Criptosistemas simétricos: Flujo

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González

uc3m | Universidad Carlos III de Madrid

COSEC

CC BY NC SA

ÍNDICE

- 6. Criptosistemas simétricos: Flujo
  - Introducción
  - Tipos
  - Serie cifrante
  - PRNG criptográficos
    - LFSR
  - Ventajas y desventajas
  - RC4

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 6. Criptosistemas simétricos: Flujo
  - **Introducción**
  - Tipos
  - Serie cifrante
  - PRNG criptográficos
    - LFSR
  - Ventajas y desventajas
  - RC4

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

INTRODUCCIÓN

- CARACTERÍSTICAS DE LOS CIFRADORES DE FLUJO

- Descomponen el mensaje en bytes (o en bits):

$$M = m_1, m_2, \ldots m_n$$

- Cifran cada m_i con el correspondiente k_i de la serie cifrante
  - idealmente infinita y aleatoria
    - $K = k_1, k_2, \ldots k_n, k_{n+1}, \ldots$

- $E_K (M) = E_{k1} (m_1) E_{k2} (m_2) \ldots E_{kn} (m_n)$

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

INTRODUCCIÓN

- CIFRADO DE VERNAM. ONE-TIME-PAD

  - Cifrado: $E(M) = M \oplus K = m_1+k_1, m_2+k_2, \ldots, m_n+k_n$

```
    1 0 0 1 1 1 0 1   M
⊕   0 0 1 0 0 1 0 1   K
    -----------------
    1 0 1 1 1 0 0 0   C
```

  - Descifrado: $M = E(M) \oplus K$
  - Shannon demostró que el cifrado de Vernam es incondicionalmente seguro si la clave K:
    - Es realmente aleatoria
    - Se usa una sola vez
    - Es de longitud igual o mayor que M

BY NC SA

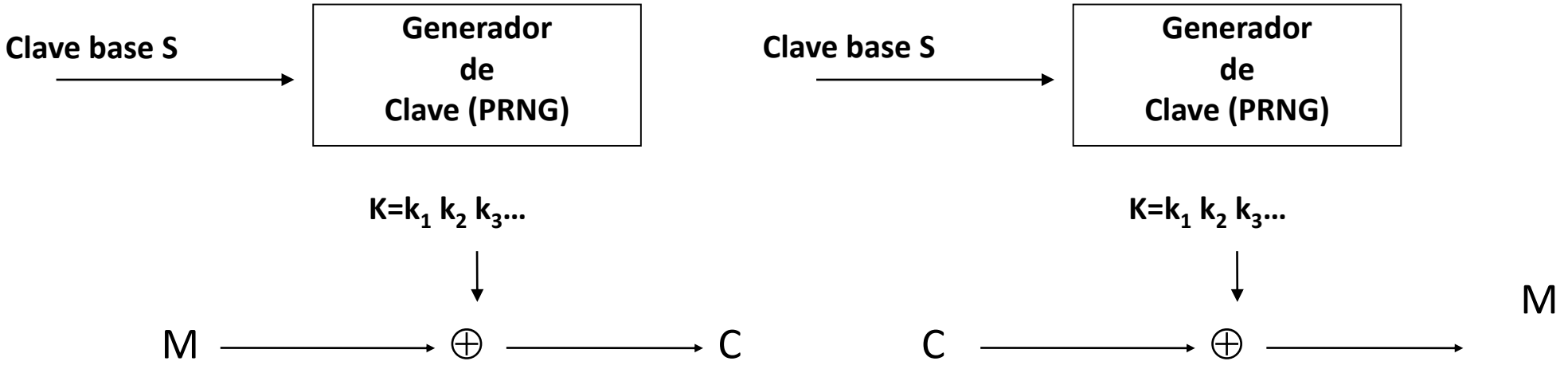
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

INTRODUCCIÓN

- VERNAM NO ES PRÁCTICO

Cifrador de flujo práctico:

