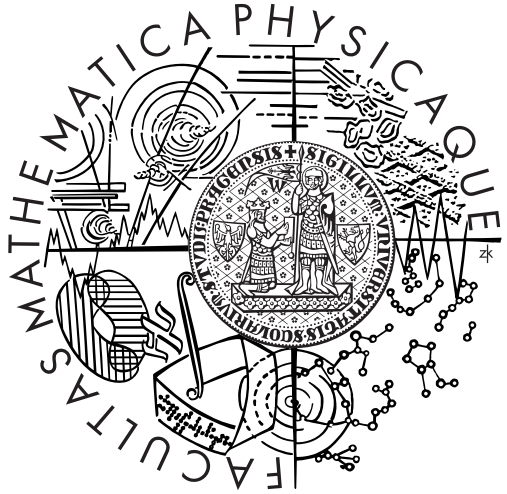
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁRSKA PRÁCA



Ria Ruppeldtová

Experimentálne overenie a rozšírenie Coppersmithovho útoku na RSA

Katedra algebry

Vedúci bakalárskej práce: **Mgr. Martin Hlaváč**
Konzultant bakalárskej práce: **Ing. Tomáš Rosa, Ph.D.**
Študijný program: **Matematika, Obecná matematika**

2008

Rada by som poďakovala Ing. Tomášovi Rosovi, Ph.D. za zaujímavý námet na tému práce, ale predovšetkým môjmu vedúcemu Mgr. Martinovi Hlaváčovi za podnetné konzultácie, na ktorých mi poskytoval konštruktívne rady a cenné pripomienky.

Prehlasujem, že som svoju bakalársku prácu napísala samostatne a výhradne s použitím citovaných prameňov. Súhlasím so zapožičiavaním práce a jej zverejňovaním.

V Prahe dňa 6.8.2008 Ria Ruppeldtová

Obsah

Názov práce: Experimentálne overenie a rozšírenie Coppersmithovho útoku na RSA

Autor: Ria Ruppeldtová

Katedra: Katedra algebry

Vedúci bakalárskej práce: Mgr. Martin Hlaváč

e-mail vedúceho: hlavm1am@artax.karlin.mff.cuni.cz

Abstrakt: Práca sa zaoberá Coppersmithovým útokom na RSA s verejným kľúčom 3 a krátkym paddingom. Jadro útoku spočíva v probléme hľadania malých koreňov modulárnych polynomiálnych rovníc s jednou neznámou. V teoretickej časti práce sme popísali a podrobne dokázali Howgrave-Grahamovu metódu riešenia tohto problému, ktorá je založená na teórii mriežok a algoritme LLL. V experimentálnej časti sme skúmali maximálnu dĺžku napadnuteľného paddingu a prezentovali naše výsledky. Tie ukazujú, že teoreticky dokázaná maximálna dĺžka paddingu sa líši od v praxi zistenej dĺžky len o niekoľko bitov.

Kľúčová slová: Coppermithov útok na RSA, malé korene modulárnych polynomiálnych rovníc, mriežka, algoritmus LLL

Title: Experimental verification and extension of Coppersmith's attack on RSA

Author: Ria Ruppeldtová

Department: Department of Algebra

Supervisor: Mgr. Martin Hlaváč

Supervisor's e-mail address: hlavm1am@artax.karlin.mff.cuni.cz

Abstract: The work deals with Coppersmith's attack on RSA with the public key equal to 3 and short padding. The heart of this attack lies in the problem of looking for small roots of univariate modular equations. In the theoretical part we have described and proved in detail Howgrave-Graham's method of solving the problem which is based on the theory of lattices and the LLL algorithm. In the experimental part we investigated the maximal length of attackable padding and we presented our results. They show that the theoretically proved maximal length of padding differs from practically observed length only by a few bits.

Keywords: Coppersmith's attack on RSA, small roots of univariate modular equations, lattice, LLL algorithm

Úvod

V roku 1996 Don Coppersmith vo svojom článku [1] popísal spôsob hľadania malých koreňov modulárnych polynomiálnych rovníc s jednou neznámou a následne jeho rozšírenie pre viac neznámych. Algoritmus využíva teóriu mriežok a redukciu bázy mriežky. Vo svojej práci ukázal možný útok na kryptosystém RSA so šifrovacím exponentom 3 a krátkym paddingom. O rok neskôr Nicholas Howgrave-Graham publikoval novú metódu hľadania malých koreňov modulárnych rovníc s jednou neznámou [5].

V teoretickej časti tejto práce sa zaoberáme podrobným a štruktúrnym popisom Howgrave-Grahamovho algoritmu. Je podaný jeho detailný dôkaz a popísané situácie, v ktorých funguje. V dôkazoch sme brali do úvahy aj nepresnosť LLL algoritmu [8] a ukázalo sa, že v tejto aplikácii je nepresnosť zanedbateľná. V experimentoch preto môžeme využívať aj rýchlejšie, no menej efektívne varianty LLL redukcie namiesto kvalitných, ale pomalých variantov popísaných v [4].

Pomocou Howgrave-Grahamovej metódy hľadania malých koreňov modulárnych rovníc sme implementovali Coppersmithov útok na RSA s verejným kľúčom 3.

Majme dve neznáme správy m a m' a predpokladajme, že poznáme ich rozdiel t

$$m' = m + t.$$

Ukážeme, že po zašifrovaní oboch správ RSA exponentom 3 vieme z ich šifrových textov, daného rozdielu a modulu odhaliť pôvodnú správu m.

V práci sa zameriavame na prípad, kedy rozdiel medzi správami nepoznáme, ale vieme, že je dostatočne malý

$$\begin{aligned} m' &= m + t \\ |t| &< 2^{-1/2} N^{1/9}. \end{aligned}$$

Predpokladajme, že správa M je zašifrovaná dvakrát, v obidvoch prípadoch doplnená iným náhodným paddingom T, resp. T'

$$\begin{aligned} c &= m^3 \mod N = \left(2^k M + T\right)^3 \mod N \\ c' &= (m')^3 \mod N = \left(2^k M + T'\right)^3 \mod N = (m+t)^3 \mod N. \end{aligned}$$

Dané dve rovnice o dvoch neznámych vyriešime eliminovaním jednej neznámej pomocou rezultantu a následne použijeme Howgrave-Grahamovu metódu na odkrytie správy M.

V experimentálnej časti práce sú prezentované výsledky našich testov, ktoré ukazujú, že odhad pre maximálnu dĺžku paddingu je primeraný, t.j. niekoľko bitov nad teoreticky dokázanou hranicou už úloha nie je riešiteľná popísaným spôsobom.

Teoretická časť

1 Základné stavebné poznatky

V tejto časti uvedieme jednoduché pozorovanie pre súčtovú a euklidovskú normu vektorov, základy teórie mriežok a algoritmu LLL, na ktorých je postavená Howgrave-Grahamová metóda hľadania malých koreňov modulárnych rovníc, a nakoniec zopár poznatkov o rezultante.

1.1 Vektorové normy

Definícia 1.1. Súčtovú, resp. euklidovskú normu vektora $v \in \mathbb{Z}^d$ definujeme

$$\|v\|_1 = \sum_{i=0}^{d-1} |v_i|, \text{ resp. } \|v\|_2 = \sqrt{\sum_{i=0}^{d-1} {v_i}^2}\,.$$

Ak dolný index nie je určený, uvažujeme normu euklidovskú, t.j. $\|v\| = \|v\|_2$.

Lemma 1.2. *Pre $v \in \mathbb{Z}^{hk}$ platí*

$$\frac{1}{\sqrt{hk}} \|v\|_1 \leq \|v\|_2 .$$

Dôkaz. Do Cauchy-Schwarzovej nerovnosti pre $x, y \in \mathbb{Z}^{hk}$

$$\left| \sum_{i=0}^{hk-1} x_i y_i \right|^2 \leq \sum_{i=0}^{hk-1} |x_i|^2 \sum_{i=0}^{hk-1} |y_i|^2$$

dosadíme $x_i = 1$, $y_i = |v_i|$, $i = 0, \ldots, hk-1$

$$\begin{aligned} \left| \sum_{i=0}^{hk-1} |v_i| \right|^2 &\leq hk \left(\sum_{i=0}^{hk-1} |v_i|^2 \right) \qquad (1) \\ \frac{1}{\sqrt{hk}} \sum_{i=0}^{hk-1} |v_i| &\leq \sqrt{\sum_{i=0}^{hk-1} {v_i}^2}\,. \end{aligned}$$

Všetky členy (1) sú nezáporné, preto je odmocnenie korektná úprava. □

1.2 Mriežky

V celom texte budeme pre jednoduchosť nazývať *úplnú mriežku* (t.j. *mriežku maximálnej hodnosti*) skrátene mriežka.

Definícia 1.3. Nech $B = \{b_0, \ldots, b_{d-1}\}$ je báza $\mathbb{Z}^d$, *mriežka* $\mathcal{L}$ je množina bodov

$$L = \left\{ y \in \mathbb{Z}^d \,\middle|\, y = \sum_{i=0}^{d-1} \alpha_i b_i, \alpha_i \in \mathbb{Z} \right\}.$$

Vektory $b_0, \ldots, b_{d-1} \in \mathbb{Z}^d$ sa nazývajú *bázové vektory mriežky* $\mathcal{L}$. Matica, ktorej riadky pozostávajú z bázových vektorov, sa nazýva *matica mriežky* $\mathcal{L}$.

V nasledujúcom texte budeme značiť symbolom B množinu bázových vektorov ako aj ich príslušnú maticu.

Lemma 1.4. *Pre mriežku $\mathcal{L} \in \mathbb{Z}^d$, $d \geq 2$, existuje nekonečne mnoho báz.*

Dôkaz. Nech $\{b_0, b_1, \ldots, b_{d-1}\}$ je báza mriežky $\mathcal{L}$, potom je bázou mriežky $\mathcal{L}$ aj $\{b_0 + b_1, b_1, \ldots, b_{d-1}\}$. □

Lemma 1.5. *Nech B a B' sú dve bázové matice mriežky $\mathcal{L} \in \mathbb{Z}^d$. Potom existuje prechodová matica C taká, že $B' = CB$ a platí*

$$|\det(C)| = 1.$$

Dôkaz. Nech $B = \{b_0, \ldots, b_{d-1}\}$ a $B' = \{b'_0, \ldots, b'_{d-1}\}$. Obe matice sú bázy mriežky $\mathcal{L}$, preto $b'_i = \sum_{j=0}^{d-1} c_{i,j}\, b_j$ pre $i = 0, \ldots, d-1$, kde $c_{i,j} \in \mathbb{Z}$. Označme $C = (c_{i,j})$, potom $B' = CB$. Analogicky existuje matica C' taká, že $B = C'B'$ a platí $B' = CB = CC'B'$, odtiaľ dostávame $CC' = I_d$. Keďže $1 = \det(I_d) = \det(CC') = \det(C)\det(C')$ a obe matice C, C' sú celočíselné, platí $|\det(C)| = |\det(C')| = 1$. □

Dôsledok 1.6. *Nech B a B' sú dve bázové matice mriežky $\mathcal{L} \in \mathbb{Z}^d$. Potom*

$$|\det(B)| = |\det(B')|\,.$$

Dôkaz. Z lemmy 1.5 vieme, že existuje matica C taká, že $B' = CB$ a $|\det(C)| = 1$. Z rovnosti $\det(B') = \det(CB) = \det(C)\det(B)$ vyplýva $\det(B') = \pm\det(B)$. □

Definícia 1.7. Pre maticu B mriežky $\mathcal{L}$ definujeme *determinant mriežky* $\mathcal{L}$

$$\mathrm{Vol}(\mathcal{L}) = |\det(B)|\,.$$

Poznámka 1.8. Podľa lemmy 1.4 existuje pre danú mriežku $\mathcal{L}$ nekonečne veľa báz B a z dôsledku 1.6 vidíme, že ich determinanty sa v absolútnych hodnotách rovnajú, preto definícia determinantu mriežky $\mathcal{L}$ je korektná.

