ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Problémy implementácie RSA

Univerzita Komenského, 2019

Mgr. Ján Kotrady

Obsah

- Popis RSA
- Základné problémy
- Chybný generátor náhodných čísel
- ROCA útok

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

RSA problém

Definujeme RSA problém podľa [1] nasledovne: Nech je dané kladné celé číslo n, ktoré je produktom dvoch odlišných nepárnych prvočísel p a q, kde $|p| \approx |q|$, kladné celé číslo e také, že $\mathrm{nsd}\big(e, (p-1)(q-1)\big) = 1$ a číslo c, pre ktoré existuje číslo m, také, že:

$$m^e \equiv c \ (\mathrm{mod}\ n)$$

Číslo pq nazývame verejný modul a číslo e verejný exponent.

RSA problém: „rozložiť (faktorizovať) verejný modul n (od 1024 bitov) na súčin dvoch rovnako veľkých prvočísel (od 512 bitov)“

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Problém faktorizácie

Definícia: Nech $n \in \mathbb{N}, n > 1$. Prvočíselný rozklad (faktorizácia) označíme každý zápis $p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_k^{m_k}$, ktorý splňuje nasledujúce podmienky:

1. $p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_k^{m_k} = n,$
2. $k, m_1, \ldots, m_k \in \mathbb{N}$
3. $p_1, \ldots, p_k$ sú rôzne prvočísla.

+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Algoritmy

- 2^16 ≈ 10^5 – Tabuľka prvočísel
- Menej ako 2^70 ≈ 10^21 Modifikácia Pollard's rho algoritmu
- Menej ako 2^166 ≈ 10^50: Lenstrov algoritmus
- Menej ako 2^332 ≈ 10^100: Quadratic Sieve
- Viac ako 2^332 ≈ 10^100: General Number Field Sieve

- [??]

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Časová zložitosť faktorizácie

- 2^60 - Čas v sekundách od vzniku vesmíru
- Number field sieve: $O\left(\exp\left(\left(\frac{64}{9}b\right)^{\frac{1}{3}}(\log(b))^{\frac{2}{3}}\right)\right)$, *b-bitové* číslo [4]
- RSA - 2048 bit ≈ 112-bit AES ≈ 2^112 operácií [nist.gov]
- (2010) Faktorizácia 768 bitového kľúča by trvala 2000 rokov na 1 jadrovom 2,2 GHz procesore [4]

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Spoločný modulus – problém so zlým N

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Spoločný modulus – problém so zlým N

- Bob

$$\langle e_b, N \rangle, \langle d_b, N \rangle$$

- Alica

$$\langle e_a, N \rangle, \langle d_a, N \rangle$$

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Spoločný modulus – problém so zlým N

- Bob

$$\langle e_b, N \rangle, \langle d_b, N \rangle$$

- Alica

$$\langle e_a, N \rangle, \langle d_a, N \rangle$$

- Je táto schéma bezpečná ?

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Spoločný modulus – problém so zlým N

- Bob

$$\langle e_b, N \rangle, \langle d_b, N \rangle$$

- Alica

$$\langle e_a, N \rangle, \langle d_a, N \rangle$$

- Je táto schéma bezpečná ?

$$e \cdot d = 1 \, mod \varphi(n)$$

$$\varphi(n) = (p-1)(q-1) = pq - p - q + 1$$

$$p + q = n - \varphi(n) + 1$$

$$f(x) = (x-p)(x-q) = x^2 + (p+q)x + pq$$

+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

„Zaslepenie“

- Bob

$$\langle e, N \rangle, \langle d, N \rangle$$

- Útočník požiada o podpis správy M
- Bob odmietne (neprevedie si nehnuteľnosť na cudziu osobu) ☺
- Útočník vyberie r náhodné a požiada o podpis $M' = r^e M$

$$S' = (r^e M)^d \ mod \ N$$

- Útočník odstráni r

$$S = \frac{(r^e M)^d}{r} \ mod \ N$$

+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Nízky privátny exponent $d < \frac{1}{3}N^{1/4}$

$$ed - k\varphi(N) = 1$$

$$\left|\frac{e}{\varphi(N)} - \frac{k}{d}\right| = \frac{1}{d\varphi(N)}$$

$$\varphi(N) = N - p - q + 1, p + q - 1 < 3\sqrt{N}$$

$$|N - \varphi(N)| < 3\sqrt{N}$$

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{ed - kN + k\varphi(N) - k\varphi(N)}{Nd}\right| = \left|\frac{1 - k(N - \varphi(N))}{Nd}\right| \leq \left|\frac{3k\sqrt{N}}{Nd}\right| = \left|\frac{3k}{\sqrt{N}d}\right|$$

