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 $M_0\ M_1\ M_2\ M_3\ M_4 \ldots$

Keystream $z_0\ z_1\ z_2\ z_3\ z_4 \ldots$

Testo cifrato $C_0\ C_1\ C_2\ C_3\ C_4 \ldots$

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

$C_i = e_{z_i}(M_i)$

Esempio di Stream Cipher: Cifrario Autokey

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

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

Test cifrato $C_i = M_i + z_i \mod 26$

Esempio di Stream Cipher: Cifrario Autokey

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

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

Test cifrato $C_i = M_i + z_i \mod 26$

Quanto è sicuro?

Cifrario Autokey

Testo in chiaro $M_0\ M_1\ M_2\ M_3\ M_4 \ldots$

Keystream $K\ M_0\ M_1\ M_2\ M_3 \ldots$

Testo cifrato $C_0\ C_1\ C_2\ C_3\ C_4 \ldots$

$C_0 = M_0 + K \mod 26$

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

Cifrario Autokey

Testo in chiaro $M_0\ M_1\ M_2\ M_3\ M_4 \ldots$

Keystream $K\ M_0\ M_1\ M_2\ M_3 \ldots$

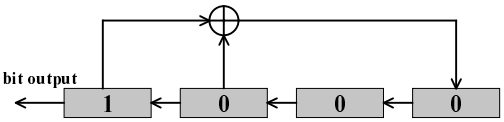
Testo cifrato $C_0\ C_1\ C_2\ C_3\ C_4 \ldots$

$C_0 = M_0 + K \mod 26$

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

Linear Feedback Shift Register

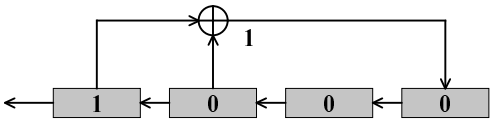
$z_{i+4} = z_i + z_{i+1} \mod 2 \qquad i=0,1,2,\ldots$



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

Linear Feedback Shift Register

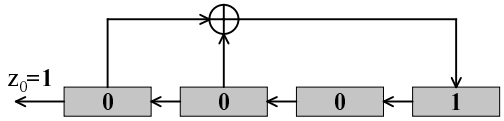
$z_{i+4} = z_i + z_{i+1} \mod 2 \qquad i=0,1,2,\ldots$



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

Linear Feedback Shift Register

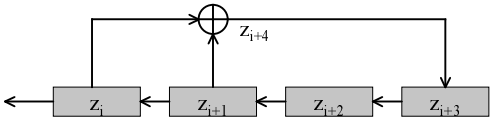
$z_{i+4} = z_i + z_{i+1} \mod 2 \qquad i=0,1,2,\ldots$



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

Linear Feedback Shift Register

$z_{i+4} = z_i + z_{i+1} \mod 2 \qquad i=0,1,2,\ldots$



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

Keystream di periodo 15: **100010011010111…**

Polinomio delle connessioni $x^4 + x^3 + 1$

Linear Feedback Shift Register

$$z_{i+m} = \sum_{j=0}^{m-1} k_j z_{i+j} \mod 2 \qquad i = 0,1,2,\ldots$$

Ricorrenza di grado m

Coefficienti $k_0 k_1 \ldots k_{m-1}$

Inizializzazione: $z_0 = \alpha_0 \ldots , z_{m-1} = \alpha_{m-1}$

Polinomio delle connessioni

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

Linear Feedback Shift Register

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

$$z_{i+m} = \sum_{j=0}^{m} k_j z_{i+j} \mod 2 \qquad i = 0,1,2,\ldots$$

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

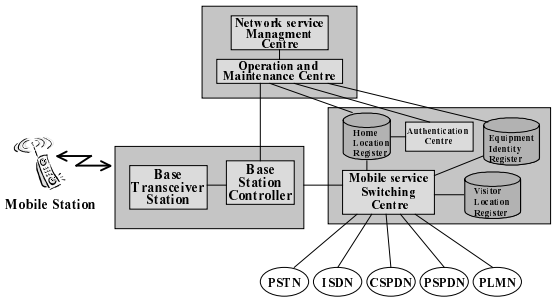
Testo in chiaro	M_0	M_1	M_2	M_3	M_4	…	
Keystream	z_0	z_1	z_2	z_3	z_4	…	**Esempio** $C_i = M_i \oplus z_i$
Testo cifrato	C_0	C_1	C_2	C_3	C_4	…	

A5

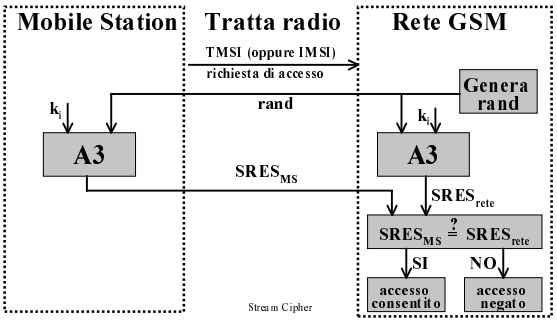
- Stream Cipher usato nel GSM (Group Special Mobile)

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

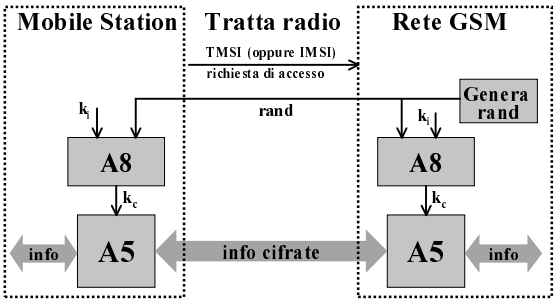
Configurazione del sistema GSM



Autenticazione utente



Cifratura



A5

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

  $x^{19} + x^5 + x^2 + x + 1$ bit 0,1,… ,18

  $x^{22} + x + 1$ bit 0,1,… ,21

  $x^{23} + x^{15} + x^2 + x + 1$ bit 0,1,… ,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