Definícia 1.9. Pre $1 \leq i \leq d$, kde $d = \dim(\mathcal{L})$, definujeme i-te *Minkowskeho minimum* $\lambda_i(\mathcal{L})$ mriežky $\mathcal{L}$ ako minimum z $\max_{0 \leq j \leq i-1} \|v_j\|$ nad všetkými i lineárne nezávislými mriežkovými vektormi $v_0, \ldots, v_{i-1} \in \mathcal{L}$.

Definícia 1.10. Prvé Minkowskeho minimim $\lambda_1(\mathcal{L})$, označované tiež $\|\mathcal{L}\|$, nazývame *norma mriežky* $\mathcal{L}$.

Tvrdenie 1.11 (LLL algoritmus)**.** *Existuje polynomiálny algoritmus, ktorý z bázy mriežky $\mathcal{L} \in \mathbb{Z}^d$ vytvorí bázu $B = \{b_0, \ldots, b_{d-1}\}$ spĺňajúcu nerovnosti*

$$\begin{aligned} \|b_0\| &\leq \kappa_T \, Vol(\mathcal{L})^{1/d}, \quad kde\ \kappa_T = 2^{(d-1)/4} \\ \|b_i\| &\leq 2^{(d-1)/2} \lambda_{i+1}(\mathcal{L}),\ 0 \leq i \leq d-1 \\ \prod_{i=0}^{d-1} \|b_i\| &\leq 2^{\binom{d}{2}/2} \, Vol(\mathcal{L}). \end{aligned} \tag{2}$$

Dôkaz. Viď [6]. □

Definícia 1.12. Bázu $B = \{b_0, \ldots, b_{d-1}\}$ mriežky $\mathcal{L}$ spĺňajúcu vlastnosti z tvrdenia 1.11 nazývame *LLL-redukovaná báza* mriežky $\mathcal{L}$.

1.3 Rezultant

Definícia 1.13. Nech $a, b \in \mathbb{Z}[x]$, označme $a = \sum_{i=0}^{n} a_i x^i, b = \sum_{j=0}^{m} b_j x^j$. Potom definujeme *Sylvestrovu maticu* $S_{a,b}$ typu $(m+n) \times (m+n)$ predpisom

$$S_{a,b} = \begin{pmatrix} a_n & a_{n-1} & \ldots & a_1 & a_0 & & 0 & 0 \\ 0 & a_n & a_{n-1} & \ldots & a_1 & a_0 & & 0 \\ & & \ddots & \ddots & & \ddots & \ddots & \\ 0 & 0 & & a_n & a_{n-1} & \ldots & a_1 & a_0 \\ b_m & b_{m-1} & \ldots & b_1 & b_0 & & 0 & 0 \\ 0 & b_m & b_{m-1} & \ldots & b_1 & b_0 & & 0 \\ & & \ddots & \ddots & & \ddots & \ddots & \\ 0 & 0 & & b_m & b_{m-1} & \ldots & b_1 & b_0 \end{pmatrix}.$$

Definícia 1.14. Nech $S_{a,b}$ je Sylvestrova matica polynómov $a = \sum_{i=0}^{n} a_i x^i$, $b = \sum_{j=0}^{m} b_j x^j$. Potom definujeme *rezultant polynómov* a, b

$$\mathrm{res}_x(a, b) = \det(S_{a,b}).$$

Lemma 1.15. *Nech a, b sú polynómy nad $\mathbb{Z}_N$, $a = \sum_{i=0}^{n} a_i x^i$ je stupňa n, $b = \sum_{j=0}^{m} b_j x^j$ je stupňa m a nech a, b majú spoločný nenulový koreň x_0, kde $NSD(x_0, N) = 1$. Potom $res_x(a, b) = 0 \pmod N$.*

Dôkaz. Majme sústavu rovníc

$$\begin{aligned} a(x_0) &= 0 \pmod N \\ b(x_0) &= 0 \pmod N. \end{aligned}$$

Podľa predpokladu má táto sústava nenulové riešenie x_0. Do tohto systému pridáme ďalšie rovnice v tvare $x_0^k a(x_0) = 0 \pmod N$ a $x_0^k b(x_0) = 0 \pmod N$, kde $k \in \mathbb{N}$. Keďže $\mathrm{NSD}(x_0, N) = 1$, vidíme, že novovzniknutý systém má rovnaké riešenie ako pôvodná sústava. Majme nasledujúce rovnice

$$\begin{aligned} x_0^{m-1} a(x_0) &= 0 \pmod N \\ x_0^{m-2} a(x_0) &= 0 \pmod N \\ &\vdots \\ a(x_0) &= 0 \pmod N \\ x_0^{n-1} b(x_0) &= 0 \pmod N \\ x_0^{n-2} b(x_0) &= 0 \pmod N \\ &\vdots \\ b(x_0) &= 0 \pmod N. \end{aligned}$$

Tento systém môžeme zapísať ako súčin

$$S_{a,b} \begin{pmatrix} x_0^{m+n-1} \\ x_0^{m+n-2} \\ \vdots \\ x_0^0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod N.$$

Vidíme, že homogénna sústava rovníc tvorená Sylvestrovou maticou $S_{a,b}$ má netriviálne riešenie, teda daná matica má aspoň dva riadky lineárne závislé, a preto jej hodnosť $h(S_{a,b}) < m + n$. Nakoniec z toho plynie

$$\mathrm{res}_x(a, b) = \det(S_{a,b}) = 0 \pmod N.$$

□

Príklad 1.16. Nech $a(x) = x^3 - c \mod N$, $b(x) = (x+t)^3 - c' \mod N$, kde $t, c, c' \in \mathbb{Z}$. Dosadením do definície Sylvestrovej matice a rezultantu dostávame

$$\operatorname{res}_x(a,b) =$$

$$= \det \begin{pmatrix} 1 & 0 & 0 & -c & 0 & 0 \\ 0 & 1 & 0 & 0 & -c & 0 \\ 0 & 0 & 1 & 0 & 0 & -c \\ 1 & 3t & 3t^2 & t^3 - c' & 0 & 0 \\ 0 & 1 & 3t & 3t^2 & t^3 - c' & 0 \\ 0 & 0 & 1 & 3t & 3t^2 & t^3 - c' \end{pmatrix} \pmod N$$

$$= t^9 + (3c - 3c')t^6 + (3c^2 + 21cc' + 3(c')^2)t^3 + (c - c')^3 \pmod N.$$

2 Problém malých modulárnych koreňov

Definícia problému: Majme monický ireducibilný polynóm p nad $\mathbb{Z}$ stupňa k. Hľadáme všetky riešenia, ktoré spĺňajú

$$|x| \leq X \quad \text{a} \quad p(x) = 0 \pmod{N}.$$

Tento problém nazveme *problém malých modulárnych koreňov - MMK.*

Inštancia: Počiatočné parametre problému MMK - polynóm $p \in \mathbb{Z}[x]$, jeho stupeň k, modul $N \in \mathbb{N}$ a hornú hranicu $X \in \mathbb{N}$, nazveme *inštancia problému MMK* a označíme ju $\mathcal{I} = \{p, k, N, X\}$.

V nasledujúcej časti popíšeme riešenie problému MMK Howgrave-Grahamovou metódou [5], zameriame sa na jej detailný a zrozumiteľný výklad.

2.1 Konštrukcia mriežky vhodnej pre problém MMK

Definícia 2.1. Nech $p(x) = \sum_{j=0}^{d} a_j x^j$ je polynóm stupňa d. Pre $i \in \mathbb{N} \cup \{0\}$ definujeme

$$\begin{aligned} v_i : \mathbb{Z}[x] &\rightarrow \mathbb{Z} \\ v_i(\sum_{j=0}^{d} a_j x^j) &= \begin{cases} a_i & , \quad i = 0, \ldots, d \\ 0 & , \quad i > d. \end{cases} \end{aligned}$$

Definícia 2.2. Nech $k \in \mathbb{N}$, $h \in \mathbb{N}$, $h \geq 2$. Potom definujeme zobrazenie

$$\begin{aligned} \varphi_{h,k} : \mathbb{Z}[x] &\rightarrow \mathbb{Z}^{hk} \\ p &\mapsto (v_0(p), v_1(p), \ldots, v_{hk-1}(p)). \end{aligned}$$

V nasledujúcom texte sú parametre h, k z kontextu jasné, preto budeme značiť $\varphi \equiv \varphi_{h,k}$.

Definícia 2.3. Nech $k \in \mathbb{N}$ a $h \in \mathbb{N}$, $h \geq 2$. Pre $m = 0, \ldots, h-1$ definujeme zobrazenie

$$\begin{aligned} \psi_{h,k,m} : \mathbb{Z}[x] &\rightarrow \mathbb{Z}^{k,hk} \\ p &\mapsto \begin{pmatrix} \varphi(x^0 p^m) \\ \varphi(x^1 p^m) \\ \vdots \\ \varphi(x^{k-1} p^m) \end{pmatrix}. \end{aligned}$$

Pre dané m označíme $\psi_m \equiv \psi_{h,k,m}$.

Definícia 2.4. Nech $N \in \mathbb{N}$, $k \in \mathbb{N}$, $h \in \mathbb{N}$, $h \geq 2$, $X \in \mathbb{N}$,

$$\mathcal{N} = diag(\underbrace{N^{h-1}, \ldots, N^{h-1}}_{k}, \underbrace{N^{h-2}, \ldots, N^{h-2}}_{k}, \ldots, \underbrace{N^0, \ldots, N^0}_{k}),$$

$$G = \begin{pmatrix} \psi_0(p) \\ \psi_1(p) \\ \vdots \\ \psi_{h-1}(p) \end{pmatrix}, \; D = diag(X^0, X^1, \ldots, X^{hk-1}),$$

kde D je diagonálna matica. Definujeme

$$\begin{aligned} \varrho_{h,k,N,X} : \mathbb{Z}[x] &\rightarrow \mathbb{Z}^{hk,hk} \\ p &\mapsto \mathcal{N}GD. \end{aligned}$$

Ak uvažujeme inštanciu $\mathcal{I}$, parametre k, N a X sú z inštancie zrejmé. Rovnako je z kontextu zrejmý aj volený parameter h, preto pre zjednodušenie zápisu označíme $\varrho \equiv \varrho_{h,k,N,X}$.

