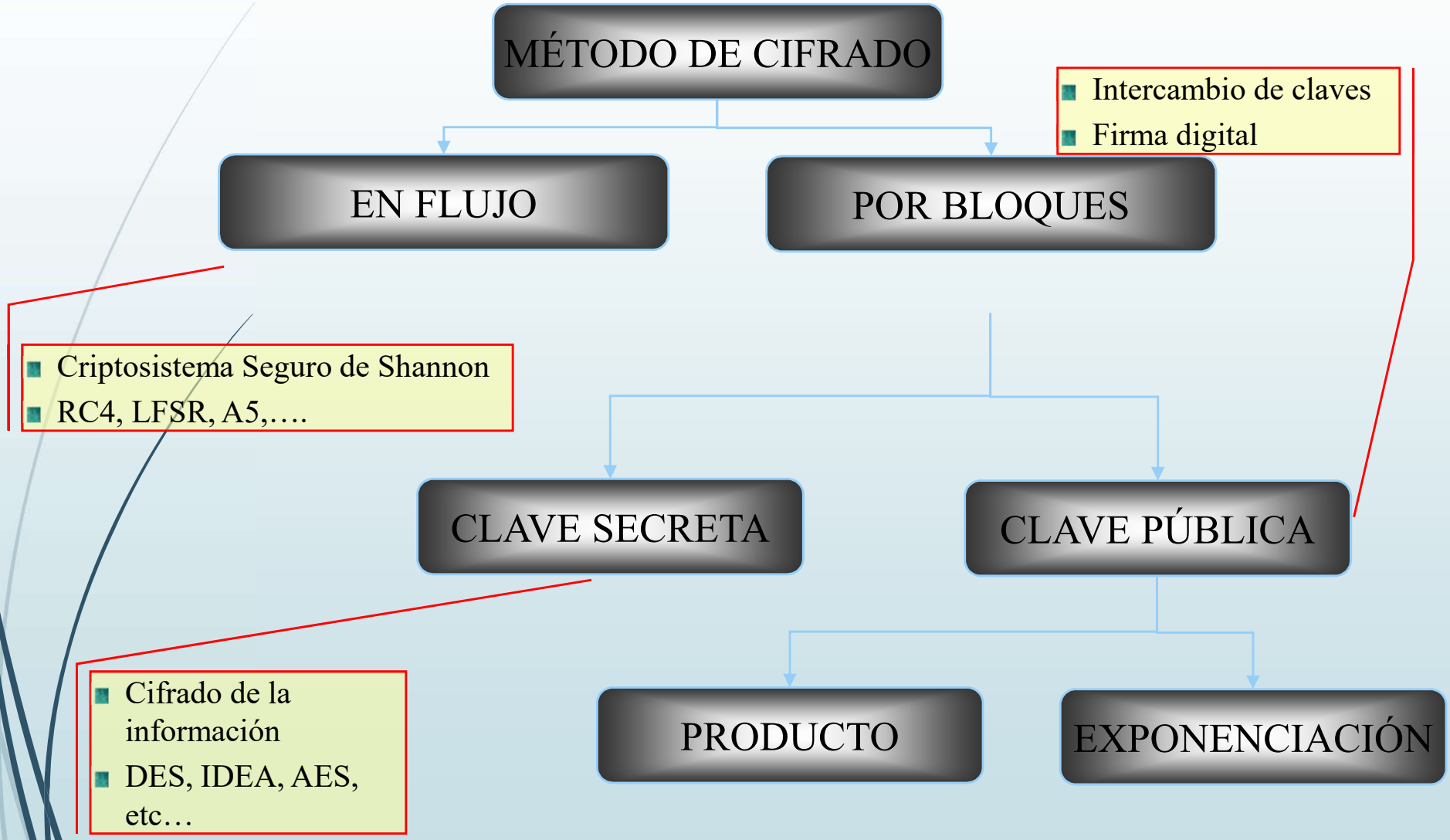
Introducción a criptosistemas modernos

- Cuando se habla de **criptografía moderna** o criptosistemas modernos, en contraposición a los estudiados anteriormente y denominados clásicos, se hace referencia a aquellos sistemas de cifrado, bien de clave secreta, bien de clave pública, que
  - por una parte, **realizan el cifrado en bits**, orientado a todos los caracteres del sistema de representación numérica que utilicen, es decir ASCII o ANSI, sin que necesariamente el módulo de trabajo deba coincidir con el número de elementos del alfabeto o código utilizado

Por lo general, mediante una operación algebraica dentro de un cuerpo finito

  - y por otra, **basan su seguridad en la fortaleza de la clave** y no en el secreto de un algoritmo de cifrado.

