RSA

Jakub Klemsa

Úvod do kryptologie
Fakulta jaderná a fyzikálně inženýrská

3. dubna 2013

1. Teorie
   - Bude se hodit
   - Asymetrická šifra RSA
2. Lámání RSA
   - Fermatova metoda
   - Pollardova $p - 1$ metoda
   - Wienerův útok
   - Využití jiných chyb nepřítele
3. Použití RSA
   - Šifrování komunikace
   - Digitální podepisování

Bude se hodit

- Eukleidův algoritmus $\big(a \geq b,\ \text{pak NSD}(a,b) = \text{NSD}(a \bmod b, b) \ldots\big)$,
- řešení celočíselné rovnice $\text{NSD}(a,b) = ax + by$,
- Eulerova funkce $\big(\varphi(n) = \#\{k \in \mathbb{N} \mid k \leq n,\ k \perp n\}\big)$,
- Eulerova věta $\big(a \perp n,\ \text{pak } a^{\varphi(n)} \equiv 1 \pmod{n}\big)$,
- ...

RSA – historie

- poprvé 1973 v tajné službě (Clifford Cocks),
- civilní 1977 (Rivest, Shamir a Adleman).

RSA – příprava

- vygenerujeme velká (opravdu velká) prvočísla p, q,
- spočteme modulus $n = p \cdot q$,
- snadno spočteme hodnotu Eulerovy fce $\varphi(n) = (p-1) \cdot (q-1)$,

RSA – příprava

- vygenerujeme velká (opravdu velká) prvočísla p, q,
- spočteme modulus $n = p \cdot q$,
- snadno spočteme hodnotu Eulerovy fce $\varphi(n) = (p-1) \cdot (q-1)$,
- vygenerujeme e takové, že $1 < e < \varphi(n)$, $e \perp \varphi(n)$,
- ověříme Eukleidovým algoritmem,

RSA – příprava

- vygenerujeme velká (opravdu velká) prvočísla p, q,
- spočteme modulus $n = p \cdot q$,
- snadno spočteme hodnotu Eulerovy fce $\varphi(n) = (p-1) \cdot (q-1)$,
- vygenerujeme e takové, že $1 < e < \varphi(n)$, $e \perp \varphi(n)$,
- ověříme Eukleidovým algoritmem,
- odtud získáme i řešení (d, k) rovnice $e \cdot d - k \cdot \varphi(n) = 1$,
- nastavíme $1 < d < \varphi(n)$.

RSA – zveřejnění

- (n, e) uveřejníme jako veřejný klíč,
- (n, d) uchováme jako soukromý klíč,
- VŠEHO ostatního (p, q, $\varphi(n)$, ...) se bezpečně zbavíme!

RSA – postup šifrování Alice → Bob

- Alice si nechá poslat od Boba jeho veřejný klíč (n, e),
- tajnou zprávu $(m \in \{0, \ldots, n-1\})$ Alice zašifruje: $c = m^e \mod n$,
- zašifrovanou zprávu c pošle Bobovi,
- Bob c dešifruje svým soukromým klíčem (n, d) stejným způsobem: $m = c^d \mod n$.

RSA – funkčnost

Tvrzení

Pro n, e, d, m, c (dle předchozího značení) platí

$$c^d \equiv (m^e)^d \equiv m \pmod{n}.$$

RSA – funkčnost

Tvrzení

Pro n, e, d, m, c (dle předchozího značení) platí

$$c^d \equiv (m^e)^d \equiv m \pmod{n}.$$

Důkaz.

$m \perp n$

$$ed = k\varphi(n) + 1 \quad \ldots \text{ze zavádění RSA}$$
$$m^{\varphi(n)} \equiv 1 \pmod{n} \quad \ldots \text{Eulerova věta}$$
$$m^{k\varphi(n)} \equiv 1 \pmod{n} \quad \ldots \text{umocnění na } k$$
$$m^{k\varphi(n)+1} = m^{ed} \equiv m \pmod{n} \quad \ldots \text{vynásobení } m$$

RSA – funkčnost

Důkaz.