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Nízky privátny exponent $d < \frac{1}{3} N^{1/4}$

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{ed - kN + k\varphi(N) - k\varphi(N)}{Nd}\right| = \left|\frac{1 - k(N - \varphi(N))}{Nd}\right| \leq \left|\frac{3k\sqrt{N}}{Nd}\right| = \left|\frac{3k}{\sqrt{N}d}\right|$$

$$k\varphi(\mathrm{N}) = \mathrm{ed} - 1 < \mathrm{ed}$$

$$\mathrm{e} < \varphi(\mathrm{N}) \Rightarrow k < \mathrm{d} < \frac{1}{3} N^{1/4}$$

$$\left|\frac{e}{N} - \frac{k}{d}\right| \leq \left|\frac{1}{dN^{\frac{1}{4}}}\right| < \left|\frac{1}{2d^2}\right|$$

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Nízky privátny exponent $d < \frac{1}{3} N^{1/4}$

$$\left|\frac{e}{N} - \frac{k}{d}\right| \leq \left|\frac{1}{dN^{\frac{1}{4}}}\right| < \left|\frac{1}{2d^2}\right|$$

Dirichlet 1842 – k/d je "continued fractions" z e/N

Rastu rýchlo $\frac{p_m}{q_m}$, $q_m > F_m$, kde F_m je m-te Fibbonaciho číslo, potom platí, že $\log N$ konvergantov existuje.

Wienerov útok

Step	Real Number	Integer part	Fractional part	Simplified	Reciprocal of f
1	$r = \frac{649}{200}$	$i = 3$	$f = \frac{649}{200} - 3$	$= \frac{49}{200}$	$\frac{1}{f} = \frac{200}{49}$
2	$r = \frac{200}{49}$	$i = 4$	$f = \frac{200}{49} - 4$	$= \frac{4}{49}$	$\frac{1}{f} = \frac{49}{4}$
3	$r = \frac{49}{4}$	$i = 12$	$f = \frac{49}{4} - 12$	$= \frac{1}{4}$	$\frac{1}{f} = \frac{4}{1}$
4	$r = 4$	$i = 4$	$f = 4 - 4$	$= 0$	 STOP

Coppersmith a Hastad

Veta: Nech N je prirodzené číslo a $f \in \mathbb{Z}[x]$ je monický polynóm stupňa d. Položme $X = N^{\frac{1}{d}-\mathcal{E}}$ pre nejaké $\mathcal{E} > 0$. Potom pre dané $\langle N, f \rangle$ vieme efektívne nájsť všetky prirodzené čísla $|x_0| < X$, splňujúce $f(x_0) = 0 \; mod \; N$.

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Coppersmith a Hastad

- Bob chce poslať správu M pre príjemcu $P_1, \ldots, P_k$, každý ma kľúč $\langle N_i, e_i \rangle$. Bob zašifruje správu pre každého príjemcu.
- Čínska veta o zbytkoch sa aplikuje na výpočet

$$C' = M^k \, mod N_1 N_2 \ldots N_k$$

Ak $k > e$, je možné správu dešifrovať.

Riešenie je padding

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Coppersmith a Hastad

- Ak je padding polynomiálny, napríklad
$$f(x) = i2^m + M$$
- Lenže Coppersmith dokázal, že pre určité polynómy vieme nájsť riešenie.
- Bob posiela:
$$f(M)^e$$
- Hastad-ová veta hovorí:

„Ak existuje $M < N_{min}$ a g_i spĺňajúce $g_i(M) = 0\ mod\ N_i$, je možné nájsť M“

+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Coppersmith a Hastad

$$g_i = f_i^e - C_i$$

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Bleichenbacher's Attack na PKCS 1

- Padding:

- Ako odpovedá server ?
- Vieme konvergovať k správnemu odhadu
- Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1, Daniel Bleichenbacher
- 2^{20}

Timing attack

- Rýchli výpočet mocniny:

1. Nastav z rovné M a C rovné 1. Pre $i = 0, \ldots, n$ vykonaj:
2. Ak $d_i = 1$, nastav C rovné $C \cdot z \; mod \; N$,
3. Nastav z rovné $z^2 \; mod \; N$.

Nakonci, C obsahuje hodnotu $M^d \; mod \; N$.

- n je veľkosť bitov d.
- Závislosť medzi časom t_i a T_i, kde t_i je čas výpočtu $M_i \cdot M_i^2 \; mod \; N$ a T_i je celkový čas

+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Problém faktorizácie v asymetrickej kryptografii alebo naozaj sa Ron mýlil ?

Bakalárska práca

Vedúci práce: RNDr. Rastislav Krivoš-Belluš, PhD.