Poznámka 2.5. Matice G a $\varrho(p)$ sú rozdelené na h blokov po k riadkoch. Každý m-tý blok matice G je určený polynómom p^m, kde $m = 0, \ldots, h-1$, a je tvorený zobrazením ψ_m. Taktiež z definície 2.4 vidíme, že m-tý blok matice $\varrho(p)$ vznikne z m-tého bloku matice G tak, že ho po riadkoch prenásobime N^{h-1-m} a zároveň j-ty stĺpec vynásobime koeficientom X^j. Výsledná matica $\varrho(p)$ vznikne spojením všetkých blokov.

Príklad 2.6. Uveďme na praktickom príklade konštrukciu matice $\varrho(p)$ z polynómu p a parametrov h a X. Majme

$$p(x) = 18 + 21x + x^2 = 0 \pmod{45}, \; h = 3, \; X = 3.$$

Vidíme, že

$$\psi_1(p) = \begin{pmatrix} 18 & 21 & 1 & 0 & 0 & 0 \\ 0 & 18 & 21 & 1 & 0 & 0 \end{pmatrix},$$

taktiež

$$\begin{aligned} (p(x))^2 &= 324 + 756x + 477x^2 + 42x^3 + x^4 \\ \psi_2(p) &= \begin{pmatrix} 324 & 756 & 477 & 42 & 1 & 0 \\ 0 & 324 & 756 & 477 & 42 & 1 \end{pmatrix}. \end{aligned}$$

Výsledná matica $\varrho(p)$ má preto tvar

$$\varrho(p) = \begin{pmatrix} 1\times45^2 & & & & & \\ 0 & 1\times45^2 & & & 0 & \\ 18\times45^1 & 21\times45^1 & 1\times45^1 & & & \\ 0 & 18\times45^1 & 21\times45^1 & 1\times45^1 & & \\ 324\times45^0 & 756\times45^0 & 477\times45^0 & 42\times45^0 & 1\times45^0 & \\ 0 & 324\times45^0 & 756\times45^0 & 477\times45^0 & 42\times45^0 & 1\times45^0 \end{pmatrix} . D =$$

$$= \begin{pmatrix} 2025 \times 3^0 & & & & & \\ 0 & 2025 \times 3^1 & & & 0 & \\ 810 \times 3^0 & 945 \times 3^1 & 45 \times 3^2 & & & \\ 0 & 810 \times 3^1 & 945 \times 3^2 & 45 \times 3^3 & & \\ 324 \times 3^0 & 756 \times 3^1 & 477 \times 3^2 & 42 \times 3^3 & 1 \times 3^4 & \\ 0 & 324 \times 3^1 & 756 \times 3^2 & 477 \times 3^3 & 42 \times 3^4 & 1 \times 3^5 \end{pmatrix} .$$

Lemma 2.7. *Nech $\mathcal{I}$ je inštancia problému MMK a $h \in \mathbb{N}$, $h \geq 2$. Potom matica G z definície 2.4 je dolná trojuholníková s jednotkami na diagonále.*

Dôkaz. Označme $G = (g_{i,j})$, $i, j = 0, \ldots, hk-1$. Uvažujme i-ty riadok matice G a zvoľme $m, u \in \mathbb{N} \cup \{0\}$ tak, že $i = mk+u$, kde $0 \leq u < k$. Vidíme, že i-ty riadok matice je zároveň u-ty riadok m-tého bloku (poznámka 2.5) a podľa definície 2.3 je obrazom polynómu $x^u p^m$ pri zobrazení φ. Stupeň tohto polynómu je $mk + u$, teda $g_{i,j} = v_j(x^u p^m) = 0$ pre $j > km + u = i$ (definícia 2.1). Keďže polynóm p je monický, sú monické aj polynómy $x^u p^m$, odtiaľ $g_{i,i} = 1$. □

Lemma 2.8. *Nech $\mathcal{I}$ je inštancia problému MMK a $h \in \mathbb{N}$, $h \geq 2$. Potom* $\det(\varrho(p)) = X^{hk(hk-1)/2} N^{hk(h-1)/2}$.

Dôkaz. Podľa definície 2.4 je $\varrho(p) = \mathcal{N}GD$. Keďže matica G je dolná trojuholníková a má jednotky na diagonále (lemma 2.7), determinanty týchto matíc sú

$$\det(\mathcal{N}) = N^{hk(h-1)/2},\ \det(G) = 1,\ \det(D) = X^{hk(hk-1)/2}.$$

Nakoniec vidíme

$$\det(\varrho(p)) = \det(\mathcal{N}GD) = \det(\mathcal{N}) \det(G) \det(D) = N^{hk(h-1)/2} X^{hk(hk-1)/2}.$$

□

Poznámka 2.9. V definícii 2.4 sme z inštancie problému MMK a parametru h skonštruovali bázovú maticu, ktorá reprezentuje príslušnú mriežku $\mathcal{L}$. Neskôr zistíme, že táto mriežka $\mathcal{L}$ je vhodná na riešenie problému MMK.

2.2 Riešenie problému MMK

V tejto časti ukážeme, ako možno pomocou Howgrave-Grahamovej metódy previesť úlohu hľadania malých koreňov monických ireducibilných polynómov $p(x) = 0$ nad $\mathbb{Z}_N$ na úlohu hľadania koreňov polynómov nad celými číslami.

Lemma 2.10. *Nech $\mathcal{I}$ je inštancia problému MMK, $h \in \mathbb{N}$, $h \geq 2$ a $B = \{b_0, \ldots, b_{hk-1}\}$ je LLL-redukovaná báza matice $\varrho(p)$. Potom*

$$\|b_0\|_2 \leq \kappa_T X^{(hk-1)/2} N^{(h-1)/2} \text{ , kde } \kappa_T = 2^{(hk-1)/4}.$$

Dôkaz. Matice M a B generujú mriežku $\mathcal{L}$, teda podľa dôsledku 1.6 platí

$$|\det(M)| = |\det(B)| .$$

Z tvrdenia 1.11 máme

$$\|b_0\|_2 \leq \kappa_T Vol(\mathcal{L})^{1/hk} = \kappa_T \left|\det(B)\right|^{1/hk}, \text{ kde } \kappa_T = 2^{(hk-1)/4}.$$

Keďže $\det(M) = X^{hk(hk-1)/2} N^{hk(h-1)/2}$ podľa lemmy 2.8, vidíme, že platí $\det(M) > 0$, a teda

$$\|b_0\|_2 \leq \kappa_T X^{(hk-1)/2} N^{(h-1)/2}.$$

□

Lemma 2.11. *Majme inštanciu $\mathcal{I}$ problému MMK, $h \in \mathbb{N}$, $h \geq 2$, maticu $A = (a_{i,j}) = \mathcal{N}G$, kde matice $\mathcal{N}, G$ sú z definície 2.4 a $B = \{b_0, \ldots, b_{hk-1}\}$ LLL-redukovanú bázu mriežky generovanej riadkami matice $\varrho(p)$. Potom existuje (súradnicový) vektor $c_0 \in \mathbb{Z}^{hk}$ taký, že $b_0 = c_0\, \varrho(p)$ a platí*

$$\begin{aligned} \|b_0\|_1 \;=\; & \left|\sum_{i=0}^{hk-1} (c_0)_i\, a_{i,0}\right| + \left|\left(\sum_{i=1}^{hk-1} (c_0)_i\, a_{i,1}\right) X\right| + \;\ldots \\ & \ldots \;+ \left|\left(\sum_{i=hk-1}^{hk-1} (c_0)_i\, a_{i,hk-1}\right) X^{hk-1}\right| , \end{aligned}$$

kde $(c_0)_i$ označuje i-tu zložku vektora c_0.

Dôkaz. Označme $M = \varrho(p)$, potom existuje matica $C = \{c_0, \ldots, c_{hk-1}\}$ taká, že $B = CM$ (lemma 1.5). Vieme, že $M = AD$, kde D je diagonálna matica $D = (d_{i,j}) = diag(X^0, X^1, \ldots, X^{hk-1})$, odtiaľ

$$\begin{aligned} B &= CM = CAD \\ b_0 &= c_0 M = c_0 AD, \end{aligned}$$

j-ta zložka vektora b_0 je

$$(b_0)_j = \sum_{i=j}^{hk-1} (c_0)_j \, m_{i,j} \;\text{ pre } j = 0, \ldots, hk-1.$$

Sumácia prebieha od indexu j, lebo z lemmy 2.7 je matica G dolná trojuholníková, teda je dolná trojuholníková aj matica M, t.j. $m_{i,j} = 0$ pre $i < j$. Prvky matice M majú preto tvar

$$m_{i,j} = \sum_{l=0}^{hk-1} a_{i,l} \, d_{l,j} = a_{i,j} \, d_{j,j} = a_{i,j} \, X^j.$$

Z toho plynie

$$\begin{aligned} \|b_0\|_1 &= |(b_0)_0| + |(b_0)_1| + \cdots + |(b_0)_{hk-1}| \\ \|b_0\|_1 &= \left|\sum_{i=0}^{hk-1} (c_0)_i \, m_{i,0}\right| + \left|\sum_{i=1}^{hk-1} (c_0)_i \, m_{i,1}\right| + \;\ldots\; + \left|\sum_{i=hk-1}^{hk-1} (c_0)_i \, m_{i,hk-1}\right| = \end{aligned}$$

$$\left|\sum_{i=0}^{hk-1} (c_0)_i \, a_{i,0}\right| + \left|\left(\sum_{i=1}^{hk-1} (c_0)_i \, a_{i,1}\right) X\right| + \;\ldots\; + \left|\left(\sum_{i=hk-1}^{hk-1} (c_0)_i \, a_{i,hk-1}\right) X^{hk-1}\right|.$$

□

Definícia 2.12. Uvažujúc inštanciu $\mathcal{I}$ problému MMK a značenie z predchádzajúcej lemmy 2.11 definujeme polynóm

$$\begin{aligned} r_{\mathcal{I}}(x) &= \sum_{i=0}^{hk-1} (c_0)_i \, a_{i,0} + \left(\sum_{i=1}^{hk-1} (c_0)_i \, a_{i,1}\right) x + \cdots + \left(\sum_{i=hk-1}^{hk-1} (c_0)_i \, a_{i,hk-1}\right) x^{hk-1} \\ &= (c_0)_0 \sum_{j=0}^{0} a_{0,j} \, x^j + (c_0)_1 \sum_{j=0}^{1} a_{1,j} \, x^j + \cdots + (c_0)_{hk-1} \sum_{j=0}^{hk-1} a_{hk-1,j} \, x^j \quad (3) \end{aligned}$$

Pre jednoduchosť budeme označovať $r \equiv r_{\mathcal{I}}$.