$m \not\perp n$

$$\exists a \in \mathbb{N}: \ m = a \cdot p \quad \text{(BÚNO } p\text{)}$$

$$m < n \Rightarrow a < q \Rightarrow a \perp q \Rightarrow ap = m \perp q$$

$$m^{\varphi(q)} \equiv 1 \pmod{q} \quad \ldots \text{Eulerova věta}$$

$$m^{k\varphi(p)\varphi(q)} = m^{k\varphi(pq)} \equiv 1 \pmod{q} \quad \ldots \text{umocnění}$$

$$\exists b \in \mathbb{N}: \ m^{k\varphi(n)} = bq + 1$$

$$m^{k\varphi(n)+1} = m^{ed} = bqm + m \quad \ldots \text{vynásobení } m$$

$$m^{ed} = bq \cdot ap + m = ban + m \equiv m \pmod{n}$$

□

RSA – příklad

Příklad

Kelišová chce poslat Cecilce nový drb. Cecilka vygeneruje dvě „velká“ prvočísla 11 a 13, spočte $n = 143$, $\varphi(n) = 120$ a vygeneruje $e = 13$. Eukleidovým algoritmem dostane

$$120 = 9 \cdot 13 + 3$$
$$13 = 4 \cdot 3 + 1$$
$$3 = 3 \cdot 1 + 0$$

Odtud zná rozklad $1 = 37 \cdot 13 - 4 \cdot 120$, tedy $d = 37$. Dvojici $(143, 13)$ pošle Kelišovej jako veřejný klíč. Kelišová bude chtít, jak jinak, poslat šifrovanou zprávu 42, spočte tedy $42^{13} \mod 143 = 3$ a odešle. Cecilka zprávu $c = 3$ stejným způsobem dešifruje svým soukromým klíčem $d = 37$ a vyjde jí dychtivě očekávaná $42 = 3^{37} \mod 143$.

Jaké jsou možnosti lámání RSA

RSA zlomíme, pokud vyřešíme alespoň jeden z problémů:

1. najít prvočíselný rozklad velkého čísla (factorization problem),
2. spočítat d ze znalosti (n, e),
3. vypočítat e-tou odmocninu modulo n.

Ani na jeden však není znám polynomiální algoritmus, jako nejslibnější cesta se jeví faktorizace n, odkud již vše dopočítáme.

Jaké jsou možnosti lámání RSA

RSA zlomíme, pokud vyřešíme alespoň jeden z problémů:

1. najít prvočíselný rozklad velkého čísla (factorization problem),
2. spočítat d ze znalosti (n, e),
3. vypočítat e-tou odmocninu modulo n.

Ani na jeden však není znám polynomiální algoritmus, jako nejslibnější cesta se jeví faktorizace n, odkud již vše dopočítáme.

Zajímavost

Za předpokladu platnosti Zobecněné Riemannovy hypotézy mají body (1) a (2) stejnou složitost až na polynomiální člen.
Nicméně zatím není znám důkaz o ekvivalenci složitosti bodů (1) a (3).

Faktorizace v číslech

- 300-bitové číslo lze rozložit na dnešním PC s volně dostupným softwarem v řádu hodin,
- 512-bitové za několik týdnů,
- zatím (2014) nejdelší rozložené je 768-bitové, 232 decimálních cifer.

Faktorizace v číslech

- 300-bitové číslo lze rozložit na dnešním PC s volně dostupným softwarem v řádu hodin,
- 512-bitové za několik týdnů,
- zatím (2014) nejdelší rozložené je 768-bitové, 232 decimálních cifer.

$$
\begin{aligned}
&123018668453011775513049495838496272077285356959533479219732\\
&245215172640050726365751874520219978646938995647494277406384\\
&592519255732630345373154826850791702612214291346167042921431\\
&160222124047927473779408066535141959745985690214341 3\\
&=\\
&334780716989568987860441698482126908177047949837137685689124\\
&313889828837938780022876147116525317430877378144679994 89\\
&\times\\
&367460436667995904282446337996279526322791581643430876426760\\
&322838157396665112792333734171433968102700927987363089 17.
\end{aligned}
$$

Máme se bát?

Zvláštní pozornost je věnována 1024-bitovému číslu – délka 1024 bitů se stále hojně používá, přestože doporučená délka je 2048 bitů.

