Symmetric encryption: Stream ciphers

CRYPTOGRAPHY AND COMPUTER SECURITY

Ana I. González-Tablas Ferreres
José M. de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo

uc3m | Universidad Carlos III de Madrid

COSEC

OUTLINE

- 6. Symmetric encryption: Stream ciphers
  - Introduction
  - Types
  - Keystream
  - Cryptographic PRNGs
    - LFSR
  - Stream ciphers: advantages and disadvantages
  - RC4

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 6. Symmetric encryption: Stream ciphers
  - Introduction
  - Types
  - Keystream
  - Cryptographic PRNGs
    - LFSR
  - Stream ciphers: advantages and disadvantages
  - RC4

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Stream ciphers. Introduction

- They divide the whole message in symbols (characters or bits):

  $M = m_1, m_2, \ldots m_n$

- They encrypt each of those symbols m_i with the corresponding symbol k_i of a keystream of a given length
- Ideally infinite and random
  - K = k1,k2,...kn,kn+1,...
- $E_K (M) = E_{k1} (m_1) E_{k2} (m_2) \ldots E_{kn} (m_n)$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Stream ciphers. Introduction

VENAM ENCRYPTION

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

$$
\begin{array}{cccccccccc}
 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & M \\
\oplus & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & K \\
\hline
 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & C
\end{array}
$$

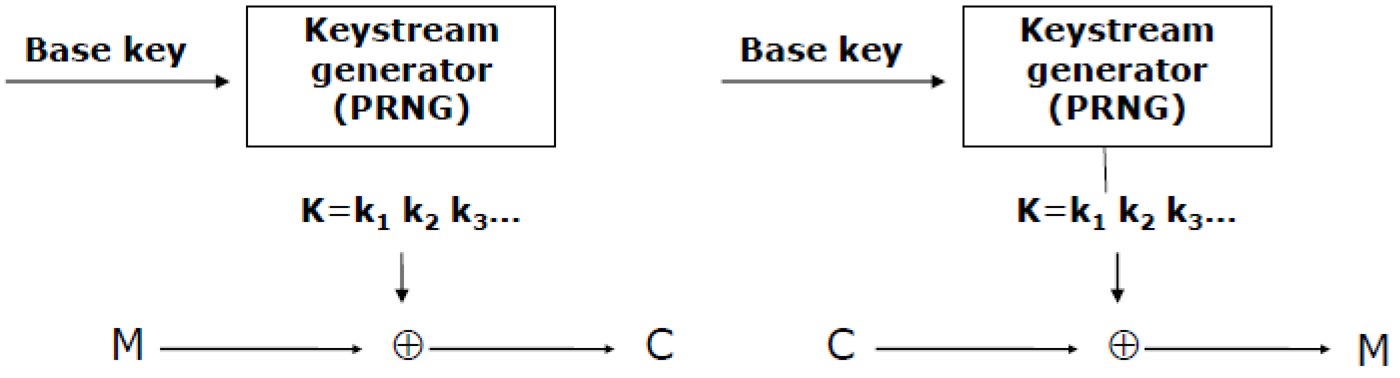
- Decryption: $M = E(M) \oplus K$
- Shannon showed that Vernam cipher is unconditionally secure (perfect secrecy) if the key K is:
  - Truly random
  - Used once
  - Its length is equal or greater to the message (M) length

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Stream ciphers. Introduction

