Sisteme de criptare fluide

Luciana Morogan

Facultatea de Matematica-Informatica
Universitatea Spiru Haret

Laborator

Outline

Sisteme de criptare

Sistemele de criptare:

- bloc(block cyphers)
  - elemente succesive ale textului clar sunt criptate folosind aceeasi cheie de criptare
  - daca $x = x_1 x_2 x_3 \ldots$ atunci $y = y_1 y_2 y_3 \ldots = e_k(x_1) e_k(x_2) e_k(x_3) \ldots$
- fluide(stream cyphers)
  - sincrone
  - asincrone

Definitii formale (1)

- Fie $\mathcal{M} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ un sistem de criptare. Secventa de simboluri $k_1 k_2 k_3 \cdots \in K^+$ se numeste **cheie fluida**.
- $\mathcal{M} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ este un **sistem de criptare fluid** daca cipteaza textul clar $x = x_1 x_2 x_3 \ldots$ in $y = y_1 y_2 y_3 \ldots = e_{k_1}(x_1) e_{k_2}(x_2) e_{k_3}(x_3) \ldots$, unde $k_1 k_2 k_3 \ldots$ este o cheie fluida din K^+

Definitii formale (2)

Problema generala: generarea cheii fluide cu ajutorul unui generator numit **generator de chei fluide**
Obs! Daca

- cheia fluida este aleasa aleator si nu mai este foloita ulterior
- lungimea cheii = lungimea textului clar

Atunci sistemul de criptare se numeste **one-time-pad**

Definitie formala

Un sistem de criptare fluid sincron este o structura $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{E}, \mathcal{D})$ unde

- Fie $\mathcal{P}, \mathcal{C}, \mathcal{K}$ sunt multimi finite, nevide, ale caror elemente se numesc *texte clare*, *texte criptate* si, respectiv, *chei*
- $\mathcal{L}$ este o multime finita, nevida numita *alfabetul sirului de chei*
- se defineste $g : \mathcal{K} \to \mathcal{L}^+$ generatorul de chei fluide astfel incat $\forall k \in \mathcal{K}$ avem $g(k) = k_1 k_2 k_3 \cdots \in K^+$ cheia fluida (teoretic infinita)
- $\forall z \in \mathcal{L}$,
  - exista regula de criptare $e_z \in \mathcal{E}$
  - exista regula de decriptare $d_z \in \mathcal{D}$

  astfel incat $\forall x \in \mathcal{P}$, $d_z(e_z(x)) = x$

Exemplu: Sistemul de criptare Vigenere

Descrierea sistemului

- m lungimea cuvantului cheie
- $\mathcal{P}, \mathcal{C}, \mathcal{K}$=$Z_{26}$, $\mathcal{K}$= $(Z_{26})^m$
- $e_z(x) = x + z(mod 26), d_z(y) = y - z(mod 26)$
- cheia $z_1 z_2 \ldots$ definita prin

$$z_i = \begin{cases} k_i & \text{dc } 1 \leq i \leq m \\ z_{i-m} & \text{dc } i \geq m+1 \end{cases}$$

va genera din cheia fixa $K = (k_1, k_2, \ldots, k_m)$, cheia fluida $k_1, k_2, \ldots, k_m k_1, k_2, \ldots, k_m k_1, k_2, \ldots$

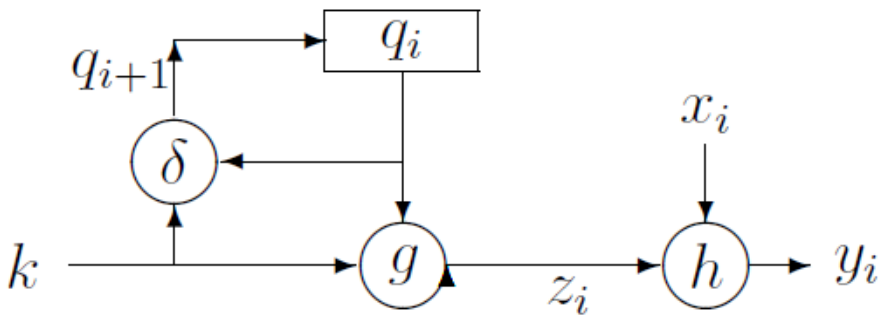
Criptarea si decriptarea

Se realizeaza ca un automat descris de $q_{i+1} = \delta(q_i, k), z_i = g(q_i, k), y_i = h(z_i, x_i)$ unde:

- q_0 - starea initiala determinata din cheia k
- δ - functia de tranzitie a starilor
- g - functia ce produce cheia fluida z_i
- h - functia iesire care produce textul criptat y_i pe baza textului clar x_i si a cheii fluide z_i