Clasificación de los criptosistemas modernos



Introducción al cifrado en flujo

- Usa el método de cifrado propuesto por Vernam, que cumple con las ideas de Shannon sobre criptosistemas con secreto perfecto:
  - El espacio de claves es igual o mayor que el de los mensajes.
  - Las claves son equiprobables.
  - La secuencia de clave se usa una sola vez y luego se destruye (one-time pad).

- Que la clave sea tan larga como el mensaje genera una serie de problemas:
  - la secuencia de bits de la clave **deberá enviarse** al destinatario a través de un canal que sabemos es inseguro.
  - si la secuencia es "**infinita**", desbordaríamos la capacidad del canal de comunicaciones.
  - Si se utiliza un **canal seguro** para enviar la clave, ¿por qué entonces no se envía directamente el texto en claro y nos dejamos de historias?

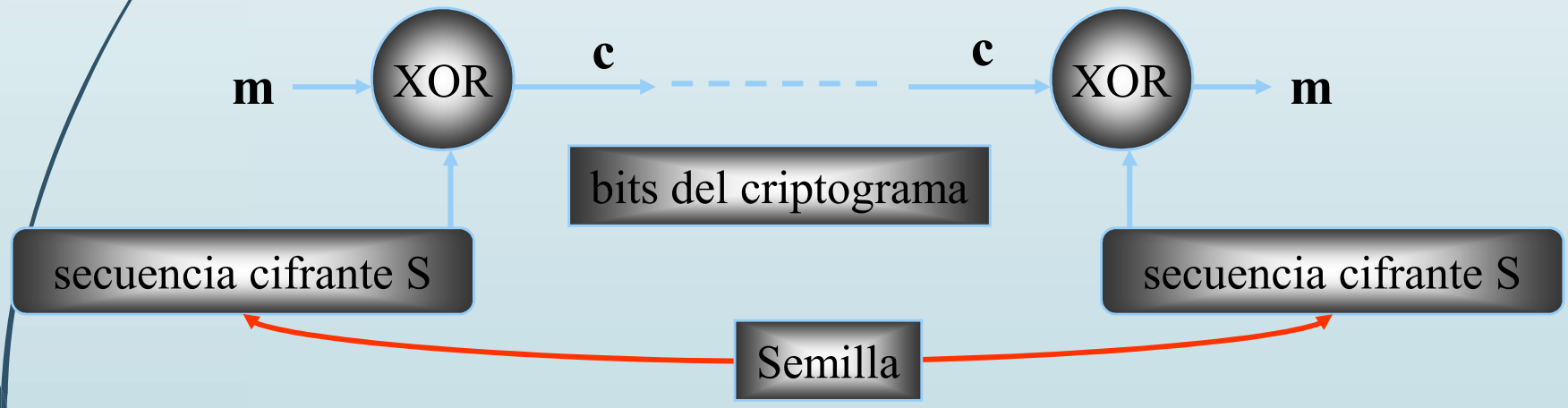
Solución

La solución consiste en generar una secuencia pseudoaleatoria con un algoritmo determinístico a partir de una semilla de sólo unas centenas de bits. Esta semilla es la que se envía al receptor por un canal seguro.

Introducción al cifrado en flujo

- El mensaje en claro se leerá bit a bit.
- Se realizará una operación de cifrado (normalmente la función XOR) con una secuencia cifrante de bits S que debe cumplir ciertas condiciones:
  - Un período muy alto.
  - Aleatoriedad en sus propiedades.