- K: serie cifrante obtenida a partir de clave base



CC BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

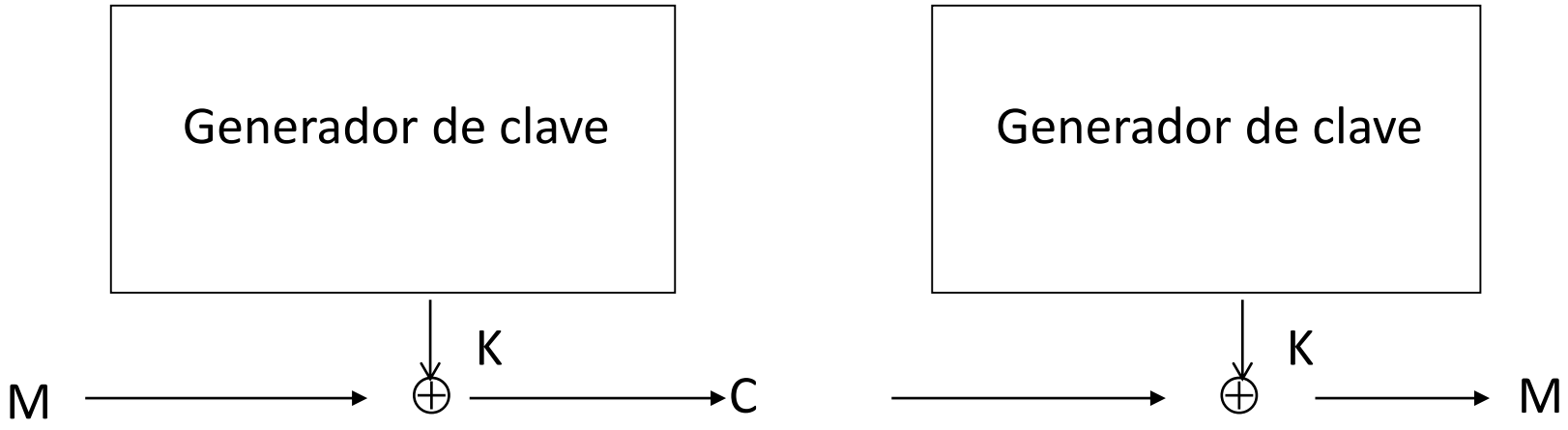
- 6. Criptosistemas simétricos: Flujo
  - Introducción
  - **Tipos**
  - Serie cifrante
  - PRNG criptográficos
    - LFSR
  - Ventajas y desventajas
  - RC4

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

TIPOS DE CIFRADORES DE FLUJO

- SÍNCRONO
  - Emisor y receptor se sincronizan externamente
  - Serie cifrante independiente del texto en claro y del criptograma