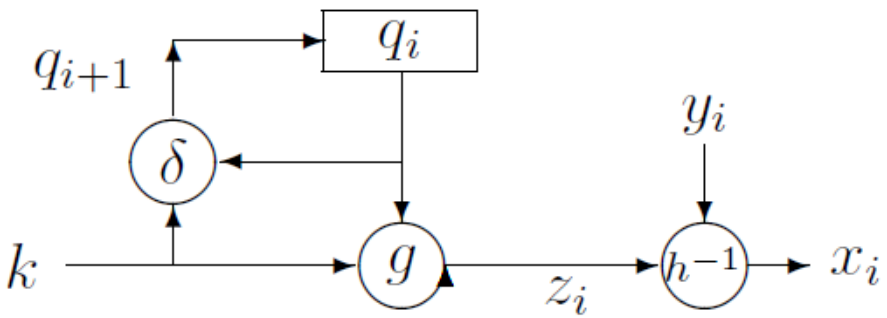
Criptarea si decriptarea: schematic

Criptarea



Decriptarea: schematic

Decriptarea



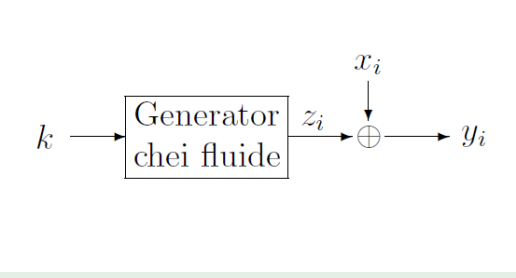
Observatii

- Sistemul de criptare bloc este un caz particular de sistem de criptare fluid: $\forall i \geq 1, z_i = k$
- (Sincronizare.) Cel care trimite mesajele si cel ce urmeaza a le primi trebuie sa isi sincronizeze cheia fluida pentru a obtine o criptare/decriptare corecta. Daca in timpul transmisiei sunt inserati sau eliminati biti in textul criptat, atunci decriptarea esueaza si poate fi reluata pe baza unor tehnici de resincronizare (de exp. reinitializarea)
- Modificarea unui bit din textul criptat (fara a se elimina sau adauga nimic) nu afecteaza decriptarea altor caractere (nepropagarea erorii)
- Adversarul activ care elimina, insereaza sau retrimite componente ale mesajului provoaca desincronizari si va fidetectat la receptie

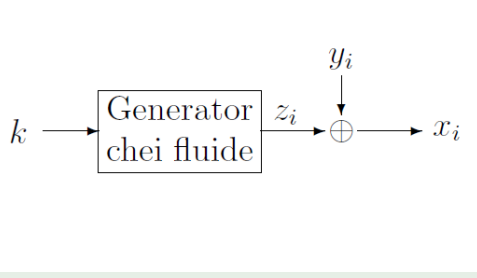
Sistemul aditiv fluid binar de criptare

Un sistem aditiv fluid binar de criptare este un sistem fluid sincron in care $\mathcal{P} = \mathcal{C} = \mathcal{L} = Z_2$ iar h reprezinta functia XOR

Criptare



Decriptare



Sistemul aditiv fluid binar de criptare - exemplu

Sa considerm exemplul in care dorim criptarea/decriptarea secventei de text clar $x = 101101$ si presupunem ca iesirea generatorului de chei fluide ofera cheia $z = 1101$. Vom avea: $x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 1, x_5 = 0, x_6 = 1$ si $z_1 = 1, z_2 = 1, z_3 = 0, z_4 = 1, z_5 = z_1 = 1, z_6 = z_2 = 1$

Criptarea

$y_1 = e_{z_1}(x_1) = x_1 \oplus z_1 = 1 \oplus 1 = 0$
$y_2 = e_{z_2}(x_2) = x_2 \oplus z_2 = 0 \oplus 1 = 1$
$y_3 = e_{z_3}(x_3) = x_3 \oplus z_3 = 1 \oplus 0 = 1$
$y_4 = e_{z_4}(x_4) = x_4 \oplus z_4 = 1 \oplus 1 = 0$
$y_5 = e_{z_1}(x_5) = x_5 \oplus z_1 = 0 \oplus 1 = 1$
$y_6 = e_{z_2}(x_6) = x_6 \oplus z_2 = 1 \oplus 1 = 0$
Se obtine astfel secventa de text cript
$y = 011010$