Esquema



Cifrado en bloque con clave secreta

- El texto en claro se **fracciona en bloques** de un tamaño constante y **se aplica**, con la misma clave, **el algoritmo** a **cada bloque** de forma independiente.

- El cifrado se realiza con una clave secreta

- Algunos de los más conocidos son
  - **DES** (*Data Encryiption Standard)* por su uso en aplicaciones bancarias.
  - **IDEA** (*International Data Encryption Algorithm)* por su uso en el cifrado de correo electrónico.
  - **AES** (*Advanced Encryption Standard*): nuevo estándar avanzado de cifrado del Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST) ***(Rijndael)***

Cifrado en bloque con clave secreta

ALGORITMOS MÁS UTILIZADOS

- AES
- DES (Triple DES)
- Serpent
- Blowfish, Twofish

OTROS ALGORITMOS

- Camellia
- CAST-128
- IDEA
- RC2, RC5, RC6
- SEED
- ARIA
- Skipjack
- TEA, XTEA

Cifrado en bloque con clave secreta

Debilidades del cifrado con clave secreta

- **Mala gestión de claves:** para una red de n usuarios el número de claves es $O(n^2)$. Para un número grande de usuarios es intratable👎.
- **Mala distribución de claves:** no existe posibilidad de enviar, de forma segura, una clave a través de un medio inseguro👎.
- **No tiene firma digital:** aunque es posible autentificar el texto en claro mediante una marca, no es posible firmarlo digitalmente👎.

Mala gestión de claves 👎.
Mala distribución de claves 👎.
No tiene firma digital 👎.

¿Tiene algo de bueno el cifrado en bloque con clave secreta?

Sí, la velocidad de cifrado es muy alta 👍

Cifrado en bloque con clave pública

- Como ya se ha comentado, uno de los mayores **inconvenientes** que presentan los sistemas de clave secreta cuando existe un gran número de usuarios, es que cada par de ellos debe poseer su clave secreta, lo que conlleva gran dificultad en la distribución segura de esas claves.

- Un sistema de clave pública permite la comunicación cifrada entre dos usuarios sin necesidad de compartir una clave.

Cifrado en bloque con clave pública

- La idea fundamental de **Diffie y Hellman** (principios de la década de los 70) para la definición de un criptosistema de clave pública proviene de la existencia de funciones unidireccionales.

- Empezó a ser conocido a través de su aplicación en los **sistemas de correo electrónico seguro** (PGP y PEM) al permitir incluir una firma digital adjunta al documento enviado.

- **Cada usuario tiene dos claves**, una secreta o privada y otra pública, inversas dentro de un conjunto finito.

Funciones unidireccionales

- Una función $f:A \longrightarrow B$ se dice ***unidireccional*** si $\forall a \in A$ **resulta fácil**, computacionalmente, **calcular f(a)**, mientras que $\forall b \in f(A)$ **no es computacionalmente factible** encontrar un $a \in A$ tal que **f(a)=b**.

- Este tipo de funciones no debe ser confundido con aquellas que no tienen inversa por no ser biyectivas.

- Son funciones matemáticas de un solo sentido (*one-way functions*) que permiten usar el sentido directo (de cálculo fácil) para cifrar y descifrar y el sentido inverso (de cálculo difícil) para los ataques.

- Un ejemplo sencillo de función **potencialmente unidireccional es el producto de números enteros**.
  - **Multiplicar dos enteros** de cien cifras cada uno **resulta rápido** incluso para el ordenador más modesto, en cambio el más potente ordenador equipado del mejor algoritmo de factorización conocido no sería capaz de **descomponer el producto** antes del tiempo previsto para el fin del Universo.