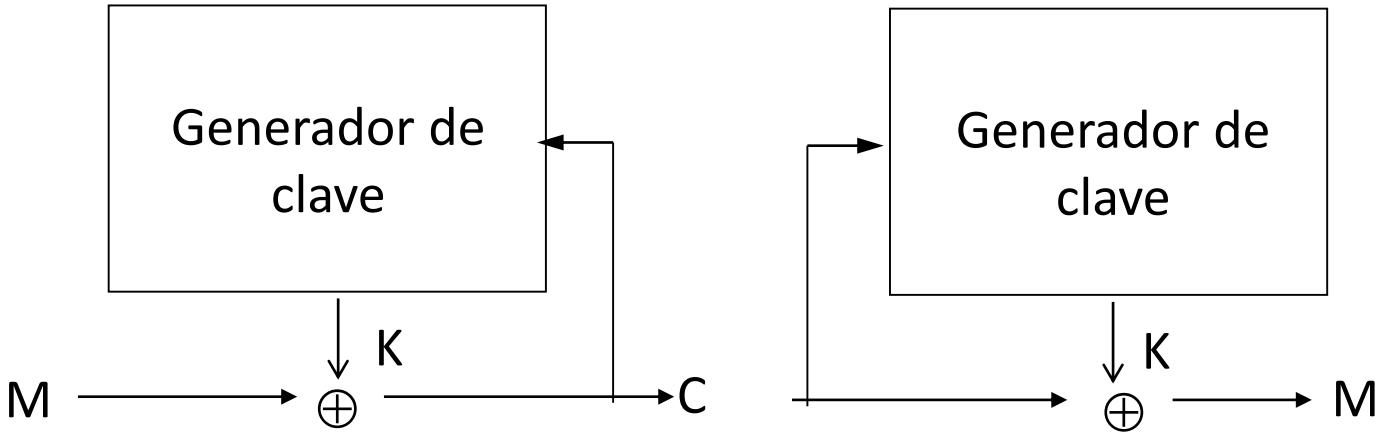


BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

TIPOS DE CIFRADORES DE FLUJO

- AUTOSÍNCRONO
  - Emisor y receptor se sincronizan automáticamente
  - La serie cifrante es una función de símbolos previamente cifrados



BY NC SA
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 6. Criptosistemas simétricos: Flujo
  - Introducción
  - Tipos
  - **Serie cifrante**
  - PRNG criptográficos
    - LFSR
  - Ventajas y desventajas
  - RC4

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

SERIE CIFRANTE

- APROXIMACIÓN PARA GENERAR LA SERIE CIFRANTE
  - Mediante un generador de números pseudoaleatorios
    - Generación determinista
  - A partir de una clave base (secreta e impredecible)
    - De centenas de bits (para evitar ataques de fuerza bruta)

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

SERIE CIFRANTE

- PROPIEDADES DESEABLES: POSTULADOS DE GOLOMB
- Postulado G1:
  - Debe existir igual número de ceros que de unos. Se acepta como máximo una diferencia igual a la unidad.
- Postulado G2:
  - La mitad de las rachas (sucesión de dígitos iguales) tiene longitud 1, la cuarta parte tiene longitud 2, la octava longitud 3, etc.
- Postulado G3:
  - Para todo k, la Autocorrelación fuera de fase AC(k) es igual a una constante.
- Función de Autocorrelación:
  - Desplazamiento de la secuencia S de período T de k bits hacia la izquierda:
  - AC(k) = (A - F) / T
  - Aciertos = bits iguales Fallos = bits diferentes

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

SERIE CIFRANTE

- PROPIEDADES DESEABLES: POSTULADOS DE GOLOMB. EJEMPLO

k=1

```
1 1 1 1 0 1 0 1 1 0 0 1 0 0 0
1 1 1 0 1 0 1 1 0 0 1 0 0 0 1
^ ^ ^         ^   ^     ^ ^
```

A = 7, F = 8 => AC(1) = -1/15

Ejercicio:

Compruebe que para esta secuencia cifrante

s_i = 1 1 1 1 0 1 0 1 1 0 0 1 0 0 0

la Autocorrelación fuera de fase AC(k) para todos los valores de k ($1 \leq k \leq 14$) es constante e igual a -1/15.

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

SERIE CIFRANTE

- PROPIEDADES DESEABLES
  - Período muy grande
  - Aleatoriedad: Distribución uniforme, independencia
  - Impredecibilidad
    - Se puede medir por su complejidad lineal LC
      - » número de bits necesarios para predecir el resto de la secuencia
      - » viene dada por la longitud mínima del LFSR capaz de reproducirla
      - » Se calcula L (número de celdas) y si se conocen 2L bits se puede predecir el resto de la serie
    - Meta: conseguir una complejidad lineal lo más alta posible

cc BY NC SA
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 6. Criptosistemas simétricos: Flujo
  - Introducción
  - Tipos
  - Serie cifrante
  - **PRNG criptográficos**
    - LFSR
  - Ventajas y desventajas
  - RC4

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

PRNG CRIPTOGRÁFICOS

- Basados en algoritmos criptográficos existentes
  - Cifradores simétricos
  - Cifradores asimétricos
  - Funciones resumen
- Ad-hoc
  - Generador de registros de desplazamiento
  - **LFSR *(linear feed-back shift register)***
  - A5/1 (2000)
  - A5/2 (2001)
  - PRNG propio de RC4