Autor: Mgr. Ján Kotrady

UPJŠ, Košice, 2017

Časová zložitosť faktorizácie

- 2^60 - Čas v sekundách od vzniku vesmíru
- Number field sieve: $O\left(\exp\left(\left(\frac{64}{9}b\right)^{\frac{1}{3}}(\log(b))^{\frac{2}{3}}\right)\right)$, *b-bitové* číslo [4]
- RSA - 2048 bit ≈ 112-bit AES ≈ 2^112 operácií [nist.gov]
- (2010) Faktorizácia 768 bitového kľúča by trvala 2000 rokov na 1 jadrovom 2,2 GHz procesore [4]

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

RSA problém

Definujeme RSA problém podľa [1] nasledovne: Nech je dané kladné celé číslo n, ktoré je produktom dvoch odlišných nepárnych prvočísel p a q, kde $|p| \approx |q|$, kladné celé číslo e také, že $\mathrm{nsd}\big(e, (p-1)(q-1)\big) = 1$ a číslo c, pre ktoré existuje číslo m, také, že:

$$m^e \equiv c \ (\mathrm{mod}\ n)$$

Číslo pq nazývame verejný modul a číslo e verejný exponent.

RSA problém: „rozložiť (faktorizovať) verejný modul n (od 1024 bitov) na súčin dvoch rovnako veľkých prvočísel (od 512 bitov)“

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Algoritmy

- 2^16 ≈ 10^5 – Tabuľka prvočísel
- Menej ako 2^70 ≈ 10^21 Modifikácia Pollard's rho algoritmu
- Menej ako 2^166 ≈ 10^50: Lenstrov algoritmus
- Menej ako 2^332 ≈ 10^100: Quadratic Sieve
- Viac ako 2^332 ≈ 10^100: General Number Field Sieve

- Algoritmus najväčšieho spoločného deliteľa

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Faktorizácia algoritmom najväčšieho spoločného deliteľa

- Euklidov algoritmus

$$O(\log(a)\log(b)) \approx O(n^2), \log(a) = n = \log(\mathrm{b})$$

- NSD Euklidovým algoritmom:

```
function nsd(u, v)
    if v = 0
        return u
    else
        return nsd(v, u mod v).
```

$$
\begin{aligned}
37894060279 &= 2 \times 18272779829 + 1348500621 \\
18272779829 &= 13 \times 1348500621 + 742271756 \\
1348500621 &= 1 \times 742271756 + 606228865 \\
742271756 &= 1 \times 606228865 + 136042891 \\
606228865 &= 4 \times 136042891 + 62057301 \\
136042891 &= 2 \times 62057301 + 11928289 \\
62057301 &= 5 \times 11928289 + 2415856 \\
11928289 &= 4 \times 2415856 + 2264865 \\
2415856 &= 1 \times 2264865 + 150991 \\
2264865 &= 15 \times \underline{150991} + 0
\end{aligned}
$$

+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Najväčší spoločný deliteľ

- Dve verejné moduly zdieľajúce práve jedno prvočíslo
  - **Veta**: Nech $p, q, r \in \mathbb{N}, p, q, r$ sú prvočísla. Nech $n_1 = pq$ a $n_2 = pr$, pričom $n_1 \neq n_2$, tak nsd(n_1,n_2) = p.
- Bez databázy prvočísel
- Efektívny algoritmus
- Databáza verejných modulov

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

NSD ako riešenie RSA problému

Pravdepodobnosť výsledku ?

Počet 512 bitový prvočísel: 1,8853 10^151

Upravený narodeninový paradox

$$1 - p', \quad p' = \frac{n(n-2)(n-4)\cdots\left(n-2(k-1)\right)}{n^k} \approx e^{\frac{[-2-4\cdots-2(k-1)]}{n}} = e^{\frac{[-(k-1)k]}{n}}$$

$$k \approx \sqrt{n\ ln(2)}$$

50 % prav., potrebujeme: 2,898881 10^150 modulov

5 % prav., potrebujeme: 9,833780957 10^74 modulov (4,2 10^9)

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Tak poďme skúsiť niečo faktorizovať...