Ejemplos de funciones unidireccionales

Problema de la factorización

Cálculo directo: producto de dos primos grandes $p*q = n$
Cálculo inverso: factorización de número grande $n = p*q$

Problema del logaritmo discreto

Cálculo directo: exponenciación discreta $b = a^x \bmod n$
Cálculo inverso: logaritmo discreto $x = \log_a b \bmod n$

Problema de la mochila

Cálculo directo: suma de elementos de mochila con trampa
Cálculo inverso: suma de elementos de mochila sin trampa

Problema de la raíz discreta

Cálculo directo: cuadrado discreto $x = a*a \bmod n$
Cálculo inverso: raíz cuadrada discreta $n = \sqrt{a} \bmod n$

Criptosistemas de clave pública

- Un criptosistema de clave pública está formado por un conjunto de claves K y para cada $k \in K$ de un conjunto de mensajes en claro M_k, un conjunto de mensajes cifrados C_k, y un par de funciones $E_k: M_k \longrightarrow C_k$ y $D_k: C_k \longrightarrow M_k$ tales que

$$\mathbf{D_k[E_k(m)]=m \quad \forall m \in M_k}$$

- Naturalmente, debe exigirse que a partir de la clave k la elaboración de los algoritmos de cifrado E_k y descifrado D_k sea sencilla.

- La **diferencia fundamental** con los criptosistemas de clave secreta es que **E_k debe ser una función unidireccional**.

Criptosistemas de clave pública

- Un sistema criptográfico de clave pública funciona del siguiente modo:
  - cada usuario dispone de una clave personal $k \in K$ que utiliza para obtener sus algoritmos de cifrado E_k y D_k.
  - La **transformación de cifrado E_k es registrada en un fichero público** mientras que la de descifrado **D_k es de uso privado**.
  - Al ser **E_k una función unidireccional** sólo el usuario al que vaya destinado el mensaje **podrá aplicar el algoritmo de descifrado D_k inverso** al de cifrado E_k.

Criptosistemas de clave pública

- Si, por ejemplo, el usuario A tiene una clave k_A y el usuario B desea enviarle un mensaje $m \in M$, deberá cifrarlo haciendo uso del algoritmo público de cifrado transmitiéndole .

$$c = E_{K_A}(m)$$

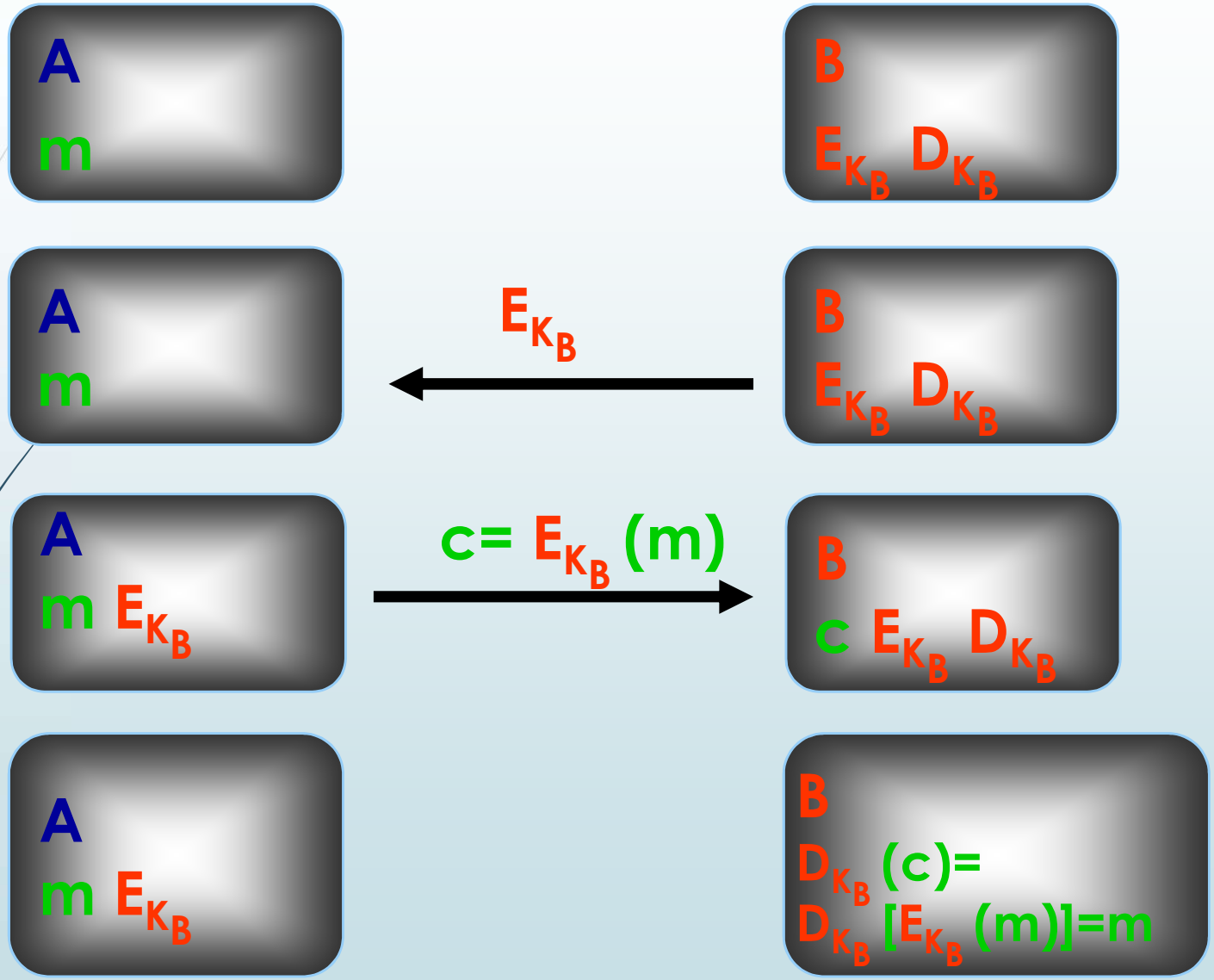
- Con la ayuda de la función unidireccional y de su transformación inversa sólo conocida por A, este usuario descifrará c

