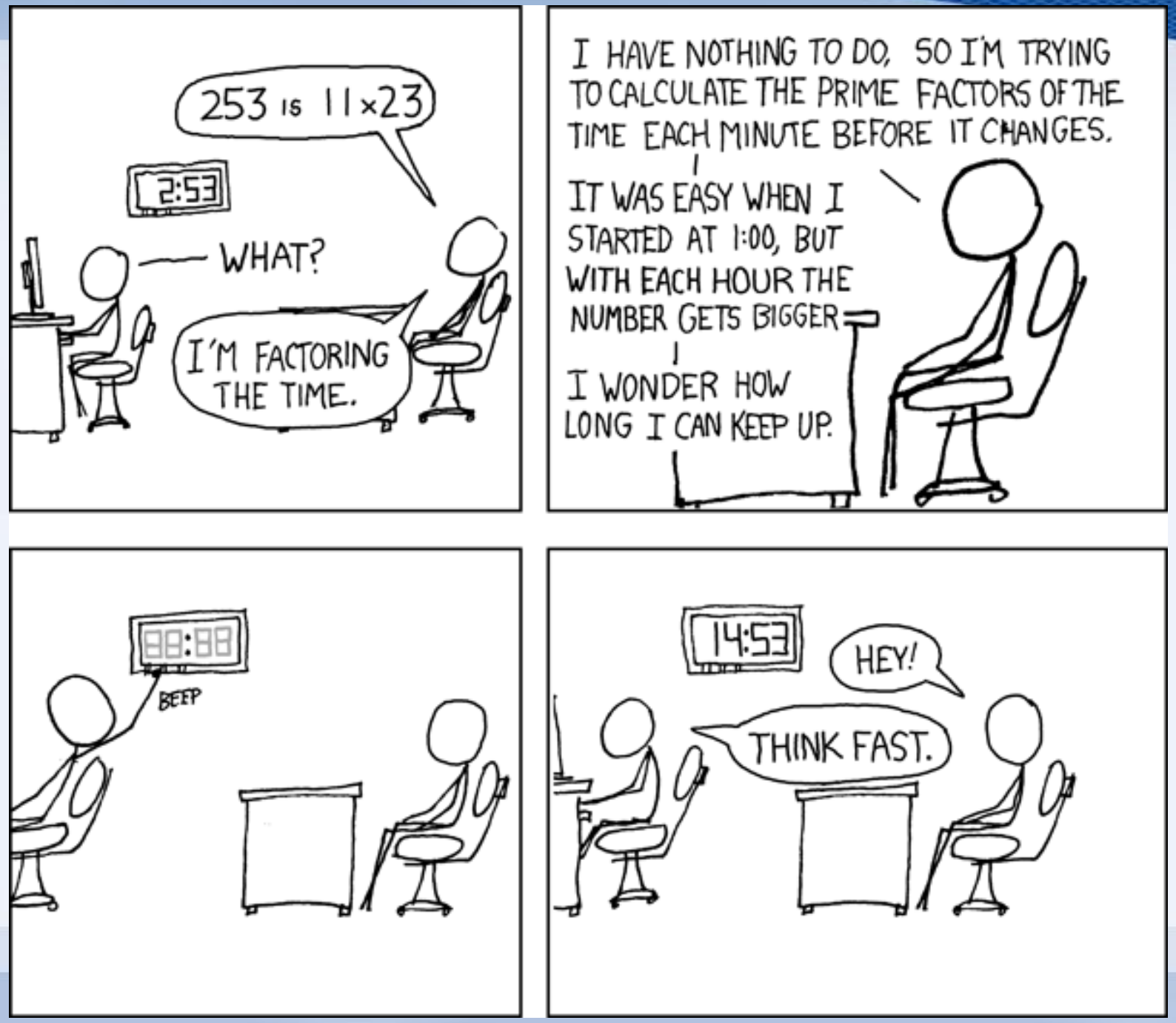

253 IS 11×23
2:53
WHAT?
I'M FACTORING THE TIME.
I HAVE NOTHING TO DO, SO I'M TRYING TO CALCULATE THE PRIME FACTORS OF THE TIME EACH MINUTE BEFORE IT CHANGES.
IT WAS EASY WHEN I STARTED AT 1:00, BUT WITH EACH HOUR THE NUMBER GETS BIGGER
I WONDER HOW LONG I CAN KEEP UP.
BEEP
14:53
HEY!
THINK FAST.

