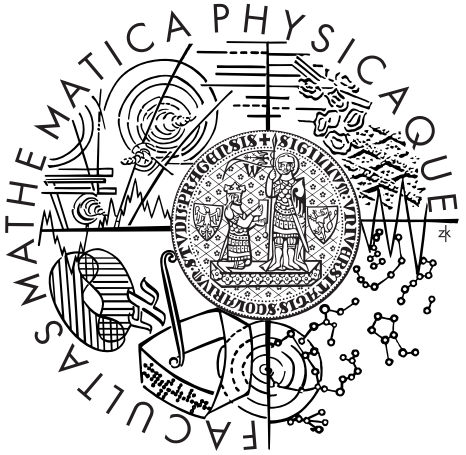
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Romana Linkeová

Diffie a Hellman si vyměňují matice nad grupovým okruhem

Katedra algebry

Vedoucí bakalářské práce:	Mgr. Pavel Příhoda, Ph.D.
Studijní program:	Matematika
Studijní obor:	Matematické metody informační bezpečnosti

Praha 2014

Děkuji svému vedoucímu Mgr. Pavlu Příhodovi, Ph.D. za vynikající, vysoce motivující a příkladné vedení bakalářské práce, za čas věnovaný konzultacím a za ochotu a vstřícnost při vysvětlování potřebné teorie.
Dále děkuji své rodině za její velkou podporu a trpělivost, kterou mi projevovala po dobu celého studia.

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Diffie a Hellman si vyměňují matice nad grupovým okruhem

Autor: Romana Linkeová

Katedra: Katedra algebry

Vedoucí bakalářské práce: Mgr. Pavel Příhoda, Ph.D., Katedra algebry

Abstrakt: Diffieho-Hellmanův protokol pro výměnu klíčů není při počítání nad grupou $\mathbb{Z}_p^*$ (kde počet cifer p je alespoň 300) vykonatelný na strojích s menší výpočetní silou. Tento fakt vedl ke snaze pracovat nad jinými algebraickými strukturami s cílem snížit výpočetní a paměťovou náročnost výpočtů. D. Kahrobaei a spol. publikoval v roce 2013 návrh na pracování nad strukturou malých matic s tím, že tato modifikace nesníží bezpečnost daného protokolu. V této práci se pokusíme napadnout takto modifikovaný Diffieho-Hellmanův protokol pomocí teorie reprezentací symetrických grup.
Nejprve připomeneme základy teorie reprezentací a uvedeme obě varianty Diffieho-Hellmanova protokolu. Dále rozebereme celý útok krok po kroku a doplníme některé kroky o příklady. Později prozkoumáme bezpečnost modifikovaného protokolu proti známému útoku baby-step giant-step.

Klíčová slova: kryptografie s veřejným klíčem, reprezentace symetrických grup, Diffieho-Hellmanův protokol

Title: Diffie and Hellman are exchanging matrices over group rings

Author: Romana Linkeová

Department: Department of Algebra

Supervisor: Mgr. Pavel Příhoda, Ph.D., Department of Algebra

Abstract: The Diffie-Hellman key exchange protocol is not suitable for devices with limited computational power while computing over group $\mathbb{Z}_p^*$ (where p is at least a 300-digit number). This fact led to the research of other algebraic structures, which may help in reducing the computational and storage cost of the protocol. D. Kahrobaei et al. posted in 2013 a proposal for working over a structure of small matrices and claimed that this modification will not affect the security of the protocol. We will attempt to attack this modification of the Diffie-Hellman protocol with the help of the theory of symmetric group representations. Firstly, we mention the basics of the theory of representations together with both the classical and the modified Diffie-Hellman protocol. Next, we elaborate the attack step by step and complement some of the steps with examples. Then, we probed security of the modified protocol against the baby-step giant-step attack.

Keywords: public key cryptography, symmetric group representations, Diffie-Hellman protocol

Obsah

Úvod

Jedním z požadavků symetrické kryptografie je, aby se dvě komunikující strany dohodly na sdíleném tajném klíči přes otevřený kanál bez toho, aniž by kdokoliv jiný mohl tento klíč z jejich komunikace zjistit. Jedním z kryptografických aparátů, který tento problém řeší, je Diffieho-Hellmanův protokol, který v roce 1976 představili Whitfield Diffie a Martin Hellman v [1].
Tento protokol, který ve své klasické podobě pracuje v grupě $\mathbb{Z}_p^*$, řeší problém s dohodou na tajném sdíleném klíči přes otevřený kanál. Nesplňuje však jiný z požadavků symetrické kryptografie, jako je například autentizace obou stran. Tento fakt vede ke snadnému prolomení protokolu pomocí známého útoku Man in the middle.
Jako další z nevýhod se považuje vysoká paměťová a výpočetní náročnost tohoto protokolu v případě, kdy pracuje s doporučenou délkou parametru p, kterou je 300 cifer. Snaha o vyřešení tohoto problému směřovala především k záměně grupy $\mathbb{Z}_p^*$ s jinou algebraickou strukturou.
To vedlo D. Kahrobaei a spol. k tomu, aby v [2] pracovali nad pologrupou $M_3(\mathbb{Z}_7[\boldsymbol{S}_5])$. Otázkou však je, zda se touto změnou nesníží bezpečnost daného protokolu. Odpovědí na tuto otázku se zabývali například A. Myasnikov a A. Ushakov v [3], kde publikovali útok, který však k výpočtům využívá kvantového počítače a M. Banin a B. Tsaban v [4]. My se v této práci pokusíme pomocí teorie reprezentací ukázat, že bezpečnost protokolu narušena bude. Velice podobný postup pro napadení takto modifikovaného Diffieho-Hellmanova protokolu je možno nalézt v preprintu [5], který se objevil až v dubnu tohoto roku.
V první kapitole této práce zavedeme potřebné věty a definice. V této části budeme vycházet především z [6] a [7]. Druhou kapitolu věnujeme popisu Diffieho-Hellmanova protokolu v jeho klasické a modifikované verzi a ve třetí kapitole popíšeme samotný útok. V další kapitole se zaměříme na bezpečnost modifikovaného protokolu proti útoků baby-step giant-step. Součástí práce je také implementace útoku, o které se stručně zmíníme v poslední kapitole.

Kapitola 1

Značení a definice

V této práci předpokládáme znalost základních pojmů z algebry (*grupa, permutace, Eukleidův algoritmus, charakteristický polynom, vlastní číslo* apod.) a kryptografie (*veřejný* a *soukromý klíč, otevřený kanál* apod.). Definice těchto pojmů, na jejichž základě budeme níže definovat některé struktury, se kterými budeme pracovat, je možné nalézt v [8] a [9].

1.1 Algebraické definice

Definice 1 (Grupový okruh)**.** *Mějme konečnou grupu* $\boldsymbol{G} = (G, *, ^{-1}, e)$ *a okruh s jednotkou* $\boldsymbol{R} = (R, +, \cdot, -, 0_R, 1_R)$*. Pak* grupovým okruhem $\boldsymbol{R}[\boldsymbol{G}]$ *rozumíme množinu všech formálních sum*

$$\sum_{g \in G} r_g g,$$

kde $r_g \in R$*.*

Pro $u = \sum_{g \in G} a_g g$*,* $v = \sum_{h \in G} b_h h$*,* $u, v \in \boldsymbol{R}[\boldsymbol{G}], a_g, b_h \in R$ *definujeme součet* $u \oplus v$ *a součin* $u \otimes v$ *následovně:*

$$u \oplus v = \sum_{q \in G} (a_q + b_q) q,$$

$$u \otimes v = \sum_{q \in G} \left(\sum_{gh = q} a_g b_h \right) q.$$

Poznámka 1 (Značení)*.*

- $\mathbb{Z}_n$ = množina celých čísel s operacemi modulo n.
- $\boldsymbol{S}_m$ = symetrická grupa m prvkových permutací.
- $\boldsymbol{GL}(n, \boldsymbol{T})$ = grupa čtvercových matic M stupně n nad tělesem $\boldsymbol{T}$ takových, že $\det(M) \neq 0$.
- $\langle v \rangle$ lineární obal vektoru v.
- $\mathrm{ord}(a)$ = řád prvku a v grupě $\boldsymbol{G}$.
- $M_n(\boldsymbol{T})$ = T-algebra čtvercových matic stupně n nad tělesem $\boldsymbol{T}$.
- $M_{m,n}(\boldsymbol{T})$ = prostor matic typu $m \times n$ nad tělesem $\boldsymbol{T}$.
- $\mathbb{F}_p$ = konečné těleso s p prvky.

Příklad 1. Pro a,$b \in \mathbb{Z}_7[\boldsymbol{S}_5]$, $a = 3(1,2,3) + 6(1,2)$, $b = 4(2,3,4) + (1,2)$, bude

$a \oplus b = 3(1,2,3) + 7(1,2) + 4(2,3,4) = 3(1,2,3) + 4(2,3,4)$,
$a \otimes b = 12(1,2,3) \circ (2,3,4) + 3(1,2,3) \circ (1,2) + 24(1,2) \circ (2,3,4) + 6(1,2) \circ (1,2) =$
$5(1,2)(3,4) + 3(1,3) + 3(2,3,4,1) + 6e$.

Věta 1. *Grupu $\boldsymbol{S}_n$ můžeme nagenerovat pomocí permutací* (1,2) *a* (1,2,...,n), *tedy $\boldsymbol{S}_n = \langle (1,2), (1,2,\ldots,n) \rangle$. (Důkaz viz [10, Věta 9.21]).*

Tvrzení 2. *Platí, že $M_m(M_n(\boldsymbol{T})) \simeq M_{mn}(\boldsymbol{T})$.*

Důkaz. (Náznak)
Hledáme isomorfismus T-algeber $\varphi : M_m(M_n(\boldsymbol{T})) \to M_{mn}(\boldsymbol{T})$.
Označme prvky matice $A \in M_m(M_n(\boldsymbol{T}))$

$$A = \begin{pmatrix} \begin{pmatrix} a_{11}^{11} & \ldots & a_{1n}^{11} \\ \vdots & \ddots & \vdots \\ a_{n1}^{11} & \ldots & a_{nn}^{11} \end{pmatrix} & \ldots & \begin{pmatrix} a_{11}^{1m} & \ldots & a_{1n}^{1m} \\ \vdots & \ddots & \vdots \\ a_{n1}^{1m} & \ldots & a_{nn}^{1m} \end{pmatrix} \\ \vdots & \ddots & \vdots \\ \begin{pmatrix} a_{11}^{m1} & \ldots & a_{1n}^{m1} \\ \vdots & \ddots & \vdots \\ a_{n1}^{m1} & \ldots & a_{nn}^{m1} \end{pmatrix} & \ldots & \begin{pmatrix} a_{11}^{mm} & \ldots & a_{1n}^{mm} \\ \vdots & \ddots & \vdots \\ a_{n1}^{mm} & \ldots & a_{nn}^{mm} \end{pmatrix} \end{pmatrix}.$$

Pak izomorfismus φ bude:

$$\varphi(A) = \begin{pmatrix} b_{1,1} & \ldots & b_{1,mn} \\ \vdots & \ddots & \vdots \\ b_{mn,1} & \ldots & b_{mn,mn} \end{pmatrix}$$

$$\varphi : a_{ij}^{kl} \longmapsto b_{i+(k-1)n,j+(l-1)n},$$

pro $i,j \in \{1,\ldots,n\}, k,l \in \{1,\ldots,m\}$.