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

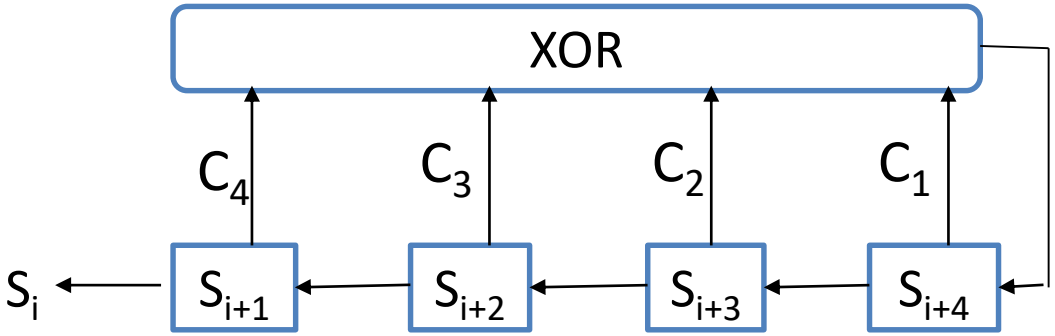
- 6. Criptosistemas simétricos: Flujo
  - Introducción
  - Tipos
  - Serie cifrante
  - **PRNG criptográficos**
    - **LFSR**
  - Ventajas y desventajas
  - RC4

BY NC SA

LFSR

- REGISTRO DE DESPLAZAMIENTO CON REALIMENTACIÓN LINEAL

[Linear Feedback Shift Register (LFSR)]



Polinomio de conexión asociado:

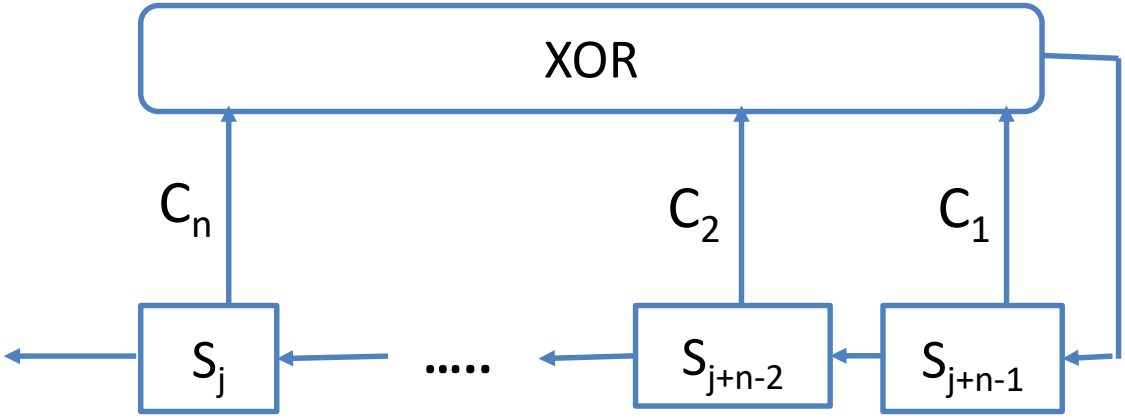
$f(x) = C_4x^4 + C_3x^3 + C_2x^2 + C_1x + 1$