Větší problém by představoval kvantový počítač, který by „uměl“ faktorizovat. Peter Shor r. 1994 ukázal, že kvantový počítač k tomuto účelu postavený by byl schopen faktorizovat v polynomiálním čase!

- problém faktorizace patří do třídy BQP (Shorův algoritmus), domnívá se nebýt ani v P, v NP-complete ani v co-NP-complete,
- jazyk prvočísel $\mathbb{P}$ patří do co-RP (Rabin-Millerův test, prvočíslo přijme vždy, složené přijme s malou pstí), AKS test dokonce P.

Frematova metoda

Předpokládá malý rozdíl p a q, prakticky $p - q < 2n^{\frac{1}{4}}$. Nahlédneme

$$n = p \cdot q = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$$

$$D^2 - n = \left(\frac{p-q}{2}\right)^2, \text{ kde } D := \frac{p+q}{2}$$

Frematova metoda

Předpokládá malý rozdíl p a q, prakticky $p - q < 2n^{\frac{1}{4}}$. Nahlédneme

$$n = p \cdot q = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$$

$$D^2 - n = \left(\frac{p-q}{2}\right)^2, \text{ kde } D := \frac{p+q}{2}$$

Pro D od $\lceil\sqrt{n}\rceil$ testujeme, je-li $D^2 - n$ čtverec.
Jakmile ano, dopočteme $p, q = D \pm \sqrt{D^2 - n}$.

Poznámka

Požadavek $p - q < 2n^{\frac{1}{4}}$ znamená, že se p, q liší v zápise pouze na poslední $1/4$ pozic.

Sieve: zefektivnil aplikováním vlastností čtverců modulo různá čísla.

Pollardova $p - 1$ metoda

Viz přednášku Lukáše Pohanky.

Wienerův útok

Tvrzení

Nechť platí $q < p < 2q$ a $d < \frac{1}{3} n^{\frac{1}{4}}$. Potom lze z (n, e) efektivně získat d včetně faktorizace $n = p \cdot q$.

Wienerův útok

Tvrzení

Nechť platí $q < p < 2q$ a $d < \frac{1}{3}n^{\frac{1}{4}}$. Potom lze z (n, e) efektivně získat d včetně faktorizace $n = p \cdot q$.

Postup:

$$ed = k(p-1)(q-1) + 1$$

$$\frac{e}{pq} = \frac{k}{d}\left(1 - \frac{p+q-1-\frac{1}{k}}{pq}\right) = \frac{k}{d}(1-\delta)$$

Podíl $\frac{k}{d}$ je blízko $\frac{e}{pq}$, který známe, přitom obsahuje menší čísla. K odhadu tak poslouží řetězové zlomky.

Wienerův útok

Příklad

$(n, e) = (90\,581, 17\,993)$, $d = ?$. Řetězový zlomek vyjde

$$\frac{17\,993}{90\,581} = 0 + \cfrac{1}{5 + \cfrac{1}{29 + \cfrac{1}{\ddots + \cfrac{1}{3}}}} = [0, 5, 29, 4, 1, 3, 2, 4, 3].$$

Wienerův útok

Příklad

$(n, e) = (90\,581, 17\,993)$, $d = ?$. Řetězový zlomek vyjde

$$\frac{17\,993}{90\,581} = 0 + \cfrac{1}{5 + \cfrac{1}{29 + \cfrac{1}{\ddots + \cfrac{1}{3}}}} = [0, 5, 29, 4, 1, 3, 2, 4, 3].$$

Odtud posloupnost odhadů

$$\frac{k}{d} = 0, \frac{1}{5}, \frac{29}{146}, \frac{117}{589}, \ldots, \frac{17\,993}{90\,581}.$$

Wienerův útok

Příklad

Zkusíme spočítat $\varphi(n)$ pro první smysluplný odhad $\frac{1}{5}$, tedy $k = 1$ a $d = 5$:

$$\varphi(n) = \frac{ed - 1}{k} = 89\,964,$$

ověříme správnost vyřešením

$$x^2 - (n - \varphi(n) + 1)\, x + n = 0,$$

dostaneme kořeny $x_{1,2} = 379,\ 239$. Opravdu, $90\,581 = 379 \cdot 239$.