Problém faktorizácie v asymetrickej kryptografii

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

Autor: Ján Kotrady

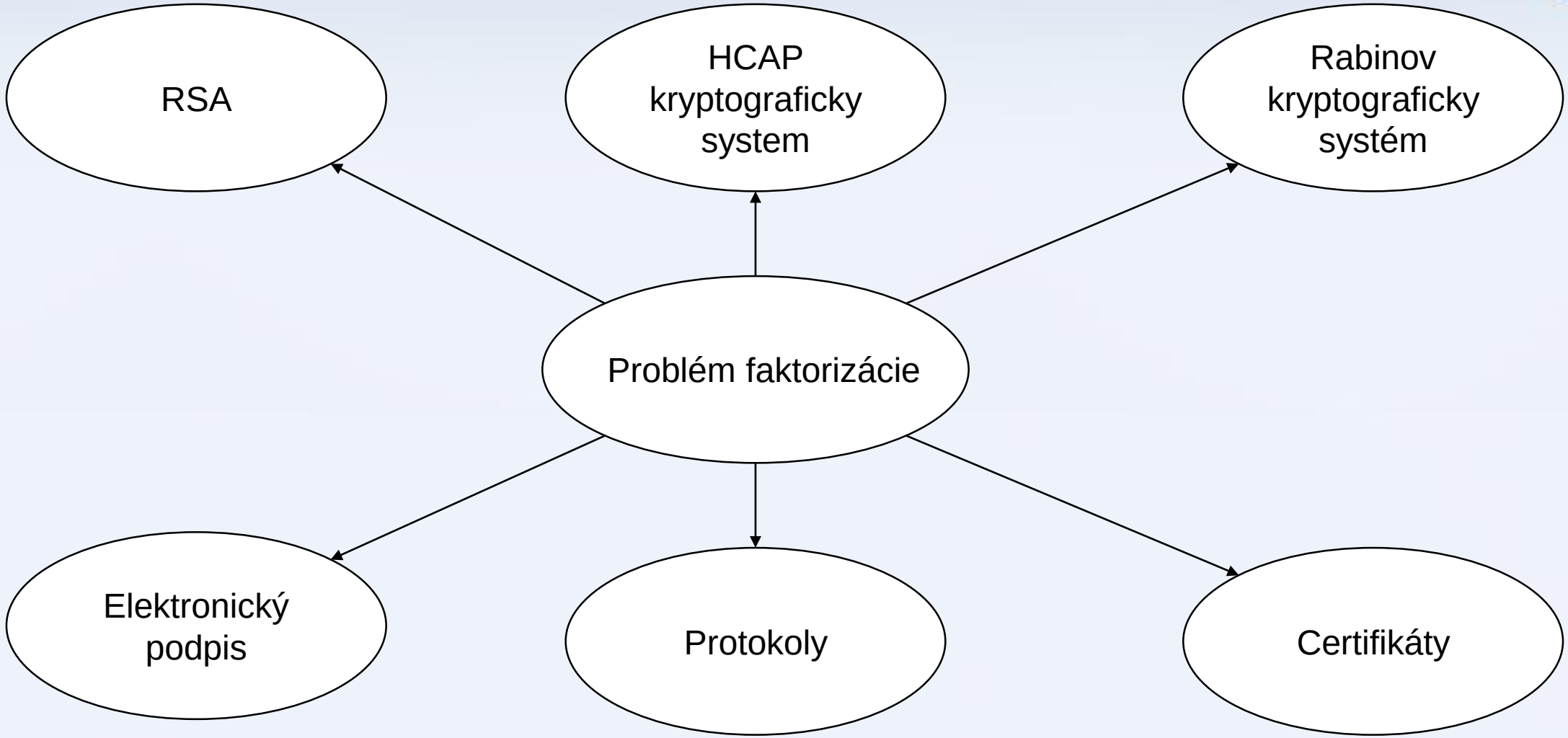
Problém faktorizácie

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.

Jednoduché, že ? Či ?

- Zozbierame všetky častice vo viditeľnom vesmíre aby sme mali dostatok pamäte
- A začíname počítať ....


RSA
HCAP kryptograficky system
Rabinov kryptograficky systém
Problém faktorizácie
Elektronický podpis
Protokoly
Certifikáty

Časová zložitosť

- 2^{60} - Čas v sekundách od vzniku vesmíru
- **General number field sieve :**

  $O(\exp((\frac{64}{9}b)^{\frac{1}{3}}(\log(b))^{\frac{2}{3}}))$, *b-bitove číslo*
- RSA - 2048 bit ≈ 112-bit AES ≈ 2^{112}
- Faktorizácia 512 bitového kľúča trvala 2000 rokov na 1 jadrovom 2,2 GHz procesore [4]

Ciele práce:

1. Preskúmať a analyzovať použitie problému faktorizácie v asymetrickej kryptografii.

-Kvalitatívna analýza problému

-Dedukcia

-Algebraická teória

Ciele práce:

2. Implementovať vybrané algoritmy faktorizácie.

-Kritéria pre výber
-Syntéza poznatkov
-Dôraz na efektivitu algoritmov

Ciele práce:

3. Porovnať implementované algoritmy faktorizácie.

-Komparácia
-Skutočná časová zložitosť a asymptotická
-Pamäť
-Profiler
-Vylepšenia

Algoritmy

- 2^16 – Tabuľka.
- Menej ako 2^70 Brentová modifikácia Pollard's rho algoritmu.
- Menej ako10^50: Lenstrov algoritmus.
- Menej ako10^100: Quadratic Sieve
- Viac ako 10^100: General Number Field Sieve
- Algoritmus NSD

Fermentová faktorizácia:

- Mnoho podobných algoritmov
- $O\left(\frac{p+q}{2}\right) ak\ \ pq = N.\ Ak\ |p| = |q|, potom\ O(\sqrt{N})$
- Rôzne vylepšenia s lepšou asymptotickou zložitosťou
- Jeden zo základných faktorizačných algoritmov
- Základ pre GNFS
- $N = a^2\ - b^2$

Fermentová faktorizácia:

Vstup: N

Výstup: faktor čísla N

```
a ← ceil(sqrt(N))
    b2 ← a*a - N
    while b2 isn't a square:
        a ← a + 1 // equivalently: b2 ← b2 + 2*a + 1
        b2 ← a*a - N // a ← a + 1
    endwhile
    return a - sqrt(b2) // or a + sqrt(b2)
```

Pollard's rho algorithm:

- Malý prvočíselný rozklad
- Polynóm modulo N
- Narodeninový problém
- $O(\sqrt{p}) \leq O(N^{\frac{1}{4}})$
- Aká je v skutočnosti ?
- 2^70

Pollard's rho algorithm:

Vstup: N

Výstup: d, faktor čísla N

$x \leftarrow 2$; $y \leftarrow 2$; $d \leftarrow 1$;

While d = 1:

$x \leftarrow g(x)$

$y \leftarrow g(g(y))$

$d \leftarrow \gcd(|x - y|, N)$

If d = N, return failure.