Función única: XOR

$T_{máx} = 2^4 - 1$

Valores iniciales = “semilla”,

prohibido cadena de ceros



$f(x) = C_nx^n + C_{n-1}x^{n-1} + ... + C_2x^2 + C_1x + 1$

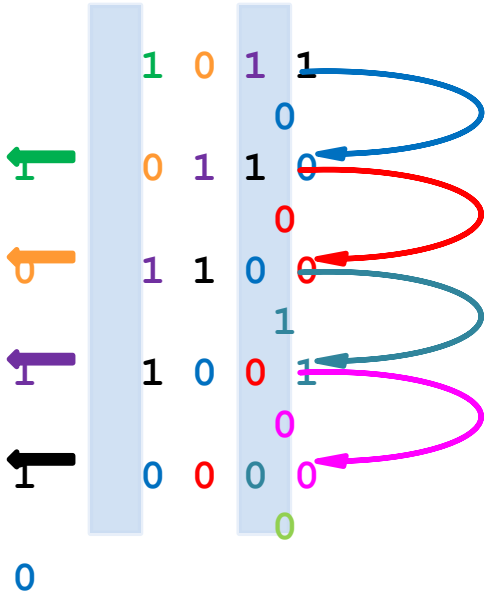
$T_{máx} = 2^n - 1$

BY NC SA

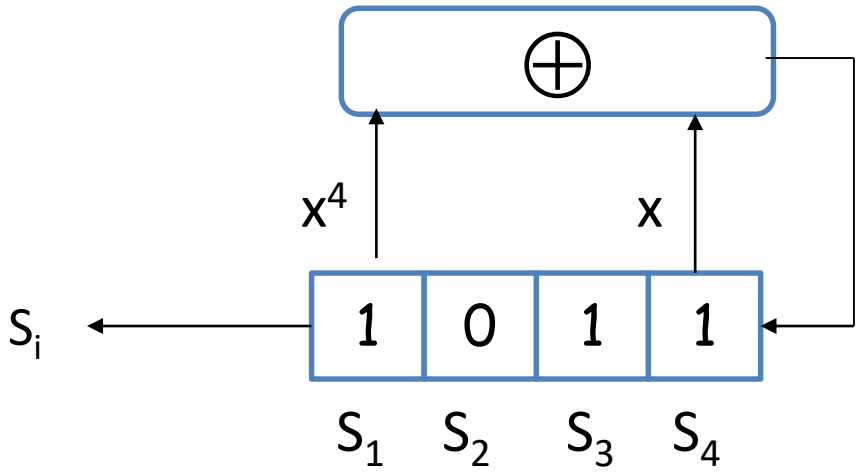
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

LFSR

- EJEMPLO – GENERADOR LFSR DE CUATRO CELDAS (n = 4)
- Clave base: $S_1S_2S_3S_4$ = **1 0 1 1**
- Polinomio de conexión $f(x) = x^4 + x + 1$
- En este ejemplo el periodo es $T = T_{máx} = 2^n - 1$



➔¡semilla!



S_i = 101100100011110

T = 15

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

LFSR

- PERIODOS ALTOS PERO COMPLEJIDAD LINEAL MUY BAJA
- Solución:
  - Aumentar la complejidad lineal del generador
  - Por ejemplo, empleando varios LFSR
    - Operaciones lineales de secuencias seudoaleatorias
    - Operaciones no lineales de las secuencias seudoaleatorias
    - Filtrado no lineal de los estados de un LFSR
    - Otros

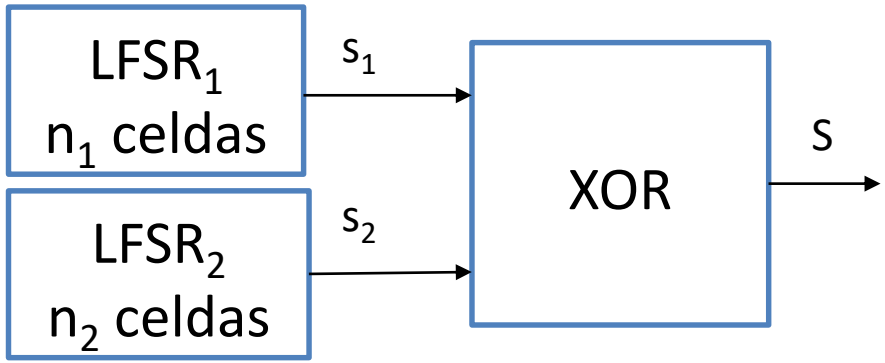
BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