Decriptarea

$x_1 = d_{z_1}(y_1) = y_1 \oplus z_1 = 1 \oplus 0 = 1$
$x_2 = d_{z_2}(y_2) = y_2 \oplus z_2 = 1 \oplus 1 = 0$
$x_3 = d_{z_3}(y_3) = y_3 \oplus z_3 = 0 \oplus 1 = 1$
$x_4 = d_{z_4}(y_4) = y_4 \oplus z_4 = 1 \oplus 0 = 1$
$x_5 = d_{z_1}(y_5) = y_5 \oplus z_1 = 1 \oplus 1 = 0$
$x_6 = d_{z_2}(y_6) = y_6 \oplus z_2 = 1 \oplus 0 = 1$
Se obtine astfel secventa de text clar
$x = 101101$

Definitie formala

Un sistem de criptare fluid se numeste asincron (auto-sincronizabil) daca functia de generare a cheii fluide depinde de un numar de caractere criptate anterior:
$q_i = (y_{i-t}, y_{i-t+1}, \ldots, y_{i-1}), z_i = g(q_i, k), y_i = h(z_i, x_i)$ unde:

- $q_0 = (y_{-t}, y_{-t+1}, \ldots, y_{-1})$ - starea initiala
- k - cheia
- g - functia ce produce cheia fluida
- h - functia iesire care produce care cripteaza textului clar x_i

Sisteme asincrone - Exemple

LFSR

- registrii lineari cu feedback

Criptarea cu auto-cheie

- $\mathcal{P} = \mathcal{C} = \mathcal{L} = Z_{26}$
- cheia fluida este data de $z_1 = k, z_i = y_{i-1}, i \geq 2$
- pentru $z \in Z_{26}$, definim
  - $e_z(x) = x + z(mod 26)$
  - $d_z(y) = y - z(mod 26)$

Exercitiu

Pentru $k = 11$
codificati/decodificati textul clar
SPIRU HARET

Solutia

Se va obtine textul criptatat
DSARLSSJNG.

Solutia detaliata a exercitiului anterior

Codificarea textului clar SPIRU HARET este x =18 15 8 17 20 7 0 17 4 19, iar $k = z_1 = 11$

Modul criptare

$y_1 = e_{z_1}(x_1) = x_1 + z_1(mod26) = 18 + 11(mod26) = 3$ si $z_2 = y_1 = 3$
$y_2 = e_{z_2}(x_2) = x_2 + z_2(mod26) = 15 + 3(mod26) = 18$ si $z_3 = y_2 = 18$
$y_3 = e_{z_3}(x_3) = x_3 + z_3(mod26) = 8 + 18(mod26) = 0$ si $z_4 = y_3 = 0$
$y_4 = e_{z_4}(x_4) = x_4 + z_4(mod26) = 17 + 0(mod26) = 17$ si $z_5 = y_4 = 17$
$y_5 = e_{z_5}(x_5) = x_5 + z_5(mod26) = 20 + 17(mod26) = 11$ si $z_6 = y_5 = 11$
$y_6 = e_{z_6}(x_6) = x_6 + z_6(mod26) = 7 + 11(mod26) = 18$ si $z_7 = y_6 = 18$
$y_7 = e_{z_7}(x_7) = x_7 + z_7(mod26) = 0 + 18(mod26) = 18$ si $z_8 = y_7 = 18$
$y_8 = e_{z_8}(x_8) = x_8 + z_8(mod26) = 17 + 18(mod26) = 9$ si $z_9 = y_8 = 9$
$y_9 = e_{z_9}(x_9) = x_9 + z_9(mod26) = 4 + 9(mod26) = 13$ si $z_{10} = y_9 = 13$
$y_{10} = e_{z_{10}}(x_{10}) = x_{10} + z_{10}(mod26) = 19 + 13(mod26) = 6$
Se obtine astfel textul criptat y = 3 18 0 17 11 18 18 9 13 6 si deci codificarea DSARLSSJNG.

Decripatrea se va realiza in mod similar.

Observatii

- Auto-sincronizare: cum h^{-1} depinde de un numar fixat de caractere criptate anterior, desincronizarea rezulta din inserarea sau stergerea de caractere criptate (se poate evita)
- Daca starea unui sistem fluid auto-sincronizabil depinde de t caractere anterioare, atunci modificarea (stergerea,inserarea) unui caracter va duce la decriptarea incorecta a maxim t caractere, dupa care decriptarea redevine corecta.

Alte exemple de sisteme fluide de criptare

- SEAL - sistem de criptare aditiv binar
- RC4 (Rist Code 4) - creat pentru RSA Data Security Inc. (astazi RSA Security), este un sistem aditiv fluid de criptare destinat scopurilor comerciale