



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



genera una keystream e poi cifra

Testo in chiaro $M_0 M_1 M_2 M_3 \dots M_i \dots$

Keystream $z_0 z_1 z_2 z_3 \dots z_i \dots$

Testo cifrato $C_0 C_1 C_2 C_3 \dots C_i \dots$

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

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



Esempio di Stream Cipher: Cifrario Autokey

Testo in chiaro lettere 0,1,..., 25

Keystream $z_0 = K, z_i = M_{i-1}$ per $i=1,2,\dots$

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



Esempio di Stream Cipher: Cifrario Autokey

Testo in chiaro lettere 0,1,..., 25

Keystream $z_0 = K, z_i = M_{i-1}$ per $i=1,2,\dots$

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



Quanto è sicuro?



Cifrario Autokey

Testo in chiaro $M_0 M_1 M_2 M_3 \dots M_i \dots$

Keystream $K M_0 M_1 M_2 \dots M_{i-1} \dots$

Testo cifrato $C_0 C_1 C_2 C_3 \dots C_i \dots$

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

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



Cifrario Autokey

Testo in chiaro $M_0 M_1 M_2 M_3 \dots M_i \dots$

Keystream $K M_0 M_1 M_2 \dots M_{i-1} \dots$

Testo cifrato $C_0 C_1 C_2 C_3 \dots C_i \dots$

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

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

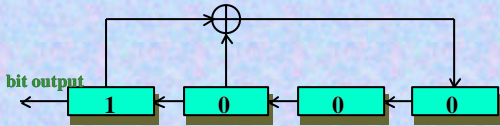
Solo 26 chiavi!





Linear Feedback Shift Register

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

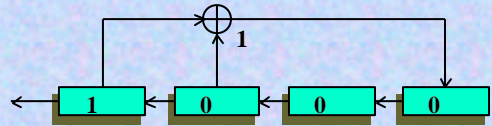


Inizializzazione: $z_0 = 1 \quad z_1 = 0 \quad z_2 = 0 \quad z_3 = 0$



Linear Feedback Shift Register

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

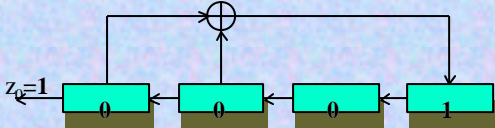


Inizializzazione: $z_0 = 1 \quad z_1 = 0 \quad z_2 = 0 \quad z_3 = 0$



Linear Feedback Shift Register

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

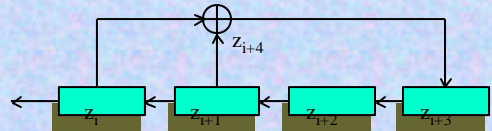


Inizializzazione: $z_0 = 1, \quad z_1 = 0, \quad z_2 = 0, \quad z_3 = 0$



Linear Feedback Shift Register

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



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



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

$$k_0 x^m + k_1 x^{m-1} + \dots + k_{m-1} x + 1$$



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
 $C_i = M_i \wedge z_i$

A5

- ❑ Stream Cipher usato nel GSM (Group Special Mobile)

- ❑ Algoritmo segreto
 - poi scoperto con reverse-engineering
- ❑ 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

Configurazione del sistema GSM

- PIN
- IMSI (International mobile subscriber identification)
- Chiave k_i di 128 bit

Stream Cipher 14

Autenticazione utente

Mobile Station

k_i

A3

Tratta radio

TMSI (oppure IMSI)
richiesta di accesso

rand

Rete GSM

Genera rand

A3

SRES_{MS}

SRES_{MS} ? SRES_{MS}

accesso consentito / accesso negato

Stream Cipher

Cifratura

Mobile Station

k_i

A8

A5

info

Tratta radio

TMSI (oppure IMSI)
richiesta di accesso

rand

Rete GSM

Genera rand

A8

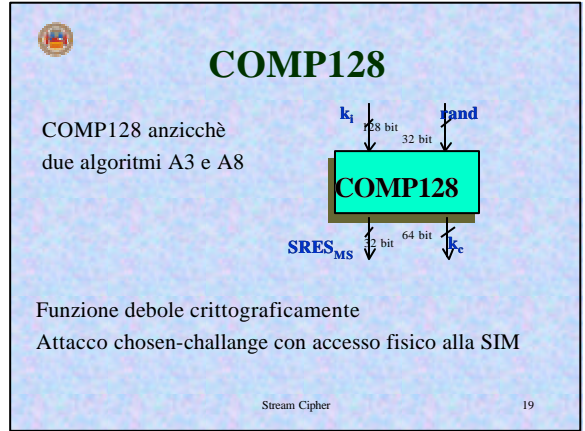
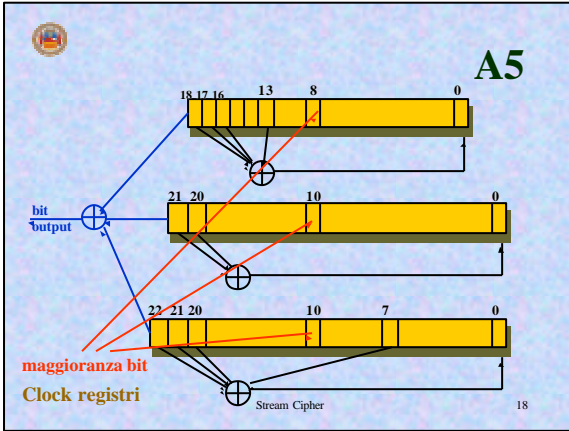
A5

info

Stream Cipher 16

A5

Stream Cipher 17



Attacco chosen-challenge a COMP128

Occorrono $2^{17.5}$ challenge (Berkeley, aprile 1998)
Se 6,25 query al secondo \Rightarrow tempo attacco: circa 8 ore

Stream Cipher 20

Attacchi ad A5

- ❑ Attacco forza bruta: complessità 2^{64}
- ❑ In genere la chiave k_c ha solo 54 bit
 - gli ultimi 10 sono posti a "0"
 - Debolezza introdotta per le intercettazioni?
 - Attacco forza bruta: complessità 2^{54}
- ❑ Attacco *known-plaintext*: complessità 2^{45}
 - Indovina i 40 bit dei 2 registri più piccoli

Stream Cipher 21