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:

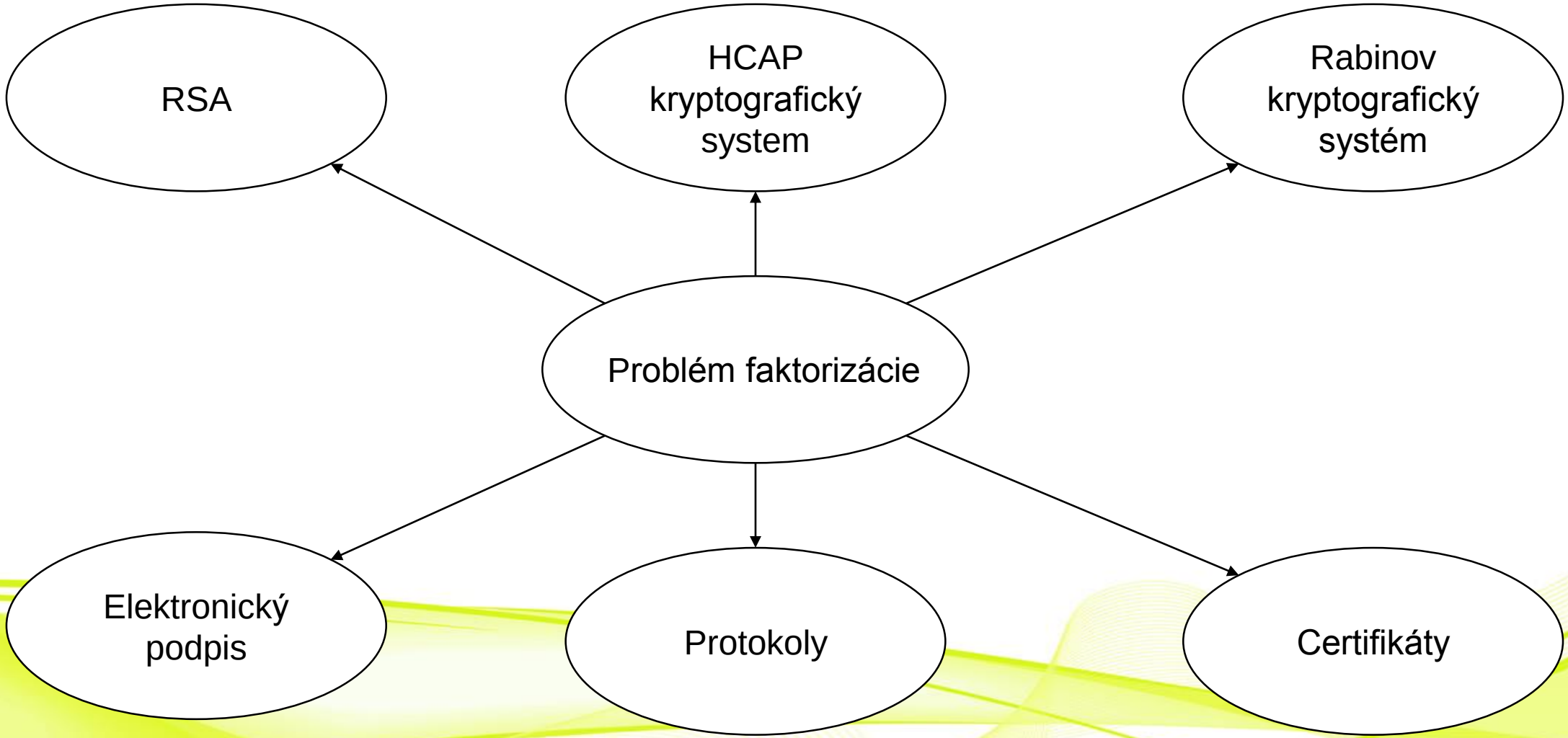
1. $p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_k^{m_k} = n,$
2. $k, m_1, \ldots, m_k \in \mathbb{N}$
3. $p_1, \ldots, p_k$ sú rôzne prvočísla.