Dôsledok 2.13. *Spojením lemmy 1.2, 2.10, 2.11 a definície 2.12 dostávame*

$$\begin{array}{ccccc} \|b_0\|_1 & \overset{(1.2)}{\leq} & \sqrt{hk}\,\|b_0\|_2 & \overset{(2.10)}{\leq} & \left(\kappa_T \sqrt{hk}\right) X^{(hk-1)/2} N^{(h-1)/2} \\ |r(x)| & \overset{(2.11,\,2.12)}{\leq} & \|b_0\|_1 & \overset{(1.2,\,2.10)}{\leq} & \left(\kappa_T \sqrt{hk}\right) X^{(hk-1)/2} N^{(h-1)/2} \end{array}$$

pre každé $|x| \leq X$, *kde* $\kappa_T = 2^{(hk-1)/4}$.

Tvrdenie 2.14. *Nech $\mathcal{I}$ je inštancia problému MMK, $h \in \mathbb{N}$, $h \geq 2$ a nech platí $p(x_0) = 0 \pmod N$ pre $|x_0| \leq X$. Potom*

$$r(x_0) = 0 \pmod{N^{h-1}}.$$

Dôkaz. Pre každú sumu v rovnosti (3) stačí dokázať

$$\sum_{j=0}^{l} a_{l,j}\, {x_0}^j = 0 \pmod{N^{h-1}}, \text{ kde } l = 0, \ldots, hk-1.$$

Z definície 2.4 je $\varrho(p) = \mathcal{N}GD = AD$. Prvky $a_{l,0}, \ldots, a_{l,l}$ tvoria l-tý riadok matice A. Tento riadok je u-ty riadok v m-tom bloku podľa poznámky 2.5, teda $l = mk+u$, kde $m, u \in \mathbb{N} \cup \{0\}$ a $0 \leq u < k$. Z definícií 2.3 a 2.4 vidíme, že l-tý riadok je obrazom polynómu $x^u p(x)^m$ pri zobrazení φ prenásobený koeficientom N^{h-m-1}, odtiaľ

$$\begin{aligned} a_{l,j} &= N^{h-m-1}\, v_j(x^u p(x)^m) \\ \sum_{j=0}^{l} a_{l,j}\, x^j &= N^{h-m-1}\, x^u p(x)^m. \end{aligned}$$

Z rovnosti $p(x_0) = 0 \pmod N$ plynie $p(x)^m = 0 \pmod{N^m}$, a teda

$$\sum_{j=0}^{l} a_{l,j}\, {x_0}^j = 0 \pmod{N^{h-1}}.$$

Nakoniec $r(x_0) = 0 \pmod{N^{h-1}}$. □

Veta 2.15. *Majme inštanciu $\mathcal{I}$ problému MMK, $h \in \mathbb{N}$, $h \geq 2$, príslušný polynóm $r \equiv r_{\mathcal{I}}$ a $X \equiv X_T = \left\lceil \left({\kappa_T}^{-2/(hk-1)}\, (hk)^{-1/(hk-1)} \right) N^{(h-1)/(hk-1)} \right\rceil - 1$, kde $\kappa_T = 2^{(hk-1)/4}$ a nech platí $p(x_0) = 0 \pmod N$. Potom*

$$r(x_0) = 0 \text{ pre } \forall\, |x_0| \leq X_T.$$

Dôkaz. Podľa tvrdenia 2.14 máme $r(x_0) = tN^{h-1}$, $t \in \mathbb{Z}$, po dosadení X_T do nerovnosti z pozorovania 2.13 dostaneme $r(x_0) < N^{h-1}$, teda $t = 0$, a preto $r(x_0) = 0$ pre každé $|x_0| \leq X_T$. □

Pozorovanie 2.16. *Všimnime si limitu hranice X_T pre $\kappa_T = 2^{(hk-1)/4}$ a parameter h konvergujúci k nekonečnu*

$$\lim_{h\to\infty} \left\lceil \left({\kappa_T}^{-2/(hk-1)} (hk)^{-1/(hk-1)} \right) N^{(h-1)/(hk-1)} \right\rceil - 1.$$

Spočítame limity jednotlivých činiteľov:

$$\begin{aligned} \lim_{h\to\infty} (hk)^{-1/(hk-1)} &= 1 \\ \lim_{h\to\infty} N^{(h-1)/(hk-1)} &= N^{1/k}. \end{aligned}$$

Konštantu ${\kappa_T}^{-2/(hk-1)} = 2^{-1/2}$ vyjmeme a nakoniec dostávame

$$\lim_{h\to\infty} \left\lceil \left({\kappa_T}^{-2/(hk-1)} (hk)^{-1/(hk-1)} \right) N^{(h-1)/(hk-1)} \right\rceil - 1 \doteq 2^{-1/2} N^{1/k}.$$

Poznámka 2.17. Podľa článku [7] autorov Nguyen a Stehlé o správaní algoritmu LLL môžeme vo výpočte hornej hranice X (veta 2.15) nahradiť teoretickú konštantu κ_T za praktickú konštantu $\kappa_P = 1,02^{\,hk-1}$, a tým dostaneme namiesto teoretickej hranice X_T novú praktickú hornú hranicu X_P pre malé korene polynómu p.

Zistíme približný rozdiel v počte bitov teoretickej hranice X_T a praktickej hranice X_P, pričom vo výpočte zanedbáme celé časti a odčítanie 1

$$\begin{aligned} \log_2 \frac{X_P}{X_T} &\approx \log_2 \frac{\left({\kappa_P}^{-2/(hk-1)} (hk)^{-1/(hk-1)} \right) N^{(h-1)/(hk-1)}}{\left({\kappa_T}^{-2/(hk-1)} (hk)^{-1/(hk-1)} \right) N^{(h-1)/(hk-1)}} = \\ &= \log_2 \left(\frac{\kappa_P}{\kappa_T} \right)^{-2/(hk-1)} = \\ &= \frac{-2}{hk-1} \left(\log_2 (1,02)^{hk-1} - \log_2 \left(2^{1/4}\right)^{hk-1} \right) = \\ &= 2 \left(\log_2 2^{1/4} - \log_2 1,02 \right) \doteq 0,44. \end{aligned}$$

Vidíme, že rozdiel je minimálny, dokonca nezávisí na dĺžke modulu N a ani na parametroch h a k. V praxi to môže znamenať maximálne 1 bit.

V príklade 2.18 nastáva práve spomenutý prípad, ak by sme počítali s teoretickou konštantou κ_T namiesto praktickej κ_P, teoretická hranica X_T by bola rovná 2, X_P praktická 3.

Keďže tento rozdiel je zanedbateľný, v experimentálnej časti našich výpočtov sme použili konštantu κ_T, pričom sme experimentovali aj s dĺžkami paddingu za touto hranicou.

Vidíme dokonca, že v prípade možnosti riešiť problém redukcie bázy mriežky presne, t.j. s aproximačných koeficientom $\kappa_E = 1$ a hornou hranicou $X_E = \left\lceil (hk)^{-1/(hk-1)} N^{(h-1)/(hk-1)} \right\rceil - 1$, je rozdiel v dĺžke napadnuteľných paddingov

$$\log_2 \frac{X_E}{X_T} \approx \log_2 \frac{1}{{\kappa_T}^{-2/(hk-1)}} = \log_2 2^{1/2} = 0,5.$$

Pri algoritmickom riešení preto môžeme voliť rýchlejšie, aj keď menej efektívne varianty LLL redukcie.

Príklad 2.18. Majme polynóm p a parameter h

$$p(x) = 18 + 21x + x^2 = 0 \pmod{45},\ h = 3.$$

Vypočítame hodnotu X_P

$$X \equiv X_P = \left\lceil \left(1,02^{-2} \left(3 \cdot 2\right)^{-1/(3\cdot 2-1)}\right) 45^{(3-1)/(3\cdot 2-1)} \right\rceil - 1 = \lceil 3,079 \rceil - 1 = 3.$$

LLL redukovaná báza B

$$\begin{pmatrix} -81\times 3^0 & -54\times 3^1 & 27\times 3^2 & 12\times 3^3 & -4\times 3^4 & 0 \\ 0 & 27\times 3^1 & 18\times 3^2 & 6\times 3^3 & 1\times 3^4 & -2\times 3^5 \\ 486\times 3^0 & 0 & 27\times 3^2 & -9\times 3^3 & -3\times 3^4 & -1\times 3^5 \\ 324\times 3^0 & 81\times 3^1 & -189\times 3^2 & 12\times 3^3 & -4\times 3^4 & 0 \\ -405\times 3^0 & 189\times 3^1 & 36\times 3^2 & -18\times 3^3 & -3\times 3^4 & 1\times 3^5 \\ 567\times 3^0 & 162\times 3^1 & 27\times 3^2 & 18\times 3^3 & 0 & 1\times 3^5 \end{pmatrix}.$$

Prechodová matica C, kde $B = CM$

$$\begin{pmatrix} 17 & 19 & -41 & 4 & -4 & 0 \\ -154 & -172 & 351 & -58 & 85 & -2 \\ -66 & -74 & 150 & -26 & 39 & -1 \\ 18 & 20 & -43 & 4 & -4 & 0 \\ 83 & 93 & -190 & 31 & -45 & 1 \\ 79 & 88 & -180 & 29 & -42 & 1 \end{pmatrix}.$$

Polynóm r

$$r = -81 - 54x + 27x^2 + 12x^3 - 4x^4.$$

Celočíselné korene polynómu r

$$x_{1,2} = 3.$$

Na konci overíme, či každý koreň polynómu r spĺňa požadovanú rovnosť $p(x_0) = 0 \pmod{N}$, a tým dostaneme malé korene polynómu p

$$x_0 = 3.$$

Experimentálna časť

3 RSA

RSA je šifrovacia schéma s verejným kľúčom, publikovaná v roku 1977 autormi Ron Rivest, Adi Shamir a Leonard Adleman. Aktuálna verzia [9] je dostupná v štandarde PKCS #1. Ide o prvý algoritmus, ktorý je vhodný ako pre šifrovanie, tak pre podpisovanie. Je založený na obtiažnosti faktorizácie veľkého prirodzeného čísla na súčin prvočísel.

Generovanie kľúčového páru

0. určíme párny parameter n
1. zvolíme dve rôzne veľké náhodné prvočísla p a q dĺžky $n/2$ *
2. spočítame súčin $N = p\,q$
3. vypočítame hodnotu Eulerovej funkcie $\phi(N) = (p-1)(q-1)$
4. zvolíme prirodzené číslo e také, že spĺňa

$$1 < e < \phi(N) \quad \text{a zároveň} \quad \mathrm{NSD}(e, \phi(N)) = 1$$

5. dopočítame prirodzené číslo d z intervalu $1 < d < \phi(N)$, pre ktoré platí kongruencia

$$de \equiv 1 \pmod{\phi(N)}$$

Verejný kľúč RSA pozostáva z dvojice čísel (N, e), pričom N sa označuje ako modul a parameter e ako šifrovací alebo verejný exponent. Súkromný kľúč RSA tvorí hodnota d, ktorú nazývame dešifrovací alebo súkromný exponent.

V súčasnosti sa pri konštrukcii kľúčového páru používa dĺžka modulu N aspoň 1024 bitov, častejšie však 2048 bitov.

*prvočísla p a q sa volia vhodným spôsobom, napr. rozdiel $|p-q|$ by mal byť dostatočne veľký, čísla $p-1$ a $q-1$ by mali mať aspoň jeden veľký prvočíselný faktor, výber prvočísel p a q je nezávislý a pod.