Else, return d.

Pollard's p-1:

- Nutnosť voľby B
- Nie príliš efektívny
- Nemá stabilnú časovú zložitosť
- $O(B),\ O(N^{\frac{1}{2}})$
- Aká je v skutočnosti ?

Pollard's p-1:

Vstup: N, B;

Výstup: d, faktor čísla N

a ← 2; j ← 2;

While j <= B:

a ← a^j (mod N)

d ← nsd(a – 1, N)

if 1 < d < N then

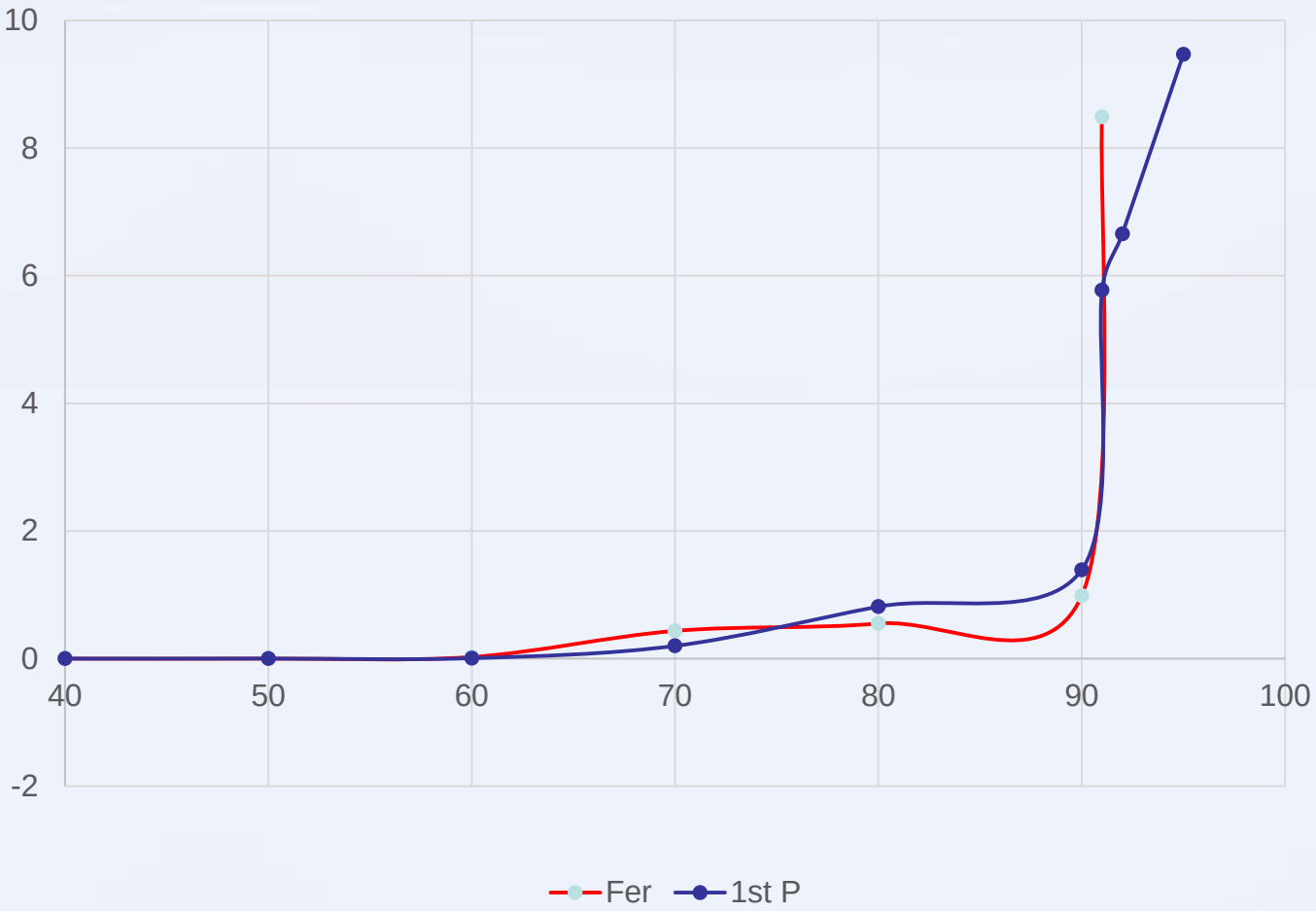
return d

j ← j + 1

(General) number field sieve

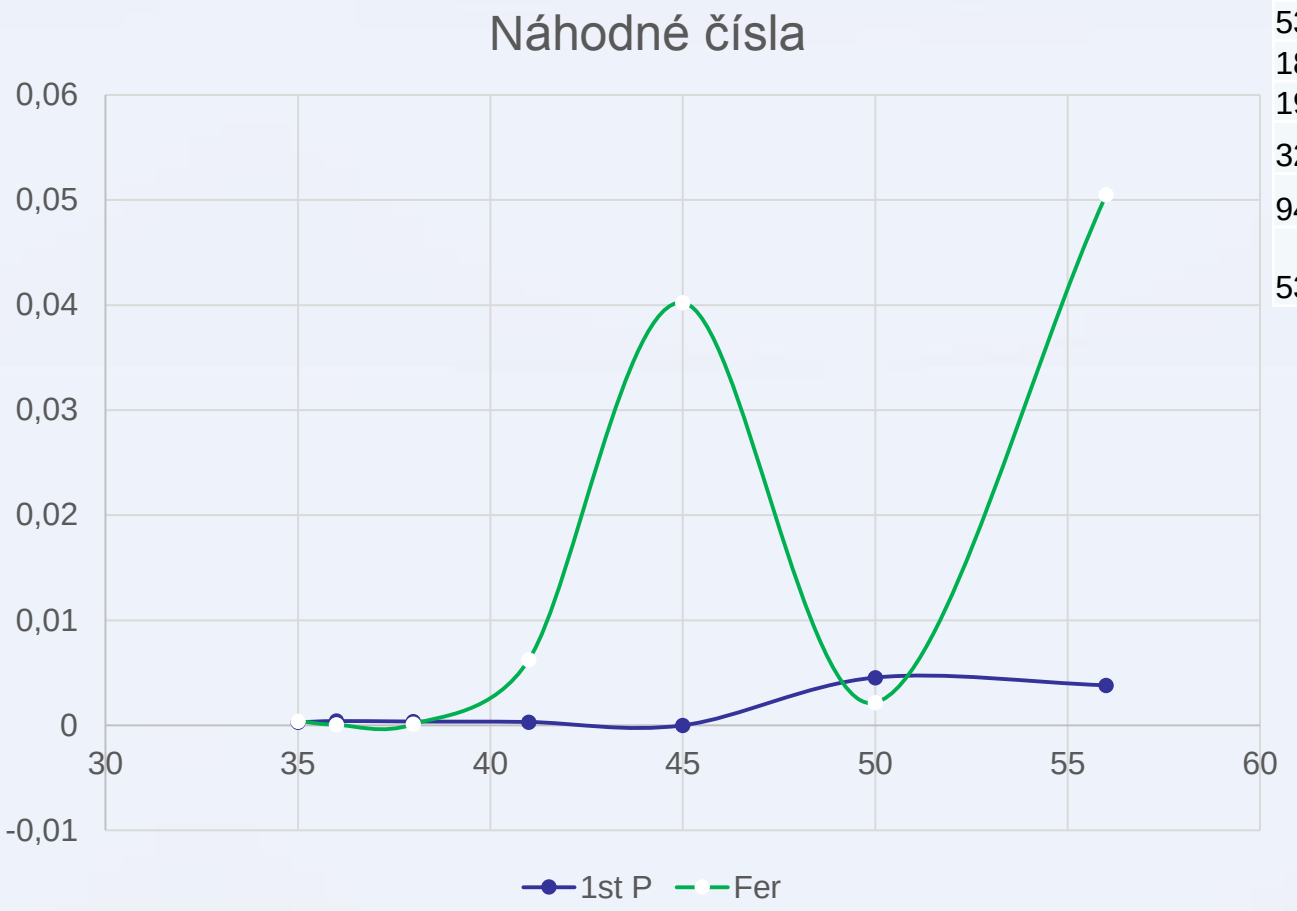
- Najlepší faktorizačný algoritmus
- Mnoho metód a funkcií
- Štatistika
- Pravdepodobnosť
