

# riptografie și Securitate

## - Prelegerea 7.1 - RC4

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică  
Universitatea din București

# Cuprins

1. Informații generale

2. Descriere

3. Securitate

# Informații generale

RC4 este:

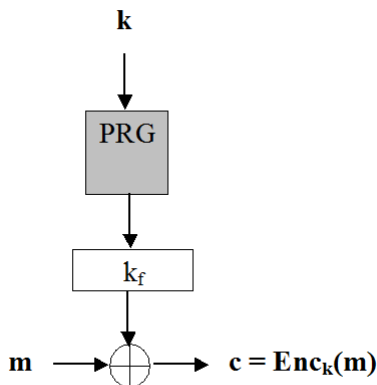
- ▶ introdus de R. Rivest la MIT (1987);
- ▶ înregistrat ca marca a RSA Data Security;
- ▶ păstrat secret până în 1994 când a devenit public;
- ▶ utilizat în WEP, SSL/TLS.

## Descriere

- ▶ RC4 este un sistem de criptare fluid pe octeți:

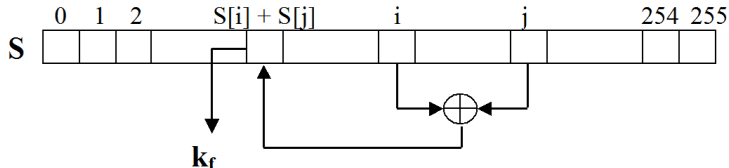
$$m \in \{0, 1\}^8, c \in \{0, 1\}^8$$

- ▶ Ramâne de definit PRG...



# Descriere

- ▶ 2 faze:
  - ▶ **inițializare**: determină starea internă, fără să producă chei fluide;
  - ▶ **generare de chei fluide**: modifică starea internă și generează un octet (*cheia fluidă*) care se XOR-ează cu  $m$  pentru a obține  $c$ ;
- ▶ Starea internă:
  - ▶ un tablou  $S$  de 256 octeți:  $S[0], \dots, S[255]$ ;
  - ▶ 2 indici  $i$  și  $j$ ;
- ▶ Toate operațiile se efectuează pe octeți (i.e. (mod 256)).



# Descriere

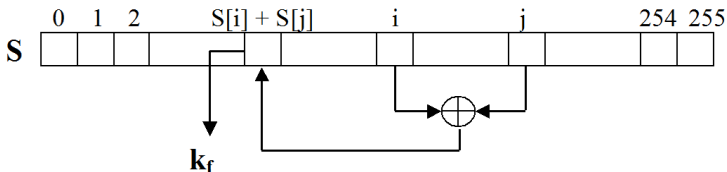
## Faza 1. Inițializare

- ▶  $n =$  numărul octeților din cheie,  $1 \leq n \leq 256$
- ▶
  - $j \leftarrow 0$
  - for**  $i = 0$  **to** 255 **do**
    - $S[i] \leftarrow i$
  - end for**
  - for**  $i = 0$  **to** 255 **do**
    - $j \leftarrow j + S[i] + k[i \pmod n]$
    - swap ( $S[i], S[j]$ )
  - end for**
  - $i \leftarrow 0$
  - $j \leftarrow 0$

# Descriere

## Faza 2. Generarea cheii fluide

- ▶ cheia se obține octet cu octet
- ▶
  - $i \leftarrow i + 1$
  - $j \leftarrow j + S[i]$
  - swap ( $S[i], S[j]$ )
  - return**  $S[S[i] + S[j]]$



# Descriere

Detalii de implementare:

- ▶  $5 \leq n \leq 16 \Rightarrow 40 \leq |k| \leq 256$ ;
- ▶ memorie: 256 octeți (pentru  $S$ ) și câteva variabile *byte*;
- ▶ operații simple, rapid de executat.



- ▶ primii octeți generați drept cheie fluidă sunt total ne-aleatori și oferă informații despre cheie (Fluhrer, Mantin and Shamir 2001)
- ▶ RC4 pe 104 biți (utilizat pentru WEP pe 128 biți) a fost spart în aprox. 1 min (algoritm al lui Tews, Weinmann, Pychkin 2001, bazat pe ideea lui Klein 2005)
- ▶ un atac recent arată că pot fi determinați primii aprox. 200 octeți din textul clar criptat cu RC4 în TLS cunoscând  $[2^{28} - 2^{32}]$  criptări independente (Royal Holloway, 2013)

# Important de reținut!

- ▶ RC4 - sistem de criptare fluid