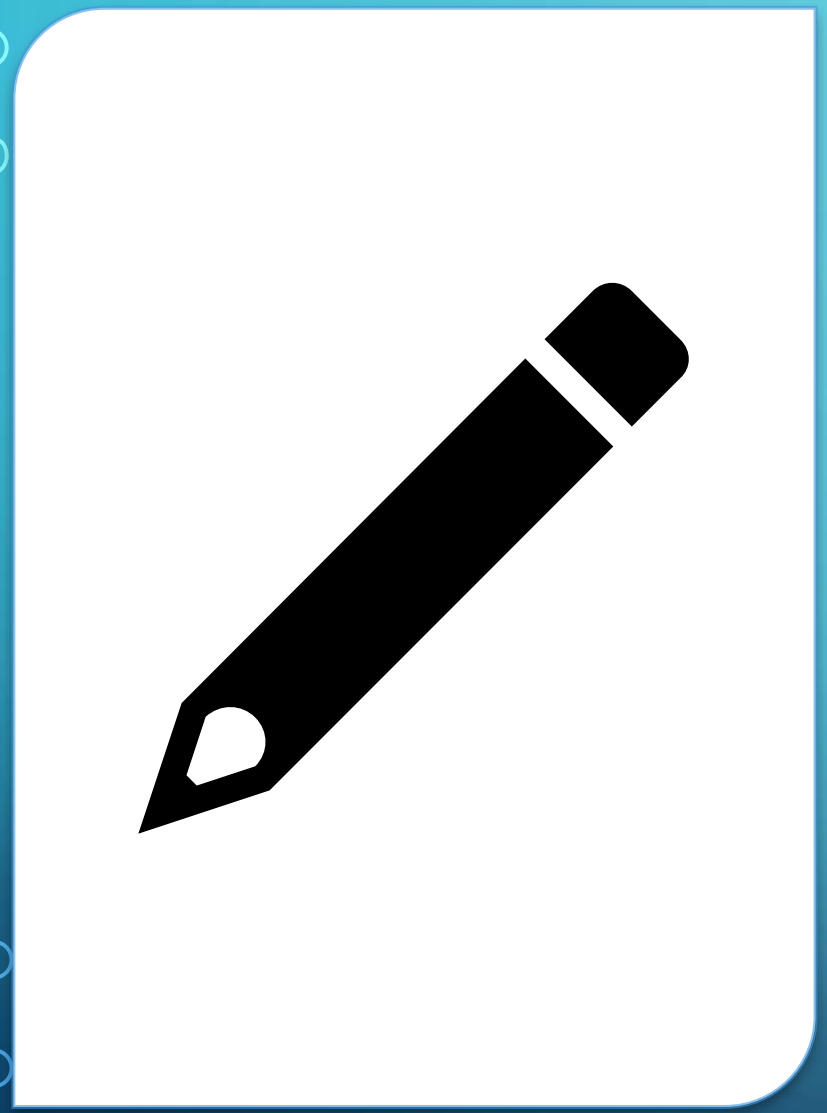
5.1. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA

Cifradores de bloque. Counter Mode (CTR)



Ejemplo.

EN EL DEPARTAMENTO DE SEGURIDAD DE UNA EMPRESA DE DIFUSIÓN DE MÚSICA POR INTERNET (STREAMING) DUDAN SOBRE CUÁL ES EL MEJOR MODO DE CIFRADO PARA OFRECER SU SERVICIO SOLO A LOS USUARIOS QUE HAYAN PAGADO LA CUOTA. LA DUDA APARECE ENTRE UN CIFRADOR DE BLOQUE Y UNO DE FLUJO. ¿CUÁL SERÍA LA OPCIÓN MÁS RECOMENDABLE?



Ejemplo. Solución.

LA TRANSMISIÓN DE MÚSICA A TRAVÉS DE INTERNET CORRESPONDE AL SISTEMA DE ENVÍO DE INFORMACIÓN EN FORMA DE FLUJO DE DATOS. ASÍ, PARA QUE EL USUARIO PUEDA ESCUCHAR LA MÚSICA SIN INTERRUPCIONES, ES NECESARIO QUE EL ENVÍO DE LA SECUENCIA MUSICAL NO SE DETENGA.

LA UTILIZACIÓN DE UN CIFRADOR DE BLOQUE PODRÍA CAUSAR LEVES RETRASOS EN EL ENVÍO, PUES LAS OPERACIONES SE APLICAN SOBRE UN CONJUNTO DE BYTES. EN OTRAS PALABRAS, HASTA QUE NO SE CIFRA UN BLOQUE NO SE PUEDE ENVIAR.

