Protokol RSA

Protokol RSA

- Autoři: Ronald Rivest, Adi Shamir a Leonard Adleman.[a]
- Publikováno: R. L. Rivest, A. Shamir a L. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Commun. ACM* 21 (1978), 294–299.
- V USA patentováno 20. září 1983.

[a] James Ellis z Government Communication Headquarters (GCHQ) tentýž protokol zřejmě vytvořil již koncem 60. let 20. století.

Historie šifrování a další info, například

- S. Singh, *Kniha kódů a šifer*, Argo + Dokořán, Praha, 2003
- A. Hodges, *Alan Turing: The Enigma*, Random House, London, 1992

Dva uživatelé

A (Alice) a B (Bob) se veřejně dohodnou na čísle N a chtějí si vyměňovat tajné zprávy $0 \leq z < N$.
Každý si vytvoří veřejný a soukromý klíč.

Tvorba Aliciných klíčů (Bob postupuje analogicky)

1. Alice si tajně zvolí dvě různá prvočísla p_A, q_A tak, aby $n_A = p_A q_A > N$.
2. Alice spočte $\varphi(n_A) = (p_A - 1) \cdot (q_A - 1)$ a tajně zvolí v $\mathbb{Z}_{\varphi(n_A)}$ invertibilní prvek d_A.
3. Alice tajně spočte $e_A = d_A^{-1}$ v $\mathbb{Z}_{\varphi(n_A)}$.
4. Alice zveřejní (n_A, e_A) (veřejný klíč) a nezveřejní (n_A, d_A) (soukromý klíč).

Provoz: Bob posílá zprávu z Alici

1. Šifrování: Bob vyhledá Alicin veřejný klíč (n_A, e_A) a spočte $x = z^{e_A}$ v $\mathbb{Z}_{n_A}$.
2. Bob veřejně odešle Alici číslo x.
3. Dešifrování: Alice přijme x a spočte $z = x^{d_A}$ v $\mathbb{Z}_{n_A}$.

Terminologie:

- n_A Alicin modul.
- e_A Alicin šifrovací (encryption) exponent.
- d_A Alicin dešifrovací (decryption) exponent.

Příklad (Alice tvoří své klíče)

Veřejně dohodnuto: $N = 2\,500$.

1. Tajně: $p_A = 37$, $q_A = 79$.
2. Alicin modul: $n_A = p_A q_A = 2\,923 > 2\,500$.
3. $\varphi(n_A) = 36 \cdot 78 = 2\,808$.
4. Alicin dešifrovací exponent: $d_A = 11$ je invertibilní v $\mathbb{Z}_{2\,808}$.
5. Alicin šifrovací exponent: $e_A = d_A^{-1} = 1\,787$ v $\mathbb{Z}_{2\,808}$.
6. Veřejný klíč: $(n_A, e_A) = (2\,923, 1\,787)$.
7. Soukromý klíč: $(n_A, d_A) = (2\,923, 11)$.

Příklad (Posíláme Alici zprávu)

Chceme poslat: $z = 42$.

1. Alicin veřejný klíč: $(n_A, e_A) = (2\,923, 1\,787)$.
2. Spočteme: $x = 42^{1\,787} = 242$ v $\mathbb{Z}_{2\,923}$ (algoritmus opakovaných čtverců).
3. Odešleme: číslo 242.

Příklad (Alice přijímá zprávu)

Přijala: $x = 242$.

1. Alicin soukromý klíč: $(n_A, d_A) = (2\,923, 11)$.
2. Alice spočítá: $x^{11} = 242^{11} = 42$ v $\mathbb{Z}_{2\,923}$ (algoritmus opakovaných čtverců).
3. Původní zpráva: číslo 42.

Věta o korektnosti protokolu RSA

Jestliže $x = z^{e_A}$ v $\mathbb{Z}_{n_A}$, potom $z = x^{d_A}$ v $\mathbb{Z}_{n_A}$.

Důkaz.

$(z^{e_A})^{d_A} = z^{k\varphi(n_A)+1}$ pro nějaké celé k.

1. $\gcd(z, n_A) = 1$: hotovo (Eulerova věta).
2. $\gcd(z, n_A) \neq 1$: rozbor případů a Eulerova věta.

Věta o bezpečnosti protokolu RSA

Ať číslo n je součinem dvou neznámých různých prvočísel p a q. Znalost těchto prvočísel je ekvivalentní (v polynomiálním čase) znalosti čísla $\varphi(n)$.

Důkaz.

1. Známe p, q. Pak $\varphi(n) = (p-1)\cdot(q-1)$ (polynomiální čas!).
2. Známe $\varphi(n)$ a n. Takže známe $pq = n$ a $p+q = n+1-\varphi(n)$. Pak p, q jsou kořeny kvadratické rovnice (polynomiální čas!)

$$(x-p)\cdot(x-q) = x^2 - (n+1-\varphi(n))x + n = 0$$

Lov na prvočísla (The Great Internet Mersenne Prime Search)

Ke dni 6. 4. 2009 je největším známým prvočíslem číslo

$$2^{43\,112\,609} - 1$$

(GIMPS, 23. 8. 2008)
Má 12 978 189 cifer.
Viz např.

1. http://primes.utm.edu/primes/
2. http://www.mersenne.org/
3. nebo dodatky skript.

Jednoduché útoky

1. Útok hrubou silou.
2. Útok insidera při sdíleném modulu (nepovinný).
3. Útok outsidera při sdíleném modulu.
4. Útok při stejném malém veřejném exponentu.