❑

Definice 2 (Akce grupy na množině)**.** *Nechť $\boldsymbol{G}$ je grupa a X je neprázdná množina. Grupový homomorfismus $\varphi : \boldsymbol{G} \to \boldsymbol{S}_X$, kde $\boldsymbol{S}_X$ je symetrická grupa nazveme* akcí grupy $\boldsymbol{G}$ *na množině X.*

Poznámka 2. Akci grupy $\boldsymbol{G}$ na množině X můžeme také chápat jako přiřazení

$$* : G \times X \to X,$$

které splňuje následující podmínky:

1. $1_G * x = x, \forall x \in X$;
2. $(g_1 g_2) * x = g_1 * (g_2 * x), \forall g_1, g_2 \in G, \forall x \in X$

Viz [11, Věta 3.18].

Definice 3 (Perioda matice)**.** Periodou *matice M nazveme nejmenší $k \in \mathbb{N}$ takové, že $M^i = M^{i+k}$, pro nějaké $i \in \mathbb{N}$. Značíme per(M).*

Definice 4 (Předperioda matice)**.** *Nejmenší $i_0 \in \mathbb{N}$ takové, že existuje $k \in \mathbb{N}$ a pro všechna $i \geq i_0$ a matici M platí, že $M^{k+i} = M^i$, nazveme* předperiodou *matice M. Značíme p-per(M).*

Věta 3 (Věta o Jordanově kanonickém tvaru)**.** *Je-li $f : \boldsymbol{V} \to \boldsymbol{V}$ lineární operátor na vektorovém prostoru $\boldsymbol{V}$ dimenze n nad tělesem $\boldsymbol{T}$, jehož charakteristický polynom se rozkládá na součin lineárních činitelů nad tělesem $\boldsymbol{T}$, pak existuje báze $B = (u_1, \ldots, u_n)$ ve $\boldsymbol{V}$, která se skládá z Jordanových řetízků viz ([12, Definice 9.57]), tj matice $[f]_B^B$ operátoru f vzhledem k bázi B je blokově diagonální matice*

$$\begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_s \end{pmatrix},$$

kde každý diagonální blok $J_1, \ldots, J_n$ se rovná nějaké Jordanově buňce viz ([12, Definice 9.57]).

Věta 4. *Buď $f : \boldsymbol{V} \to \boldsymbol{V}$ lineární operátor na konečně generovaném vektorovém prostoru $\boldsymbol{V}$ nad tělesem $\boldsymbol{T}$. Pak jsou následující dvě tvrzení ekvivalentní:*

1. *operátor f je diagonalizovatelný;*
2. *charakteristický polynom $p(\lambda)$ operátoru f se rozkládá na součin lineárních činitelů a algebraická násobnost každého vlastního čísla operátoru f se rovná jeho geometrické násobnosti.*

Tvrzení 5. *Geometrická násobnost vlastního čísla λ je rovna počtu Jordanových buněk s prvkem λ na diagonále a jeho algebraická násobnost je rovna součtu stupňů Jordanových buněk s prvkem λ na diagonále.*

1.2 Definice z teorie reprezentací

Definice 5 (Reprezentace)**.** Reprezentací *grupy $\boldsymbol{G}$ stupně n rozumíme homomorfismus $\varphi : \boldsymbol{G} \to \boldsymbol{GL}(n,\boldsymbol{T})$ a značíme $\varphi(g) = \varphi_g$, pro $g \in \boldsymbol{G}$.*

Definice 6 (Ekvivalentní reprezentace)**.** *Řekneme, že dvě reprezentace $\varphi : \boldsymbol{G} \to \boldsymbol{GL}(n, \boldsymbol{T})$ a $\psi : \boldsymbol{G} \to \boldsymbol{GL}(m, \boldsymbol{T})$ jsou* ekvivalentní*, pokud $m = n$ a pokud existuje matice $F \in \boldsymbol{GL}(n, \boldsymbol{T})$ taková, že $\psi_g = F\varphi_g F^{-1}$, $\forall g \in \boldsymbol{G}$.*

Definice 7 (φ-invariantní podprostor)**.** *Nechť $\varphi : \boldsymbol{G} \to \boldsymbol{GL}(n, \boldsymbol{T})$ je reprezentace. Pak podprostor $\boldsymbol{S} \leq \boldsymbol{T}^n$ je* φ-invariantní*, jestliže $\varphi_g s \in S$, $\forall g \in G$,$s \in S$.*

Definice 8 (Ireducibilní reprezentace)**.** *Řekneme, že reprezentace $\varphi : \boldsymbol{G} \to \boldsymbol{GL}(n, \boldsymbol{T})$ je* ireducibilní*, právě tehdy když φ-invariantní podprostory $\boldsymbol{T}^n$ jsou právě $\{0\}$ a $\boldsymbol{T}^n$.*

Definice 9 (Rozklad čísla n)**.** *Něchť $n \in \mathbb{N}$, pak* rozklad čísla n *definujeme jako nerostoucí posloupnost m kladných celých čísel $\lambda = (\lambda_1, \ldots, \lambda_m)$ takovou, že $\lambda_1 + \ldots + \lambda_m = n$ a značíme $\lambda \vdash n$.*

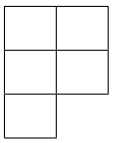
Příklad 2.

- (2,2,1) je rozklad čísla 5;

- (2,1,2) není rozklad čísla 5 (prvky netvoří nerostoucí posloupnost).

Definice 10 (Youngův diagram)**.** *Nechť $\lambda = (\lambda_1, \ldots, \lambda_m)$, $\lambda \vdash n$, pak* Youngovým diagramem *posloupnosti λ rozumíme n čtverců v m řádcích, kde každý i-tý řádek má λ_i čtverců.*

Příklad 3. Pro $\lambda = (2,2,1)$, $\lambda \vdash 5$, bude



Youngův diagram posloupnosti λ.

Definice 11 (Youngovo tableau)**.** *Nechť $\lambda \vdash n$, pak* Youngovo tableau *tvaru λ je pole t získané vyplněním čtverců Youngova diagramu posloupnosti λ čísly $1, \ldots, n$.*

Příklad 4. Nechť $\lambda = (2,2,1)$, pak

$$\begin{array}{|c|c|}\hline 3 & 4 \\ \hline 2 & 1 \\ \hline 5 \\ \cline{1-1}\end{array}, \qquad \begin{array}{|c|c|}\hline 5 & 3 \\ \hline 4 & 1 \\ \hline 2 \\ \cline{1-1}\end{array}$$

jsou Youngova tableaux tvaru λ.

Definice 12 (Tabloid)**.** *Řekneme, že dvě tableaux T_1, T_2 jsou ekvivalentí, jestliže mají stejné řádky až na permutaci a značíme $T_1 \sim T_2$. Třídu této ekvivalence nazveme* tabloidem.

Poznámka 3.
- Předešlá definice vyžaduje ověření, že $\sim$ je ekvivalence, což je snadné.
- Zřejmě mohou být dvě tableaux ekvivalentní pouze tehdy, pokud mají totožný Youngův diagram.

Příklad 5.

- Uvažujme grupu $\boldsymbol{S}_3$ a $\lambda = (2,1)$, $\lambda \vdash 3$. Pak pro Youngův diagram tvaru λ máme

$$\begin{array}{|c|c|}\hline 3 & 2 \\ \hline 1 \\ \cline{1-1}\end{array} \sim \begin{array}{|c|c|}\hline 2 & 3 \\ \hline 1 \\ \cline{1-1}\end{array}.$$

- Pro grupu $\boldsymbol{S}_5$ a $\lambda = (2,2,1)$, $\lambda \vdash 5$ bude

$$\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 4 \\ \hline 5 \\ \cline{1-1}\end{array} \sim \begin{array}{|c|c|}\hline 2 & 1 \\ \hline 3 & 4 \\ \hline 2 \\ \cline{1-1}\end{array} \sim \begin{array}{|c|c|}\hline 2 & 1 \\ \hline 4 & 3 \\ \hline 2 \\ \cline{1-1}\end{array} \sim \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 4 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}.$$

Definice 13 (Akce permutace na tableau)**.** *Mějme permutaci $\pi \in \boldsymbol{S}_n$ a tableau t tvaru λ, kde $\lambda \vdash n$. Označme $t(a)$ hodnotu tableau t v čtverci a. Pak $\pi * t$ je tableau $\tilde{t}$ tvaru λ, pro které platí*

$$\tilde{t}(a) = \pi(t(a)),$$

pro každý čtverec a tableau $\tilde{t}$.

Poznámka 4. Označme $X^\lambda = \{\text{tableau } t \text{ tvaru } \lambda\}$. Pak $*$ je zobrazení $\boldsymbol{S}_n \times X^\lambda \to X^\lambda$, které splňuje požadavky akce grupy $\boldsymbol{S}_n$ na množině X^λ.

Příklad 6. Permutace $\pi = (1,2) \in \boldsymbol{S}_3$ působí na tableau t

3	2
1	

takto:

$$\pi * t = \begin{array}{|c|c|}\hline \pi(3) & \pi(2) \\ \hline \pi(1) \\ \cline{1-1} \end{array} = \begin{array}{|c|c|}\hline 3 & 1 \\ \hline 2 \\ \cline{1-1} \end{array}.$$

Definice 14 (Akce permutace na tabloidu)**.** *Mějme permutaci $\pi \in \boldsymbol{S}_n$ a tabloid $\bar{t}$ tvaru λ, kde $\lambda \vdash n$. Označme t reprezentant tabloidu $\bar{t}$. Pak akce $\pi * \bar{t}$ je*

$$\pi * \bar{t} = [\pi * t]_\sim.$$

Poznámka 5. Poznamenejme, že akce permutace na tabloidu je korektně definovaná. Tedy pro dvě tableaux t_1, t_2 taková, že $t_1 \sim t_2$ a permutaci $\pi \in \boldsymbol{S}_n$ platí, že $\pi * t_1 \sim \pi * t_2$.