POR ESTE MOTIVO, UN CIFRADOR DE FLUJO ES MÁS ADECUADO PARA ESTE ESCENARIO, YA QUE OPERA A NIVEL DE BIT Y, POR TANTO, PERMITE QUE LOS DATOS SE ENVÍEN DE MANERA CONSTANTE.

5.2. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PÚBLICA

5.2. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PÚBLICA

En función de la relación matemática utilizada, se distinguen:

Reversibles: las operaciones de cifrar y descifrar el mensaje se anulan entre sí, por lo que es posible obtener el mensaje en claro a partir del cifrado.

Irreversibles: no es posible obtener el texto en claro a partir del texto cifrado.

5.2. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PÚBLICA

Los sistemas de clave pública han de basarse en problemas matemáticos (conocidos como problemas NP y NP-completos) que sean complejos de resolver con la ayuda de ordenadores.

Los algoritmos más conocidos son:

- **Algoritmo RSA,** basado en el problema de la factorización
- **Algoritmo El Gamal,** basado en el problema del logaritmo discreto

5.2. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PÚBLICA

Problema de la factorización

Calcular la descomposición de un número como producto de números primos elevados a potencias.

Por ejemplo:

3630 = 10·363 = 2·3·5·121 = 2·3·5·11^2

5.2. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PÚBLICA

Problema del logaritmo discreto

El logaritmo consiste en calcular la potencia x, a la que hay que elevar un número, utilizando como base a, para obtener otro número dado b, logab=x.

Por ejemplo:

ln 375 = 5,926926 log10 375 = 2,574031 log2 375 = 8,550747

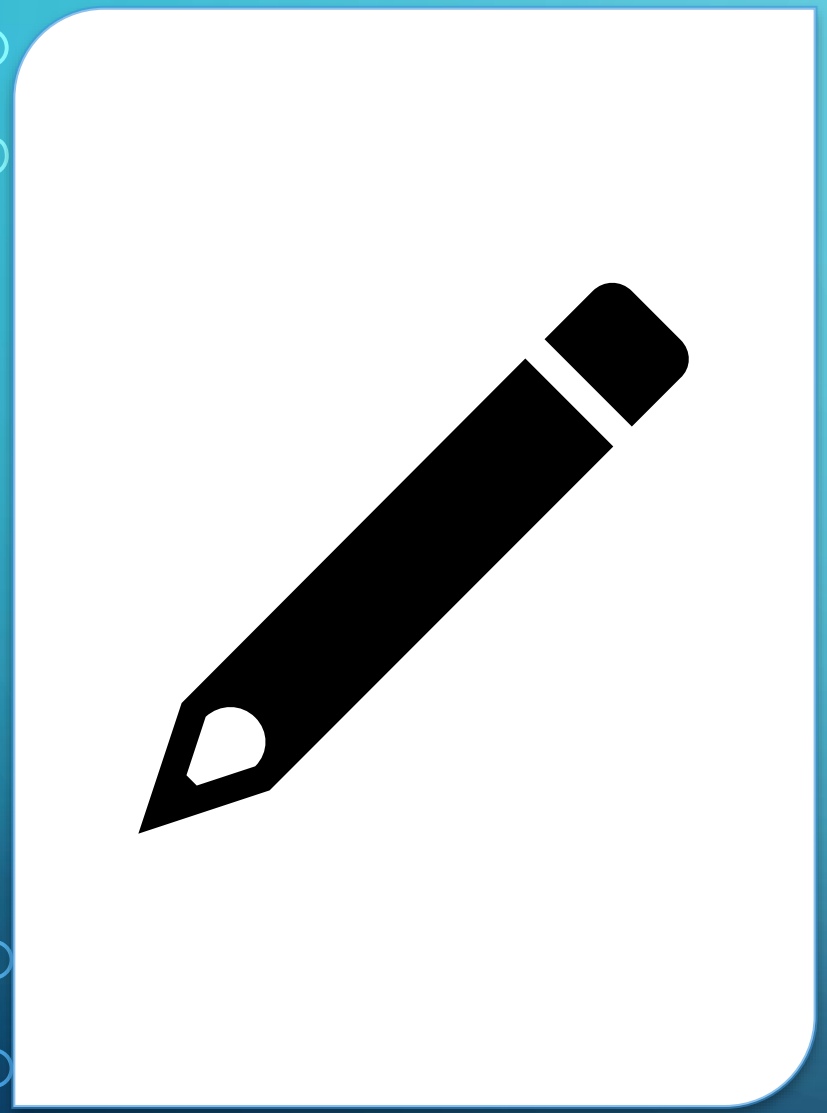
5.3. CRIPTOGRAFÍA DE CLAVE PÚBLICA, CURVAS ELÍPTICAS

Entre las ventajas principales de esta rama de la criptografía está la utilización de claves de menor tamaño que en criptosistemas de clave pública.