Faktorizácie modulov

- 1.768.019 rôznych IP adries, port 22 (SSH), 443 (SSL)
  - SSL – 209.499
  - SSH – 1.558.520
    - 20 dní
- 1.363.129 SSH kľúčov, unikátnych iba 591.864
- 93.505 SSL kľúčov, unikátnych iba 53.487
- 591.267 pgp výpis
- Zmap, openssl, ssh-keyscan, ssh-keygen, x509, pgpdump, asn1

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Faktorizácie modulov

- Získali sme približne 1,2M rôznych RSA modulov
- Spustili algoritmus NSD na každú dvojicu kľúčov
- Približný čas trvania tohto algoritmu bol 40 dní
- $O(m^2n^2)$, kde m je počet verejných modulov

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Faktorizácie modulov

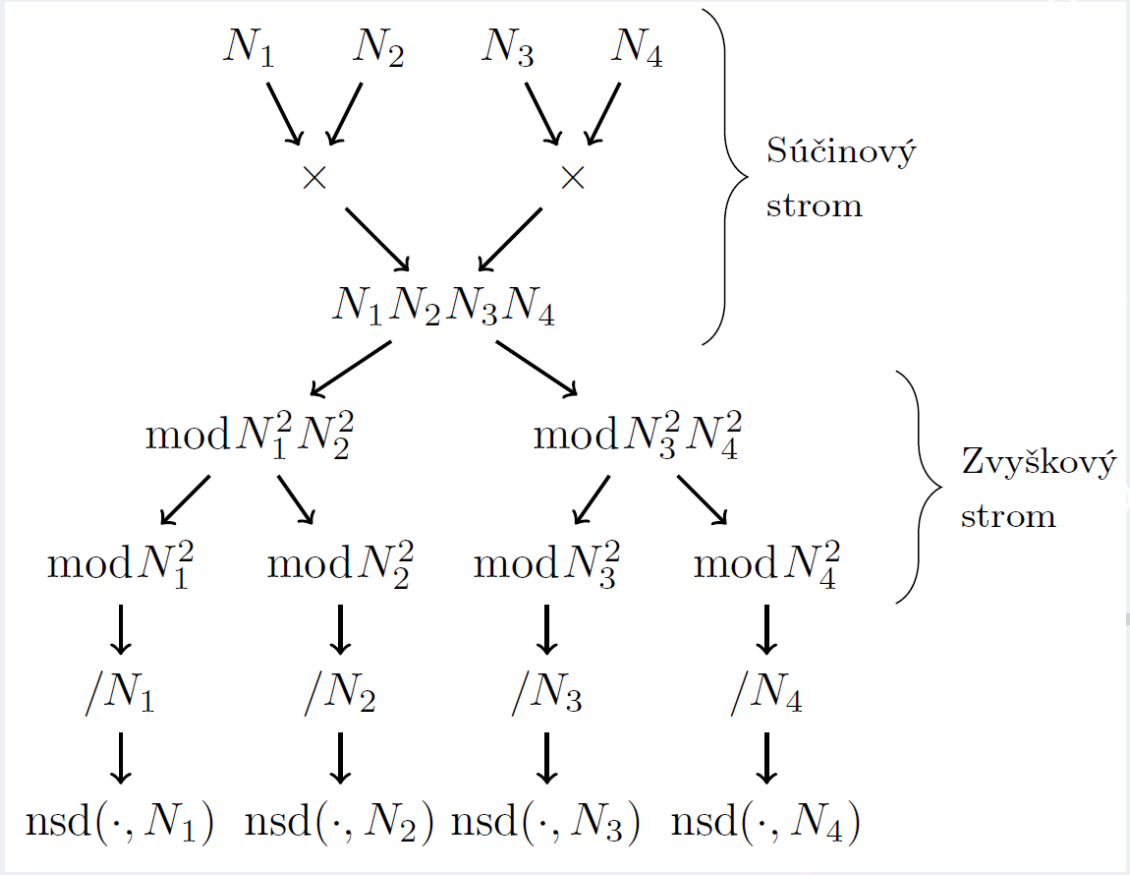
- Získali sme približne 1,2M rôznych RSA modulov
- Spustili algoritmus NSD na každú dvojicu kľúčov
- Približný čas trvania tohto algoritmu bol 40 dní
- $O(m^2n^2)$, kde m je počet verejných modulov
- Toľko času ale nemáme

