

## Laborator 9

### Algoritmul de criptare RSA

#### 1. Scurt istoric

Algoritmul RSA (Rivest-Shamir-Adleman) a fost inventat de Ron Rivest, Adi Shamir et Leonard Adleman în 1977 și este proprietate a societății americane RSA Data Security. Odată cu acest algoritm, părăsim zona algoritmilor istorici, ușor de supus criptanalizei.

RSA face parte din clasa algoritmilor de criptare cu cheie publică ce au drept principală caracteristică existența a două chei: o cheie publică ce poate fi cunoscută de orice expeditor și o cheie privată cunoscută doar de destinatar.

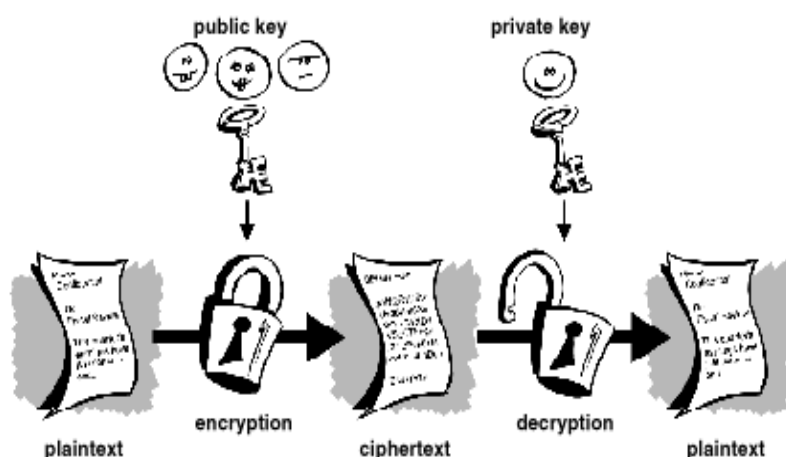


Fig. 1. Criptarea cu cheie publică

Din punct de vedere matematic, algoritmii de criptare cu două chei sunt denumiți algoritmi asimetrii. Prin contrast, toți algoritmii studiați până acum, vor fi numiți algoritmi de criptare simetrici.

#### 2. Descrierea algoritmului

Să presupunem că două persoane, Bob și Alice doresc să comunice într-un mod cât mai sigur mesaje secrete. Există însă și o treia persoană, Eve, care dorește să intercepteze și să decripteze traficul de mesaje dintre Bob și Alice. Alice și Bob pot fi oameni de afaceri aflați la distanță, avioane aflate în zbor sau chiar doi prieteni ce doresc să comunice într-un mod cât mai privat. În nici unul din cazuri Eve nu poate fi oprită să "asculte" traficul radio sau cel de pe internet.

## 2.1 Criptografia cu cheie privată

Soluția clasică a problemei este utilizarea algoritmilor de criptare cu cheie privată (criptare simetrică, Fig. 2). Pentru a fi sigură, această soluție implică un schimb de chei între Alice și Bob. Acest schimb de chei poate fi făcut printr-o întâlnire prealabilă între cele două persoane sau, în cazul unor instituții, companii sau guverne, cu ajutorul unor curieri.