En la actualidad, la criptografía de curvas elípticas es susceptible de ser utilizada en dispositivos móviles, tarjetas inteligentes o redes de sensores, entre otras aplicaciones

Ejemplo.

UNA EMPRESA DE GESTIÓN DE FLOTAS DE TAXIS NECESITA ASEGURAR SUS COMUNICACIONES. PARTICULARMENTE, SE DISTINGUE LA COMUNICACIÓN EN LA QUE LOS CLIENTES CONTACTAN CON LA CENTRAL PARA RESERVAR LOS TAXIS, Y LA QUE USA LA CENTRAL PARA AVISAR A LOS TAXISTAS. SE PRETENDE DAR CABIDA AL USO DE DISPOSITIVOS MÓVILES POR PARTE DE LOS CLIENTES. ¿EN CUÁL UTILIZARÍA CRIPTOGRAFÍA SIMÉTRICA Y EN CUÁL CURVAS ELÍPTICAS?



Ejemplo. Solución.

EN LA COMUNICACIÓN DE LOS CLIENTES CON LA CENTRAL NO SE PUEDE ASUMIR UN CONOCIMIENTO PREVIO ENTRE LAS PARTES: PODRÍA SER UN NUEVO CLIENTE QUE NUNCA ANTES HA UTILIZADO EL SERVICIO. POR ESTE MOTIVO, PARECE MÁS ADECUADA LA CRIPTOGRAFÍA DE CLAVE PÚBLICA. DADO QUE PRETENDEN UTILIZARSE DISPOSITIVOS MÓVILES, SERÍA RECOMENDABLE UTILIZAR CRIPTOSISTEMAS QUE SEAN LIGEROS, COMO LOS BASADOS EN CRIPTOGRAFÍA DE CURVAS ELÍPTICAS.

POR SU PARTE, EN LA COMUNICACIÓN CENTRAL-TAXISTAS SÍ HAY UN CONOCIMIENTO Y UNA RELACIÓN PREVIA. POR ESTE MOTIVO ES MÁS CONVENIENTE EL USO DE ALGORITMOS DE CRIPTOGRAFÍA SIMÉTRICA (TALES COMO DES) QUE, ADEMÁS, TIENEN LA VENTAJA DE SER MÁS RÁPIDOS QUE LOS ASIMÉTRICOS.

6. CARACTERÍSTICAS Y ATRIBUTOS DE LOS CERTIFICADOS DIGITALES

Un certificado digital es un documento electrónico que vincula a una entidad (persona, servidor, etc.) con un par de claves que pueden utilizarse tanto para firmar digitalmente como para cifrar.

La clave pública se almacena dentro del certificado mientras que la privada tendrá que ser almacenada y protegida por la entidad correspondiente.

6. CARACTERÍSTICAS Y ATRIBUTOS DE LOS CERTIFICADOS DIGITALES

En base a las clases de certificados establecidas por VeriSign, se encuentran los certificados de:

- **Clase 1**, para los usuarios, especialmente para el correo.
- **Clase 2**, para las organizaciones, de modo que se pueda probar su identidad.
- **Clase 3**, para los servidores y las firmas de los programas.
- **Clase 4**, para trámites online entre empresas.
- **Clase 5**, para empresas privadas y de seguridad gubernamentales

7. PROTOCOLOS DE INTERCAMBIO DE CLAVES

Los protocolos de intercambio de claves son mecanismos por los que un par de entidades se comunican sobre un canal inseguro para generar una clave secreta común.

7. PROTOCOLOS DE INTERCAMBIO DE CLAVES

Se han de considerar las siguientes características:

- **Naturaleza de la autenticación**
- **Reciprocidad de la autenticación**
- **Frescura de la clave**
- **Control sobre la clave**
- **Eficiencia**
- **Requisitos de tercera parte**
- **Uso de certificados, en caso de utilizarse**

7.1. PROTOCOLO DIFFIE-HELLMAN

1.A y B acuerdan dos números *p*, *g*. El número *p* es un número primo muy grande (ej. 300 dígitos decimales). Por su parte, g es un número que cumple que, si dividimos sus sucesivas potencias entre el número p, se obtienen todos los restos entre 1 y p-1.
2.A escoge un número aleatorio *a* y computa $M_A = g^a mod(p)$ y, enviando M_A a la entidad B. Recuérdese que la notación a mod(b) = r se interpreta como el resto "r" de dividir "a" entre "b".
3.B escoge un número aleatorio *b* y calcula $M_B = g^b mod(p)$, el cual envía a A.
4.B computa $K_s = (M_A)^b mod(p)$.
5.A computa $K_s = (MB)^a mod(p)$.