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Vylepšenie počítania NSD

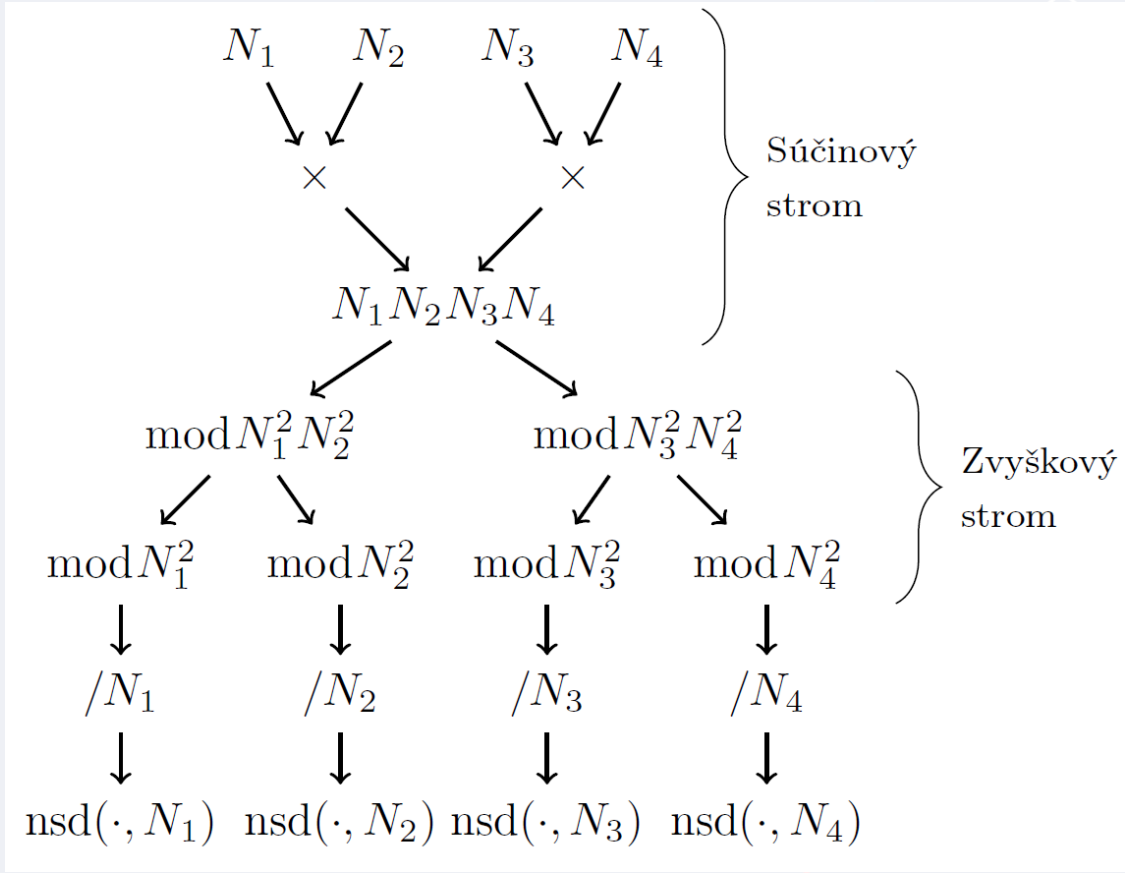
- Súčinový strom
- $n \bmod a = (n \bmod ab) \bmod a$
- Modulárny strom
- m krát nsd
- RFT



+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Vylepšenie počítania NSD

- Súčinový strom [5]
  - $O(n\log(n)\log(\log(n)))$
  - $O(mn\log(m)\log(mn)\log(\log(mn)))$
- Modulárny strom [5]
  - $O(n\log(n)\log(\log(n)))$
  - $O(mn\log(m)\log(mn)\log(\log(mn)))$
- m krát nsd [5]
  - $O(n\,(\log(n))^2\log(\log(n)))$
  - $O(mn(\log(n))^2\log(\log(n)))$



+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Výsledok výpočtu

- Čas do 3 000 sekúnd (16 GB RAM)
- Z 1,2M kľúčov sme faktorizovali 66.
- Ron was wrong, Whit is right. Lenstra a kol. 2012 – počet faktorizovaných RSA kľúčov touto metódou bol [2] :
  - 20251 zdieľaných modulov zo 3.7M rozdielnych kľúčov,
  - ovplyvnených 31620 X509 certifikátov,
- Pravdepodobnosť ?
- Čo je na tom zle ?

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Výsledok výpočtu SSH

„Správne“ generované kľúče:

Kórejská telekomunikačná spoločnosť

Frontier Communications Solutions, NY USA

- Naviac: 74.45.0.0-255 – 101 kľúčov z portu 22, unikátnych 44, 3 faktorizované

•Brazília, poskytovateľ internetového pripojenia.

wirelessdataspco.org

UPJŠ – žiadne výsledky

+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Výsledok výpočtu SSH

„Správne“ generované kľúče:

Kórejská telekomunikačná spoločnosť

Frontier Communications Solutions, NY USA

- Naviac: 74.45.0.0-255 – 101 kľúčov z portu 22, unikátnych 44, 3 faktorizované

•Brazília, poskytovateľ internetového pripojenia.

