Semnături digitale. Aplicaţii.

Emil Simion

Cuprins

Capitolul 1

Algoritmul RSA

1.1 Breviar teoretic

Algoritmul *RSA* a fost inventat de către *Ron Rivest, Adi Shamir* şi *Leonard Adleman* şi a fost studiat în cadrul unor studii criptanalitice extinse. Securitatea RSA-ului se bazează pe dificultatea factorizării numerelor mari. Cheia publică şi cheia privată sunt funcţie de o pereche de numere prime mari (de 200 de cifre sau chiar mai mari). Factorizarea produsului a două numere prime implică recuperarea textului clar din textul cifrat, cunoscând cheia publică.

Pentru generarea a două chei (publică şi privată) se aleg aleatoriu două numere prime mari p şi q. Din raţionamente de securitate p şi q au acelaşi ordin de mărime. Se va calcula produsul $n = p \cdot q$. Se va alege apoi, aleatoriu, exponentul public (de cifrare) e astfel ca e şi $(p-1)(q-1)$ să fie relativ prime. Utilizând algoritmul extins al lui Euclid vom calcula exponentul privat (de descifrare) d astfel ca

$$ed \equiv 1 \bmod (p-1)(q-1).$$

Cu alte cuvinte

$$d \equiv e^{-1} \bmod (p-1)(q-1).$$

Remarcăm faptul că d şi n sunt relativ prime. Perechea (e, n) constituie cheia publică iar (d, p, q) este cheia privată. Cele două numere p şi q nu mai sunt necesare la cifrare/descifrare, dar nu vor fi niciodată făcute publice (cunoaşterea lor şi a exponentului de cifrare e conduce imediat la determinarea coeficientului de descifrare d, deci sistemul de criptare devine inutil).

Pentru a cifra un mesaj M îl vom diviza în blocuri de lungime mai mică n (cu date binare vom alege cea mai mare putere a lui 2 mai mică decât n). Dacă p şi q sunt numere prime de 100 cifre atunci n va avea sub 200 de cifre iar fiecare mesaj bloc M_i va avea sub 200 de cifre. Dacă trebuie cifrate blocuri de lungime fixă atunci vom apela la operaţia de padding cu zero. Mesajul cifrat C se va obţine prin concatenarea mesajelor C_i care au aproximativ aceeiaşi lungime. Formula de cifrare va fi:

$$C_i \equiv M_i^e \bmod n.$$

Pentru a descifra un mesaj se calculează:

$$M_i \equiv C_i^d \bmod n,$$

deoarece

$$\begin{aligned} C_i^d &\equiv (M_i^e)^d \equiv M_i^{ed} \equiv M_i^{k(p-1)(q-1)+1} \\ &\equiv M_i M_i^{k(p-1)(q-1)} \equiv M_i \bmod n. \end{aligned}$$

Observaţia 1.1 *Pentru a evita metodele de factorizare cunoscute numerele p şi q trebuie să fie numere prime tari. Un număr prim p se numeşte număr prim tare dacă:*
i) $p-1$ are un factor mare r;
ii) $p+1$ are un factor mare s;
iii) $r-1$ are un factor mare t.

Operaţia de semnare a unui mesaj M se realizează prin exponenţierea amprentei $H(M)$ cu ajutorul cheii private: $s = H(M)^d \bmod n$. Verificarea semnăturii se realizează prin comparaţia lui $H(M)$ cu $s^e \bmod n$.

În cazurile practice valoarea lui e este un număr relativ mic, deci d are o valoare mare. Acest lucru conduce la timpi de rulare diferiţi între operaţiile private (descifrare/semnare) şi cele publice(cifrare/verificare semnătură).

Pentru optimizarea calculelor de verificare a semnăturii se poate utiliza lema chinezească a resturilor (CRT), însă acest lucru induce vulnerabilităţi în mediul de implementare.

Astfel, dacă $p > q$, sunt **precalculate** valorile:

$$\begin{aligned} &dP = (e^{-1} \bmod n) \bmod (p-1), \\ &dQ = (e^{-1} \bmod n) \bmod (q-1), \\ &qInv = q^{-1} \bmod p. \end{aligned}$$

În **faza de calcul** se execută:

$$\begin{aligned} &m_1 = c^{dP} \bmod p, \\ &m_2 = c^{dQ} \bmod q, \\ &h = qInv(m_1 - m_2) \bmod p, \\ &m = m_2 + hq. \end{aligned}$$

Cheia privată ce se stochează fiind $(p, q, dP, dQ, qInv)$.

1.2 Exerciţii rezolvate

Exerciţiul 1.2.1 *Se dă numărul $n = 36187829$ despre care se cunoaste faptul că este un produs de două numere cu valoarea $\phi(n) = 36175776$. Factorizaţi numărul n.*

Rezolvare: Folosim relaţile $p+q = n-(p-1)(q-1)+1$ şi $p-q = \sqrt{(p+q)^2-4n}$. Obţinem $p = 5657$ şi $q = 6397$.