Příklad 7. Permutace $\pi = (1,2) \in \boldsymbol{S}_3$ působí na tabloid $\bar{t}$

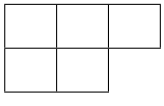
$$\left[\begin{array}{|c|c|}\hline 3 & 2 \\ \hline 1 \\ \cline{1-1} \end{array}\right]_\sim$$

takto:

$$\pi * \bar{t} = \left[\begin{array}{|c|c|}\hline \pi(3) & \pi(2) \\ \hline \pi(1) \\ \cline{1-1} \end{array}\right]_\sim = \left[\begin{array}{|c|c|}\hline 3 & 1 \\ \hline 2 \\ \cline{1-1} \end{array}\right]_\sim.$$

Definice 15 (Standardní tableau)**.** *Tableau, ve kterém tvoří čísla v řádcích i sloupcích rostoucí posloupnost nazveme* standardní tableau.

Příklad 8. Pro Youngův diagram tvaru



budou všechna standardní tableaux

$$\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4&5\\\cline{1-2}\end{array},\quad \begin{array}{|c|c|c|}\hline 1&2&4\\\hline 3&5\\\cline{1-2}\end{array},\quad \begin{array}{|c|c|c|}\hline 1&2&5\\\hline 3&4\\\cline{1-2}\end{array},\quad \begin{array}{|c|c|c|}\hline 1&3&4\\\hline 2&5\\\cline{1-2}\end{array},\quad \begin{array}{|c|c|c|}\hline 1&3&5\\\hline 2&4\\\cline{1-2}\end{array}.$$

Definice 16. *Nechť $\lambda \vdash n$. Pak pro tableau t tvaru λ označíme*

$$C_t = \{\pi \in \boldsymbol{S}_n : \forall i \in \{1, \ldots, n\}, i \text{ a } \pi(i) \text{ jsou ve stejném sloupci } t\}.$$

Definice 17 (Polytabloid)**.** *Nechť $\lambda \vdash n$. Označme T_a^λ množinu tabloidů tvaru λ a $\boldsymbol{V}^\lambda$ vektorový prostor nad tělesem $\boldsymbol{T}$ s bází T_a^λ. Pak pro λ-tableau t definujeme $P_t \in \boldsymbol{V}^\lambda$*

$$P_t = \sum_{\pi \in C_t} zn(\pi)\pi * [t]_\sim$$

polytabloid asociovaný s tableau t.

Příklad 9. Pro tableau

$$\begin{array}{|c|c|}\hline a&b\\\hline c\\\cline{1-1}\end{array}$$

budeme jemu příslušnou třídu ekvivalence $\sim$ značit $\tilde{c}$. Pak pro tableau

$$\begin{array}{|c|c|}\hline 1&2\\\hline 3\\\cline{1-1}\end{array}$$

bude polytabloid P vypadat následovně:

$$P = \tilde{3} + \mathrm{zn}(1{,}3) \cdot \tilde{1} = \tilde{3} - \tilde{1}.$$

Poznámka 6. Podprostor prostoru $\boldsymbol{V}^\lambda$ generovaný všemi polytabloidy asociovanými s tableau λ označíme S^λ.

Tvrzení 6. *Podprostor S^λ má bázi $\{P_t : t$ je standardní tableau tvaru $\lambda\}$ (viz [7, Věta 8.5]).*

Poznámka 7. Označme

$$\sigma^\lambda : \boldsymbol{S}_n \to \boldsymbol{Aut_T}(\boldsymbol{V}^\lambda),$$

pro které platí

$$\sigma_\pi^\lambda[t] = \pi * [t],$$

pro každý tabloid $[t] \in T_a^\lambda$.
Pak S^λ je σ-invariantní, tj. $\sigma_\pi^\lambda(v) \in S^\lambda$, $\forall \pi \in \boldsymbol{S}_n, \forall v \in S^\lambda$.
Dále označme

$$\tilde{\sigma}^\lambda : \boldsymbol{S}_n \to \boldsymbol{Aut_T}(S^\lambda)$$

takové, že

$$\tilde{\sigma}_\pi^\lambda = \sigma_\pi^\lambda|_{S^\lambda}.$$

Definice 18 (Spechtova reprezentace)**.** *Nechť* $\lambda \vdash n$*,*

$$B = \{P_t : t \text{ standardní tableau tvaru } \lambda\}$$

je báze S^λ*. Pak*

$$\varphi^\lambda : \boldsymbol{S}_n \to \boldsymbol{GL}(d, \boldsymbol{T}),$$

$d = |B|$*, takové, že*

$$\varphi^\lambda_\pi = [\tilde{\sigma}^\lambda_\pi]_B,$$

kde $[\tilde{\sigma}^\lambda_\pi]_B$ *je matice automorfismu* $\tilde{\sigma}^\lambda_\pi$ *vzhledem k bázi* B*, nazveme* Spechtovou reprezentací*.*

S výše zavedeným označením a dle [7, Věta 11.5] dostáváme následující tvrzení.

Tvrzení 7. *Pro těleso* $\boldsymbol{T}$ *charakteristiky 0 nebo* p*, kde* p *je prvočíslo a* $p > n$ *platí následující:*

- φ^λ *je ireducibilní reprezentace pro všechna* $\lambda \vdash n$*;*
- $\lambda \neq \eta$*,* $\lambda, \eta \vdash n$*, pak* φ^λ *a* φ^η *nejsou ekvivalentní;*
- *každá ireducibilní reprezentace* $\boldsymbol{S}_n$ *nad* $\boldsymbol{T}$ *je ekvivalentní některé reprezentaci* φ^λ*.*

1.3 Definice z teorie konečných těles

Definice 19 (Rozšíření tělesa)**.** *Nechť* $\boldsymbol{T}, \boldsymbol{S}$ *jsou tělesa a* $\boldsymbol{T} \leq \boldsymbol{S}$*. Řekneme, že* $\boldsymbol{S}$ *je* rozšířením tělesa $\boldsymbol{T}$*. Jsou-li* $a_1, \ldots, a_n \in S$*, potom nejmenší podtěleso tělesa* $\boldsymbol{S}$*, které obsahuje* $\boldsymbol{T} \cup \{a_1, \ldots, a_n\}$ *značíme* $\boldsymbol{T}(a_1, \ldots, a_n)$*.*

Věta 8. *Nechť* $f(x) \in \boldsymbol{F}[x]$ *je stupně* $n > 1$ *ireducibilní na* $\boldsymbol{F}$*. Pak množina* E *všech polynomů z* $\boldsymbol{F}[x]$ *stupně menšího než* n *se sčítáním a násobením modulo* $f(x)$ *je těleso. Těleso* $\boldsymbol{E}$ *je izomorfní a budeme jej ztotožňovat s* $\boldsymbol{F}[x]/(f(x))$*.*

Definice 20 (Kořenové rozšíření)**.** *Nechť* $\boldsymbol{K}$ *je těleso a* $f(x) \in \boldsymbol{K}[x]$ *je ireducibilní polynom. Těleso* $\boldsymbol{E}$ *se pak nazývá* kořenové rozšíření *tělesa* $\boldsymbol{K}$ *určené polynomem* $f(x)$*, jestliže*

- $\boldsymbol{K} \leq \boldsymbol{E}$*,*
- $f(x)$ *má v* $\boldsymbol{E}$ *nějaký kořen* θ*,*
- $\boldsymbol{K}(\theta) = \boldsymbol{E}$*.*

Definice 21 (Rozkladové rozšíření)**.** *Nechť* $\boldsymbol{K}$ *je těleso,* $f(x) \in \boldsymbol{K}[x]$*. Rozšíření* $\boldsymbol{K} \leq \boldsymbol{E}$ *se nazývá* rozkladové rozšíření *tělesa* $\boldsymbol{K}$ *určené polynomem* $f(x)$*, pokud*

- *polynom* $f(x)$ *se v* $\boldsymbol{E}$ *rozkládá na součin lineárních činitelů, tj.* $\exists \theta_1, \ldots, \theta_m \in E$*,* $t \in K$ *takové, že* $f(x) = t(x - \theta_1) \ldots (x - \theta_m)$*.*
- $\boldsymbol{K}(\theta_1, \ldots, \theta_m) = \boldsymbol{E}$*.*

Věta 9. *Nechť $f(x)$ je ireducibilní polynom nad $\mathbb{F}_q$ stupně m. Potom má $f(x)$ v $\mathbb{F}_{q^m}$ nějaký kořen α, prvky $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ jsou navzájem různé a tvoří množinu všech kořenů polynomu f.*

Důsledek. Kořenové rozšíření konečného tělesa $\boldsymbol{F}$ určeného ireducibilním polynomem $f(x)$ je již rozkladovým rozšířením tělesa $\boldsymbol{F}$ určeným polynom $f(x)$. Speciálně $\boldsymbol{F}_{q^m}$ je rozkladové rozšíření $\boldsymbol{F}_q$ určené libovolným ireducibilním polynomem $f \in \boldsymbol{F}_q[x]$ stupně m.

Definice 22 (Konjugované prvky)**.** *Buď $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ konečná tělesa, $\alpha \in \mathbb{F}_{q^n}$. Pak se prvky $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ nazývají* konjugované *k α nad $\mathbb{F}_q$.*

Kapitola 2

Diffieho–Hellmanův protokol

V této kapitole připomeneme klasický Diffieho-Hellmanův protokol a představíme jeho modifikaci, kterou uvedl D. Kahrobaei a spol. v [2]. Společně s tím zmíníme problém diskrétního logaritmu, který s Diffieho-Hellmanovým protokolem úzce souvisí. Ke konci této kapitoly se zaměříme na požadavky na vstupní data pro modifikovaný protokol.

2.1 Diskrétní logaritmus

Mějme konečnou cyklickou grupu $\boldsymbol{G} = \langle a \rangle$ řádu n. Pak pro každý prvek $b \in G$ existuje právě jedno $x \in \{0, \ldots, n-1\}$ takové, že $b = a^x$. Číslo x nazýváme *diskrétní logaritmus* prvku b o základu a v grupě $\boldsymbol{G}$ a značíme $\mathrm{Dlog}_a(b)$.
Úloha, kdy se pro $\boldsymbol{G}$, a, b hledá takové x, nazveme *problém diskrétního logaritmu*.