VENAM ENCRYPTION => No practical

- K: keystream obtained from a base key



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

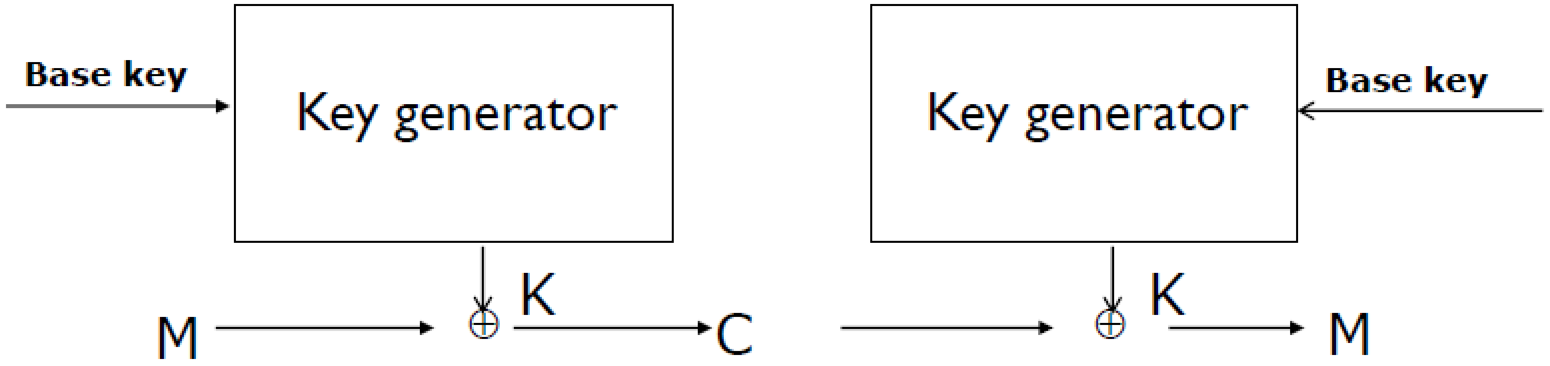
OUTLINE

- 6. Symmetric encryption: Stream ciphers
  - Introduction
  - Types
  - Keystream
  - Cryptographic PRNGs
    - LFSR
  - Stream ciphers: advantages and disadvantages
  - RC4

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Types of stream ciphers

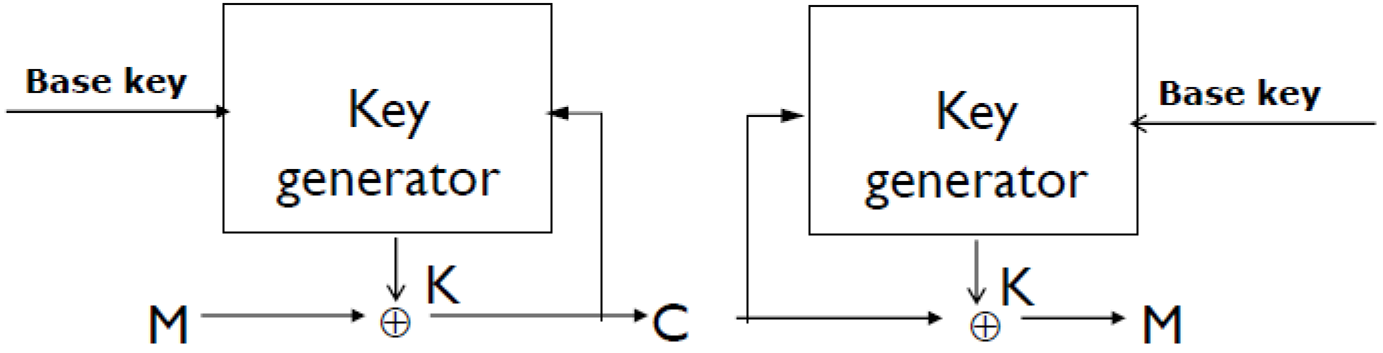
- Synchronous
  - Sender and receiver have to be externally synchronized
  - Keystream generation is done independently of the plaintext and the ciphertext



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Types of stream ciphers

- Self-synchronyzed
  - Sender and receiver are automatically synchronyzed
    - by means of a certain number of keystream bits
  - Keystream is a function of previously encrypted symbols



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 6. Symmetric encryption: Stream ciphers
  - Introduction
  - Types
  - Keystream
  - Cryptographic PRNGs
    - LFSR
  - Stream ciphers: advantages and disadvantages
  - RC4

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Keystream

- Keystream generation in both sender and receiver
- By means of a PseudoRandom Number Generator (PRNG)
  - Deterministic generation
- From a base key (secret and unpredictable)
  - Generated keystream has to be hundreds of bits long (to avoid brute force attacks)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Keystream

GOLOMB postulates to verify the randomness of a sequence.