Dle Wienerova teorému má útok fungovat pro $d < \frac{N^{\frac{1}{4}}}{3} \doteq 5{,}7828$.

Wienerův útok

Příklad

Zkusíme spočítat $\varphi(n)$ pro první smysluplný odhad $\frac{1}{5}$, tedy $k = 1$ a $d = 5$:

$$\varphi(n) = \frac{ed - 1}{k} = 89\,964,$$

ověříme správnost vyřešením

$$x^2 - (n - \varphi(n) + 1)\, x + n = 0,$$

dostaneme kořeny $x_{1,2} = 379,\ 239$. Opravdu, $90\,581 = 379 \cdot 239$.

Dle Wienerova teorému má útok fungovat pro $d < \frac{N^{\frac{1}{4}}}{3} \doteq 5{,}7828$.

Nicméně není znám útok pokud e je malé (samozřejmě za předpokladu velkého m, bude zmíněno). Přesto je dle směrnice NIST v USA zakázáno používat $e < 65537$, a to bez odůvodnění.

Využití jiných chyb nepřítele – dvojí použití p

- použije-li někdo p se dvěma $q_{1,2}$, potom $p = \mathrm{NSD}(n_1, n_2)$,
- L.P. 2012 takto otestovány miliony klíčů získatelných z internetu,
- 0.2% (tisíce) prolomeno Eukleidovým algoritmem!
- typicky v embedded aplikacích: firewally, routery, VPN, vzdálené správy, tiskárny, projektory, VoIP telefony, od více než 30 firem,
- problém nebyl v ignoraci dvojího použití, ale ve slabých RNG,
- doporučení zní
  - zaseedovat RNG alespoň dvakrát delším seedem než požadovaný výstup,
  - dopočítat q deterministicky.

Využití jiných chyb nepřítele – slabiny zpráv

„Malé“ zprávy

- může se stát, že $m^e < n$,
- myšlenka: doplnit krátkou zprávu zepředu náhodnými znaky,
- problém: původní verze standardu doplňování PKCS#1 měla slabinu.

Využití jiných chyb nepřítele – slabiny zpráv

„Malé“ zprávy

- může se stát, že $m^e < n$,
- myšlenka: doplnit krátkou zprávu zepředu náhodnými znaky,
- problém: původní verze standardu doplňování PKCS#1 měla slabinu.

Pozor na Čínskou zbytkovou větu

- pošleme stejnou zprávu e nebo více příjemcům,
- ti používají stejné e, ale různá p, q,

$$m^e \mod n_1$$
$$\vdots$$
$$m^e \mod n_e$$

dostanu $m^e \mod n_1 \cdot \ldots \cdot n_e = m^e$, stačí odmocnit.

Využití jiných chyb nepřítele – jeho vlastní blbost

- zachytíme komunikaci Alice $\rightarrow$ Bob (získáme c),
- přemluvíme Boba, aby dešifroval $c \cdot r^e \mod n$ pro náhodné r,
- vrátí nám $m \cdot r \mod n$, stačí dopočítat m.

Využití jiných chyb nepřítele – doba dešifrování

- kryptologie velí využít veškerý důvtip (např. Enigma),
- Kocher (1995) – měřme čas strávený dešifrováním (délka odezvy, EM pole poblíž procesoru, ...),
- získáme informaci navíc – množina klíčů se výrazně zmenšuje,
- doporučení zní
  - vygenerovat tajné náhodné r,
  - dešifrovat $c \cdot r^e \mod n$ (podobně jako popsáno dříve),
  - tedy jinou zprávu než mohl útočník zachytit.

Šifrování komunikace

- pro přenos dat je náročnost RSA příliš velká,
- používá se pouze pro přenos klíče symetrické šifry (tzv. hybridní kryptosystém),
- doporučená délka modulu je u RSA 2048 bitů, u symetrické šifry 128–256 bitů,
- standardně se používá $e = 65537$ (má malou bitovou váhu).

Digitální podepisování

Viz přednášku Katky Pastirčákové.