- $O\left(\exp\left(\left(\frac{64}{9}b\right)^{\frac{1}{3}}(\log(b))^{\frac{2}{3}}\right)\right)$, *b-bitove číslo*

Výsledky výpočtov faktorizácie RSA

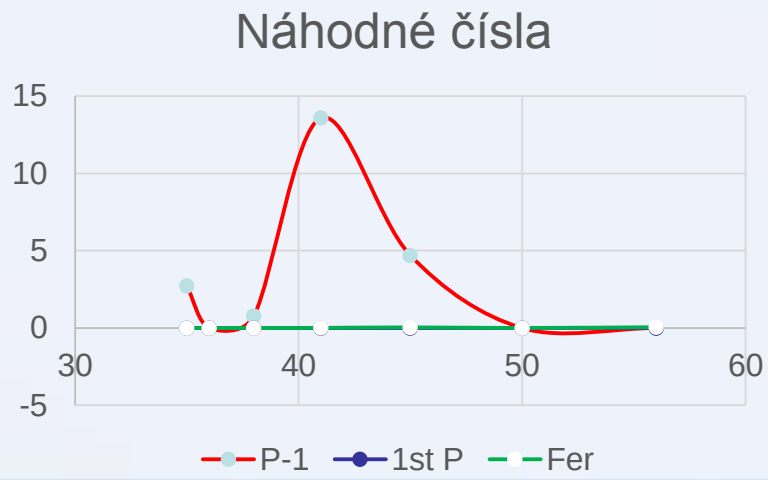


		Fer	1st P	P-1
640452262147	40	0,000021	0,000297	2,268636
698859554554279	50	0,000046	0,000929	
1031503157807531911	60	0,026032	0,0066	
847879425053701606567	70	0,435088	0,199696	
728628605374387956686443	80	0,550785	0,814837	
785291132940913157728617139	90	0,983017	1,391858	
161410421639133951893554123 9	91	8,488684	5,77218	
415781682446243673578805640 3	92		6,65647	
371387963509980575519183160 01	95		9,470728	