Exerciţiul 1.2.2 *Să se cifreze mesajul* $M = 3$, *utilizând sistemul RSA cu următorii parametrii:* $N = 187$ *(modulul de cifrare),* $e = 7$ *(exponentul de cifrare).*

Rezolvare: Criptograma este: $C = M^e = 3^7 = 2187 = 130 \bmod 187$.

Exerciţiul 1.2.3 *Să se descifreze mesajul* $C = 130$, *utilizând sistemul RSA cu următorii parametrii:* $N = 187 = 11 \cdot 17$ *(modulul de cifrare),* $e = 7$ *(exponentul de cifrare).*

Rezolvare: Deoarece se cunoaşte factorizarea $N = 11 \cdot 17$, se poate calcula $\varphi(N) = 16 \cdot 10 = 160$, $\varphi(\varphi(N)) = 64$.

Exponentul de descifrare va fi:

$d = e^{\varphi(\varphi(N))-1} = 7^{63} = (7^9)^7 = (40353607)^7 = 7^7 = 823543 = 23 \bmod 160$.

Descifrarea mesajului cifrat C va fi: $C^d = 130^{23} = 3 = M \bmod 187$.

Exerciţiul 1.2.4 *Se consideră algoritmul de semnare RSA specificat de parametrii* $n = 971743$, $\phi(n) = 969760$, $d = 74597$, *aplicat asupra mesajului* $m = 2134$, *obţinându-se* $s = 689844$. *Semnătura* s *este validă?*

Rezolvare: Utilizând algoritmul lui Euclid obţinem: $e = d^{-1} \bmod \phi(n) = 13$. Calculăm $c^d \bmod n = 2134 = m$, deci semnătura este validă.

Exerciţiul 1.2.5 *Să se descifreze, utilizând CRT, mesajul cifrat* $c = 8363$, *pentru cazul în care* $p = 137$, $q = 131$, $n = p \cdot q = 17947$, $e = 3$, $d = 11787$.

Rezolvare: În faza de precalcul avem:

$$\begin{aligned}
&dP = (e^{-1} \bmod n) \bmod (p-1) = 91,\\
&dQ = (e^{-1} \bmod n) \bmod (q-1) = 87,\\
&qInv = q^{-1} \bmod p = 114.
\end{aligned}$$

Calculăm apoi:

$$\begin{aligned}
&m_1 = c^{dP} \bmod p = 102,\\
&m_2 = c^{dQ} \bmod q = 120,\\
&h = qInv(m_1 - m_2) \bmod p = 3,\\
&m = m_2 + hq = 513.
\end{aligned}$$

1.3 Exerciţii propuse

Exerciţiul 1.3.1 *Fie numerele prime* $p = 211$ *şi* $q = 167$. *Să se cifreze mesajul TEST cu ajutorul algoritmului RSA, utilizând exponentul public* $e = 2^8 + 1$. *Elementele din mesajul clar se codifică conform codului ASCII.*

Răspuns: $N = 35237$, $\phi(N) = 34860$, $d = 23873$, mesajul cifrat este: 01154 05746 04357 01154.

Exerciţiul 1.3.2 *Să se descifreze mesajul 01154 05746 04357 01154 cu ajutorul algoritmului RSA (*$p = 211$ *şi* $q = 167$*), utilizând exponentul public* $e = 2^8 + 1$. *Elementele din mesajul clar se decodifică conform codului ASCII.*

Răspuns: $N = 35237$, $\phi(N) = 34860$, $d = 23873$, mesajul clar este TEST.

Exerciţiul 1.3.3 *Să se cifreze mesajul* $M = 146$, *utilizând sistemul RSA cu următorii parametrii:* $n = 187$ *(modulul de cifrare),* $e = 7$ *(exponentul de cifrare).*

Răspuns: $C = 141$.

Exerciţiul 1.3.4 *Să se descifreze mesajul* $C = 141$, *utilizând sistemul RSA cu următorii parametrii:* $n = 187$ *(modulul de cifrare),* $d = 23$*(exponentul de descifrare).*

Răspuns: $M = 146$.

Capitolul 2

Semnătura ElGamal

2.1 Breviar teoretic

Fie p un număr prim pentru care problema logaritmului discret în Z_p este dificilă şi $\alpha \in {Z_p}^*$ un element primitiv. Cheia publică β se construieşte din cheia privată a: $\beta = \alpha^a \bmod p$.

Semnătura mesajului x, calculată cu ajutorul valorii secrete $k \in Z_{p-1}$, este definită ca fiind (γ, δ) unde:

$$\gamma = \alpha^k \bmod p \text{ şi } \delta = (H(x) - a\gamma)k^{-1} \bmod (p-1),$$

unde $H(\cdot)$ este o funcţie hash (sau x).