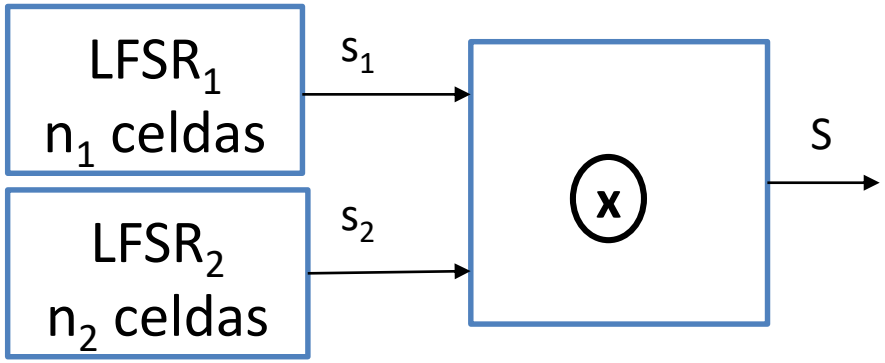
LFSR

- AUMENTANDO LA COMPLEJIDAD LINEAL DE LOS LFSR

- Operaciones lineales de secuencias seudoaleatorias:



- Operaciones no lineales de las secuencias seudoaleatorias:



BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 6. Criptosistemas simétricos: Flujo
  - Introducción
  - Tipos
  - Serie cifrante
  - PRNG criptográficos
    - LFSR
  - **Ventajas y desventajas**
  - RC4

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

VENTAJAS Y DESVENTAJAS

- VENTAJAS
  - Transformación byte a byte, o bit a bit
    - Altas velocidades de cifrado
  - Los errores de transmisión no se propagan

- DESVENTAJAS
  - Escasa difusión de la información
    - Cada símbolo de M se corresponde con uno de C
  - Las series cifrantes no son realmente aleatorias
    - Generación determinista
  - Problemas de reutilización de la clave →

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

VENTAJAS Y DESVENTAJAS

- PROBLEMAS DE REUTILIZACIÓN DE CLAVE
  - Ataque con texto original conocido

    Se puede obtener K, teniendo M y C:

    $$M \oplus C = M \oplus M \oplus K = K$$

  - Ataque sólo al criptograma

    M_i a partir de C_i y C_j escogidos si M_j predecible:

    $$C_i \oplus C_j = M_i \oplus K \oplus M_j \oplus K = M_i \oplus M_j$$

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 6. Criptosistemas simétricos: Flujo
  - Introducción
  - Tipos
  - Serie cifrante
  - PRNG criptográficos
    - LFSR
  - **Ventajas y desventajas**
  - **RC4**

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

RC4

- Algoritmo propietario de RSA
- Inicialmente secreto, luego desensamblado y publicado en sci.crypt
- Diseño de Ron Rivest, simple pero muy efectivo
- Tamaño variable de clave, trabaja sobre bytes
- Muy simple → rápido en software
- Muy usado (web SSL/TLS, wireless WEP, etc.)

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

RC4

- FASE DE INICIALIZACIÓN
- Clave base variable de 1 a 256 bytes
- Vector de estados S={S[0],S[1],...,S[255]}
  - S es el estado interno del cifrador
- Usa la clave para permutar el vector S
- Dada una clave k de longitud l bytes

```
for i = 0 to 255 do
        S[i] = i
j = 0
for i = 0 to 255 do
        j = (j + S[i] + k[i mod l]) (mod 256)
        swap (S[i], S[j])
```


BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

RC4

- SERIE CIFRANTE Y CIFRADO
- En cada paso de cifrado se modifica S
- La suma de un par de valores en S determina el byte de salida

i = j = 0

for each message byte Mi

i = (i + 1) (mod 256) // contador simple

j = (j + S[i]) (mod 256) // simula un random-walk

swap(S[i], S[j])

t = (S[i] + S[j]) (mod 256)