- Postulate G1:
  - In every period, the number of zeros is nearly equal to the number of ones. (More precisely, the disparity will not to exceed 1 bit)
- Postulate G2:
  - In every period, half of the runs (consecutive equal values) have length one, one fourth have length two, one-eight have length three, etc. for each of these lengths, there are equally many runs of 0's and of 1's
- Postulate G3:
  - For any k, the auto-correlation function out of phase,AC(k),is a constant } Auto-correlation function:
  - Left shifting of k bits of the sequence S (of period P)
  - AC(k) = (H - F) / P
  - Hits (H) = equal bits Failures (F) = different bits

Keystream

GOLOMB postulates

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

^ ^ ^ ^ ^ ^ ^

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

<u>Exercise:</u>

- Given the keystream $\mathbf{s_i}$ prove that

  $\mathbf{s_i}$ **= 1 1 1 1 0 1 0 1 1 0 0 1 0 0 0**

- the AC(k) is constant and equal to -1/15 for any values of k (**1 ≤ k ≤ 14**)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Keystream

- Desirable properties
  - Very long period (approximately 10^{50})
  - Uniform distribution
  - Unpredictability (knowing part of the keystream must be insufficient to generate the whole sequence)
  - It is measured by its Linear Complexity LC
    - number of bits needed to predict the remainder of the keystream
    - which stems from the minimum length of the LFSR that is able to generate the keystream
    - Once L (number of cells) is calculated, if 2L bits of the keystream are known, the remainder of the keystream can be predicted
  - Goal: to obtain the maximum possible LC

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 6. Symmetric encryption: Stream ciphers
  - Introduction
  - Types
  - Keystream
  - Cryptographic PRNGs
    - LFSR
  - Stream ciphers: advantages and disadvantages
  - RC4

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Cryptographic PRNGs

- Based on existing algorithms
  - Symmetric algorithms
  - Asymmetric algorithms
  - Hash functions
- Ad-hoc
  - Sift registers
  - LFSR (linear feed-back shift register)
  - A5/1 (2000)
  - A5/2 (2001)
  - RC4 PRNG

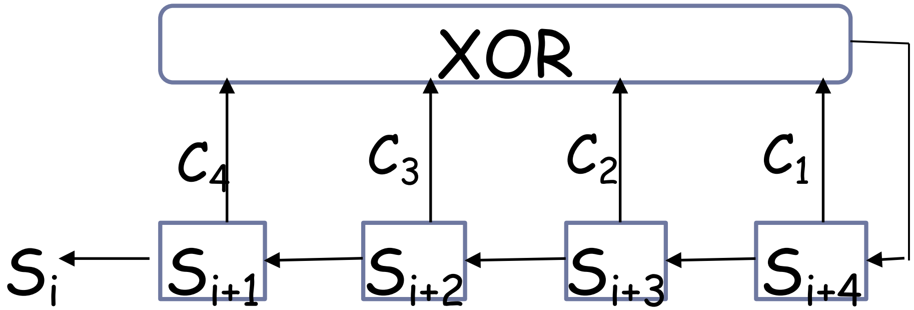
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

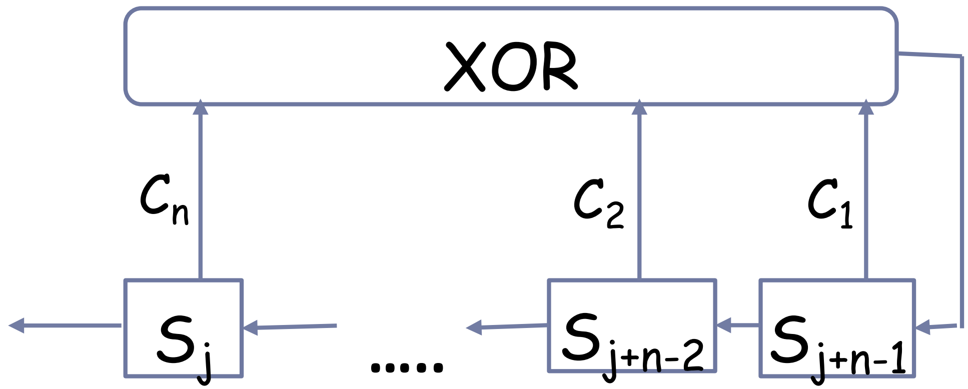
OUTLINE

- 6. Symmetric encryption: Stream ciphers
  - Introduction
  - Types
  - Keystream
  - Cryptographic PRNGs
    - LFSR
  - Stream ciphers: advantages and disadvantages
  - RC4

