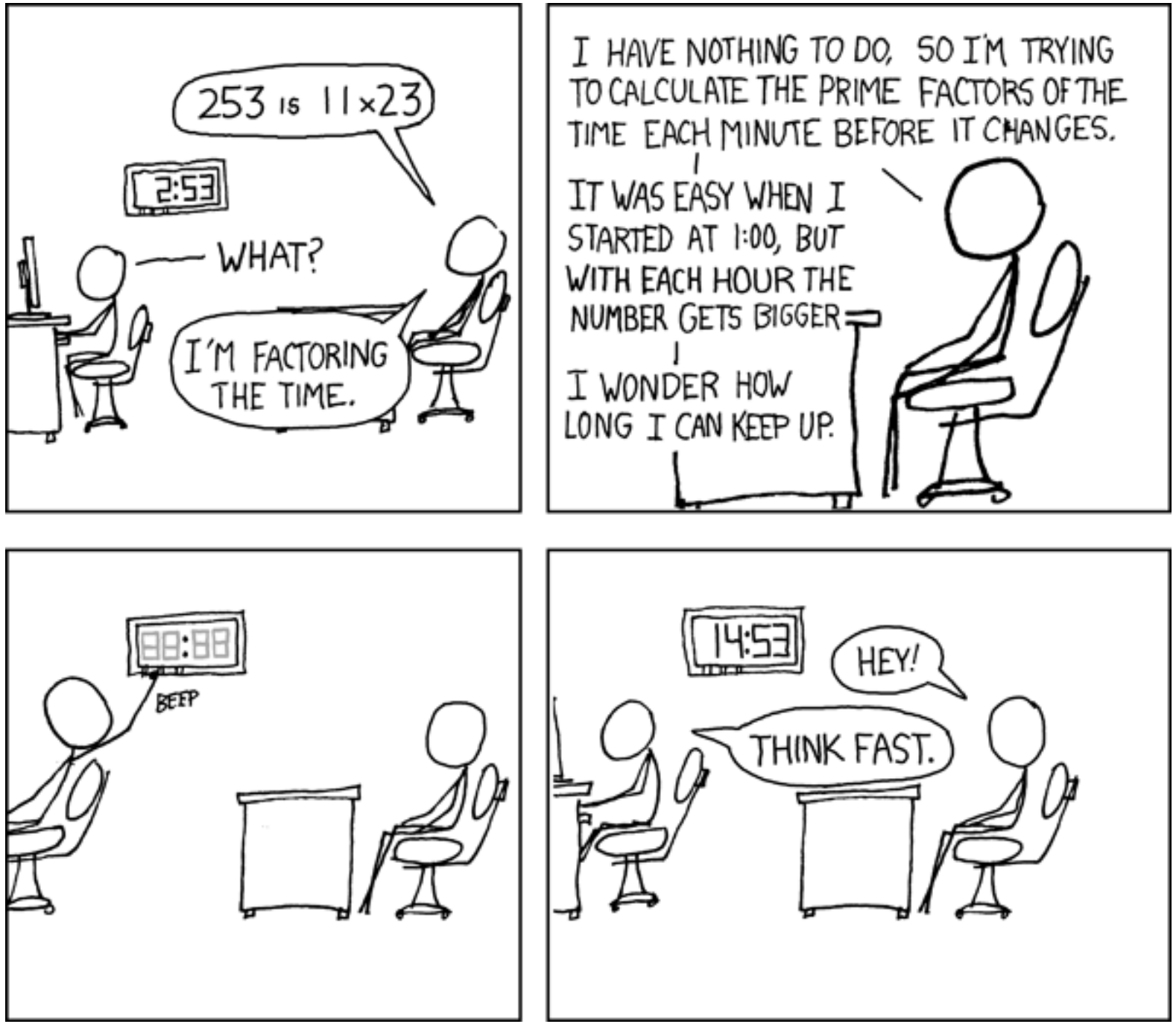

253 IS 11×23
2:53
WHAT?
I'M FACTORING THE TIME.
I HAVE NOTHING TO DO, SO I'M TRYING TO CALCULATE THE PRIME FACTORS OF THE TIME EACH MINUTE BEFORE IT CHANGES.
IT WAS EASY WHEN I STARTED AT 1:00, BUT WITH EACH HOUR THE NUMBER GETS BIGGER
I WONDER HOW LONG I CAN KEEP UP.
BEEP
14:53
HEY!
THINK FAST.