2.2 Klasický Diffieho-Hellmanův protokol

Požadavek na vytvoření tajné sdílené informace mezi dvěma stranami při komunikaci přes otevřený kanál dal roku 1976 za vznik Diffieho-Hellmanovu protokolu. Tento protokol popisuje výměnu informací mezi stranami A a B, která i přes to, že může být kýmkoliv odposlechnuta (například osobou E), vede k dohodě na tajném klíči, který znají pouze osoby A a B.

Protokol probíhá následovně:

Algoritmus 1: Diffieho-Hellmanův protokol

Vstup: cyklická grupa $\boldsymbol{G} = (G, \cdot, ^{-1}, 1)$, generátor g grupy $\boldsymbol{G}$
Výstup: sdílený tajný klíč g^{ab}

A:	**B:**
zvolí vhodné tajné číslo $a \in (0, \lvert G \rvert)$	zvolí vhodné tajné číslo $b \in (0, \lvert G \rvert)$
spočte $u = g^a$	spočte $v = g^b$
pošle u osobě B	pošle v osobě A
spočte $v^a = g^{ab}$	spočte $u^b = g^{ab}$

Poznámka 8. Jak A, tak B používají při počítání g^a, g^b, g^{ab} tzv. *binární mocnění.* Popis tohoto algoritmu je možno nalézt jako [13, Algoritmus 7].

Při snaze protivníka odhalit tajný klíč g^{ab}, se znalostí g, g^a a g^b, osoba E řeší problém, který se nazývá *Diffieho-Hellmanův problém.*

Jedno z původních použití Diffieho-Hellmanova protokolu je pro grupu $\boldsymbol{G} = \mathbb{Z}_p^*$, p prvočíslo, g generátor grupy $\boldsymbol{G}$. Volba této grupy je výhodná, protože v ní umíme rychle spočítat mocninu, ale není znám žádný rychlý postup na výpočet diskrétního logaritmu. V dnešní době se tento protokol bere jako bezpečný, pokud se p volí alespoň o 300 cifrách a a a b alespoň o 100 cifrách. Tyto velikosti parametrů však nedovolují efektivní použití Diffie-Hellmanova protokolu pro stroje s nižší výpočetní silou. Tento fakt vedl D. Kahrobaei a spol. k návrhu protokolu, který pracuje nad strukturou malých matic s operací násobení matic, ve které je počítání velice rychlé a efektivní a protokol potom tudíž není tak výpočetně náročný.

2.3 Modifikovaný Diffieho-Hellmanův protokol

Jak již bylo zmíněno, modifikace původního protokolu je především v tom, že se nepočítá nad celými čísly, ale nad strkturou malých matic. Konkrétně se jedná o pologrupu matic nad grupovým okruhem $\mathbb{Z}_n[\boldsymbol{S}_m]$, kde $\mathbb{Z}_n$ je množina celých čísel s operacemi modulo n a $\boldsymbol{S}_m$ je symetrická grupa řádu $m!$. Parametry, navrženy v [2], jsou matice stupně 2 nebo 3 nad $\mathbb{Z}_7[\boldsymbol{S}_5]$.

Hlavní výhoda této struktury spočívá ve skutečnosti, že násobení matic je díky možnosti předpočítání multiplikativní tabulky pro prvky grupy $\boldsymbol{S}_5$ velice efektivní. Násobení dvou prvků ze $\mathbb{Z}_7[\boldsymbol{S}_5]$ tak obnáší pouze násobení prvků ze $\mathbb{Z}_7$ a zaindexování do multiplikativní tabulky.

Samotný protokol probíhá následovně:

Algoritmus 2: Modifikovaný Diffieho-Hellmanův protokol

Vstup: pologrupa $M_3(\mathbb{Z}_7[\boldsymbol{S}_5])$, M vhodně zvolená z $M_3(\mathbb{Z}_7[\boldsymbol{S}_5])$
Výstup: sdílený tajný klíč M^{ab}

A:	**B:**
zvolí tajné číslo $a \in \mathbb{N}$	zvolí tajné číslo $b \in \mathbb{N}$
spočte M^a	spočte M^b
pošle M^a osobě B	pošle M^b osobě A
spočte $(M^a)^b = M^{ab}$	spočte $(M^a)^b = M^{ab}$

Příklad 10. Ukážeme, jak může vypadat multiplikativní tabulka pro grupu $\boldsymbol{S}_3$. V tomto příkladě rozumíme výrazem (1,2,3) permutaci

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Pak pro

1	2	3	4	5	6
(1,2,3)	(1,3,2)	(2,1,3)	(2,3,1)	(3,1,2)	(3,2,1)

očíslování prvků grupy $\boldsymbol{S}_3$, bude

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	5	6	3	4
3	3	4	1	2	6	5
4	4	3	6	5	1	2
5	5	6	2	1	4	3
6	6	5	4	3	2	1

multiplikativní tabulka grupy $\boldsymbol{S}_3$.

2.3.1 Požadavky na vstupní matici M

Je zřejmé, že chceme, aby matice M měla dostatečnou velikost periody ($> 10^{10}$), jinak by bylo při hledání tajného exponentu a možné protokol prolomit pouhým vyzkoušením všech možností.Toho, aby matice M měla dostatečně velkou periodu, lze dosáhnout následujícím postupem, který byl představen v [2].

Matice $M = M_1 \cdot S$, kde M_1 je libovolná invertibilní matice z $M_3(\mathbb{Z}_7[\boldsymbol{S}_5])$ a S je skalární matice, která má nuly všude kromě prvků na diagonále, přičemž každý prvek na diagonále je $s = (3 + g_1)(3 + g_2)(3 + g_3)(3 + g_4)(3 + g_5)(3 + g_6)(5 + h)$. Prvky $g_i \in \boldsymbol{S}_5$ a každý z nich generuje jinou podgrupu grupy $\boldsymbol{S}_5$ řádu 5 a prvek h je součin nezávislých cyklů délky 2 a 3.

Příklad 11. Pro ilustraci ukážeme, jak vypadají prvky g_i, $i \in \{1, \ldots, 6\}$ a prvek h pro grupový okruh $\mathbb{Z}_7[\boldsymbol{S}_5]$ a jak může vypadat matice M_1.

$$
\begin{aligned}
g_1 &= (1,2,3,4,5),\\
g_2 &= (1,2,4,5,3),\\
g_3 &= (1,2,5,3,4),\\
g_4 &= (1,2,3,5,4),\\
g_5 &= (1,2,4,3,5),\\
g_6 &= (1,2,5,4,3),\\
h &= (1,2)(3,4,5),
\end{aligned}
$$

$$
M_1 = \begin{pmatrix}
(1,\,2,\,4,\,3,\,5) & (1,\,4,\,3,\,2) & 4(1,\,4,\,3,\,5)\\
3(1,\,5,\,3)(2,\,4) & 6(1,\,2,\,4) & 3(1,\,2,\,3)(4,\,5)\\
(1,\,5,\,2) & 6(1,\,4,\,3,\,5) & 6(1,\,5)(2,\,4,\,3)
\end{pmatrix}.
$$

Kapitola 3

Útok

Víme již, že k prolomení Diffieho-Hellmanova protokolu stačí umět řešit problém diskrétního logaritmu, pro který není známo polynomiální řešení při vhodně zvolené cyklické grupě.
Diffieho-Hellmanův problém bude pro pologrupu $M_3(\mathbb{Z}_7[\boldsymbol{S}_5])$, matici $M \in M_3(\mathbb{Z}_7[\boldsymbol{S}_5])$,

$$\langle M \rangle = \{M^1, M^2, \ldots, M^u\},$$

kde u = p-per(M) + per$(M)-1$ a $N \in \langle M \rangle$ vypadat tak, že hledáme $a \in \mathbb{N}$ takové, že $M^a = N$.
Idea útoku, který v této kapitole podrobně probereme, je založena na tom, že místo toho, abychom pro nalezení tajného exponentu a počítali diskrétní logaritmus v pologrupě velkého řádu (pologrupa $M_3(\mathbb{Z}_7[\boldsymbol{S}_5])$ má řád přibližně 10^{913}), využijeme teorie reprezentací, díky níž umíme nalézt izomorfní zobrazení matic M a N jako sedmice matic $(M_1, \ldots, M_7)$, $(N_1, \ldots, N_7)$ kde $M_i, N_i \in M_{d_i}(\mathbb{Z}_7)$, $d_i \in \{1, \ldots, 18\}, i \in \{1, \ldots, 7\}$. Pro každou z těchto matic pak zjistíme pomocí počítání diskrétních logaritmů v grupách mnohem menších řádů (bude upřesněno v 3.4) čísla $a_i, i \in \{1, \ldots, 7\}$ taková, že $M_i^{a_i} = N_i$. Z těchto čísel a_i pak umíme zkonstruovat číslo a' (viz 13), které bude rovno zbytku po dělení tajného exponentu a periodou matice M. Dostaneme tedy množinu

$$A = \{a' + k \cdot \text{per}(M) : k \in \mathbb{N}\},$$

pro kterou bude platit $M^x = N, \forall x \in A$.
V první řadě představíme samotnou kostru útoku, jejíž každý bod bude následně podrobněji probrán a doplněn jednoduchými příklady pro lepší ilustraci dané situace. Celý útok nejprve ukážeme pro speciální případ, který situaci poměrně zjednodušuje. Postup v obecném případě uvedeme ke konci této kapitoly.

3.1 Kostra útoku

Cílem útoku je pro grupu $\boldsymbol{G} = \boldsymbol{S}_u$, těleso $\boldsymbol{T} = \mathbb{Z}_v$ $(v > u)$, čtercové matice M a M^a stupně m nad $\boldsymbol{TG} = \mathbb{Z}_v[\boldsymbol{S}_u]$, určit a' takové, aby $M^a = M^{a'}$. Se znalostí takového a' a matice M^b vypočítáme tajný klíč jako $(M^b)^{a'} = M^{a'b} = M^{ab}$.
Pro ukázku útoku jsme sestavili matici $M \in M_3(\mathbb{Z}_7[\boldsymbol{S}_5])$ postupem, který je uveden v 2. Tuto matici nebudeme uvádět, ale ve všech příkladech s ní budeme pracovat.