Šifrovanie správy

V prípade, že Bob chce poslať Alici správu m, Alica vygeneruje verejný a súkromný kľúč, pričom verejný kľúč (N, e) pošle Bobovi otvoreným kanálom a naopak súkromný kľúč (N, d) uchová v tajnosti. Bob spočíta šifrový text

$$c = m^e \mod N,$$

ktorý môže poslať Alici nezabezpečeným kanálom.

Poznámka: Môžeme predpokladať, že pre správu m platí $1 < m < N$, v opačnom prípade rozdelíme správu m na viac častí.

Dešifrovanie správy

Alica získa pôvodnú správu m zo šifrového textu c výpočtom

$$m = c^d \mod N.$$

Korektnosť RSA

Správnosť algoritmu RSA spočíva v nasledujúcej vete 3.1, známej ako *Malá Fermatova veta*.

Veta 3.1 (Malá Fermatova veta)**.** *Pre každé $a \in \mathbb{Z}$, $N \in \mathbb{N}$ také, že $NSD(a, N) = 1$ platí*

$$a^{\phi(N)} \equiv 1 \mod N,$$

kde $\phi(N)$ označuje Eulerovu funkciu čísla N.

Dôkaz. Viď [2]. □

Veta 3.2 (Korektnosť RSA)**.** *Majme inštanciu RSA - modul N, šifrovací a dešifrovací exponent e a d. Potom pre každú správu $m \in Z_N$ platí*

$$(m^e \mod N)^d \mod N = m.$$

Dôkaz. Špeciálny prípad $m = 0$ je zrejmý. Ďalej teda predpokladajme, že $m \in \mathbb{Z}_N \setminus \{0\}$. Z konštrukcie kľúčového páru máme $ed \equiv 1 \pmod{\phi(N)}$, takže existuje $k \in \mathbb{N}$ také, že $ed = 1 + k\phi(N)$.

Najskôr uvažujme prípad $\mathrm{NSD}(m, N) = 1$. Z Malej Fermatovej vety pomocou rovnosti $m^{\phi(N)} = 1 \pmod N$ dostávame

$$\begin{aligned}(m^e \mod N)^d \mod N &= m^{ed} \mod N \\ &= m^{1+k\phi(N)} \mod N \\ &= m(m^{\phi(N)})^k \mod N = m.\end{aligned}$$

Nakoniec uvažujme $\mathrm{NSD}(m, N) \neq 1$. Bez ujmy na všeobecnosti môžeme predpokladať, že číslo m je deliteľné p, ale nie q. Podľa Malej Fermatovej vety platí $p^{\,q-1} \equiv 1 \pmod{q}$, odtiaľ

$$\begin{aligned} p^{(p-1)(q-1)} &\equiv 1 \pmod{q} \\ p^{k\phi(N)} &= 1 + cq, \text{ pre nejaké } c \in \mathbb{Z} \\ p^{1+k\phi(N)} &= p + cpq = p + cN \\ p^{1+k\phi(N)} &\equiv p \pmod{N}. \end{aligned}$$

Správu m zapíšeme ako $m = lp^s$, kde $s \in \mathbb{N}$, $s \geq 1$, $l \in \mathbb{N}$ a $\mathrm{NSD}(l, N) = 1$. Použitím vety 3.1 máme $l^{\,\phi(N)} \equiv 1 \pmod{N}$, nakoniec dostávame

$$\begin{aligned} (m^e \mod N)^d \mod N &= m^{ed} \mod N \\ &= (lp^s)^{1+k\phi(N)} \mod N \\ &= l(p^{1+k\phi(N)})^s \mod N \\ &= lp^s \mod N = m. \end{aligned}$$

□

4 Coppersmithov útok na RSA

Jednoduchá aplikácia Howgrave-Grahamovej metódy je Coppersmithov útok na RSA s malým šifrovacím exponentom a krátkym paddingom.

Útok Franklina a Reitera [3]: Majme dve neznáme správy m a m' a predpokladajme, že poznáme ich rozdiel t

$$m' = m + t.$$

Obe správy zašifrujeme verejným RSA exponentom 3

$$\begin{aligned} c &= m^3 \pmod N \\ c' &= (m')^3 \pmod N = m^3 + 3m^2t + 3mt^2 + t^3 \pmod N. \end{aligned}$$

Vidíme, že zo znalosti šifrových textov c, c', rozdielu t a modulu N vieme odhaliť pôvodnú správu m

$$\begin{aligned} c' - c &= 3m^2t + 3mt^2 + t^3 && \pmod N && / + 2t^3 \\ c' - c + 2t^3 &= t(3m^2 + 3mt + 3t^2) && \pmod N && / m \\ m(c' - c + 2t^3) &= t((2m^3) + (m^3 + 3m^2t + 3mt^2)) && \pmod N \\ m(c' - c + 2t^3) &= t((2c) + (c' - t^3)) && \pmod N \\ m &= \frac{t\,(c' + 2c - t^3)}{c' - c + 2t^3} && \pmod N. \end{aligned}$$

Pravdepodobnosť, že $c' - c + 2t^3 = 0 \pmod N$ je zanedbateľná vzhľadom k štandartnej dĺžke paddingu t, preto poslednú úpravu môžeme považovať za korektnú.

Coppersmithov útok [1]: Uvažujme dve neznáme správy m a m'. Predpokladajme, že daný rozdiel medzi správami nepoznáme, ale vieme, že je dostatočne malý

$$\begin{aligned} m' &= m + t \\ |t| &< X_T, \end{aligned}$$

kde X_T je horná hranica definovaná vo vete 2.15, pričom parametre h a k upresníme neskôr. Uvažujme, že správa M je pred zašifrovaním RSA doplnená náhodným paddingom T, čiže M sa posunie o k bitov doľava a T sa doplní na koniec. Správa sa zašifruje

$$c = m^3 \pmod N = \left(2^k M + T\right) \pmod N.$$

Ďalej správu M zašifrujeme druhýkrát, tentoraz ale s novým náhodným paddingom $T' = T + t$, takže otvorený text je $m' = m + t$,

$$\begin{aligned} c &= m^3 \pmod N = \left(2^k M + T\right)^3 \pmod N \\ c' &= (m')^3 \pmod N = \left(2^k M + T'\right)^3 \pmod N = (m + t)^3 \pmod N. \end{aligned}$$

Zvolením vhodných polynómov a a b,

$$\begin{aligned} a(x) &= x^3 - c \mod N \\ b(x) &= (x+t)^3 - c' \mod N, \end{aligned}$$

dostaneme dve rovnice o dvoch neznámych x a t, ktoré majú spoločný nenulový koreň $x = m$. Keďže platí $\mathrm{NSD}(m, N) = 1$, použitím lemmy 1.15 o rezultante eliminujeme neznámu x (príklad 1.16)

$$\begin{aligned} &\mathrm{res}_x\left(x^3 - c, (x+t)^3 - c'\right) = \\ &= t^9 + (3c - 3c')\,t^6 + (3c^2 + 21cc' + 3(c')^2)\,t^3 + (c - c')^3 = 0 \pmod N. \end{aligned}$$

Posledná rovnosť ukazuje na problém riešenia modulárnych polynómov s jednou neznámou. Parametre vstupujúce do výpočtu hornej hranice X_T sú v tomto prípade stupeň polynómu v poslednej rovnosti, t.j. 9, a voliteľný parameter h. Ak je teda veľkosť paddingu $|t| < X_T < 2^{-1/2}N^{1/9}$, môžeme použiť Howgrave-Grahamovu metódu na nájdenie rozdielu t medzi správami m a m'. Definujeme inštanciu $\mathcal{I} = \{p, k, N, X\}$ problému MMK - polynóm p, jeho stupeň k, modul N a hornú hranicu $X = X_T$

$$\begin{aligned} p(t) &= t^9 + (3c - 3c')\,t^6 + (3c^2 + 21cc' + 3(c')^2)\,t^3 + (c - c')^3 \\ k &= 9 \\ N &= N \\ X_T &= \left\lceil \left(2^{-1/2}\,(9h)^{-1/(9h-1)}\right) N^{(h-1)/(9h-1)} \right\rceil - 1 < 2^{-1/2}N^{1/9}. \end{aligned}$$

Použitím vety 2.15 a overením koreňov pre polynóm p zistíme daný rozdiel t a nakoniec odhalíme správu M pomocou útoku Franklina a Reitera. Útok môžeme zosumarizovať do algoritmu 1.

Algoritmus 1 Zhrnutie Coppermithovho útoku na RSA

Vstup: c, c', X_T, N také, že $c = m^e \mod N, c' = (m+t)^e \mod N, |t| < X_T$
Výstup: m

1: položíme polynómy $a(x) = x^3 - c \mod N$ a $b(x) = (x+t)^3 - c' \mod N$
2: vypočítame rezultant $\mathrm{res}_x(a(x), b(x)) = p(t) \pmod N$
3: definujeme inštanciu $\mathcal{I} = \{p(t), k, N, X_T\}$ problému MMK, parameter h a pomocou Howgrave-Grahamovej metódy zistíme kandidátov na korene polynómu $p(t)$ - padding t
4: odfiltrujeme správnych kandidátov dosadením do polynómu $p(t)$, pre koreň má platiť $p(t) \equiv 0 \pmod N$
5: zo znalosti c, c' a t dopočítame správu $m = \frac{t\left(c' + 2c - t^3\right)}{c' - c + 2t^3} \pmod N$

5 Výsledky experimentov

V tejto časti budeme skúmať Coppersmithov útok z viacerých hľadísk. Najskôr podľa získaného vzťahu pre výpočet hornej hranice napadnuteľného paddingu z vety 2.15 zistíme presné hodnoty pre jednotlivé dĺžky modulu RSA. Následne budeme prezentovať výsledky experimentov, ktoré zahŕňajú napríklad meranie času útoku a zistenie úspešnosti útoku, ak dĺžku paddingu zvolíme o pár bitov viac, ako nám udávajú teoretické výpočty.