Výsledky výpočtov faktorizácie NČ



	Bits	P-1	1st P	Fer
25858125301	35	2,734242	0,000287	0,000407
53967856009	36	0,001121	0,000409	0,000052
185659644463	38	0,780795	0,000359	0,000115
1969245695161	41	13,59229	0,000317	0,006257
32139249574837	45	4,703653	null	0,040232
949771145777617	50	null	0,004548	0,002165
53565878997888211	56	13.449674	0,00381	0,0505

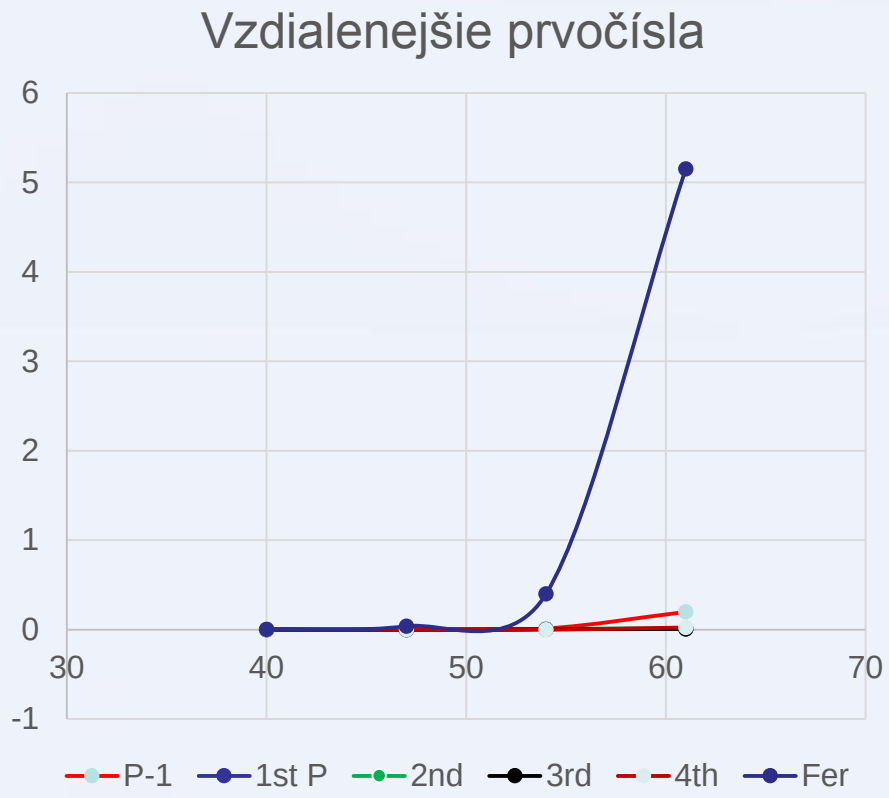


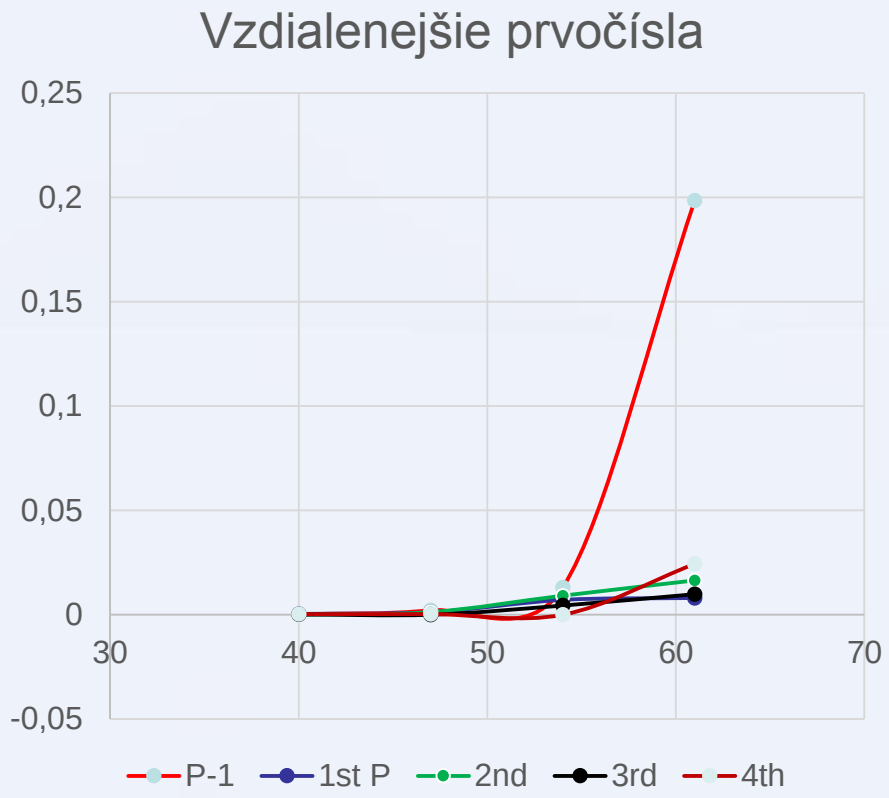
Výsledky výpočtov faktorizácie podľa vzdialenosti