wirelessdataspco.org

UPJŠ – žiadne výsledky

Faktorizácie len v rámci organizácie

Chybné zariadenia a os

- /dev/random
- DD-WRT v24 – SP2
- Cisco RV042 WAP – stále v predaji
- Huawei S9300 switch
- Cisco ASR 9010 router
- pravdepodobne tlačiareň C2380
- Linux 2.6.x
- Ubuntu 10.x

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Výsledok výpočtu SSL

- Čínska telekomunikačná spoločnosť
  - SSL certifikát
  - 2048 bitový kľúč
  - login stránky do spoločnosti HUAWEI a mnoho iných ...
- BACKDOOR alebo implementačná chyba?
- 115.183.28.0-255, 124.193.190.0-255, 124.205.10.0-255
  - 23 faktorizovaných ver. modulov, 3 rôzne prvočísla
  - rozdielne zariadenia

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Výsledok výpočtu databázy PGP

- Väčšinou zlé generované prvočísla
  - 4294967297, 12884901891, 6242474487359, 357, 2, 5485
- Iba 1 faktorizácia „správne“ generovaného modulu
- Kľúče generované napr. Fedorou alebo gnupg

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Záver

- Implementačné chyby [2,3]
- /dev/random
- Backdoor ?
- Ron sa nemýlil, ale programátor áno
- Nedostatok testovania verejných modulov (výrobca)
- Neschopnosť alebo nezáujem riešiť problém
- **Aktualizácia OS**

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Zoznam použitej literatúry

1. Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. 1996. Handbook of Applied Cryptography (1st ed.). CRC Press, Inc., Boca Raton, FL, USA
2. Lenstra, A., Hughes, J. P., Augier, M., Bos, J. W., Kleinjung, T., & Wachter, C. (2012). *Ron was wrong, Whit is right* (No. EPFL-REPORT-174943). IACR.
3. Heninger, Nadia, et al. "Mining your Ps and Qs: Detection of widespread weak keys in network devices." *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)*. 2012.
4. Kleinjung, T., Aoki, K., Franke, J., Lenstra, A. K., Thomé, E., Bos, J. W., ... & Te Riele, H.: Factorization of a 768-bit RSA modulus. Advances in Cryptology–CRYPTO 2010 , 333-350 (2010)
5. BERNSTEIN, D. J.: Fast multiplication and its applications. Algorithmic Number Theory(May 2008), 325–384.
6. Twenty Years of Attacks on the RSA Cryptosystem, Dan Boneh

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli

Matus Nemec, Marek Sys, Petr Svenda

Dusan Klinec, Vashek Matyas

ACM CCS 2017

Coppersmith

- Ak poznáme časť bitov prvočísla p alebo q, vieme celkom rýchlo faktorizovať

$$problem \rightarrow f(x) \equiv 0\ mod\ p\ \rightarrow g(x) = 0 \rightarrow\ x_0$$

- Transformovať problém na modulárnu polynomiálnu rovnicu

$$f(x) \equiv 0\ mod\ p \text{ (p neznáme)}$$

- Transformovať polynóm na polynóm $g(x)$ v rámci $\mathbb{Z}[x]$ a tým eliminovať neznámu p pri zachovaní koreňov
- Vyriešiť tento problém jednoducho nad $\mathbb{Z}[x]$

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Formát prvočísel

$$p = k * M + (65537^a \, mod \, M)$$

- Kde premenné k, a sú neznáme
- $M = P_n\# = \prod_{i=1}^{n} P_i$, kde P_i je i – té prvočíslo
- M závisí od veľkosti generovaného prvočísla
- Pre $n = 39,71,126,225$ sú veľkosti kľúčov nasledovné:
  $[512,960], [992,1952], [1984,3936], [3968,4096]$
- Veľkosť M musí byť dostatočná $\approx$ veľkosť p
  - Priamy dôsledok tohto je, že veľkosť k, a je malá ...!
  - $(256 - 219 = 37)$ pre 512 bitový modulus, kde 219 bitov je veľkosť M

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Formát prvočísel - Dôsledok

$$p = k * M + (65537^a \, mod \, M)$$

- Fingerprint
  - $\log_{65537} N \, mod \, M$
  - Možnosť vypočítať ľahko, pretože M má malý rozklad
- Faktorizácia
  - Povedzme, že prejdeme každé a, položíme $65537^a \, mod \, M$, „to je časť bitov“ – a vypočítame Coppersmith-ovou metódou
    - Stále zlá časová zložitosť
    - Je možné vylepšiť – viď. ďalej