V této kapitole si ukážeme postup pro určení a' a pro větší přehlednost budeme matici M^a značit N.
Mějme tedy grupu $\boldsymbol{G} = \boldsymbol{S}_u$, těleso $\boldsymbol{T} = \mathbb{Z}_v$ a matice M, N jako výše ($N = M^a$) a označme $(\omega_1, \ldots, \omega_r)$ všechny rozklady čísla v. Útok pak probíhá následovně:

1. pro každý rozklad $\omega_i, i \in \{1, \ldots, r\}$ čísla u nalezneme jeho Spechtovu reprezentaci
$$\varphi^{\omega_i} : \boldsymbol{G} \to \boldsymbol{GL}(n_i, \boldsymbol{T}))$$
(viz definice 18);
2. rozšíříme Spechtovy reprezentace φ^{ω_i} na homomorfismy T-algeber
$$\tilde{\varphi}^{\omega_i} : \boldsymbol{TG} \to M_{n_i}(\boldsymbol{T});$$
3. zobrazíme matice M a N pomocí $\psi = (\psi^{\omega_1}, \ldots, \psi^{\omega_r})$,
$$\psi^{\omega_i} : M_m(\boldsymbol{TG}) \to M_{mn_i}(\boldsymbol{T})$$
$$\psi : M \to (M_1, \ldots, M_r)$$
$$\psi : N \to (N_1, \ldots, N_r);$$
4. nalezneme $a_i : M_i^{a_i} = N_i$, $\forall i \in \{1, \ldots, r\}$;
5. pomocí a_i nalezneme a' takové, aby $M^{a'} = N$.

Poznámka 9. Dle [14, Věta 3.9] a [15, Věta 2.1.12] máme společně s konstrukcí popsanou v 1.1 a tvrzení 7 fakt, že zobrazení ψ bude izomorfismus algeber.

3.2 Nalezení reprezentací

V této části budeme pracovat s konkrétní grupou $\boldsymbol{G} = \boldsymbol{S}_5$ a tělesem $\boldsymbol{T} = \mathbb{Z}_7$. Reprezentace φ^{ω_i}, $i \in \{1, \ldots, r\}$ nalezneme tak, že definujeme obraz $\varphi^{\omega_i}(\pi)$ pro každou $\pi \in \boldsymbol{S}_5$. Situaci v tomto kroku můžeme zjednodušit pomocí věty 1.
Konstrukce reprezentací φ^{ω_i}, $i \in \{1, \ldots, r\}$ probíhá dle sekce 1.1 následovně:

1. nalezneme všechny $(\omega_1, \ldots, \omega_r)$ rozklady čísla 5 a jimi určené Youngovy diagramy;
2. pro každý $\omega_i \vdash 5$ uděláme:
   - nalezneme všechna standardní tableaux a jimi určené polytabloidy;
   - nalezneme φ^{ω_i}(1,2) a φ^{ω_i}(1,2,3,4,5), $i \in \{1, \ldots, r\}$;
   - rozšíříme φ^{ω_i} na celé $\boldsymbol{S}_5$, $i \in \{1, \ldots, r\}$.

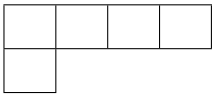
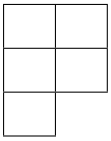
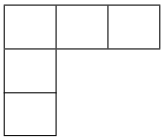
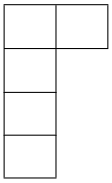
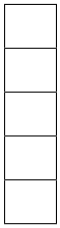
Pro jeden konkrétní Youngův diagram Y^{ω_i} čísla 5 označme $\boldsymbol{T}_a^{\omega_i}$ množinu všech jeho tabloidů. Dále označme $\boldsymbol{V}^{\omega_i}$ vektorový prostor nad tělesem $\mathbb{Z}_7$ s bází

$\boldsymbol{T}_a^{\omega_i}$. Uvážíme-li nyní všechna standardní tableaux daného Youngova diagramu společně s jejich polytabloidy, můžeme označit S^{ω_i} podprostor $\boldsymbol{V}^{\omega_i}$ generovaný těmito polytabloidy stejně jako v poznámce 6.
Víme, že akce grupy $\boldsymbol{S}_5$ na množině $\boldsymbol{T}_a^{\omega_i}$ dává akci $\boldsymbol{S}_5$ na $\boldsymbol{V}^{\omega_i}$, která se dá zúžit na S^{ω_i}. Budeme mít tedy reprezentace (homomorfismy)

$$\varphi^{\omega_i} : \boldsymbol{S}_5 \to \mathbf{Aut}(S^{\omega_i}) \simeq \boldsymbol{GL}(\dim\,(S^{\omega_i}), \mathbb{Z}_7).$$

Rozklady čísla 5, Youngovy diagramy. Každý rozklad čísla 5 bude dle tvrzení 7 určovat jednu z reprezentací φ^{ω_i}. Následující tabulka ilustruje situaci pro grupu $\boldsymbol{S}_5$.

Tabulka 3.1: Rozklady čísla 5

φ^{ω_i}	λ	Youngův diagram	Stupeň reprezentace	Poznámka
1	(5)		1	$\varphi^{\omega_1}(\pi) = 1$
2	(4,1)		4	
3	(3,2)		5	
4	(2,2,1)		5	
5	(3,1,1)		6	
6	(2,1,1,1)		4	
7	(1,1,1,1,1)		1	$\varphi^{\omega_7}(\pi) = \mathrm{zn}(\pi)$

Vidíme tedy, že dle tvrzení 7 dostáváme 7 ireducibilních navzájem neekvivalentních reprezentací.

Poznámka 10. Dále v textu předpokládejme očíslování reprezentací dle tabulky 3.2.

Nalezení standardních tableaux a polytabloidů. V tomto kroku máme pro každé z výše uvedených Youngových diagramů najít všechna standardní tableaux a jimi určené polytabloidy. Pro ilustraci ukážeme, jak bude situace vypadat pro φ^{ω_i}, $i = 2$.
Z příkladu 8 již víme, jak vypadají všechna standardní tableaux. Označme jim příslušné tabloidy takto:

$$\overline{4,5} = \left[\begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 \\ \cline{1-2}\end{array}\right]_{\sim}, \quad \overline{3,5} = \left[\begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline 3 & 5 \\ \cline{1-2}\end{array}\right]_{\sim}, \quad \overline{3,4} = \left[\begin{array}{|c|c|c|}\hline 1 & 2 & 5 \\ \hline 3 & 4 \\ \cline{1-2}\end{array}\right]_{\sim},$$

$$\overline{2,5} = \left[\begin{array}{|c|c|c|}\hline 1 & 3 & 4 \\ \hline 2 & 5 \\ \cline{1-2}\end{array}\right]_{\sim}, \quad \overline{2,4} = \left[\begin{array}{|c|c|c|}\hline 1 & 3 & 5 \\ \hline 2 & 4 \\ \cline{1-2}\end{array}\right]_{\sim}.$$

Uvedomme si, že $\overline{4,5} = \overline{5,4}$, jelikož dvě tableaux jsou ekvivalentní, pokud se jsou jejich řádky stejné až na permutaci prvků.
Pro každý z tabloidů výše vytvoříme polytabloidy postupným permutováním prvků v sloupcích. Dostaneme

$$\begin{aligned} P_{4,5} &= \overline{4,5} - \overline{1,5} - \overline{2,4} + \overline{1,2}, \\ P_{3,5} &= \overline{3,5} - \overline{1,5} - \overline{2,3} + \overline{1,2}, \\ P_{3,4} &= \overline{3,4} - \overline{1,4} - \overline{2,3} + \overline{1,2}, \\ P_{2,5} &= \overline{2,5} - \overline{1,5} - \overline{2,3} + \overline{1,3}, \\ P_{2,4} &= \overline{2,4} - \overline{1,4} - \overline{2,3} + \overline{1,3} \end{aligned}$$

a máme prostor

$$S^{\omega_2} = \langle P_{4,5}, P_{3,5}, P_{3,4}, P_{2,5}, P_{2,4} \rangle.$$

Nalezení $\boldsymbol{\varphi^{\omega_i}(1,2)}$ a $\boldsymbol{\varphi^{\omega_i}(1,\ldots,5)}$. Situaci opět ukážeme pouze pro $i = 2$. Obrazy permutací (1,2) a (1,2,3,4,5) určíme tak, že jimi budeme působit na výše nalezené polytabloidy (viz definice 14 a 17). Toto zobrazení vedoucí z $\boldsymbol{S}_5$ do $\mathbf{Aut}(S^{\omega_i})$ označíme f.
Pro permutaci (1,2) budeme mít:

$$\begin{aligned} (1,2) * P_{4,5} &= \overline{4,5} - \overline{2,5} - \overline{4,1} + \overline{1,2} = P_{4,5} - P_{2,5} + P_{2,4}; \\ (1,2) * P_{3,5} &= \overline{3,5} - \overline{2,5} - \overline{1,3} + \overline{1,2} = P_{3,5} - P_{2,5}; \\ (1,2) * P_{3,4} &= \overline{3,4} - \overline{2,4} - \overline{1,3} + \overline{1,2} = P_{3,4} - P_{2,4}; \\ (1,2) * P_{2,5} &= \overline{1,5} - \overline{2,5} - \overline{1,3} + \overline{2,3} = -P_{2,5}; \\ (1,2) * P_{2,4} &= \overline{1,4} - \overline{2,4} - \overline{1,3} + \overline{2,3} = -P_{2,4}. \end{aligned}$$

Tímto jsme získali obraz působení permutace (1,2) na všech prvcích báze prostoru S^{ω_2}. Abychom získali její obraz pomocí homomorfismu φ^{ω_2}, podíváme se, jak vypadá matice $f((1,2))$ vzhledem k bázi $B = \{P_{4,5}, P_{3,5}, P_{3,4}, P_{2,5}, P_{2,4}\}$ prostoru S^{ω_2} (viz definice 18):

$$\varphi^{\omega_2}((1,2)) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 6 & 6 & 0 & 6 & 0 \\ 1 & 0 & 6 & 0 & 6 \end{pmatrix}.$$

Stejným způsobem, jakým jsme získali $\varphi^{\omega_2}(1,2)$, získáme i $\varphi^{\omega_2}(1,2,3,4,5)$.

Rozšíření φ^{ω_i} na celou grupu $\boldsymbol{S}_5$. Nyní zbývá poslední krok, a to je rozšířit zobrazení φ^{ω_i} na celou grupu $\boldsymbol{S}_5$. K tomu využijeme faktu, že φ^{ω_i} má být homomorfismus a větu 1.
Budeme tedy mít

$$\varphi^{\omega_i}(g \circ h) = \varphi^{\omega_i}(g)\varphi^{\omega_i}(h). \tag{3.1}$$

Dle věty 1 víme, že libovolnou permutaci $\pi \in \boldsymbol{S}_5$ umíme vyjádřit jako složení permutací (1,2) a (1,2,3,4,5). Označme toto složení

$$\pi = \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_l,$$

kde $\alpha_j = (1,2)$ nebo $\alpha_j = (1,2,3,4,5)$ pro všechna $j \in \{1, \ldots, l\}$. Dále pro jednu z reprezentací φ^{ω_i} označíme $\varphi^{\omega_i}(\alpha_j) = A_j$ obraz permutace α_j. Pak máme

$$\varphi^{\omega_i}(\pi) = A_1 \cdot \ldots \cdot A_l.$$

Zopakujeme-li tento postup pro každou permutaci z $\boldsymbol{S}_5$, dostaneme rozšíření zobrazení φ^{ω_i} na celou grupu $\boldsymbol{S}_5$.