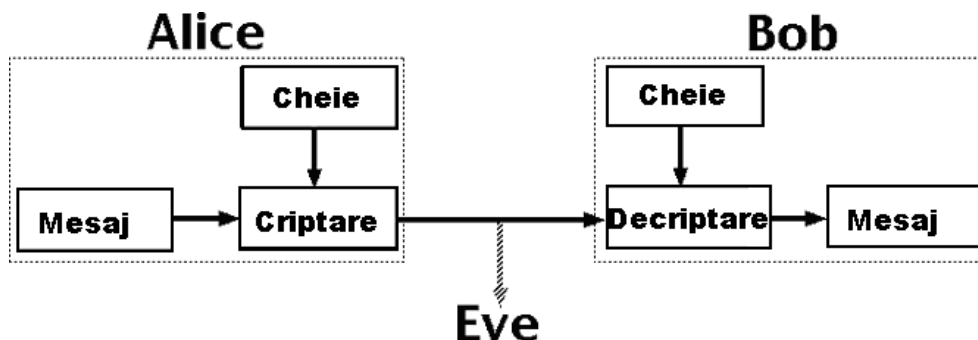


Fig. 2. Criptarea cu cheie privată

Dacă cele două persoane Alice și Bob locuiesc în zone aflate la distanță mare între ele, întâlnirea se poate dovedi foarte costisitoare, uneori aproape imposibilă. Soluția ar putea fi schimbarea unei chei digitale folosind internetul sau chiar poșta clasică. Nici una dintre aceste metode nu este însă sigură.

## 2.2 Criptografia cu cheie publică

Soluția problemei anterioare este utilizarea algoritmilor de criptare cu cheie publică. Acest tip de criptare implică folosirea a două tipuri de chei:

- chei private știute doar de destinatarul mesajelor;
- chei publice.

Fiecare utilizator al acestui sistem de criptare va avea două chei (Fig. 3): cea privată pe care o păstrează secretă și cea publică pe care o poate trimite la toți cei care doresc să-i trimită mesaje criptate. Orice "adversar" de tipul Eve descris anterior va cunoaște cheia publică dar nu va putea decripta mesajul dacă nu cunoaște cheia privată.

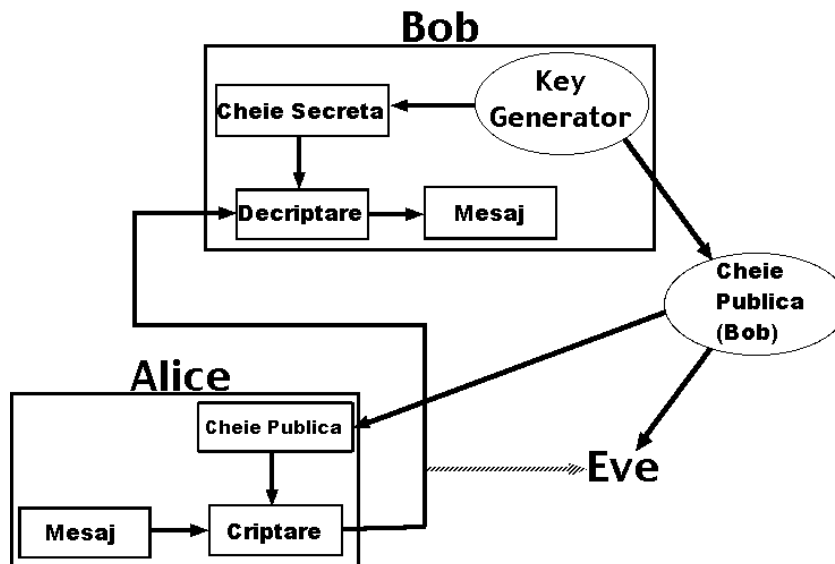


Fig. 3 Criptarea/decriptarea cu cheie publică

## 2.3 Descrierea algoritmului RSA

### 2.3.1 Generarea cheilor

1. Generați 2 numere prime  $p$  și  $q$  cât mai mari
2. Fie  $n = p * q$
3. Fie  $m = (p-1)*(q-1)$
4. Alegeți  $e$  astfel încât  $\text{cmmdc}(e,m) = 1$
5. Găsiți  $d$  astfel încât  $(d*e) \% m = 1$

Se vor publica cheile publice:  $e$  și  $n$ .

Se vor păstra cheile private:  $d$  și  $n$ .