+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Faktorizácia

$$N = (k * M + (65537^{a} \; mod \; M)) * (l * M + (65537^{b} \; mod \; M))$$

$$N \equiv (65537^{a+b=c} \; mod \; M)$$

- Coppersmith – parametrizovaný black box
- Čím viac bitov, tým lepší je algoritmus ...
- Časová náročnosť určená ako $ord(a)$ a časová zložitosť coppersmith algoritmu
- ord – označuje rád prvku a v grupe $\mathbb{Z}_M^*$
- V praxi - $ord(\mathrm{a})$ je to najhoršie a dlhotrvajúce – určuje časovú zložitosť

+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Faktorizácia

$$N = (k * M + (65537^{a} \ mod \ M)) * (l * M + (65537^{b} \ mod \ M))$$

$$N \equiv (65537^{a+b=c} \ mod \ M)$$

- Veľkosť M je analogická veľkosti známych bitov v Coppersmith-ovom algoritme
- Postačuje $\log_2(N)/4$
- $\log_2 M > \log_2(N)/4$
- Nájdeme menšie M', také že $ord(a)$ je lepšie a stále budú prvočísla v takom tvare...

+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Faktorizácia

1. Prvočísla p, q sú stále v danom tvare $(M' \mid M)$
2. Coppersmith-ov útok nájde k' pre správne uhádnuté a', dostatočne bitov musí byť známych $\log_2 M' > \log_2(N)\,/4$
3. Celkový čas faktorizácie bude minimálny, tj. $ord_{M'}(\mathrm{a})$

- Takéto M' stačí nájsť jeden krát pre danú veľkosť kľúča ...

- $f(x) = x * M' + \left(65537^{a'} mod\ M'\right)$, koreň je k' a
$$f(x) \equiv 0\ mod\ p$$
  - Vylepšenia – LLL algoritmus – vybratie lepších polynómov

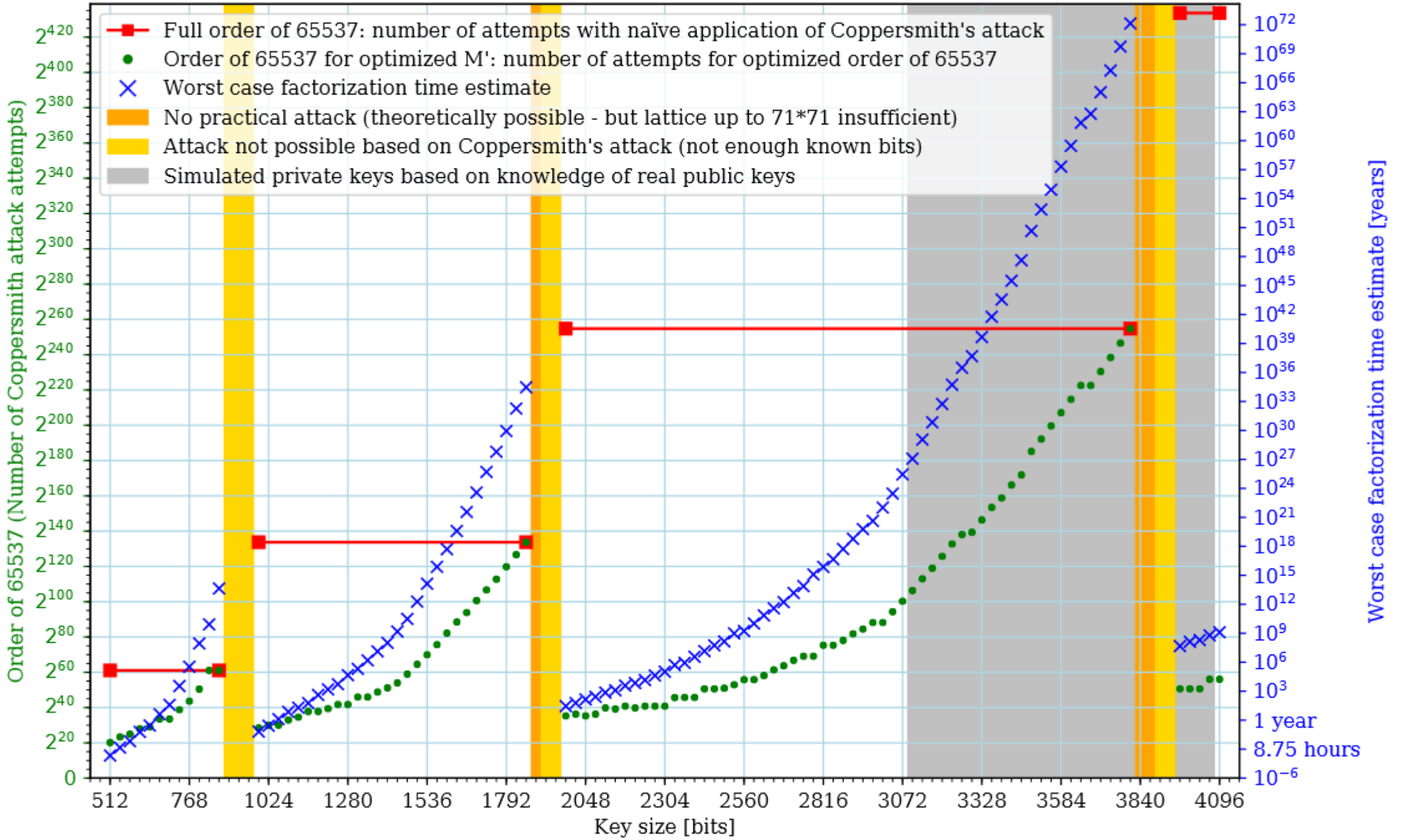
+421 2 59 278 262
jan.kotrady@csirt.sk
Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Porovnanie zložitostí