Problém faktorizácie v asymetrickej kryptografii

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

Autor: Ján Kotrady

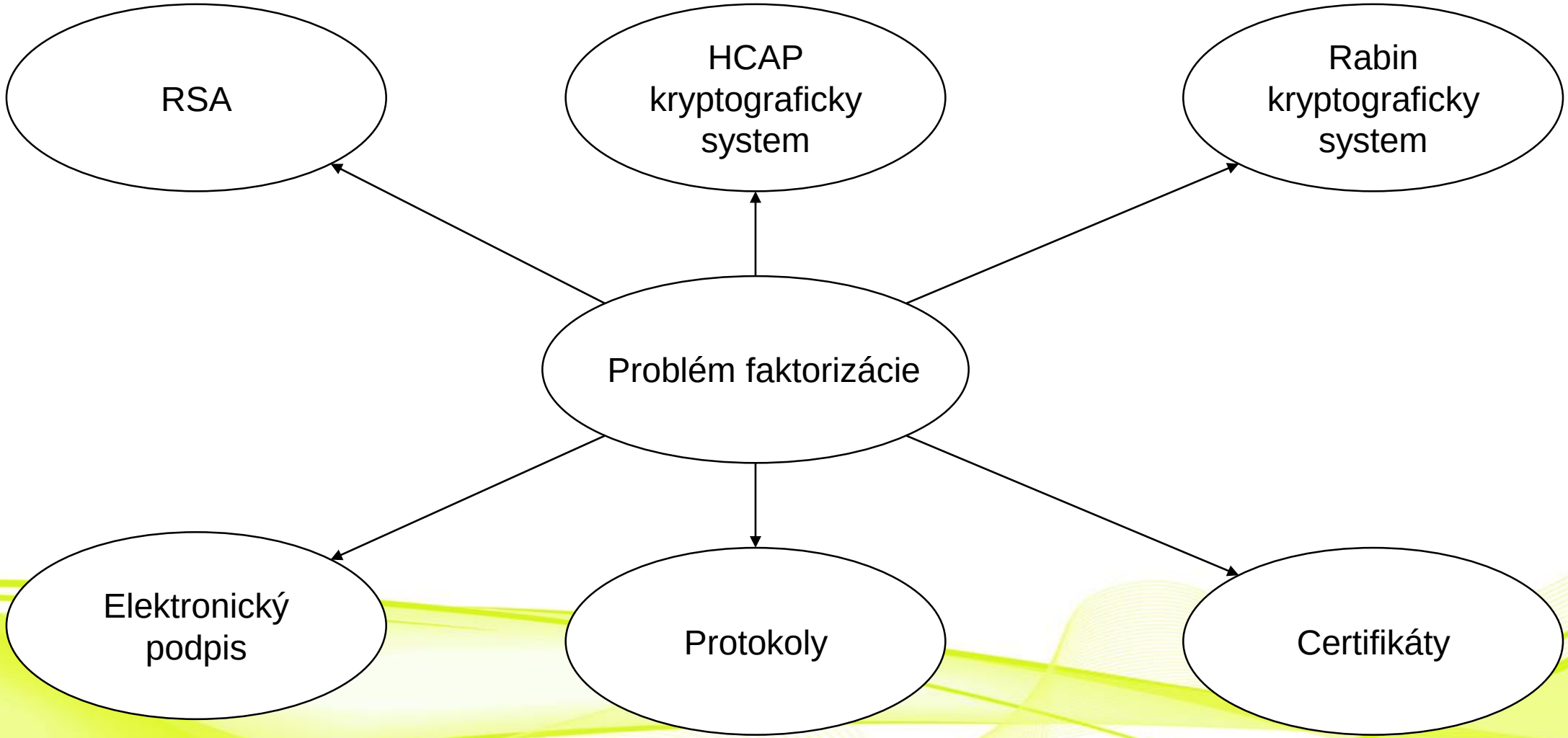
Problém faktorizácie

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
Rabin kryptograficky system
Problém faktorizácie
Elektronický podpis
Protokoly
Certifikáty

Časová zložitosť

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

$$O\left(\exp\left(\left(\frac{64}{9}b\right)^{\frac{1}{3}}(\log(b))^{\frac{2}{3}}\right)\right),\ b\text{-bitove číslo}$$

- RSA - 2048 bit ≈ 112-bit AES ≈ 2^{112}

Prečo práve faktorizácia?

- NP = P ?
- NP-complete ?
- Kam patri ?

- RSA challenge 200 000 $
- Zložitosť obecne
- Kryptografia

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

Fermentová faktorizácia:

- Mnoho podobných algoritmov
- $O((p+q)/2)\ if\ \ pq = n,\ \ |p| = |q|\ than\ O(\sqrt{n})$
- Rôzne vylepšenia s lepšou asymptotickou zložitosťou
- Jeden zo základných faktorizačných algoritmov