### 2.3.2 Criptarea RSA

$$C = M^e \% n,$$

Unde:

- $M$  = Mesaj
- $e$  și  $n$  sunt cheia publică
- $C$  = CipherText (mesajul criptat)

### 2.3.3 Decriptarea RSA

$$M = C^d \% n$$

Unde:

- $C$  = CipherText
- $d$  și  $n$  sunt cheia privată
- $M$  = Mesajul inițial

## 2.4 Dezavantaje ale algoritmului RSA:

- După cum se poate observa și din descrierea algoritmului, RSA criptează numere și nu litere. Pentru a cripta secvențe de text sau imagini, va trebui să aplicăm algoritmul pentru fiecare octet în parte. După cum am văzut deja, acest tip de criptare poate ușura foarte mult munca unui criptanalist care utilizează testul Kasiski și poate conduce în cele din urmă la aflarea cheii private. Pentru a evita astfel de situații, de obicei, criptarea RSA mai introduce și octeți cu valori aleatorii.
- Din cauza complexității algoritmului de criptare / decriptare, RSA este considerat lent în comparație cu algoritmi simetrici de criptare.

### 3. Exemplu de criptare / decriptare RSA

#### 3.1 Generarea Cheilor

1) Generați 2 numere prime  $p$  și  $q$  cât mai mari

Pentru a face exemplul cât mai ușor de urmărit, vom folosi numerele prime 7 și 19.

$$p = 7$$

$$q = 19$$

2) Fie  $n = p * q$

$$n = 7 * 19$$

$$n = 133$$

3) Fie  $m = (p-1)*(q-1)$

$$m = (7-1)*(19-1)$$

$$m = 6 * 18$$

$$m = 108$$

4) Alegeți  $e$  astfel încât  $\text{cmmdc}(e, m) = 1$

$$e = 2 \Rightarrow \text{cmmdc}(e, 108) = 2 \quad (\text{NU})$$

$$e = 3 \Rightarrow \text{cmmdc}(e, 108) = 3 \quad (\text{NU})$$

$$e = 4 \Rightarrow \text{cmmdc}(e, 108) = 4 \quad (\text{NU})$$

$$e = 5 \Rightarrow \text{cmmdc}(e, 108) = 1 \quad (\text{DA})$$

5) Găsiți  $d$  astfel încât  $(d*e) \% m = 1$

sau altfel spus,  $d*e = 1 + x*m$  (unde  $x$  poate fi orice număr întreg)  $\Rightarrow$

$$d = (1 + x*m)/e$$

$$x = 0 \Rightarrow d = 1/5 \quad (\text{NU})$$

$$x = 1 \Rightarrow d = 109/5 \quad (\text{NU})$$

$$x = 2 \Rightarrow d = 217/5 \quad (\text{NU})$$

$$x = 3 \Rightarrow d = 326/5 \quad (\text{DA})$$

$$d = 65$$

Cheie publică = 133, 5

Cheie privată = 133, 65

#### 3.2 Criptarea RSA

Vom calcula  $C = M^e \% n$

Fie  $M = 6 \Rightarrow$

$$C = M^e \% n$$

$$= 6^5 \% 133$$

$$= 7776 \% 133$$

$$= 62$$

## 3.3 Decriptarea RSA

Vom calcula  $\mathbf{M} = \mathbf{C}^d \% \mathbf{n}$

$$\begin{aligned} M &= C^d \% n \\ &= 62^{65} \% 133 \\ &= 62 * 62^{64} \% 133 \\ &= 62 * (62^2)^{32} \% 133 \\ &= 62 * 3844^{32} \% 133 \\ &= 62 * (3844 \% 133)^{32} \% 133 \\ &= 62 * 120^{32} \% 133 \\ &= 62 * 36^{16} \% 133 \\ &= 62 * 99^8 \% 133 \\ &= 62 * 92^4 \% 133 \\ &= 62 * 85^2 \% 133 \\ &= 62 * 43 \% 133 \\ &= 2666 \% 133 \\ &= 6 \end{aligned}$$

**Temă de laborator:**

Implementați funcțiile `Encrypt_RSA()` și `Decrypt_RSA()`.