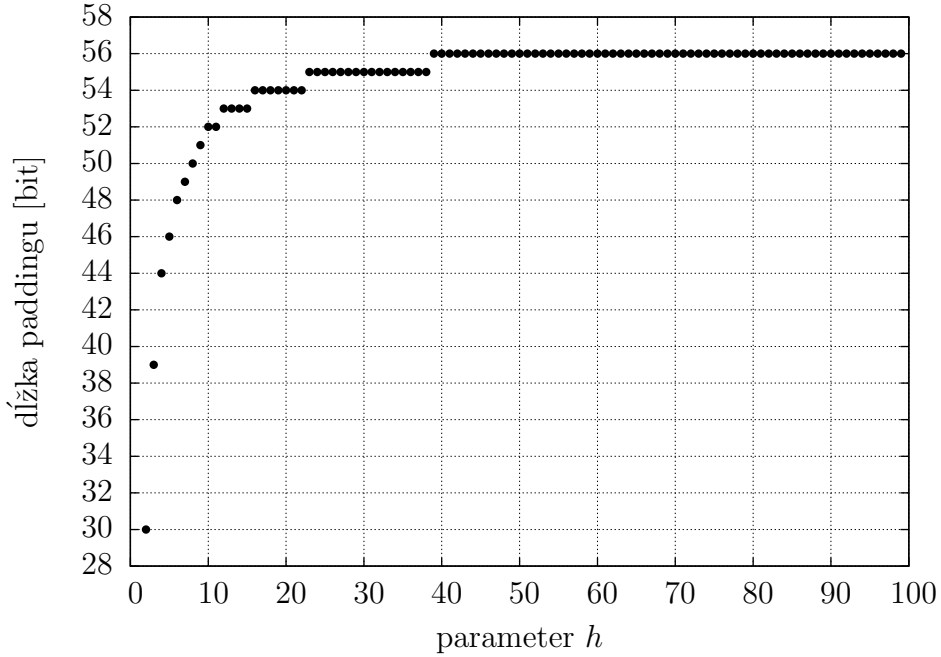
5.1 Závislosť dĺžky paddingu na parametri h

Pred samotnými experimentami sme skúmali hornú hranicu X, konkrétne maximálny počet bitov napadnuteľného paddingu pre RSA 512, 1024 a 2048 v závislosti na parametri h. Limita dĺžky paddingu pre $h \to \infty$

dĺžka modulu	**limita dĺžky paddingu**
512	57
1024	114
2048	228

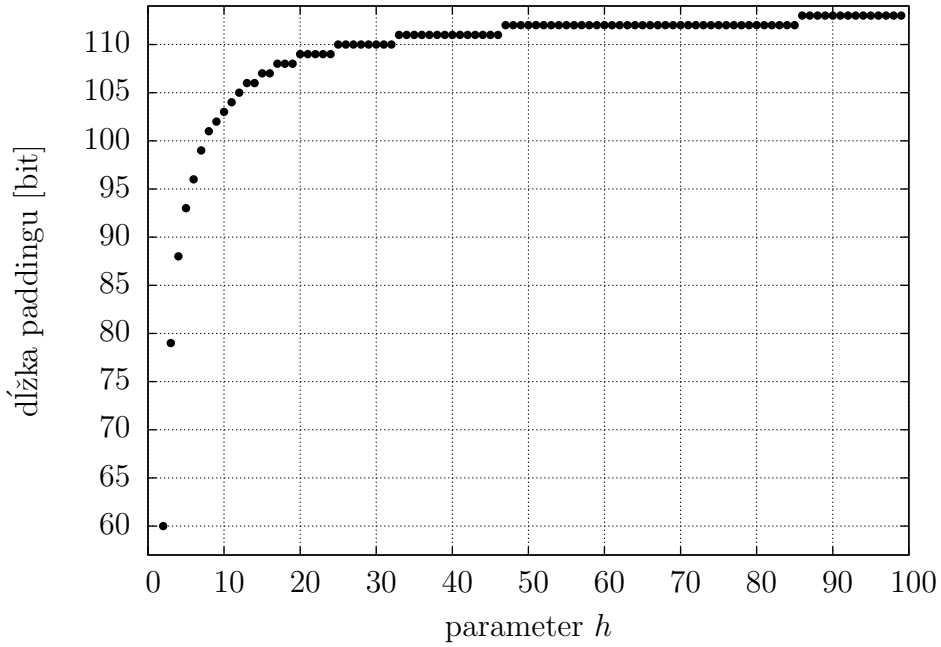
Tabuľka 1: Limita dĺžky paddingu pre parameter $h \to \infty$

Na obrázku 1 vidíme, že pre RSA 512 dĺžka paddingu rastie až k hodnote 56 bitov pre parameter h od 2 do 100.

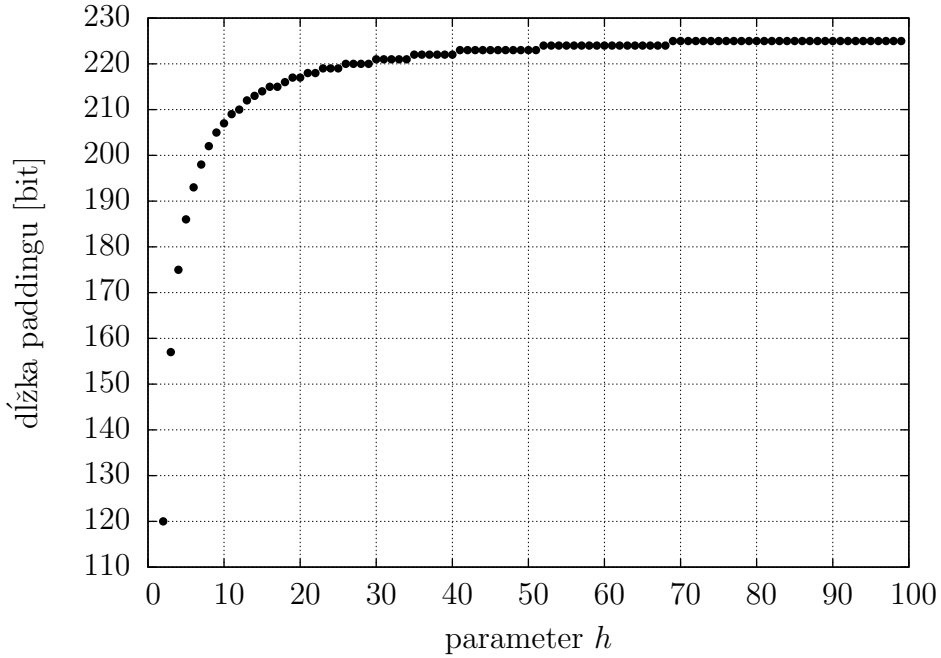


Obrázok 1: Závislosť dĺžky paddingu na parametri h pre RSA 512

Podobne z obrázkov 2 a 3 je vidieť, že dĺžka paddingu pre RSA 1024 stúpa k 113 bitom (h rovné 86) a pre RSA 2048 k 225 bitom ($h = 69$). Tieto hodnoty sa však dosahujú až pre veľký parameter h, pri ktorom je podľa nasledujúceho experimentu tento útok z časového hľadiska už nepoužiteľný.



Obrázok 2: Závislosť dĺžky paddingu na parametri h pre RSA 1024



Obrázok 3: Závislosť dĺžky paddingu na parametri h pre RSA 2048

5.2 Coppersmithov útok v praxi

Ako výpočetnú základňu sme použili karlínsky cluster Sněhurka zložený zo 64-bitových procesorov CPU AMD Opteron 246. Algoritmus sme implementovali v jazyku C++ využitím knižníc GMP a NTL. Knižnica NTL [10] ponúka viac možností LLL redukcie. V poznámke 2.17 sme upozornili na možnosť použiť rýchlejšie, aj keď menej efektívne varianty. Na druhej strane sme limitovaní veľkosťou čísel, ktoré do tejto redukcie vstupujú. Nakoniec pre veľkosť modulu 512 a 1024 bitov bola použitá funkcia G_LLL_RR s parametrom $delta = 0,99$ a pre 2048-bitový modul základná funkcia LLL.

5.2.1 Overenie teóriou garantovaných hodnôt

Na základe Howgrave-Grahamovej metódy hľadania malých koreňov modulárnych rovníc sme aplikovali Coppersmithov útok na RSA s verejným kľúčom 3 a dĺžkou modulu 512, 1024 a 2048 bitov. Parameter h sme pre RSA 512 volili od 2 do 20, pre RSA 1024 od 2 do 15 a pre RSA 2048 od 2 do 7.

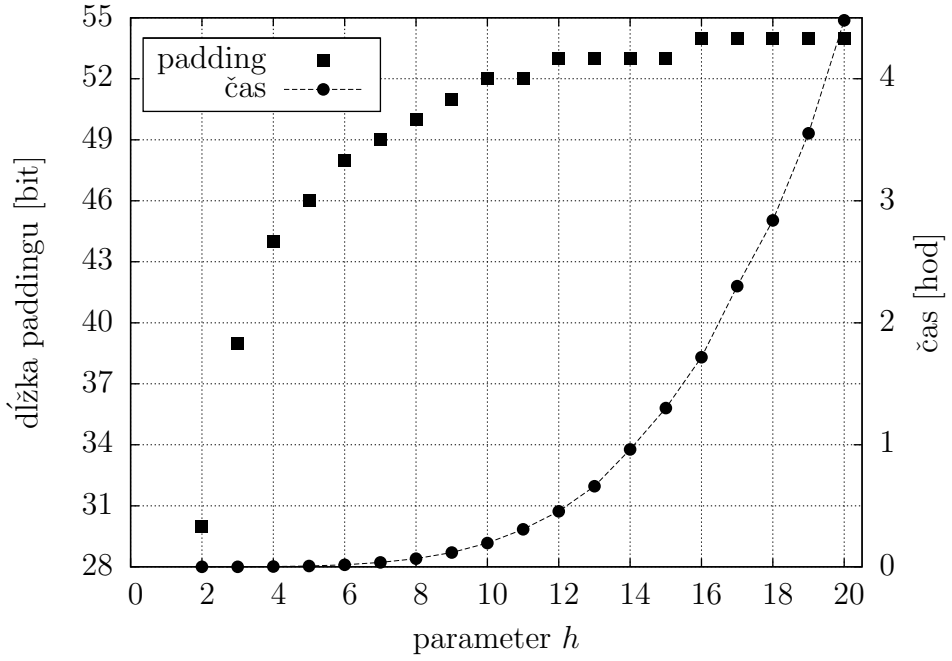
Pre každé fixne zvolené h sme určili dĺžku napadnuteľného paddingu a spravili 10 meraní času Coppersmithovho útoku, kde dĺžka paddingu bola tesne pod teoreticky spočítanou hranicou. Nakoniec sme z týchto meraní urobili priemer.

Vo všetkých experimentoch bol padding nájdený a tým aj odhalená pôvodná správa m. Z grafov vidíme exponenciálny rast času so zväčšujúcim sa parametrom h, čo zodpovedá najnáročnejšej časti útoku - LLL algoritmu, ktorý z bázy danej mriežky vytvorí LLL - rekudovanú bázu (definícia 1.12). Časová zložitosť LLL algoritmu závisí od dimenzie mriežky a od dĺžky najdlhšieho vektora bázy na vstupe. Dimenzia mriežky je daná súčinom stupňa modulárnaho polynómu, v našom prípade 9, a zvoleného parametra h.