$$D_{K_A}(c) = D_{K_A}\left[E_{K_A}(m)\right] = m$$

- Conviene hacer notar que, a diferencia de los sistemas de clave privada, si el usuario B cifra el texto en claro m para enviárselo a A y por algún motivo pierde el mensaje original, si desea recuperarlo se encuentra en la misma situación que cualquier criptoanalista. El criptograma sólo es descifrable mediante .

$$D_{K_A}$$

CRIPTOSISTEMA DE CLAVE PÚBLICA



Firma digital

- Estamos pasando, gracias a Internet y a la aparición de las nuevas tecnologías, de un sistema tradicional de realizar operaciones comerciales a uno nuevo que las efectúa mediante métodos electrónicos.

- Resulta necesario contar con técnicas electrónicas que suplanten la tradicional firma autógrafa y dar así validez a documentos electrónicos.

- La firma digital se justifica desde el momento en que los contratos, las transacciones económicas, las compras, etc. se realizan on-line

Firma digital

- Dos problemas aquejan a estos documentos electrónicos:

- ***Confidencialidad***: Capacidad de mantener un documento electrónico inaccesible a todos, excepto a una lista determinada de personas.
  - Se resuelve con métodos de cifrado.

- ***Autenticidad***: Capacidad de averiguar de forma segura e irrevocable la procedencia del mensaje.
  - Se resuelve con técnicas como la firma digital.

Firma digital

- Si A desea firmar digitalmente el mensaje m, envía el mensaje cifrado $c=E_{k_B}(m)$ al usuario B y para firmarlo,
  - en primer lugar calcula su **rúbrica** cifrando el mensaje a enviar con su clave secreta, $r= D_{k_A}(m)$, y
  - a continuación determina su firma para el mensaje m, cifrando con la clave pública de B esa rúbrica, $s= E_{k_B}(r)= E_{k_B}[D_{k_A}(m)]$.

- B verifica la firma digital de A determinando,
  - en primer lugar, la rúbrica de A, $D_{k_B}(s) = D_{k_B}[E_{k_B}(r)]$, y
  - a continuación comprobando que $E_{k_A}(r) = E_{k_A}[D_{k_A}(m)]$ coincide con el mensaje m.

Esquema de firma digital sin cifrado