		P-1	1st P	2nd	3rd	4th	Fer	
p50*p100000000	39	0,00008	0,000033	0,00001	null	null	null	2038074514
p5*p10000000000	42	0,000047	0,000046	null	0,000016	0,194638	null	252097800612

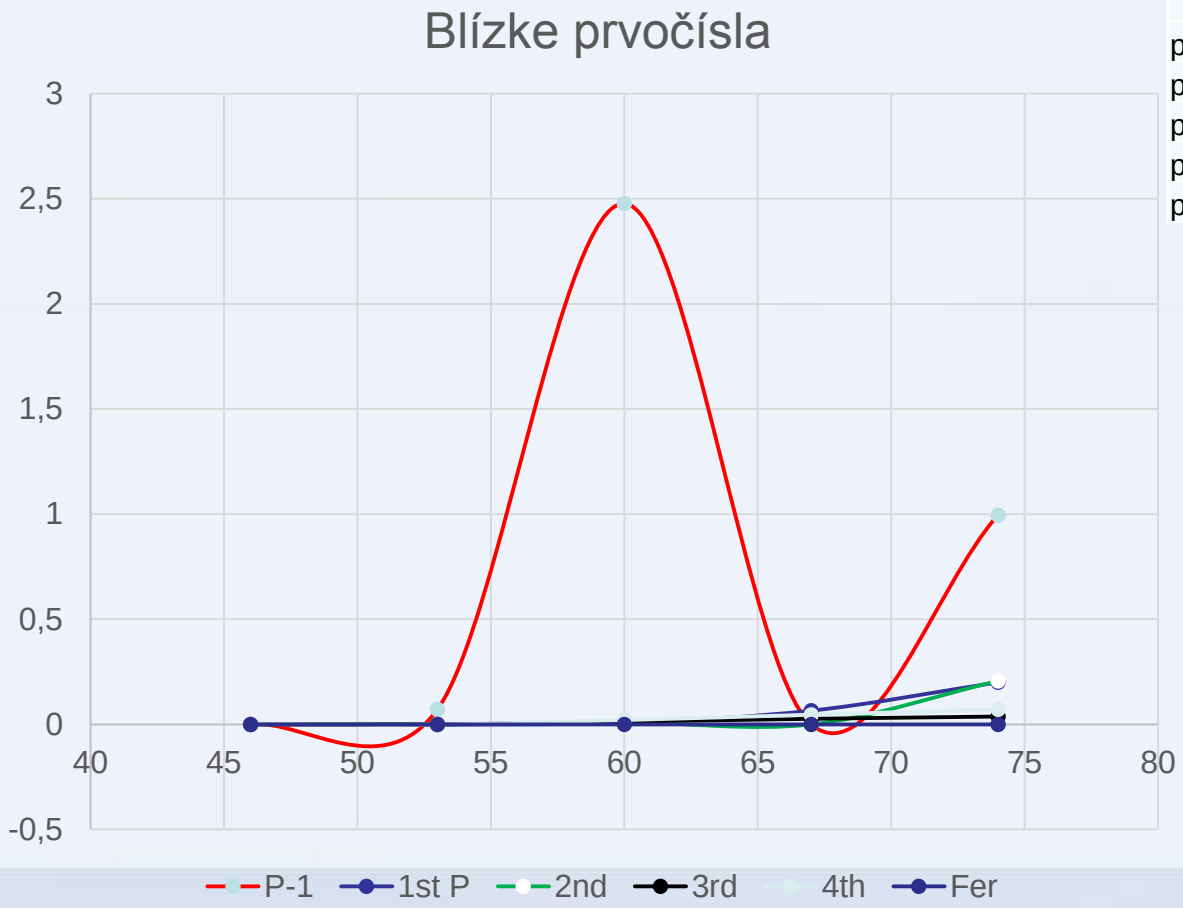
		P-1	1st P	2nd	3rd	4th	Fer	
p50000*p100000	40	0,000174	0,00040	null	0,00017	0,00029	0,003699	687756
p500000*p1000000	47	0,002186	0,00126	0,001284	null	0,000316	0,039137	8117076
p5000000*p10000000	54	0,013068	0,00713	0,009134	0,004416	null	0,398727	93396552
p50000000*p100000000	61	0,19837	0,00803	0,016464	0,009858	0,024376	5,151872	1055623090

