Laborator 09

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 şi este proprietate a societăţii americane RSA Data Security. Odată cu acest algoritm, părăsim zona algoritmilor istorici, uşor de supus criptanalizei.

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

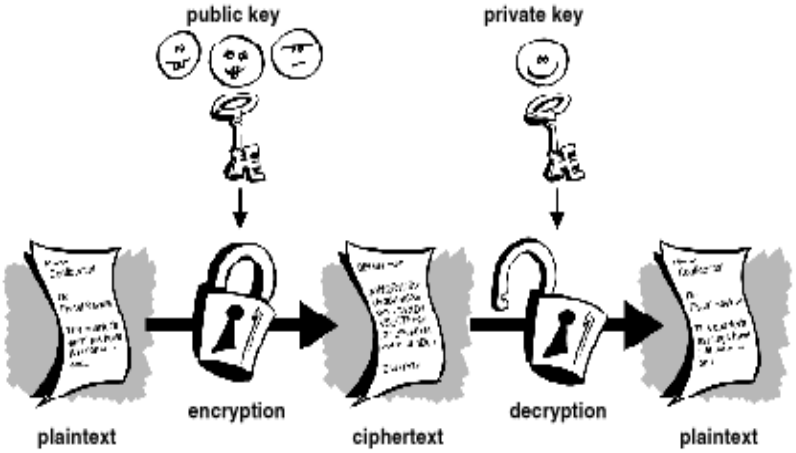

Fig. 1. Criptarea cu cheie publică

Din punct de vedere matematic, algoritmii de criptare cu două chei sunt denumiţi algoritmi asimetrici. Prin contrast, toţi algoritmii studiaţi până acum, vor fi numiţi algoritmi de criptare simetrici.

2. Descrierea algoritmului

Să presupunem că două persoane, Bob şi Alice doresc să comunice într-un mod cât mai sigur mesaje secrete. Există însă şi o treia persoană, Eve, care doreşte să intercepteze şi să decripteze traficul de mesaje dintre Bob şi Alice. Alice şi Bob pot fi oameni de afaceri aflaţi la distanţă, 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

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

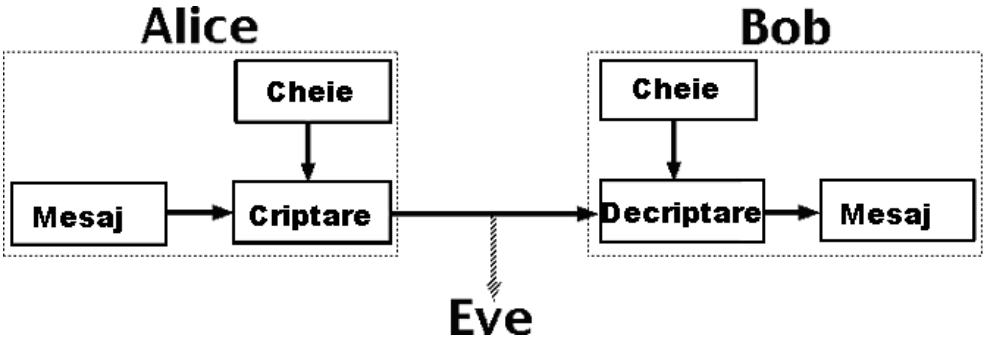

Fig. 2. Criptarea cu cheie privată

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

2.2 Criptografia cu cheie publică

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

- chei private ştiute doar de destinatarii mesajelor;
- chei publice.

