



## Stream Cipher

I crittosistemi simmetrici possono essere:

**Cifrari a blocchi:** trasformazione di grandi blocchi del testo in chiaro

**Stream Cipher:** trasformazione dipendente dal tempo di singoli caratteri del testo in chiaro

Stream Cipher 0



## Stream Cipher



genera una keystream e poi cifra

Testo in chiaro	$M_0 M_1 M_2 M_3 M_4 \dots$
Keystream	$Z_0 Z_1 Z_2 Z_3 Z_4 \dots$
Testo cifrato	$C_0 C_1 C_2 C_3 C_4 \dots$

$$z_i = f_i(\text{chiave}, M_0, M_1, \dots, M_{i-1})$$

$$C_i = e_{z_i}(M_i)$$

Stream Cipher 1



## Esempio di Stream Cipher: Cifrario Autokey

Testo in chiaro lettere  $0, 1, \dots, 25$

Keystream  $Z_0 = K, Z_i = M_{i-1}$  per  $i=1, 2, \dots$

Testo cifrato  $C_i = M_i + z_i \pmod{26}$

Stream Cipher 2



## Esempio di Stream Cipher: Cifrario Autokey

Testo in chiaro lettere  $0, 1, \dots, 25$

Keystream  $Z_0 = K, Z_i = M_{i-1}$  per  $i=1, 2, \dots$

Testo cifrato  $C_i = M_i + z_i \pmod{26}$



Quanto è sicuro?

Stream Cipher 3



## Cifrario Autokey

Testo in chiaro	$M_0 M_1 M_2 M_3 M_4 \dots$
Keystream	$K M_0 M_1 M_2 M_3 \dots$
Testo cifrato	$C_0 C_1 C_2 C_3 C_4 \dots$

$$C_0 = M_0 + K \pmod{26}$$

$$C_i = M_i + M_{i-1} \pmod{26}, \quad i=1, 2, \dots$$

Stream Cipher 4



## Cifrario Autokey

Testo in chiaro	$M_0 M_1 M_2 M_3 M_4 \dots$
Keystream	$K M_0 M_1 M_2 M_3 \dots$
Testo cifrato	$C_0 C_1 C_2 C_3 C_4 \dots$

$$C_0 = M_0 + K \pmod{26}$$

$$C_i = M_i + M_{i-1} \pmod{26}$$


Stream Cipher 5

**Linear Feedback Shift Register**

$$z_{i+4} = z_i + z_{i+1} \pmod 2 \quad i=0,1,2,\dots$$

bit output ← **1** ← **0** ← **0** ← **0**

Inizializzazione:  $z_0 = 1 \quad z_1 = 0 \quad z_2 = 0 \quad z_3 = 0$

Stream Cipher 6

**Linear Feedback Shift Register**

$$z_{i+4} = z_i + z_{i+1} \pmod 2 \quad i=0,1,2,\dots$$

← **1** ← **0** ← **0** ← **0**

Inizializzazione:  $z_0 = 1 \quad z_1 = 0 \quad z_2 = 0 \quad z_3 = 0$

Stream Cipher 7

**Linear Feedback Shift Register**

$$z_{i+4} = z_i + z_{i+1} \pmod 2 \quad i=0,1,2,\dots$$

$z_0=1$  ← **0** ← **0** ← **0** ← **1**

Inizializzazione:  $z_0 = 1, \quad z_1 = 0, \quad z_2 = 0, \quad z_3 = 0$

Stream Cipher 8

**Linear Feedback Shift Register**

$$z_{i+4} = z_i + z_{i+1} \pmod 2 \quad i=0,1,2,\dots$$

←  $z_i$  ←  $z_{i+1}$  ←  $z_{i+2}$  ←  $z_{i+3}$

Inizializzazione:  $z_0 = 1, \quad z_1 = 0, \quad z_2 = 0, \quad z_3 = 0$   
 Keystream di periodo 15: **100010011010111...**  
 Polinomio delle connessioni  $x^4 + x^3 + 1$

Stream Cipher 9

**Linear Feedback Shift Register**

$$z_{i+m} = \sum_{j=0}^{m-1} k_j z_{i+j} \pmod 2 \quad i = 0,1,2,\dots$$

Ricorrenza di grado  $m$   
 Coefficienti  $k_0 \ k_1 \ \dots \ k_{m-1}$   
 Inizializzazione:  $z_0 = \alpha_0 \ \dots \ z_{m-1} = \alpha_{m-1}$   
 Polinomio delle connessioni  
 $k_0 x^m + k_1 x^{m-1} + \dots + k_{m-1} x + 1$

Stream Cipher 10

**Linear Feedback Shift Register**

Fissati  $m$  coefficienti  $k_0 \ k_1 \ \dots \ k_{m-1}$

$$z_{i+m} = \sum_{j=0}^{m-1} k_j z_{i+j} \pmod 2 \quad i = 0,1,2,\dots$$

**Chiave:** i valori di inizializzazione  $\alpha_0 \ \alpha_1 \ \dots \ \alpha_{m-1}$

Testo in chiaro	$M_0 \ M_1 \ M_2 \ M_3 \ M_4 \ \dots$
Keystream	$z_0 \ z_1 \ z_2 \ z_3 \ z_4 \ \dots$
Testo cifrato	$C_0 \ C_1 \ C_2 \ C_3 \ C_4 \ \dots$

**Esempio**  
 $C_i = M_i \oplus z_i$

Stream Cipher 11

### A5

- Stream Cipher usato nel GSM (Group Special Mobile)

- Algoritmo conosciuto
- Chiave memorizzata nella memoria del modulo SIM (Subscriber Identity Module)
- 3 Linear Feedback Shift Register di grado 19, 22, 23

Stream Cipher 12

### Configurazione del sistema GSM

Stream Cipher 13

### Autenticazione utente

**Mobile Station**

$k_i$  ↓

A3

**Tratta radio**

TMSI (oppure IMSI)  
richiesta di accesso

rand

**Rete GSM**

Genera rand

$k_i$  ↓

A3

SRES<sub>rete</sub>

$SRES_{MS} \stackrel{?}{=} SRES_{rete}$

SI → accesso consentito

NO → accesso negato

Stream Cipher

### Cifratura

**Mobile Station**

$k_i$  ↓

A8

$k_c$  ↓

A5

← info

**Tratta radio**

TMSI (oppure IMSI)  
richiesta di accesso

rand

← info cifrate →

**Rete GSM**

Genera rand

$k_i$  ↓

A8

$k_c$  ↓

A5

← info

Stream Cipher 15

### A5

- Tre Linear Feedback Shift Register che corrispondono ai polinomi (primitivi) delle connessioni

$$x^{19} + x^5 + x^2 + x + 1 \quad \text{bit } 0,1,\dots,18$$

$$x^{22} + x + 1 \quad \text{bit } 0,1,\dots,21$$

$$x^{23} + x^{15} + x^2 + x + 1 \quad \text{bit } 0,1,\dots,22$$

- Viene fatto il "clock" dei registri il cui bit centrale è uguale alla maggioranza dei bit centrali (bit 8, 10, 10)
- L'output è lo xor dei bit 18, 21, 22
- Vi è una prima fase di inizializzazione

Stream Cipher 16