Poznámka 11. V implementaci útoku jsme zobrazení φ^{ω_i} rozšířili na celou grupu $\boldsymbol{S}_5$ postupným generováním všech permutací z grupy $\boldsymbol{S}_5$ pomocí skládání permutací $(1,2)$ a $(1,2,3,4,5)$. U každé permutace jsme si pamatovali, z jakých permutací byla vytvořena a její obraz v zobrazení φ^{ω_i} jsme vytvořili jako součin obrazů permutací, ze kterých byla složena.
Označme $C_i = \{[\pi, \varphi^{\omega_i}(\pi)], \pi \in \boldsymbol{S}_5\}$ množinu všech permutací π z grupy $\boldsymbol{S}_5$ společně s jejich obrazy $\varphi^{\omega_i}(\pi)$. Postup pak může být ilustován takto:

Algoritmus 3: Rozšíření φ^{ω_i} na celou grupu $\boldsymbol{S}_5$

Vstup: $(1,2)$, $(1,2,3,4,5)$
Výstup: C_i

$X = \{(1,2),(1,2,3,4,5)\}$;
$C_i = \{[(1,2),\varphi^{\omega_i}((1,2))],[(1,2,3,4,5),\varphi^{\omega_i}((1,2,3,4,5))]\}$;
početPermutací $= 2$;
While (početPermutací ≤ 120) **do**
    forall $x, y \in X$ **do**
        $z = x \circ y$;
        if $(z \notin X)$ **then**
            $X = X \bigcup \{z\}$;
            $\varphi^{\omega_i}(z) = \varphi^{\omega_i}(x)\varphi^{\omega_i}(y)$;
            $C_i = C_i \bigcup \{[z, \varphi^{\omega_i}(z)]\}$;
            početPermutací ++;
return C_i.

Připomeňme, že skládání permutací není komutativní, tedy je důležité dbát na správné pořadí při násobení jejich obrazů.

Poznámka 12. Celou situaci výše jsme ilustrovali pouze pro $i = 2$ (kromě části 3.2, kde byla situace nastíněna pouze pro jedno i). Nesmíme zapomenout, že hledáme 7 reprezentací, tedy se tento postup musí zopakovat pro každý rozklad čísla 5.

3.3 Zobrazení matic M a N pomocí izomorfismu ψ

Pro grupu $\boldsymbol{G}$ již máme zobrazení $\varphi^{\omega_i} : \boldsymbol{G} \to \boldsymbol{GL}(n_i, \boldsymbol{T})$, $i \in \{1, \ldots, r\}$. Tato zobrazení nejprve rozšíříme na zobrazení z $\boldsymbol{TG}$, které dále rozšíříme na zobrazení z $M_m(\boldsymbol{TG})$.
Pro jednu reprezentaci φ^{ω_i}, $i \in (1, \ldots, r)$ bude homomorfismus T-algeber $\tilde{\varphi}^{\omega_i} : \boldsymbol{TG} \to M_{n_i}(\boldsymbol{T})$, kde n_i je stupeň reprezentace φ^{ω_i}, fungovat následovně:

$$\tilde{\varphi}^{\omega_i}\left(\sum_{g\in G} t_g g\right) = \sum_{g\in G} t_g \varphi^{\omega_i}(g).$$

Označme homomorfismus T-algeber ψ^{ω_i}, pro který bude platit

$$\psi^{\omega_i} : M_m(\boldsymbol{TG}) \to M_m(M_n(\boldsymbol{T})),$$

$$\psi^{\omega_i} : \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \mapsto \begin{pmatrix} \tilde{\varphi}^{\omega_i}(a_{11}) & \cdots & \tilde{\varphi}^{\omega_i}(a_{1m}) \\ \vdots & \ddots & \vdots \\ \tilde{\varphi}^{\omega_i}(a_{m1}) & \cdots & \tilde{\varphi}^{\omega_i}(a_{mm}) \end{pmatrix}.$$

Dle tvrzení 2 víme, že $M_m(M_n(\boldsymbol{T})) \simeq M_{mn}(\boldsymbol{T})$. Máme tedy

$$\psi^{\omega_i} : M_m(\boldsymbol{TG}) \to M_{mn}(\boldsymbol{T}).$$

Poznamenejme, že předešlé úvahy byly pouze pro jednu z reprezentací φ^{ω_i}. Výsledné zobrazení, které nás zajímá, je izomorfismus algeber $\psi = (\psi^{\omega_1}, \ldots, \psi^{\omega_r})$, které zobrazí matice M a N následovně:

$$\psi(M) = (\psi_1(M), \ldots, \psi_r(M));$$
$$\psi(N) = (\psi_1(N), \ldots, \psi_r(N)).$$

Dostáváme tedy zobrazení matic M a N na r-tice matic.
Následující tabulka zachycuje situaci pro grupový okruh $\mathbb{Z}_7[\boldsymbol{S}_5]$ a zobrazení ψ^{ω_i}.

Tabulka 3.2: Stupně $\psi^{\omega_i}(M)$

i	stupeň $\psi^{\omega_i}(M)$
1	3
2	12
3	15
4	15
5	18
6	12
7	3

Poznámka 13. Matice M a N mají stejný stupeň. Tedy i matice $\psi^{\omega_i}(M)$ a $\psi^{\omega_i}(N)$ budou mít stejný stupeň pro všechna i.
Dále platí, že matice M je regulární právě tehdy, je-li regulární i matice N (plyne z [16, Věta 7.21]).

3.4 Nalezení a_i

V této části redukujeme problém hledání diskrétního logaritmu v podpologrupě pologrupy řádu přibližně 10^{913} na hledání diskrétních logaritmů v grupách s podstatně menším řádem. I přes to se může stát, že v těchto grupách nebude možno diskrétní logaritmus spočítat hrubou silou v reálném čase. V takovém případě použijeme Pohligovu-Hellmanovu redukci.

Připomeňme, že se nacházíme v situaci, kdy již máme izomorfismus algeber $\psi = (\psi^{\omega_1}, \ldots, \psi^{\omega_7})$, který matice M i N zobrazí na sedmice matic nad tělesem $\mathbb{Z}_7$ takto:

$$\psi(M) = (M_1, \ldots, M_7)$$
$$\psi(N) = (N_1, \ldots, N_7),$$

což bude značení, kterého se budeme držet po zbytek kapitoly.

Poznámka 14. Díky tomu, že máme $M^a = N$, musí nutně platit, že i $(\psi^{\omega_i}(M))^a = \psi^{\omega_i}(N)$, $\forall i \in \{1, \ldots, 7\}$. Zde si ukážeme, jak se nejmenší taková a_i naleznou.

3.4.1 Diagonalizovatelné matice M_i a N_i

Nejprve se zaměříme na případ, kdy jsou matice M_i a N_i, $i \in \{1, \ldots, 7\}$ diagonalizovatelné. Dle věty 4 víme, že je to v případě, kdy se jejich charakteristický polynom rozkládá na součin lineárních činitelů (což zaručíme tím, že budeme počítat v rozkladovém nadtělese daného polynomu) a kdy je algebraická násobnost každého vlastního čísla rovna jeho geometrické násobnosti.
Zafixujme $i \in \{1, \ldots, 7\}$ a podívejme se na situaci pro jednu z matic M_i. Označme $H = M_i$, její stupeň k a $G = N_i$ se stejným stupněm k. Bez újmy na obecnosti předpokládáme, že 0 není vlastním číslem matice H (nulové vlastní číslo naši situaci nijak neovlivní viz poznámka 23). Dále označme $\lambda_1, \ldots, \lambda_k$ vlastní čísla matice H (ne nutně různá) a $u_1, \ldots, u_k$ bázi prostoru $\mathbb{Z}_7^k$ složenou z odpovídajících vlastních vektorů, která existuje, protože H je diagonalizovatelná.
Nechť U je invertibilní matice, která má v sloupcích vlastní vektory $u_1, \ldots, u_k$, a pro kterou platí

$$U^{-1}HU = \begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda_k \end{pmatrix}.$$

Potom

$$U^{-1}H^aU = \begin{pmatrix} \lambda_1^a & 0 & \ldots & 0 \\ 0 & \lambda_2^a & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda_k^a \end{pmatrix} = U^{-1}GU.$$

Najdeme-li pak číslo $\overline{b} \in \mathbb{N}_0$ takové, aby $\lambda_j^{\overline{b}} = \lambda_j^a, \forall j \in \{1, \ldots, k\}$, bude platit, že $H^{\overline{b}} = G$.

Poznámka 15. Veškeré výpočty, které budeme níže popisovat, budou stejné pro navzájem konjugované prvky (protože pro polynom p, jeho kořen α a k němu konjugovaný prvek β platí, že $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$ v rozkladovém nadtělese polynomu p). Všemi vlastními čísly budeme tedy dále v textu rozumět všechna vlastní čísla až na konjugovanost.

Pro každou matici M_i bude postup vypadat takto:

- nalezneme charakteristický polynom p, všechna vlastní čísla λ_j a jejich vlastní vektory v_j, $j \in \{1, \ldots, k\}$;
- pro každé vlastní číslo λ_j spočítáme ze vztahu

$$N_j v_j = \lambda_j^a v_j \tag{3.2}$$

  číslo b_j takové, aby platilo, že $\lambda_j^{b_j} = \lambda_j^a$;
- určíme $\overline{b}$ takové, aby $\lambda_j^{\overline{b}} = \lambda_j^a$, $\forall j \in \{1, \ldots, k\}$. Toto $\overline{b}$ pak bude hledané a_i pro každou matici M_i.