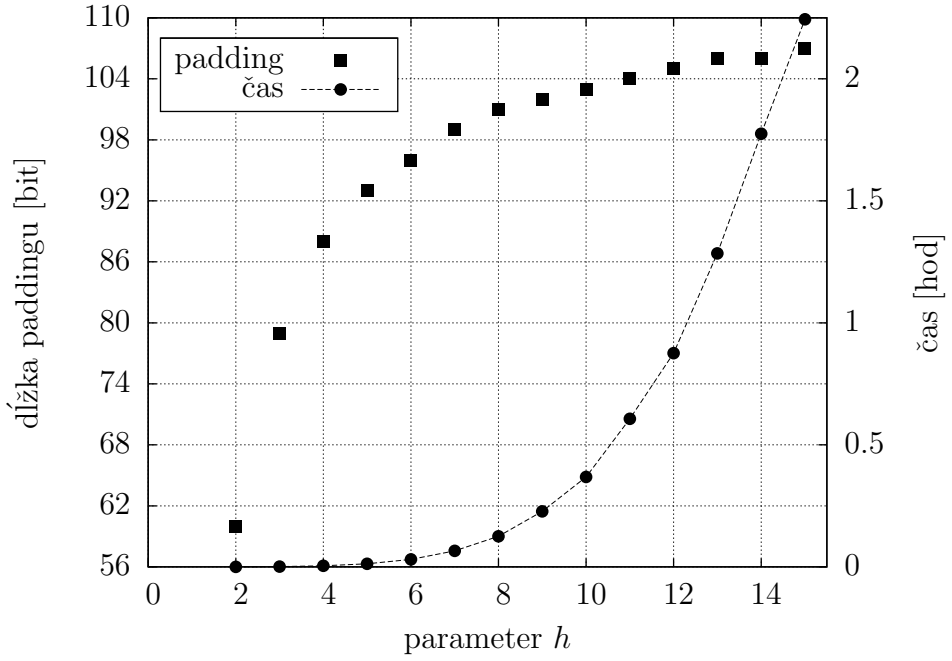
Otázkou je určiť optimálny prípad voleného parametru h v závislosti na dĺžke napadnuteľného paddingu a času útoku.

V grafe na obrázku 4 pre RSA 512 si môžeme všimnúť, že pre parameter h od 10 do 20 je rozdiel v paddingu len 2 bity, ale rozdiel v dĺžke trvania útoku sú až 4 hodiny, preto za optimálne h môžeme zvoliť hodnotu okolo 16.

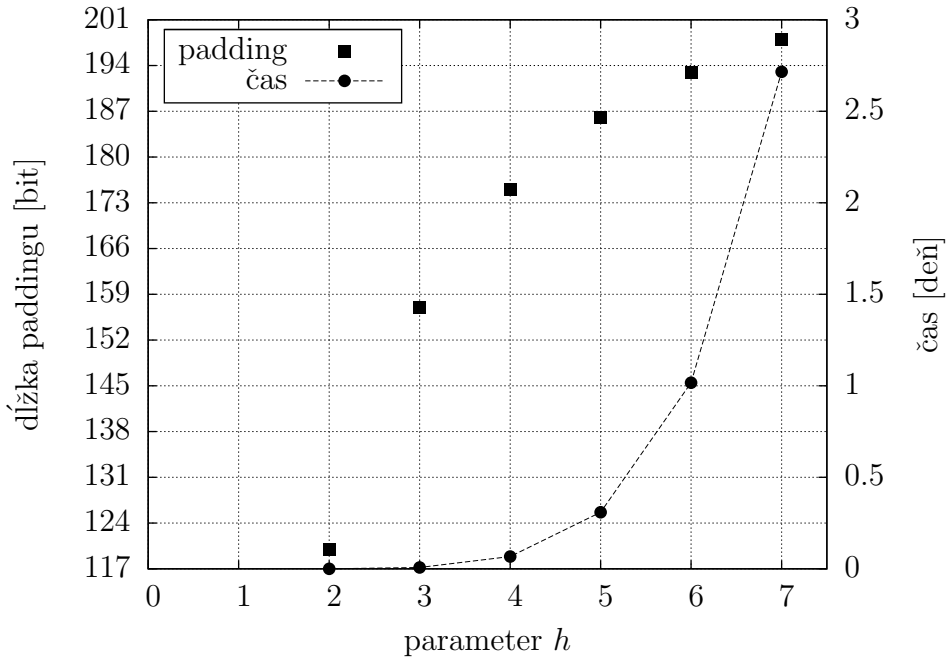
Podobne z obrázkov 5 a 6 vidíme, že vzhľadom k experimentálnej zložitosti LLL redukcie je vhodné voliť najkratší akceptovateľný parameter h, teda aj dĺžku paddingu t.



Obrázok 4: Dĺžka paddingu a čas útoku pre RSA 512



Obrázok 5: Dĺžka paddingu a čas útoku pre RSA 1024

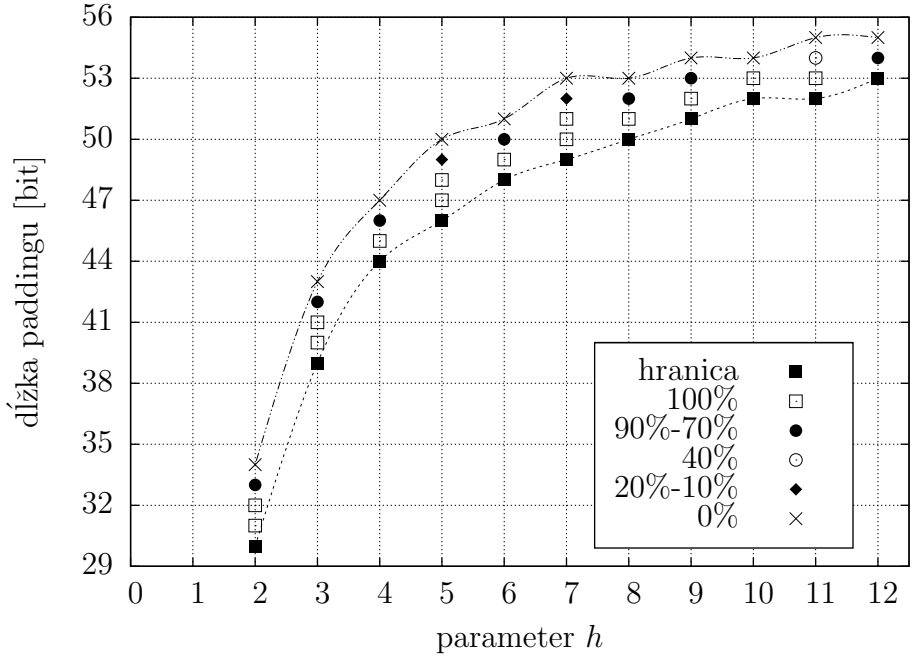


Obrázok 6: Dĺžka paddingu a čas útoku pre RSA 2048

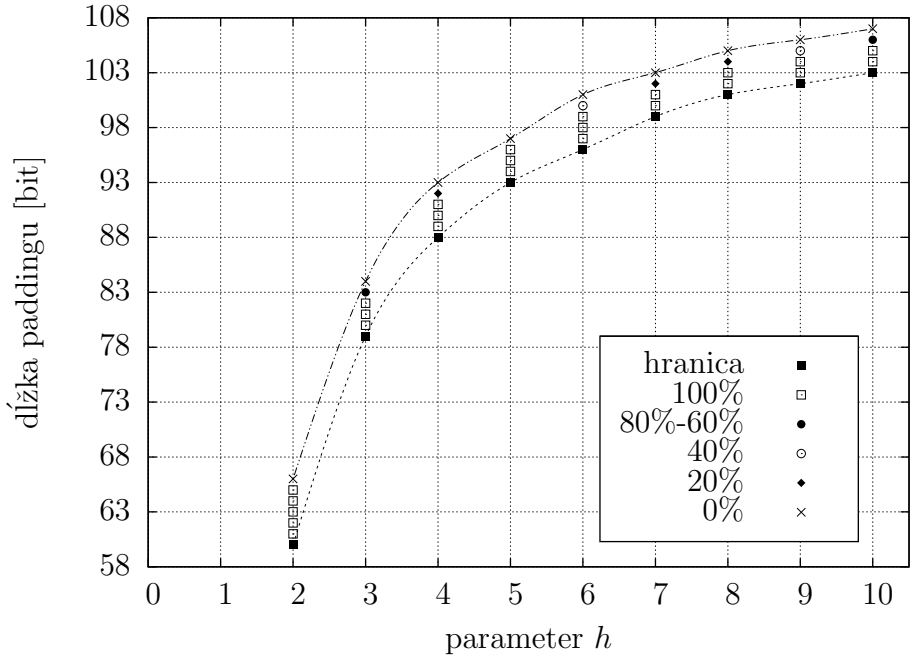
5.2.2 Za hranicami teórie

V druhom experimente sme skúmali úspešnosť Coppersmithovho útoku pre padding v niekoľkobitovom okolí garantovanej napadnuteľnej dĺžky. Vo výpočtoch sme použili teoretickú konštantu $\kappa_T = 2^{(hk-1)/4}$, kde k je stupeň modulárneho polynómu, v našom prípade 9, a h je volený parameter.

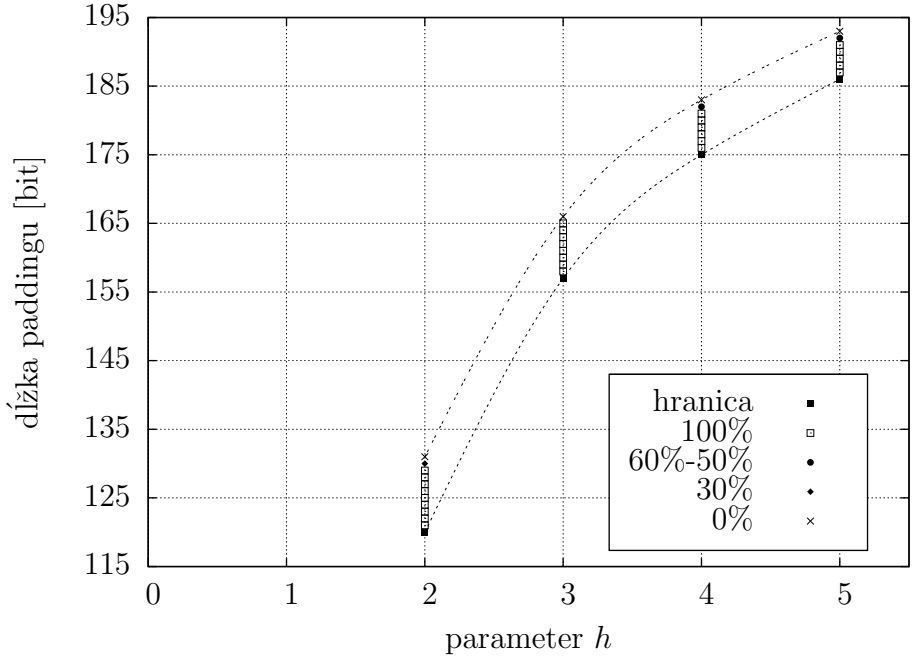
Naskôr sme overili, že teoretické výpočty dávajú na našej testovacej vzorke naozaj 100 percentnú úspešnosť útoku a ďalej sme skúšali zvyšovať dĺžku paddingu. Vo väčšine prípadov vyšla 100 percentná úspešnosť aj pri zvýšení o 1 bit, čo si čiastočne môžeme vysvetliť priemerným správaním LLL algoritmu, ktorý je popísaný v článku [7]. Podľa neho môžeme vo výpočtoch nahradiť teoretickú konštantu κ_T za praktickú konštantu $\kappa_P = 1,02^{hk-1}$, ale z poznámky 2.17 vieme, že dĺžka paddingu môže z tohto dôvodu narásť maximálne o 1 bit. Z obrázkov 8 a 9 pre RSA 1024 a 2048 dokonca vidíme, že útok je úspešný aj 2 až 5 bitov za teoretickou hranicou. Aj napriek tomu môžeme usúdiť, že algoritmus útoku v praxi funguje podľa teoretických výpočtov a maximálna hranica dĺžky paddingu je stanovená primerane.



