Securitatea sistemelor informatice
Criptarea asimetrică folosind RSA

Aldea Constantin Lucian

Universitatea Transilvania din Brașov

costel.aldea@unitbv.ro

April 14, 2016

Cuprins

1. Introducere
2. Exemplu
3. Întrebări

Introducere

RSA este un sistem de criptare cu cheie publică dezvoltat în anul 1977 de către profesorii de la MIT (Massachusetts Institute of Technology), Ronald L. *Rivest*, Adi *Shamir* și Leonard M. *Adleman*, cu scopul de a asigura securitatea datelor pe Internet.
Puterea sa criptografică se bazează pe dificultatea problemei factorizării numerelor întregi, problema la care se reduce criptanaliza RSA și pentru care toți algoritmii de rezolvare cunoscuți au complexitate exponențială. Există însă câteva metode de criptanaliză care ocolesc factorizarea efectivă.
RSA este un algoritm de criptare pe *blocuri*. Aceasta înseamnă că un mesaj de dimensiune mai mare decât log_n este împărțit în segmente de lungime corespunzătoare, numite blocuri, care sunt cifrate rând pe rând. De asemenea este algoritm criptografic asimetric, cu chei publice și functionează pe baza unei perechi de chei legate matematic între ele: o cheie publica, cunoscută de *toată lumea*, și o cheie secretă, cunoscută doar de deținătorul acesteia.

Caracteristici

Deoarece se bazează pe o operație destul de costisitoare din punct de vedere al timpului de calcul și al resurselor de calcul folosite, și anume exponențierea modulo n, viteza RSA este mult mai mică decât a algoritmilor de criptare cu cheie secretă (simetrici). *Bruce Schneier* estima, pe baza unor calcule efectuate în anii 1990, că o implementare hard de RSA este de 1000 de ori mai lentă decât o implementare DES, iar în soft, RSA este de 100 de ori mai lent.
Există anumite modificări care pot aduce performanțe sporite, precum alegerea unui exponent de criptare mic, care astfel reduce calculele necesare criptării, rezolvând în același timp și unele probleme de securitate. De asemenea, operațiile cu cheia secretă pot fi accelerate pe baza teoremei chineze a resturilor, dacă se stochează p, q și unele rezultate intermediare, folosite des. Cu toate acestea, îmbunătățirile nu sunt mari, iar ordinul de mărime al diferențelor de performantă fată de implementările algoritmilor cu cheie secretă rămân aceleași. De aceea, în sistemele de comunicație în timp real, în care viteza de criptare și decriptare este esențială (cum ar fi de exemplu, aplicațiile de fluxuri video sau audio securizate), RSA se folosește doar la începutul comunicației, pentru a transmite cheia secretă de comunicație, care ulterior este folosită într-un algoritm cu cheie secretă, cum ar fi 3DES sau AES.

Exemplu (1)

1. Se aleg numerele prime $p = 11$ și $q = 3$
2. Se calculează $n = p * q = 11 * 3 = 33$
3. Se alege $e = 3$
   - Se verifică $cmmdc(e, p - 1) = cmmdc(3, 10) = 1$
   - Se verifică $cmmdc(e, q - 1) = cmmdc(3, 2) = 1$
   - Rezultă
     $cmmdc(e, \phi) = cmmdc(e, (p - 1) * (q - 1)) = cmmdc(3, 20) = 1$
4. Se calculează d astfel încât $ed\%\phi = 1$. Adică $3d\%20 = 1$. Prin încercarea valorilor $(d = 1, 2, \ldots)$ se găsește valoarea $d = 7$, care îndeplinește condiția.
   - Se verifică: $e * d\%20 = 3 * 7\%20 = 1$
5. Cheile rezultate în urma calculului sunt:
   - cheia publică $= (e, n) = (3, 33)$
   - cheia privată $= (d, n) = (7, 33)$

Exemplu (2)

Valoarea modulului $n = 33$, este cea mai mică valoare posibilă a modulului pentru care algoritmul RSA poate funcționa.
După ce sunt determinate cheile se pot cripta mesaje. Dacă mesajul este $m = 7$, atunci : $c = m^e \mod n = 7^3 \mod 33 = 343 \mod 33 = 13$. Astfel că se obține mesajul cifrat $c = 13$.
Pentru a decripta mesajul $c = 13$ obținut prin criptarea de mai sus se calculează: $m' = c^d \mod n = 13^7 \mod 33 = 7$. Atenție la faptul că nu s-a calculat 13 la puterea 7. Pentru astfel de calcule se poate folosi următoarea proprietate: $a = b * c \mod n = (b \mod n) * (c \mod n) \mod n$. Astfel numerele mari pot fi descompuse în componente mai mici, care pot fi calculate ușor. O modalitate de a calcula m' este următoarea:

$$\begin{aligned} m' &= 13^7 \mod 33 = 13^{3+3+1} \mod 33 = 13^3 \cdot 13^3 \cdot 13 \mod 33 = \\ &= (13^3 \mod 33) \cdot (13^3 \mod 33) \cdot (13 \mod 33) \mod 33 = \\ &= (2197 \mod 33) \cdot (2197 \mod 33) \cdot (13 \mod 33) \mod 33 = \\ &= 19 \cdot 19 \cdot 13 \mod 33 = 7 \end{aligned}$$

Lungimea cheilor pentru o transmitere a datelor securizată folosind RSA este de obicei mai mare de 1024 biți.

Bibliografie

1. http://en.wikipedia.org/wiki/Public_key_cryptography
2. http://en.wikipedia.org/wiki/Key_authentication
3. http://en.wikipedia.org/wiki/Public_key_infrastructure
4. http://www.sun.com/blueprints/0801/publickey.pdf
5. http://en.wikipedia.org/wiki/Public_key_certificate
6. Securitatea datelor și criptografie, Aldea Constantin Lucian, 2007

Întrebări