Fermentová faktorizácia:

```
FermatFactor(N): // N should be odd
    a ← ceil(sqrt(N)) //rounds N upward
    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:

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

Lenstrov algoritmus

- Subexponencionálny
- Generalizácia Pollardovej p-1 metódy
- $O\left(L(p)^{\sqrt{2}+o(1)}M(\log n)\right), L(x) = e^{\sqrt{\log x \log\log x}}$,
  $M(\log n)$ - zložitosť modulo n,
- Jedna z najlepších pre malé čísla
- Do 40 znakov

(General) number field sieve

- Najlepší faktorizačný algoritmus
- Mnoho metód
- 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*

Kontext asymetrickej kryptografie

Pre asymetrickú kryptografiu platí nasledovne:

- $n=pq$
- $\phi=(p-1)(q-1)$
- $gcd(e,\phi)=1$
- $de=1(mod\phi)$
- e – private key, d – public key

Z teórie grup môžeme odvodiť faktorizáciu zo znalosti e, d

Kontext asymetrickej kryptografie

- [Initialize] Set $k \leftarrow de-1$.
- [Try a random g] Choose g at random from $\{2,\ldots,N-1\}$ and set $t \leftarrow k$.
- [Next t] If t is divisible by 2, set $t \leftarrow t/2$ and $x \leftarrow g^t \bmod N$. Otherwise go to step 2.
- [Finished?] If $x>1$ and $y=\gcd(x-1,N)>1$ then set $p \leftarrow y$ and $q \leftarrow N/y$, output (p,q) and terminate the algorithm. Otherwise go to step 3.

Kontext asymetrickej kryptografie

- Ako sa dá ešte faktorizovat ?
- Vezmeme množinu použitých modulusov. (A tá že je naozaj veľká)
- Hľadáme gcd(n,m), kde m != n, m,n partí do množiny použitých modulusov
- Už to niekto skúšal?
- **Coppersmith's Attack** (využíva v niektorých typoch útokoch faktorizáciu)

Iné metódy asymetrickej kryptografie

- **NTRUEncrypt**
  - Faktorizácia polynómov
    - Čo je ľahšie ?
  - Lattice Reduction (mriežka)
  - NP úplný problém
- **McEliece cryptosystem**
  - Žiadna faktorizácia
  - **Post-quantums – 250 qubitech**
  - **Prvý krát použité náhodné čísla**

Iné metódy asymetrickej kryptografie

- **Diffie-Hellman**
  - Zvoliť parametre odolné Pohlig–Hellman
  - Konkrétne rád prvku musí mať dostatočne veľký rozklad na prvočísla
    - Čo je ľahšie ?
- ElGamal, Paillier cryptosystem, Cramer–Shoup cryptosystem
  - Bez faktorizácie

Aktuálny stav

- Pollard p – Kompletný algoritmus
- Fermentová faktorizácia – Kompletný algoritmus
- Lenstrov algoritmus – 99%
- Prebieha analýza Pollardového algoritmu
  - Zameranie na polynóm ktorý sa v algoritme vyskytuje
    - Vysoká mocina – pomalé, malá mocnina – slabý generátor
- Dokončovanie testovacích vstupov (generujú sa prvočísla)

Aktuálny stav

- Analýza GNFD algoritmu
  - Algoritmus máme kompletný z externých zdrojov
- Pribudla nová literatúra, začala sa študovať
- Napísaných ‘pár strán’
- Zhodnotenie získaných poznatkov

Plán práce

- November
  - Dokončiť algoritmy a spustiť testy
  - Pokračovať v písaní teórie (cca 20 strán)
- December
  - Konzultácia
  - Návrh vlastnej knižnice
  - Testy s Javou
  - + 20 strán

Plán práce

- Január – Február
  - Teória + vlastný návrh knižníc //skúškové ☹
- Marec
  - Dokončenie teórie, práce, predfinálne konzultácie
- Apríl
  - Finálne konzultácie, drobné úpravy, abstrakt, záver

Literatúra

- 1. L. Barto, D. Stanovský: Počítačová algebra, MatfyzPress, 2011, ISBN 9788073781675
- 2. D. Stinson: Cryptography - Theory and Practice, Third Edition (Discrete Mathematics and Its Applications), Chapman and Hall/CRC, 2005, ISBN 9781584885085
- 3. J. Katz, Y. Lindell: Introduction to Modern Cryptography, Second Edition, Chapman and Hall/CRC, 2014, ISBN 9781466570269

a ďalej:

- **Stanovský, David: Základy algebry –MATFYZ PRESS** ISBN 9788073781057
- **http://www.karlin.mff.cuni.cz/~stanovsk/**
- **http://www.karlin.mff.cuni.cz/~sebek/teaching/ls1314/palg/**
- Matthew E. Briggs: An Introduction to the General Number Field Sieve
- **https://www.youtube.com/watch?v=3cicTG3zeVQ**

a ďalej:

- C. Kaufman (Microsoft) (December 2005). "RFC 4306 Internet Key Exchange (IKEv2) Protocol". Internet Engineering Task Force (IETF).
- http://www.di-mgt.com.au/rsa_factorize_n.html
- 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.