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


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

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

Ciele práce:

3. Porovnať implementované algoritmy faktorizácie.

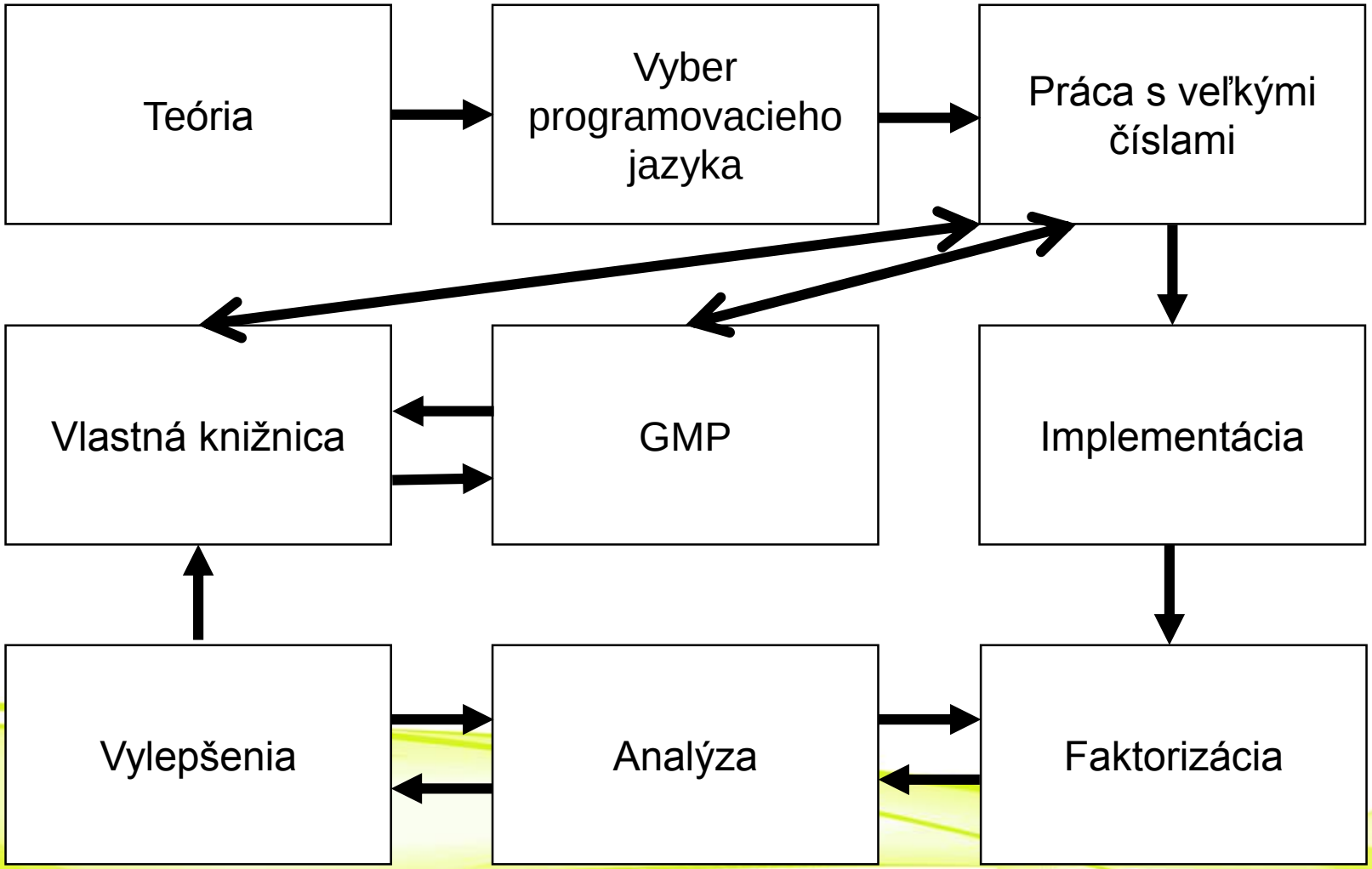
-Komparácia
-Skutočná časová zložitosť a asymptotická
-Pamäť
-Profiler
-Vylepšenia

Zámer:

- Využitie GPU?
- Porovnať jednotlivé programovacie jazyky
- Práca s veľkými číslami:
  - Problém reprezentácie
  - Pomalé algoritmy
  - Obmedzená pamäť

Zámer:

- The GNU multiple precision arithmetic library (GMP) alebo vlastný návrh:
  - Rýchlosť
  - Použiteľnosť
- Vlastná knižnica
  - Rýchle algoritmy
  - Vylepšenia
  - Rozdeľ a panuj
- Skutočná faktorizácia veľkých čísel
- Kauzalita (skúmanie príčin daného javu)


Teória
Vyber programovacieho jazyka
Práca s veľkými číslami
Vlastná knižnica
GMP
Implementácia
Vylepšenia
Analýza
Faktorizácia

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
- s.ics.upjs.sk/~jkotrady/

Ďakujem za pozornosť.