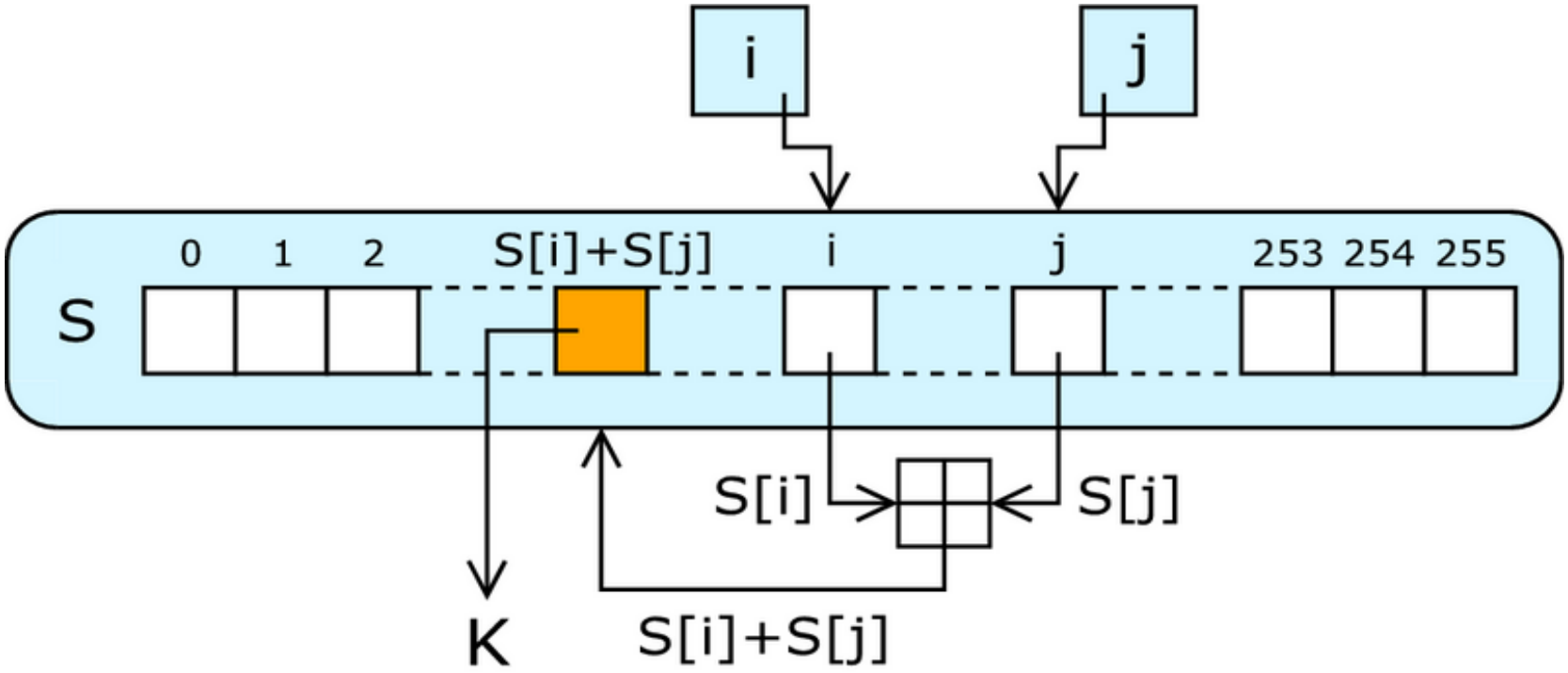
$C_i = M_i \oplus S[t]$

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

RC4

SERIE CIFRANTE



BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

RC4

- SEGURIDAD

- El resultado es muy no-lineal

- Ningún ataque práctico con tamaño de clave base razonable (128 bits o más) **HASTA** el año 2015
  - había ataques contra malas implementaciones concretas
    - La serie cifrante sufre un sesgo (*bias*)…

BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

RC4

- SEGURIDAD
  - En 2015 investigadores de KU Leuven demostraron ataques “prácticos”
    - Recuperar una cookie segura (enviada sobre HTTP con TLS) en 75 horas
    - Descifrar e inyectar paquetes arbitrarios en WPA-TKIP en 1 hora
  - Se está prohibiendo poco a poco su uso en los protocolos que lo contemplan (eg, RFC 7465 lo prohibe para TLS)
  - Se están buscando nuevos algoritmos para sustituir a RC4
  - De momento:
    - AES-CTR (AES con Counter Mode) o AES-GCM
    - Salsa 20 (resultado del proyecto europeo eSTREAM)

cc BY NC SA

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

COSEC

uc3m | Universidad Carlos III de Madrid

CC BY NC SA