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

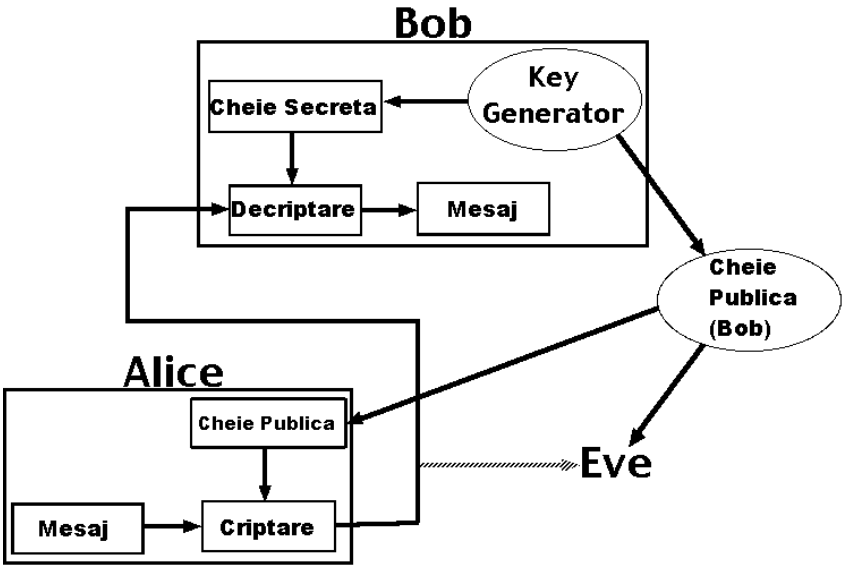

Fig. 3 Criptarea/decriptarea cu cheie publică

2.3 Descrierea algoritmului RSA

2.3.1 Generarea cheilor

1. Generaţi 2 numere prime p şi q cât mai mari
2. Fie n = p * q
3. Fie m = (p-1)*(q-1)
4. Alegeţi e astfel încât cmmdc(e,m) = 1
5. Găsiţi d astfel încât (d*e) % m = 1

Se vor publica cheile publice: e şi n.
Se vor păstra cheile private: d şi n.

2.3.2 Criptarea RSA

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

Unde:

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

2.3.3 Decriptarea RSA

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

Unde:

- C = CipherText
- d şi n sunt cheia privată
- M = Mesajul iniţial

2.4 Dezavantaje ale algoritmului RSA:

- După cum se poate observa şi din descrierea algoritmului, RSA criptează numere şi nu litere. Pentru a cripta secvenţe de text sau imagini, va trebui sa aplicăm algoritmul pentru fiecare octet în parte. După cum am văzut deja, acest tip de criptare poate uşura foarte mult munca unui criptanalist care utilizează testul Kasiski şi poate conduce în cele din urmă la aflarea cheii private. Pentru a evita astfel de situaţii, de obicei, criptarea RSA mai introduce şi octeţi cu valori aleatorii.
- Din cauza complexităţii algoritmului de criptare / decriptare, RSA este considerat lent în comparaţie cu algoritmii simetrici de criptare.

3. Exemplu de criptare / decriptare RSA

3.1 Generarea Cheilor

1) Generaţi 2 numere prime p şi q cât mai mari
Pentru a face exemplul cât mai uşor de urmărit, vom folosi numerele prime 7 şi 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) Alegeţi e astfel încât cmmdc(e,m) = 1
e = 2 => cmmdc(e, 108) = 2 (NU)
e = 3 => cmmdc(e, 108) = 3 (NU)
e = 4 => cmmdc(e, 108) = 4 (NU)
e = 5 => cmmdc(e, 108) = 1 (DA)

5) Găsiţi d astfel încât (d*e) % m = 1
sau altfel spus, d*e = 1 + x*m (unde x poate fi orice număr întreg) =>
d = (1 + x*m)/e
x = 0 => d = 1/5 (NU)
x = 1 => d = 109/5 (NU)
x = 2 => d = 217/5 (NU)
x = 3 => d = 326/5 (DA)
d = 65

Cheie publică = 133, 5
Cheie privată = 133, 65

3.2 Criptarea RSA

Vom calcula $\mathbf{C = M^e \% n}$
Fie M = 6 =>
$C = M^e \% n$
$= 6^5 \% 133$
$= 7776 \% 133$
$= 62$

3.3 Decriptarea RSA

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

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

Temă de laborator:

Creați și Implementaţi funcţiile Enrypt_RSA() şi Decrypt_RSA().

Exercitii:

1. Fie numerele prime p = 211 ,si q = 167. Sa se cifreze mesajul TEST cu ajutorul algoritmului RSA, utilizand exponentul public e = 28 + 1. Elementele din mesajul clar se codifica conform codului ASCII.
2. Sa se descifreze mesajul 01154 05746 04357 01154 cu ajutorul algoritmului RSA (p = 211 ,si q = 167), utilizand exponentul public e = 28 + 1. Elementele din mesajul clar se decodifica conform codului ASCII.
3. Sa se cifreze mesajul M = 146, utilizand sistemul RSA cu urmatorii parametrii: n = 187 (modulul de cifrare), e = 7 (exponentul de cifrare).
4. Sa se descifreze mesajul C = 141, utilizand sistemul RSA cu urmatorii parametrii: n = 187 (modulul de cifrare), d = 23(exponentul de descifrare).