Nalezení charakteristického polynomu, vlastních čísel a vlastních vektorů. V případě, že se charakteristický polynom rozkládá na lineární činitele

nad tělesem $\mathbb{Z}_7$, použijeme k určení charakteristického polynomu, vlastních čísel a vlastních vektorů postup z [12, Kapitola 9].
V opačném případě nalezneme jeho rozklad na ireducibilní činitele nad tělesem $\mathbb{Z}_7$ a výpočty budeme provádět v rozkladových nadtělesech těchto ireducibilních činitelů.
Pro těleso $\boldsymbol{T}$, polynom p a jeho kořen $\lambda \notin \boldsymbol{T}$ budeme rozkladové nadtěleso $\boldsymbol{T}[\lambda]/p(\lambda)$ polynomu p značit $\boldsymbol{T}_p$.
Připomeňme, že pracujeme s diagonalizovatelnými maticemi, tedy můžeme všechny vlastní vektory příslušné vlastnímu číslu λ hledat jako řešení homogenní soustavy lineárních rovnic s maticí $M - \lambda E$. Dále ale víme, že pro dva vlastní vektory u_1 a u_2 vlastního čísla λ, povede vztah 3.2 k tomu samému výsledku, a tedy stačí pro vlastní číslo λ najít pouze jeden vlastní vektor.

Poznámka 16. Ve výsledku tedy pracujeme s nenulovými navzájem nekojnugovanými vlastními čísly, pro která hledáme pouze jeden vlastní vektor.

Nalezení b_j. Nejprve odvodíme vztah 3.2, pomocí kterého budeme moci najít hledaná b_j.

Poznámka 17. Připomeňme, že vztah 3.2 platí v této podobě pro všechna vlastní čísla a jim příslušné vlastní vektory.

Z vlastností vlastních vektorů a vlastních čísel víme, že pro diagonalizovatelnou matici S, její vlastní číslo λ a vlastní vektor v příslušný λ platí

$$Sv = \lambda v.$$

Pak máme

$$\begin{aligned} S^a v &= \underbrace{S \cdot \ldots \cdot S}_{a\text{-krát}} v = \underbrace{S \cdot \ldots \cdot S}_{a-1\text{-krát}}(Sv) = \underbrace{S \cdot \ldots \cdot S}_{(a-1)\text{-krát}} \lambda v \\ &= \underbrace{S \cdot \ldots \cdot S}_{a-2\text{-krát}} \lambda(Sv) = \underbrace{S \cdot \ldots \cdot S}_{(a-2)\text{-krát}} \lambda^2 v = \ldots = \lambda^a v. \end{aligned}$$

Nyní můžeme přistoupit k nalezení samotných b_j.
Pro lepší přehlednost ilustrujeme výpočty pro zobrazení ψ^{ω_1} a matice M_1 a N_1, které vypadají následovně:

$$M_1 = \begin{pmatrix} 6 & 6 & 3 \\ 4 & 1 & 4 \\ 6 & 1 & 1 \end{pmatrix}, N_1 = \begin{pmatrix} 2 & 4 & 5 \\ 0 & 6 & 6 \\ 6 & 1 & 1 \end{pmatrix}.$$

Charakteristický polynom matice M_1

$$p = 6x^3 + x^2 + 5x + 5,$$

se nad tělesem $\mathbb{Z}_7$ rozkládá takto:

$$p = 6(x+2)(x^2 + 4x + 1).$$

Vidíme tedy, že jedno z vlastních čísel je $\lambda_1 = 5$.
Víme, že polynom stupně 3 nemůže mít víc jak 3 kořeny, zbývá tedy najít λ_2 a

λ_3. Z teorie konečných těles (viz [17] a věta 9) víme, že pro takové kořeny bude platit

$$\lambda_2^2 + 4\lambda_2 + 1 = 0,$$
$$\lambda_3 = \lambda_2^7$$

a vlastní čísla λ_2 a λ_3 jsou konjugované prvky.
Výpočty budeme dále provádět pouze pro λ_1 a λ_2, jelikož víme, že výsledek bude pro konjugované prvky stejný. Dle [12] vypočítáme vlastní vektory v_i příslušné prvkům λ_i, $i = 1{,}2$, jako řešení homogenní soustavy lineárních rovnic s maticí

$$M_1 - E\lambda_i, i = 1{,}2.$$

Dostaneme

$$v_1 = (1{,}1{,}0)^T,$$
$$v_2 = (3 + 2\lambda, 2 + 3\lambda, 1)^T.$$

Tedy

$$N_1 v_1 = \begin{pmatrix} 2 & 4 & 5 \\ 0 & 6 & 6 \\ 6 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 6 \\ 6 \\ 0 \end{pmatrix}, \tag{3.3}$$

$$N_1 v_2 = \begin{pmatrix} 2 & 4 & 5 \\ 0 & 6 & 6 \\ 6 & 1 & 1 \end{pmatrix} \begin{pmatrix} 3 + 2\lambda_2 \\ 2 + 3\lambda_2 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 + 2\lambda_2 \\ 4 + 4\lambda_2 \\ \lambda_2 \end{pmatrix} \tag{3.4}$$

a vztah 3.2 dává pro rovnice 3.3 a 3.4

$$(6{,}6{,}0) = \lambda_1^a (1{,}1{,}0),$$

$$(5 + 2\lambda_2, 4 + 4\lambda_2, \lambda_2) = \lambda_2^a (3 + 2\lambda_2, 2 + 3\lambda_2, 1).$$

Nyní se můžeme zaměřit pouze na jednu nenulovou souřadnici vektoru. Dostaneme tedy

$$6 = \lambda_1^a,$$
$$(5 + 2\lambda_2) = \lambda_2^a (3 + 2\lambda_2).$$

Hledáme tedy b_1, které splňuje

$$5^{b_1} = 6,$$

odkud dostaneme $b_1 = 3$.
Dále hledáme b_2, aby platilo

$$\lambda_2^{b_2} = \lambda_2,$$

což dává $b_2 = 1$.
Připomeňme, že b_1 jsme hledali jako diskrétní logaritmus v grupě $\mathbb{Z}_7^*$ a b_2 jako diskrétní logaritmus v $\langle \lambda_2 \rangle \subseteq (\mathbb{Z}_7[x]/(x^2 + 4x + 1))^*$.

Vidíme, že v tomto kroku hledáme v případě grupy $\mathbb{Z}_7^*$ diskrétní logaritmus buď v grupě řádu 6, nebo pro nějaký kořen λ polynomu p v grupě řádu $\mathrm{ord}(\lambda)$. Pro počítání diskrétního logaritmu v grupách větších řádů ($7^8 - 1$ a výše) použijeme k výpočtům Pohligovu-Hellmanovu redukci.

Pohligova-Hellmanova redukce. Pohligovu-Hellmanovu redukci ukážeme pro obecný případ, kdy máme grupu $\boldsymbol{G} = \langle a \rangle$ řádu n, $n = p_1^{e_1} \cdot \ldots \cdot p_s^{e_s}$ prvočíselný rozklad a prvek $b \in \langle a \rangle$ a hledáme $x \in \{1, \ldots, n\}$ takové, že $b = a^x$. Tento algoritmus redukuje hledání diskrétního logaritmu v grupě řádu n do grup s řády $p_i^{e_i}$ pro nějaké $i \in \{1, \ldots, s\}$.
Základní myšlenkou je, že pokud budeme mít hodnoty x_i takové, že

$$x = x_i \bmod (p_i^{e_i}), \tag{3.5}$$

pro všechna $i \in \{1, \ldots, s\}$, pak umíme soustavu kongruencí 3.5 vyřešit pomocí Čínské věty o zbytcích (viz [8, Věta 3.13]) a získat tak řešení $x \bmod n$.

Algoritmus pro vstupní data stejná jako výše probíhá následovně:

Algoritmus 4: Pohligova-Hellmanova redukce

Vstup: $\boldsymbol{G}, a, b$
Výstup: $x = \mathrm{Dlog}_a(b), x \in \mathbb{Z}_n$

for $i = 1, \ldots, s$ **do**
$a_i = a^{n/p_i^{e_i}}$;
$b_i = b^{n/p_i^{e_i}}$;
$x_i = \mathrm{Dlog}_{a_i}(b_i)$;
Spočti $x \in \mathbb{Z}_n, x = x_i \bmod (p_i^{e_i}), \forall i \in \{1, \ldots, s\}$.

Pohligova-Hellmanova redukce, kterou jsme zde připomněli, vede na počítání diskrétních logaritmů v grupách s řády $p_i^{e_i}$. V [18] je možno nalézt postup, který bude vést na výpočty v grupách řádů p_i.
Víme, že v našem případě bude $n = |\boldsymbol{G}| = |\langle \lambda \rangle|$. Potřebujeme tedy umět nalézt řády vlastních čísel, čímž se zabývá následující část.

Řády vlastních čísel. Mějme charakteristický polynom p a

$$p = q_1 \cdot \ldots \cdot q_k$$

jeho rozklad na ireducibilní faktory nad tělesem $\mathbb{Z}_7$. Musíme postupovat pro každý z ireducibilních faktorů jednotlivě, tedy pro každé q_j najdeme jeho kořeny (vlastní čísla) a vypočítáme jejich řády v tělese $\boldsymbol{T}_{q_j}^*$.
Poznámka 18. Připomeňme, že řády konjugovaných prvků jsou stejné.

Uvažme tedy jeden faktor q_j ireducibilního rozkladu polynomu p a označme jej q. Dále označíme d jeho stupeň a u kořen polynomu q, jehož řád v tělese $\boldsymbol{T}_q^*$ chceme zjistit. Pak máme $|\boldsymbol{T}_q^*| = 7^d - 1$ pro $\boldsymbol{T} = \mathbb{Z}_7$.
Z teorie grup (viz [8, Tvrzení 15.2]) víme, že $\mathrm{ord}(u)$ dělí $|\boldsymbol{T}_q^*|$ a že pro

$$|\boldsymbol{T}_q^*| = s_1^{l_1} \cdot s_2^{l_2} \cdot \ldots \cdot s_n^{l_n} \tag{3.6}$$

prvočíselný rozklad řádu grupy $\boldsymbol{T}_q^*$ existuje $w \in \mathbb{N}$, kde $w = c^t$, c je prvočíslo a $t \in \mathbb{N}$ takové, že $\frac{|\boldsymbol{T}_q^*|}{w} \in \mathbb{N}$, a pro které platí, že

$$u^{\frac{|\boldsymbol{T}_q^*|}{w}} = \begin{cases} 1 & \Rightarrow \mathrm{ord}(u) \mid \left(\frac{|\boldsymbol{T}_q^*|}{w}\right) \\ \text{jinak} & \Rightarrow c \mid \mathrm{ord}(u). \end{cases} \tag{3.7}$$

Víme již, že ord(u) dělí $|\boldsymbol{T}_q^*|$, tedy se v prvočíselném rozkladu ord(u) budou vyskytovat pouze ta prvočísla, která jsou v rozkladu 3.6 $|\boldsymbol{T}_q^*|$. Nemusí se tam ale vyskytovat všechna. K tomu, abychom zjistili, která prvočísla máme uvažovat, slouží rovnice 3.7.