Obrázok 7: Úspešnosť útoku nad teoretickou hranicou pre RSA 512



Obrázok 8: Úspešnosť útoku nad teoretickou hranicou pre RSA 1024

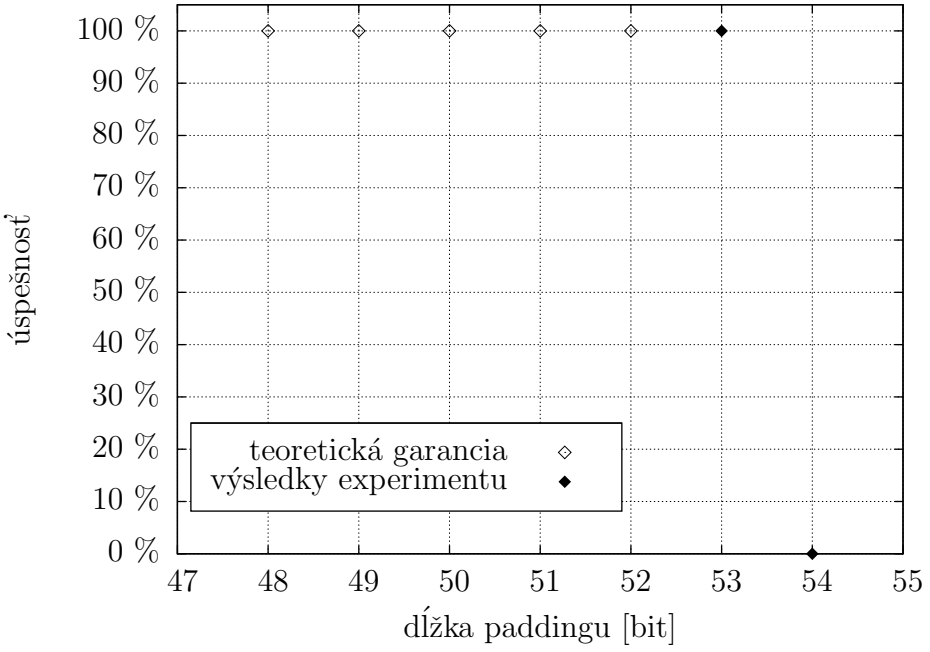


Obrázok 9: Úspešnosť útoku nad teoretickou hranicou pre RSA 2048

5.2.3 Úspešnosť útoku pod lupou

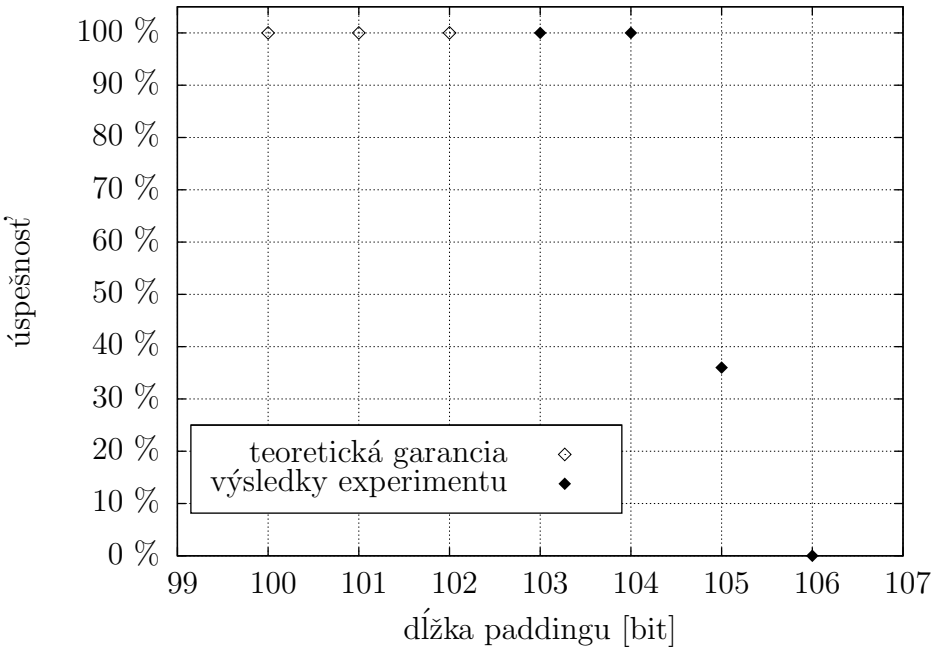
V poslednom experimente sme podrobnejšie rozobrali predchádzajúci experiment. Pre každú dĺžku RSA modulu sme vybrali jeden parameter h a skúmali postupné klesanie úspešnosti algoritmu pri zväčšovaní dĺžky paddingu. Medzi 100 percentnou a nulovou hranicou sme urobili pre každý počet bitov paddingu 100 pozorovaní.

Z obrázkov vidíme, že s rastúcou dĺžkou modulu rastie aj úspešnosť útoku za teoretickou hranicou, no spoločným znakom je prudký pokles zo stopercentnej úspešnosti na nulovú. Napríklad pre RSA 2048 pri dĺžke paddingu 165 bitov je útok vždy úspešný, ale pri dĺžke 166 bitov nebol úspešný ani jeden z pokusov.

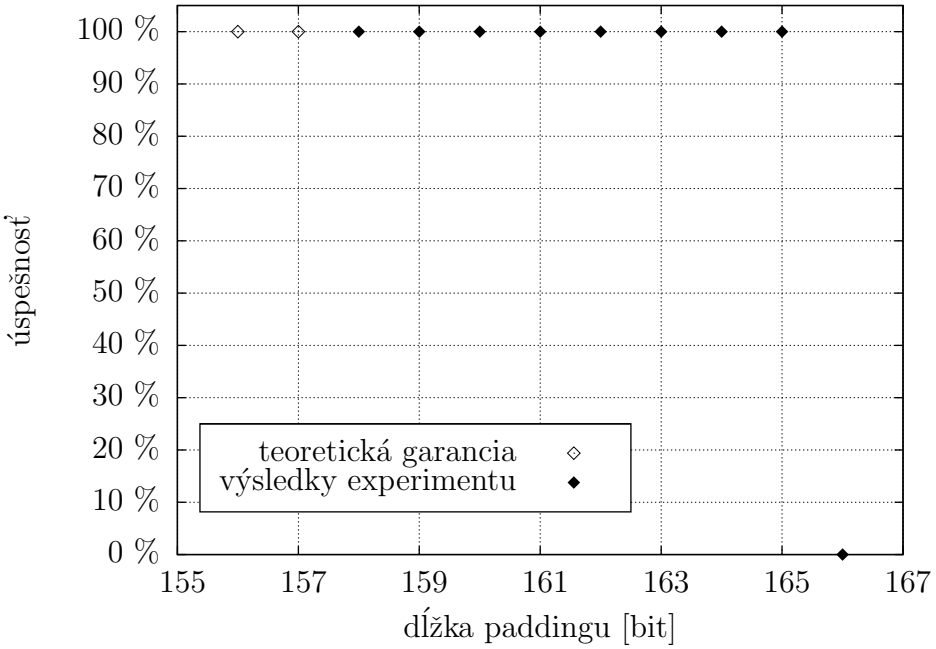


Obrázok 10: Úspešnosť útoku pre RSA 512, $h = 10$

Kvôli veľkosti čísel, ktoré vstupujú do LLL redukcie pre modul 2048, sme museli použiť pomalú funkciu LLL implementovanú v knižnici NTL. Z tohto dôvodu sme pre RSA 2048 experimentovali len pre parameter $h = 3$, ako je poznamenané v popise obrázku 12. Naopak z obrázkov 7, 8 a 9 vidíme, že pre menšie hodnoty parametru h je úspešnosť útoku nad teoretickou hranicou o pár bitov väčšia ako je priemer pre danú dĺžku modulu.



Obrázok 11: Úspešnosť útoku pre RSA 1024, $h = 9$



Obrázok 12: Úspešnosť útoku pre RSA 2048, $h = 3$

Záver

V tejto práci sme popísali Howgrave-Grahamovu metódu hľadania malých koreňov modulárnych rovníc s jednou neznámou [5]. Algoritmus sme vysvetlili prístupnejšou formou a podali jeho exaktný dôkaz. Následne sme Coppersmithov útok na RSA s verejným exponentom 3 popísaný v [1] experimentálne overili, pričom sme nahradili hľadanie malých modulárnych koreňov Howgrave-Grahamovou metódou. Brali sme do úvahy aj nepresnosti LLL redukcie, no zistili sme, že v tomto útoku sú zanedbateľné. Z toho dôvodu sme použili rýchlejšie, aj keď menej efektívne varianty algoritmu LLL. Z našich experimentov sme zistili, že odhady na dĺžku napadnuteľného paddingu sú primerané, t.j. v garantovanom intervale bola úspešnosť 100%, ale pár bitov nad teoretickou hranicou vyšla úspešnosť nulová.

Literatúra

[1] Coppersmith D.: Finding a Small Root of a Univariate Modular Equation. *Advances in Cryptology – Proceedings of Eurocrypt '96*, Lecture Notes in Computer Science 1070, Springer-Verlag, 1996, 155–165.

[2] Drápal A.: Teorie čísel a RSA, skriptá. MFF UK, Praha.

[3] Franklin M., Reiter M.: A Linear Protocol Failure for RSA with Exponent Three. *Presented at the Rump Session of CRYPTO '95*, 1995.

[4] Gama N., Nguyen P. Q.: Predicting Lattice Reduction. *Advances in Cryptology – Proceedings of Eurocrypt '08*, Lecture Notes in Computer Science 4965, Springer-Verlag, 2008, 31–51.

[5] Howgrave-Graham N.: Finding Small Roots of Univariate Modular Equations Revisited. *Proceedings of IMA International Conference on Cryptography and Coding*, Lecture Notes in Computer Science 1355, London, UK, Springer-Verlag, 1997, 131–142.

[6] Lenstra A. K., Lenstra H. W., Lovász L.: Factoring Polynomials with Rational Coefficients. Mathematische Ann. 261, Springer-Verlag, 1982, 515–534.

[7] Nguyen P. Q., Stehlé D.: LLL on the Average. *ANTS*, Lecture Notes in Computer Science 4076, Springer-Verlag, 2006, 238–256.

[8] Nguyen P. Q., Stern J.: The Two Faces of Lattices in Cryptology. *CaLC '01: Revised Papers from the International Conference on Cryptography and Lattices*, Lecture Notes in Computer Science 2146, London, UK, Springer-Verlag, 2001, 146–180.

[9] RSA Data Security, Inc.: PKCS #1: RSA Encryption Standard. 2002.

[10] Shoup V.: NTL: A Library for doing Number Theory.
URL: `http://www.shoup.net/ntl/`