Rafinovanější útoky

1. Wienerův útok (dodatek skript — nepovinné).
2. Řada dalších — viz literatura, např.
   D. Boneh, Twenty Years of Attacks on the RSA Cryptosystem, *Notices Amer. Math. Soc. (AMS)* 46(2), 1999, 203–213
   http://crypto.stanford.edu/~dabo/abstracts/RSAattack-survey.html

Příklad (Útok hrubou silou)

Eve[a] zachytila zprávu 11 pro Alici, zná Alicin veřejný klíč $(36\,181, 3\,989)$.
Eve postupuje takto:

1. Hrubou silou faktorizuje $36\,181 = 97 \cdot 373$.
   Vyzkouší prvočísla $\leq \sqrt{36\,181} \leq 191$.
2. Spočte $\varphi(36\,181) = \varphi(97) \cdot \varphi(373) = 96 \cdot 372 = 35\,712$.
3. Spočte $3\,989^{-1} = 16\,601$ v $\mathbb{Z}_{35\,712}$ a zná Alicin soukromý klíč $(36\,181, 16\,601)$.
4. $11^{16\,601} = 9\,703$ v $\mathbb{Z}_{36\,181}$ (čínská věta, opakované čtverce a Eulerova věta — minulá přednáška).
   9 703 je odeslaná zpráva.

[a] Z anglického eavesdropper — ten, kdo tajně naslouchá.

Slabiny útoku hrubou silou

Jediná, ale zásadní: faktorizační algoritmus hrubou silou. Pracuje v exponenciálním čase, únosný pro čísla $< 10^{12}$.

Modernější faktorizační algoritmy:

1. Pollardova $p - 1$ metoda, Pollardova ρ metoda (dodatek skript — nepovinné).
2. Number Field Sieve — nemáme vybudovanou teorii, viz např. V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge Univ. Press, 2005.
3. Shorův kvantový faktorizační algoritmus (polynomiální čas!), viz předmět Kvantové počítání, Libor Nentvich & Jiří Velebil.

Příklad (Útok outsidera při sdíleném modulu)

Alice posílá stejnou zprávu z dvěma účastníkům s veřejnými klíči $(n, e_1) = (703, 11)$ a $(n, e_2) = (703, 7)$. Eve zachytí dvě zprávy $c_1 = 694$ a $c_2 = 78$ v $\mathbb{Z}_{703}$.

Eve postupuje takto:

1. Spočítá $\gcd(11, 7) = 1$. Bezoutova rovnost
$$1 = 11 \cdot 2 + 7 \cdot (-3)$$
neboli
$$7 \cdot 3 + 1 = 11 \cdot 2$$
v $\mathbb{Z}$.
2. Dále
$$z^{7 \cdot 3 + 1} = z^{11 \cdot 2} \quad \text{v } \mathbb{Z}_{703}$$
čili
$$78^3 \cdot z = 694^2 \quad \text{v } \mathbb{Z}_{703}$$

Příklad (Útok outsidera při sdíleném modulu)

3. Takže máme vyřešit
$$27 \cdot z = 81 \quad \text{v } \mathbb{Z}_{703}$$
Protože $\gcd(703, 27) = 1$, existuje jediné řešení $z = 3$.
4. Odeslaná zpráva je $z = 3$.

Co kdyby výše uvedená rovnice neměla jednoznačné řešení?

To poznáme nalezením $\gcd$. Pak ale faktorizujeme modul RSA v polynomiálním čase. Viz skripta.

Ztížení útoku outsidera

Soudělnost exponentů: pak musíme řešit problém diskrétní odmocniny:

$$z^d = x \quad \text{v } \mathbb{Z}_n \quad \Rightarrow \quad z = \sqrt[d]{x} \quad \text{v } \mathbb{Z}_n$$

Příklad (Útok při stejném malém veřejném exponentu)

Tři účastníci s veřejnými klíči $(n_1, e) = (253, 3)$, $(n_2, e) = (51, 3)$ a $(n_3, e) = (145, 3)$.
Eve zachytí zprávy $c_1 = 86$, $c_2 = 9$ a $c_3 = 40$ pro tyto účastníky, které vznikly zašifrováním stejné neznámé zprávy z.
Eve postupuje takto:

1. Platí soustava rovnic

$$x = z^3 = 86 \text{ v } \mathbb{Z}_{253} \quad x = z^3 = 9 \text{ v } \mathbb{Z}_{51} \quad x = z^3 = 40 \text{ v } \mathbb{Z}_{145}$$

2. $x = 3\,375$ v $\mathbb{Z}_{1\,870\,935}$ (čínská věta, protože moduly $n_1 = 253$, $n_2 = 51$ a $n_3 = 145$ jsou navzájem nesoudělné).
3. Platí $3\,375 = z^3 < n_1 n_2 n_3 = 1\,870\,935$. Eve nalezne zprávu z obyčejnou třetí odmocninou: $z = 15$.

Ztížení útoku při stejném malém veřejném exponentu

Soudělnost modulů a současně velká zpráva: pak nemůžeme použít čínskou větu o zbytcích, ani její zobecnění.

Další kryptosystémy založené na počítání modulo

1. Výměna klíče podle Diffieho a Helmanna (viz skripta — nepovinné).
2. Elgamalův protokol (viz skripta — nepovinné).
3. k-Threshold System for Sharing a Secret (viz skripta — nepovinné).
4. . . . a řada dalších, viz např.
   M. J. Atallah, *Algorithms and Theory of Computation Handbook*, CRC Press, New York, 1999

Více o rozložení prvočísel a testech prvočíselnosti

1. Skripta — dodatky (nepovinné).
2. V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge Univ. Press, 2005.
3. Předmět Kvantové počítání, Libor Nentvich & Jiří Velebil.