Semnătura (γ, δ) a mesajului x este verificată dacă are loc:

$$\beta^\gamma \gamma^\delta = \alpha^x \bmod p.$$

2.2 Exerciţii rezolvate

Exerciţiul 2.2.1 *Să se semneze mesajul $x = 101$ cu ajutorul algoritmului ElGamal specificat de parametrii următori: $p = 467$, $\alpha = 2$, cheia privată $a = 127$, alegând valoarea $k = 213$.*

Rezolvare: Se calculează $\beta = \alpha^a \bmod p = 2^{127} \bmod 467 = 132$

Semnătura mesajului $x = 101$ cu $k = 213$ (de remarcat faptul că $(213, 466) = 1$ şi $213^{-1} \bmod 466 = 431$) este:

$$\gamma = \alpha^k \bmod p = 2^{213} \bmod 467 = 29 \text{ şi } \delta = (101 - 127 \cdot 29) \cdot 431 \bmod 466 = 16.$$

2.3 Exerciţii propuse

Exerciţiul 2.3.1 *Să se semneze mesajul $x = 100$ cu ajutorul algoritmului ElGamal specificat de parametrii următori: $p = 163$, $\alpha = 2$, cheia privată $a = 127$, alegând valoarea $k = 215$.*

Răspuns: Semnătura mesajului este $(\gamma, \delta) = (52, 24)$.

Exerciţiul 2.3.2 *Să se semneze mesajul* $x = 102$ *cu ajutorul algoritmului ElGamal specificat de parametrii următori:* $p = 467$, $\alpha = 2$, *cheia privată* $a = 127$, *alegând valoarea* $k = 213$.

Răspuns: Semnătura mesajului este $(\gamma, \delta) = (29, 447)$.

Capitolul 3

Semnătura DSA

3.1 Breviar teoretic

Fie p un număr prim de 512 biţi şi q un factor prim de 160 biţi ai lui $p-1$ şi $\alpha \in {Z_p}^*$ o rădacină primitivă de ordin q a unităţii.

Cheia publică β se construieşte din cheia privată a: $\beta = \alpha^a \bmod p$. Semnătura mesajului x, calculată cu ajutorul valorii secrete $k \in Z_q^*$, este definită ca fiind (γ, δ) unde:

$$(\gamma, \delta) = ((\alpha^k \bmod p) \bmod q, (x + a\gamma)k^{-1} \bmod q).$$

Semnătura (γ, δ) a mesajului x este verificată dacă are loc următoarea egalitate, unde $e_1 = x\delta^{-1} \bmod q$ şi $e_2 = \gamma\delta^{-1} \bmod q$:

$$(\alpha^{e_1}\beta^{e_2} \bmod p) \bmod q = \gamma.$$

3.2 Exerciţii rezolvate

Exerciţiul 3.2.1 *Să se semneze mesajul $x = 100$ cu ajutorul algoritmului DSA specificat de parametrii următori: $p = 7879$, $q = 101$, $\alpha = 170$, valoarea aleatoare utilizată $k = 50$, cheia secretă fiind $a = 75$. Verificaţi rezultatul obţinut.*

Rezolvare: Se calculează:

$\gamma = (\alpha^k \bmod p) \bmod q = (170^{50} \bmod 7879) \bmod 101 = 2518 \bmod 101 = 94.$

$\delta = (x + a\gamma)k^{-1} \bmod q = (100 + 75 \cdot 94)50^{-1} \bmod 101 = 7150 \cdot 50^{-1} \bmod 101 = 7150 \cdot 99 \bmod 101 = 42.$

S-a folosit $50^{-1}(\bmod 101) = -2 \bmod 101 = 99$ (fiindcă $101 = 50 \cdot 2 + 1$).

Verificare:
$\beta = \alpha^a \bmod p = 170^{75} \bmod 7879 = 4567.$
$e_1 = x\delta^{-1} \bmod q = 100 \cdot 42^{-1} \bmod 101 = 100 \cdot 89 \bmod 101 = 12.$
$e_2 = \gamma\delta^{-1} \bmod q = 94 \cdot 42^{-1} \bmod 101 = 94 \cdot 89 \bmod 101 = 84.$
Se obţine:
$(\alpha^{e_1}\beta^{e_2} \bmod p) \bmod q = (170^{12} \cdot 4567^{84} \bmod 7879) \bmod 101 = 2518 \bmod 101 = 94 = \gamma.$

3.3 Exerciţii propuse

Exerciţiul 3.3.1 *Să se semneze mesajul* $x = 101$ *cu ajutorul algoritmului DSA specificat de parametrii următori:* $p = 7879$, $q = 101$, $\alpha = 170$, *valoarea aleatoare utilizată* $k = 50$, *cheia secretă fiind* $a = 75$. *Verificaţi rezultatul obţinut.*

Răspuns: Semnătura mesajului este $(\gamma, \delta) = (94, 40)$. Cheia publică este $\beta = 4567$.

Exerciţiul 3.3.2 *Să se semneze mesajul* $x = 102$ *cu ajutorul algoritmului DSA specificat de parametrii următori:* $p = 7879$, $q = 101$, $\alpha = 170$, *valoarea aleatoare utilizată* $k = 50$, *cheia secretă fiind* $a = 75$. *Verificaţi rezultatul obţinut.*

Răspuns: Semnătura mesajului este $(\gamma, \delta) = (94, 38)$. Cheia publică este $\beta = 4567$.