Výsledky výpočtov faktorizácie podľa vzdialenosti

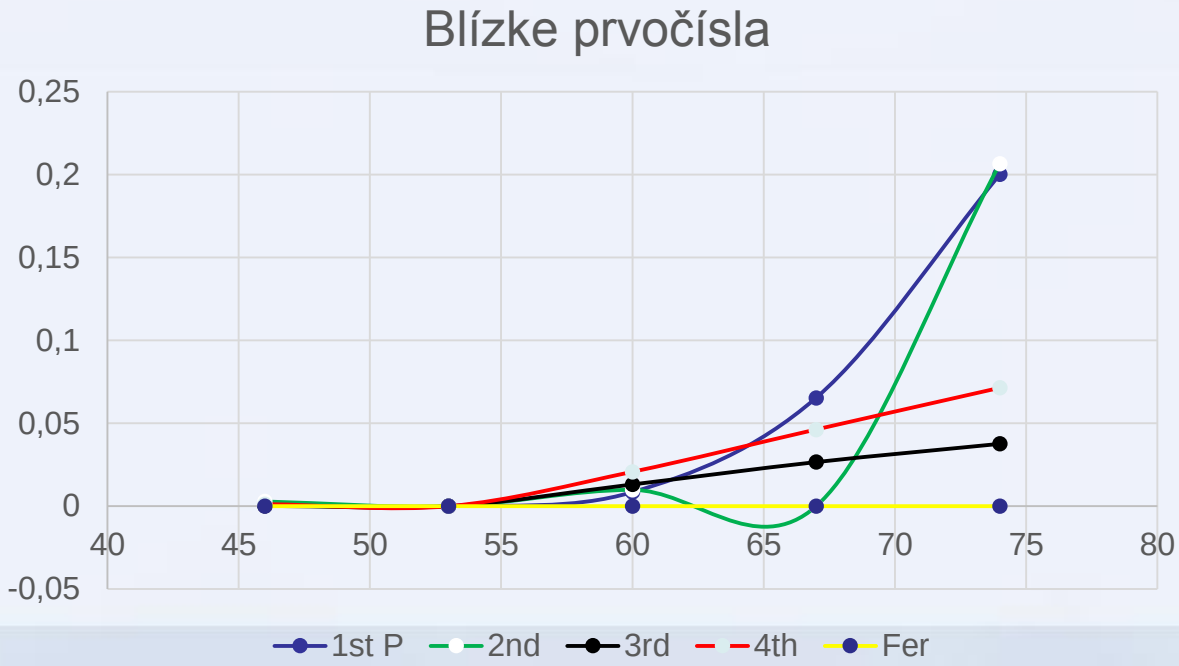




Výsledky výpočtov faktorizácie podľa vzdialenosti



		P-1	1st P	2nd	3rd	4th	Fer
p500000*p500001	46	0,001759	0,001095	0,002855	0,000195	0,001268	0,000013
p5000000*p5000001	53	0,071535	0,000022	0,000007	0,000002	0,000002	0,000019
p50000000*p50000001	60	2,477171	0,008488	0,009853	0,013131	0,020751	0,000017
p500000000*p500000001	67	null	0,065377	null	0,026602	0,046269	0,000017
p5000000000*5000000001	74	0,995784	0,20014	0,206592	0,037607	0,071413	0,000018