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

LFSR





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

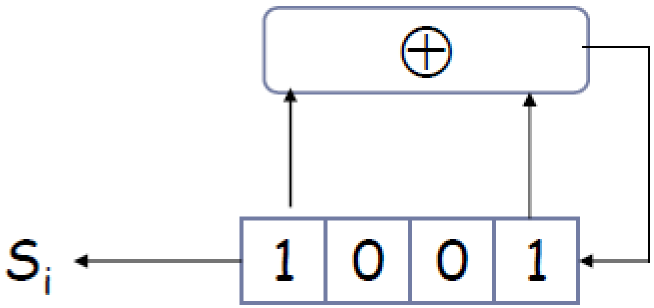
Unique function: XOR
$T_{máx} = 2^4 – 1$
Initial values = “seed”,
Sequence of zeros not possible $f(x) = C_nx^n + C_{n-1}x^{n-1} + ... + C_2x^2 + C_1x + 1$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

LFSR

- LFSR generator of four cells (n = 4)
  - Base key: $S_1S_2S_3S_4$ = **1 0 0 1**
  - $f(x) = x^4 + x + 1$
  - In this example, the period is $T = T_{máx} = 2^n - 1$

Record	bit s_i	
1 0 0 1	1	
0 0 1 0	0	
0 1 0 0	0	
1 0 0 0	1	
0 0 0 1	0	
. . .		
1 0 0 1	1	➔ ¡seed!



S_i = **100100011110101** T = 15

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

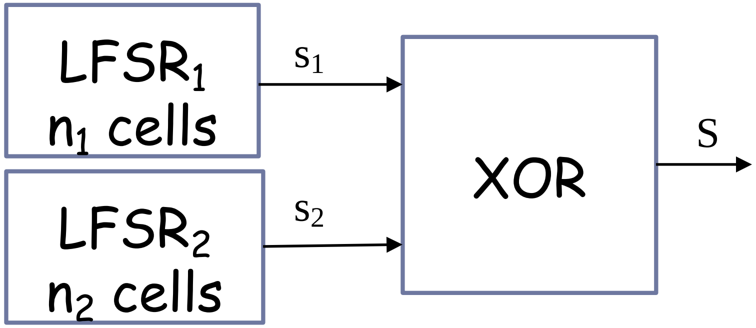
LFSR

- Long periods
- Very low Linear Complexity. Solution:
  - To increase the LC of the generator
  - Using several LFSRs
    - Linear operations of pseudorandom sequences
    - Non linear operations on the pseudorandom sequences
    - Non linear filtering of the states of an LFSR
    - Others

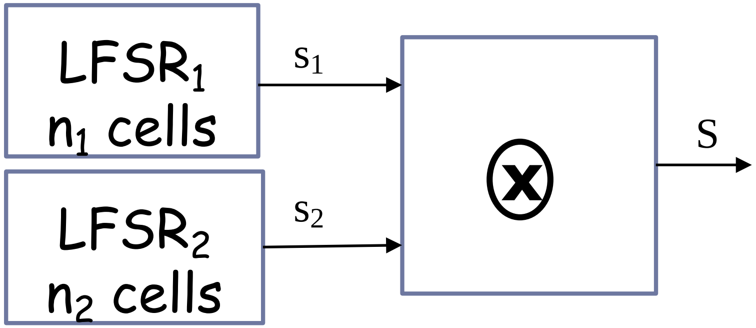
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

LFSR

- Linear operations on pseudorandom sequences:



- Non linear operations on pseudorandom sequences:



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 6. Symmetric encryption: Stream ciphers
  - Introduction
  - Types
  - Keystream
  - Cryptographic PRNGs
    - LFSR
  - Stream ciphers: advantages and disadvantages
  - RC4

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Stream ciphers. Advantages and disadvantages

- <u>Advantages:</u>
  - Character by character or bit by bit transformation
    - High encryption rates
  - Error resistance. Channel errors do not propagate through the sequence
- <u>Disadvantages</u>:
  - Poor diffusion of the information
    - Information of each symbol of plaintext M is exclusively passed onto the corresponding ciphertext (C) element
  - Keystreams are never purely random
    - Deterministic keystream generation
  - Key reuse issue

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

Stream ciphers. Advantages and disadvantages

- Key reuse issue:
  - Known plaintext attack

    Having M and C, K is calculated as follows:

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

  - Known ciphertext attack

    It is possible to obtain K_i choosing 2 ciphertexts (C_j y C_j chosen, M_j predictable):

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

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

OUTLINE

- 6. Symmetric encryption: Stream ciphers
  - Introduction
  - Types
  - Keystream
  - Cryptographic PRNGs
    - LFSR
  - Stream ciphers: advantages and disadvantages
  - RC4

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

RC4

- RSA proprietary algorithm
- Initially secret, disassembled and published in sci.crypt later
- Designed by Ron Rivest, simple but highly effective
- Variable key size, operates on bytes
- Highly used (web SSL/TLS, wireless WEP, etc.)
- Very simple -> fast on sw

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

RC4. Initialization

- Base key variable from 1 to 256 bytes
- States vector S={S[0],S[1],...,S[255]}
  - S is the internal cipher state
- The key is used to permute the contents of vector S
- Given a key k of length 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])
```


Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

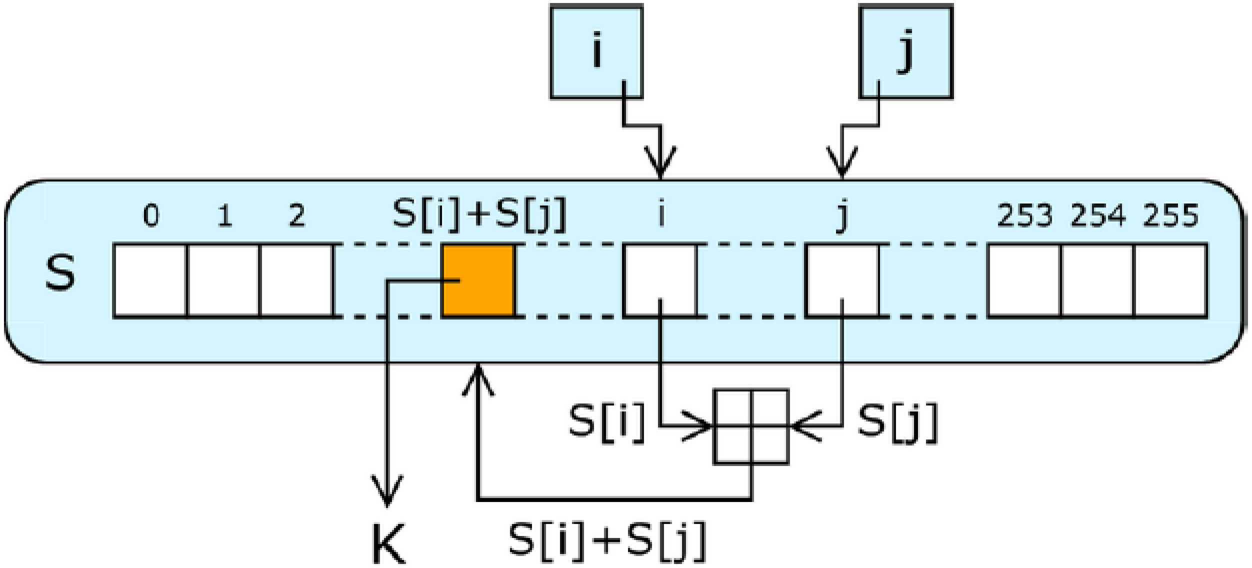
RC4. Encryption

- S is modified on each cipher step
- The addition of a pair of values in S determines the output byte

```
i = j = 0
for each message byte Mi
        i = (i + 1) (mod 256)  // simple counter
        j = (j + S[i]) (mod 256) // simulates a random-walk
        swap(S[i], S[j])
        t = (S[i] + S[j]) (mod 256)
        C_i = M_i ⊕ S[t]
```


Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

RC4. Keystream



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Sergio Pastrana Portillo

RC4. Security

- Result is highly non-linear
- There WAS no practical attack with a reasonable base key length (128 or more bits) until 2015
  - There are attacks against weak specific implementations (example: Wireless WEP). Also, weak keys
- Nowadays, it is better to avoid its use
  - NOMORE attack (2015):
    - Against TLS, a secure HTTP cookie can be decrypted within 75 hours.
    - Against WPA-TKIP, within an hour an attacker is able to decrypt and inject arbitrary packets

CRYPTOGRAPHY AND COMPUTER SECURITY

COSEC

uc3m | Universidad Carlos III de Madrid