Key size	M	Size of M	Size of M'	Naïve BF # attempts $(ord_M(65537)/2)$	Our BF # attempts $(ord_{M'}(65537)/2)$	Time per attempt	Worst case
512 b	$P_{39}\# = 167\#$	219.19 b	140.77 b	$2^{61.09}$	$2^{19.20}$	11.6 ms	1.93 CPU hours
1024 b	$P_{71}\# = 353\#$	474.92 b	285.19 b	$2^{133.73}$	$2^{29.04}$	15.2 ms	97.1 CPU days
2048 b	$P_{126}\# = 701\#$	970.96 b	552.50 b	$2^{254.78}$	$2^{34.29}$	212 ms	140.8 CPU years
3072 b	$P_{126}\# = 701\#$	970.96 b	783.62 b	$2^{254.78}$	$2^{99.29}$	1159 sec	$2.84 * 10^{25}$ years
4096 b	$P_{225}\# = 1427\#$	1962.19 b	1098.42 b	$2^{433.69}$	$2^{55.05}$	1086 ms	$1.28 * 10^{9}$ years

+421 2 59 278 262
jan.kotrady@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk


Full order of 65537: number of attempts with naïve application of Coppersmith's attack
Order of 65537 for optimized M': number of attempts for optimized order of 65537
Worst case factorization time estimate
No practical attack (theoretically possible - but lattice up to 71*71 insufficient)
Attack not possible based on Coppersmith's attack (not enough known bits)
Simulated private keys based on knowledge of real public keys
Order of 65537 (Number of Coppersmith attack attempts)
Worst case factorization time estimate [years]
Key size [bits]
1 year
8.75 hours

Domain name	Used length (bits)	Pub. key availability	Misuse
TLS/HTTPS	2048	easy	MitM/eavesdropping
Message security (PGP)	1024/2048	easy	message eavesdropping, forgery
Trusted boot (TPM)	2048	limited	unseal data, forged attestation
Electronic IDs (eID, ePassport)	2048	limited	clone passport, e-gov document forgery
Payment cards (EMV)*	768/960/1024/1182	limited	clone card, fraudulent transaction
Certification authorities (root, intermediate)*	2048 or higher	easy	forged certificates, MitM
Authentication tokens	2048 or higher	limited	unauthorized access or operation
Software signing	2048 or bigger	easy	malicious application update
Programmable smartcard (Java Card)	1024-4096	depends on use	depends on use

Table 3: The summary of the impact of key factorization in the different usage domains. The fingerprinted keys were found within all listed domains with exceptions marked with an asterisk (*). No fingerprinted keys were found in the very limited dataset of 13 EMV cards that we collected or for large datasets of browser-trusted root and intermediate CAs.

Domain name	Analyzed datasets	# Vuln. keys/devices	% Vulnerable
Complete/larger-scale datasets			
Certification authorities	all browser-trusted roots (173), level ⩽ 3 intermediates (1,869)	0 keys	0
ePass signing certificates	ICAO Document Signing Certificates, CSCA Master Lists	0 keys	0
Estonian eID	sample of 130,152 randomly selected citizens	71,417 keys	54.87
Estonian mobile eID	sample of 30,471 randomly selected citizens	0 keys	0
Estonian e-residents	sample of 4,414 e-residents	4,414 keys	100
Message security (PGP)	complete PGP key server dump (9 M)	2,892 keys	0.03
Software signing (GitHub)	SSH keys for GitHub developers (4.7 M)	447 keys	0.01
Software signing (Maven)	signing keys for all public Maven artifacts	5 keys	0.003
TLS/HTTPS	complete IPv4 scan, Certificate Transparency	15 keys	<0.001
Trusted boot (TPM)	41 laptops with different chips by 6 TPM manufacturers	10 devices	24.39

Ďakujem
za pozornosť