Faktorizácia algoritmom najväčšieho spoločného deliteľa

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)“

Najväčší spoločný deliteľ

- 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).
```

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

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

NSD ako riešenie RSA problému

- Pravdepodobnosť výsledku ?
- Počet 512 bitový prvočísel: 1,8853 10^151
- Upravený narodeninový paradox
- $1 - p', \;\; p' = \frac{n(n-2)(n-4)\cdots\left(n-2(k-1)\right)}{n^k} \approx e^{\frac{[-2-4\cdots-2(k-1)]}{n}} = e^{\frac{[-(k-1)k]}{n}}$
- $k \approx \sqrt{n\, ln(2)}$
- 50 % prav., potrebujeme: 2,898881 10^150 modulov
- 5 % prav., potrebujeme: 9,833780957 10^74 modulov (4,2 10^9)

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

Faktorizácie modulov

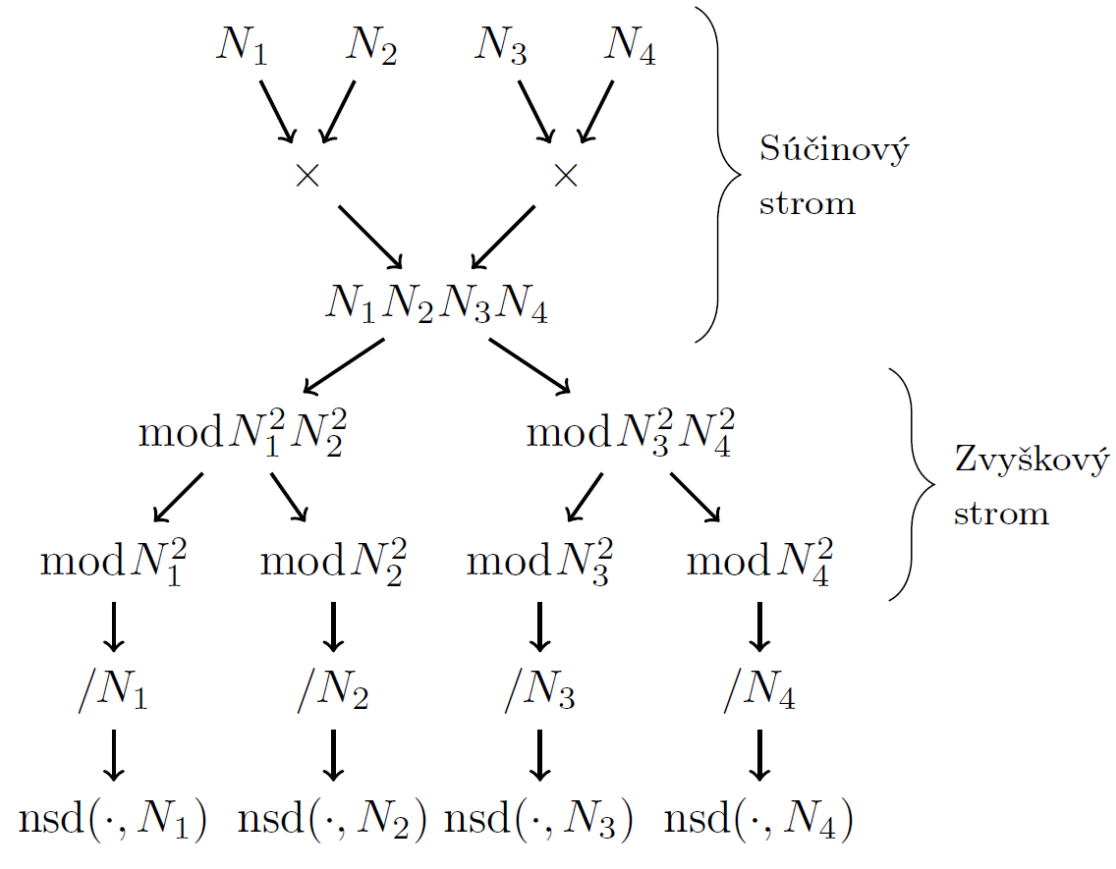
- Získali sme približne 1,2M rôznych RSA modulov
- Spustili algoritmus NSD na každú dvojicu kľúčov
- Približný čas trvania tohto algoritmu bol 40 dní
- $O(m^2n^2)$, kde m je počet verejných modulov

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

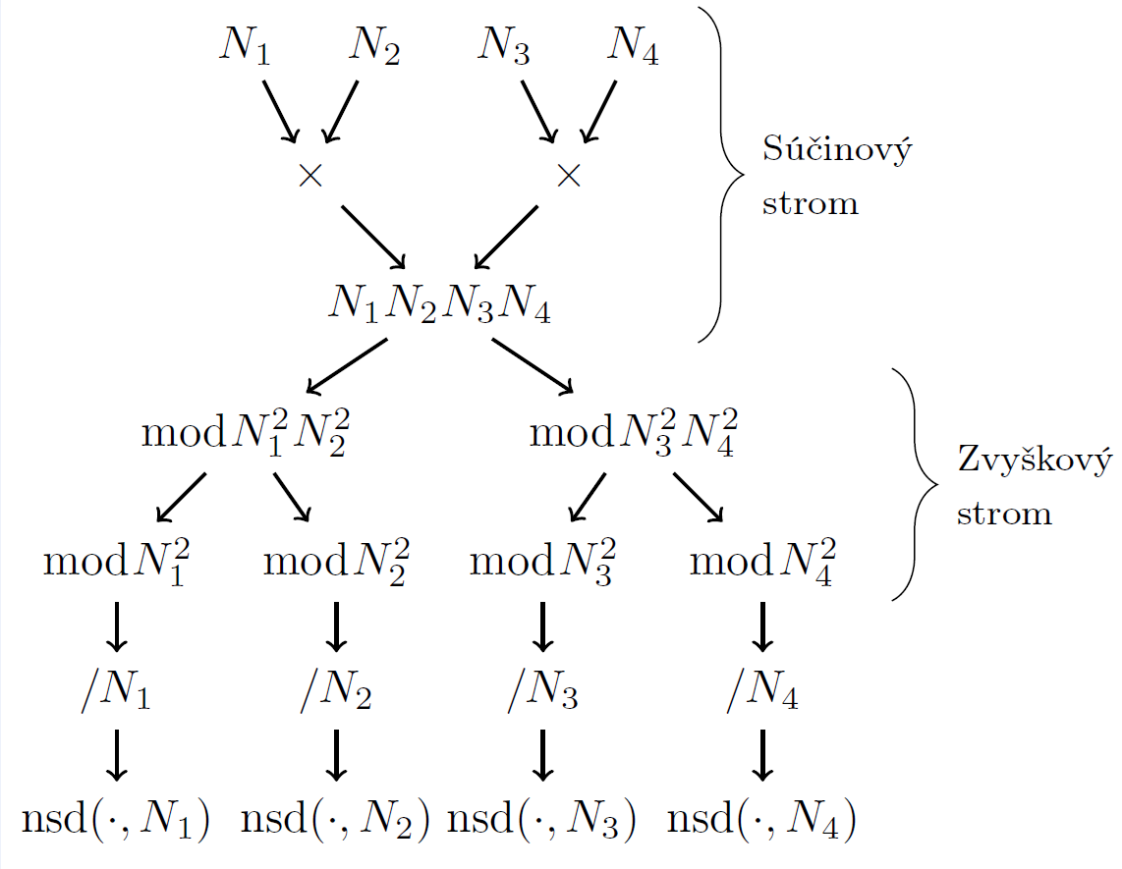
Vylepšenie počítania NSD

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



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]
  - $O(n\,(\log(n))^2\log(\log(n)))$
  - $O(mn(\log(n))^2\log(\log(n)))$



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 ?

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

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

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

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

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**

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.

... a ďalšia odporúčaná literatúra

- L. Barto, D. Stanovský: Počítačová algebra, MatfyzPress, 2011, ISBN 9788073781675
- D. Stinson: Cryptography - Theory and Practice, Third Edition (Discrete Mathematics and Its Applications), Chapman and Hall/CRC, 2005, ISBN 9781584885085
- J. Katz, Y. Lindell: Introduction to Modern Cryptography, Second Edition, Chapman and Hall/CRC, 2014, ISBN 9781466570269
- Brent, R. P. Some integer factorization algorithms using elliptic curves. Australian Computer Science Communications 8 (1986), 149-163 http://web.comlab.ox.ac.uk/oucl/work/richard.brent/pub/pub102.html

Ďakujem za pozornosť.