Nyní, když máme řády všech vlastních čísel, můžeme přistoupit k popisu použití samotné Pohligovy-Hellmanovy redukce. Připomeňme ještě, že tato redukce je potřeba až v druhém kroku, kdy hledáme b_j takové, aby platilo, že $\lambda_j^{b_j} = \lambda_j^a$. Víme již tedy, jak vypadá λ^a.

Příklad 12. Pohligovu-Hellmanovu redukci částečně ukážeme pro zobrazení ψ^{ω_5}. V této situaci pracujeme s charakteristickým polynomem

$$p = x^{15}+6x^{14}+5x^{13}+x^{12}+6x^{11}+5x^{10}+2x^9+2x^8+5x^7+3x^5+x^3+4x^2+5x+5,$$

jeho kořenem λ, kde ord(λ) = 2373780754971 = $3^2 \cdot 19 \cdot 31 \cdot 2801 \cdot 159871$ a hledáme b, takové, že $\lambda^a = \lambda^b$. Označíme-li

$$u = 9 \cdot 19 \cdot 31 \cdot 2801,$$
$$v = 159871$$

taková, aby NSD(u,v) = 1, pak λ^u je prvek řádu v a λ^v je prvek řádu u.
Dále označíme $K = \lambda^a$, $K_u = K^u$ a $K_v = K^v$, pro něž najdeme a_u takové, že $K_u = (\lambda^u)^{a_u}$ a a_v takové, že $K_v = (\lambda^v)^{a_v}$. Při hledání a_u a a_v budeme počítat diskrétní logaritmus hrubou silou v grupách řádu u nebo v.
Jelikož jsou čísla u a v nesoudělná, tak víme, že můžeme najít α,$\beta \in \mathbb{Z}$ taková, že

$$\alpha u + \beta v = 1.$$

Pak máme

$$\lambda^a = K = K^{\alpha u+\beta v} = (K^u)^\alpha \cdot (K^v)^\beta = \lambda^{u a_u \alpha} \cdot \lambda^{v a_v \beta}$$

a tedy $b = u a_u \alpha + v a_v \beta \bmod \text{ord}(\lambda)$.

Ve výše zmíněném příkladu jsme počítali diskrétní logaritmus v grupách řádu u nebo v hrubou silou, což pro velké u nebo v může být výpočetně velice náročné. Rozeberme tedy výpočetní náročnost tohoto kroku podrobněji.
Víme, že pro polynom p a jeho kořen λ platí, že ord(λ) dělí $|T_p^*|$. Uvažujme tedy nejhorší případ, kdy ord(λ) = $|T_p^*|$. Označíme-li

$$|T_p^*| = s_1^{l_1} \cdot s_2^{l_2} \cdot \ldots \cdot s_n^{l_n}$$

prvočíselný rozklad, pak dokážeme problém zredukovat až na grupy, které budou mít řád maximálně $s_j^{l_j}$, pro nějaké $j \in \{1,\ldots,n\}$. Dále pro polynom p stupně d bude $|T_p^*| = 7^d - 1$. Jelikož matice M_i mají maximální stupeň 18 (viz tabulka 3.3), pak že d může být maximálně 18.

V následující tabulce jsou prvočíselné rozklady $|T_p^*|$, pro stupeň d polynomu p takové, že $1 < d \leq 18$.

Tabulka 3.3: Prvočíselné rozklady $|T_p^*|$

$\lvert T_p^*\rvert$	Prvočíselný rozklad
7^2-1	$2^4 \cdot 3$
7^3-1	$2 \cdot 3^2 \cdot 19$
7^4-1	$2^5 \cdot 3 \cdot 5^2$
7^5-1	$2 \cdot 3 \cdot 2801$
7^6-1	$2^4 \cdot 3^2 \cdot 19 \cdot 43$
7^7-1	$2 \cdot 3 \cdot 29 \cdot 4733$
7^8-1	$2^6 \cdot 3 \cdot 5^2 \cdot 1201$
7^9-1	$2 \cdot 3^3 \cdot 19 \cdot 37 \cdot 1063$
$7^{10}-1$	$2^4 \cdot 3 \cdot 11 \cdot 191 \cdot 2801$
$7^{11}-1$	$2 \cdot 3 \cdot 1123 \cdot 293459$
$7^{12}-1$	$2^5 \cdot 3^2 \cdot 5^2 \cdot 13 \cdot 19 \cdot 43 \cdot 181$
$7^{13}-1$	$2 \cdot 3 \cdot 16148168401$
$7^{14}-1$	$2^4 \cdot 3 \cdot 29 \cdot 113 \cdot 911 \cdot 4733$
$7^{15}-1$	$2 \cdot 3^2 \cdot 19 \cdot 31 \cdot 2801 \cdot 159871$
$7^{16}-1$	$2^7 \cdot 3 \cdot 5^2 \cdot 17 \cdot 1201 \cdot 169533$
$7^{17}-1$	$2 \cdot 3 \cdot 14009 \cdot 2767631689$
$7^{18}-1$	$2^4 \cdot 3^3 \cdot 19 \cdot 37 \cdot 43 \cdot 1063 \cdot 117307$

Vidíme, že nejhorší situace nastává pro případ $7^{13}-1$, kde se vyskytuje prvočíslo $q' = 16148168401$. Pomocí programové implementace navrhovaného útoku jsme změřili, že umíme ověřit přibližně 27240 polynomů za vteřinu. Tedy k ověření přibližně 16148168401 polynomů potřebujeme přibližně 7 dnů. Uvážím-li možnost provádění výpočtů na grafické kartě, která zrychlí výpočty nejméně desetkrát, pak se pro tento nejhorší případ dostáváme na 17 hodin, což je přijatelná doba výpočtu.

Poznámka 19. Poznamenejme, že pro počítání diskrétního logaritmu může být také použit algoritmus *Pollardovo-ϱ* nebo *baby-step giant-step*.

Nalezení $\overline{b}$. Již jsme pro všechna vlastní čísla charakteristického polynomu spočítali b_j taková, že $\lambda_j^{b_j} = \lambda_j^a$, $j \in \{1,\ldots,k\}$. Nyní pomocí nich potřebujeme najít $\overline{b}$ takové, aby $\lambda_j^{\overline{b}} = \lambda_j^a$, $\forall j \in \{1,\ldots,k\}$. K tomu využijeme vztahu

$$\mathrm{ord}(\lambda_j) | (b_j - \overline{b}),$$

ze kterého můžeme sestavit soustavu diofantických rovnic

$$\overline{b} = b_j - \mathrm{ord}(\lambda_j) \cdot h_j, \tag{3.8}$$

pro $j \in \{1,\dots,k\}$,$h_j \in \mathbb{Z}$, o které víme, že má určitě řešení (původní hledané a) a jejíž minimální řešení umíme najít pomocí [19, Algoritmus 2.4.10] nebo rozšířeného Eukleidova algoritmu (viz [8, str. 38]). V této práci jsme použili postup, který je ilustrován v příkladě 13.

Připomeňme, že všechny výpočty jsou pouze pro jednu matici M_i, $i \in \{1,\dots,7\}$ a výše nalezené $\overline{b}$ odpovídá hledanému a_i pro matici M_i.

3.4.2 Nediagonalizovatelné matice M_i a N_i

V této části nastíníme postup pro nediagonalizovatelné matice M_i a N_i, $i \in \{1,\dots,7\}$.
Opět zafixujeme jedno $i \in \{1,\dots,7\}$ a postup ukážeme pouze pro jednu matici M_i, $i \in \{1,\dots,7\}$. Označme $H = M_i$, $G = N_i$.
Předpokládejme, že máme bázi B vlastních vektorů takovou, že $[H]_B$ matice H vzhledem k bázi B, má Jordanův kanonický tvar. (Postup pro nalezení takové báze B je možno nalézt v [12, Kapitola 9]).
Máme tedy invertibilní matici U, která má v sloupcích vektory báze B a pro kterou platí, že

$$U^{-1}HU = \begin{pmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_l \end{pmatrix}$$

je blokově diagonální matice s Jordanovými buňkami J_j, $j \in \{1,\dots,l\}$ na diagonále a

$$U^{-1}GU = \begin{pmatrix} J_1^a & 0 & \dots & 0 \\ 0 & J_2^a & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_l^a \end{pmatrix}.$$

Výpočtem $U^{-1}GU$ zjistíme $J_j^a, \forall j \in \{1,\dots,l\}$.

Postup bude probíhat následovně:

- pro každou Jordanovu buňku $J_j, j \in \{1,\dots,l\}$ najdeme b_j takové, aby $J_j^{b_j} = J_j^a$;
- spočítáme $\overline{b}$ takové, aby $J_j^{\overline{b}} = J^a$. Toto $\overline{b}$ pak opět bude hledané a_i takové, že $M_i^{a_i} = N_i$.

Nalezení b_j pro Jordanovu buňku Zafixujme $j \in \{1,\dots,l\}$ a ukažme postup pro jednu dvojici Jordanových buněk J_j, J_j^a, J_j Jordanova buňka příslušná vlastnímu číslu λ_j. Označme $J = J_j$, její stupeň k, $\lambda_j = \lambda$, hledané $b_j = b$ a $J_a = J_j^a$ (máme tedy $J^a = J_a$ a hledáme b takové, že $J^b = J_a$).
Bez újmy na obecnosti předpokládejme, že geometrická násobnost vlastního čísla λ je 1. Z věty 3 víme, že báze B obsahuje Jordanův řetízek $u_1,\dots,u_k$ délky k s

počátkem u_1 příslušným k vlastnímu číslu λ, pro který platí

$$\begin{aligned} Hu_1 &= \lambda u_1, \\ Hu_2 &= \lambda u_2 + u_1, \\ &\vdots \\ Hu_k &= \lambda u_k + u_{k-1}. \end{aligned} \tag{3.9}$$

Poznamenejme, že stejně jako v diagonalizovatelném případě nebude potřeba pracovat s konjugovanými prvky zvlášť, jelikož tyto prvky dávají stejné tvary Jordnanových buněk. O tom pojednává následující tvrzení.

Tvrzení 10. *Nechť p je prvočíslo a $\boldsymbol{T} = \mathbb{F}_p$. Uvažujme matici H nad tělesem $\boldsymbol{T}$ a označme g její charekteristický polynom stupně n a $\boldsymbol{T}_g$ jeho rozkladové nadtěleso. Dále označme $\lambda \in \boldsymbol{T}_g^*$ jeho kořen a Γ množinu konjugovaných prvků k λ. Dále mějme matici B pro kterou platí, že matice*

$$B^{-1}HB$$

je v Jordanově kanonickém tvaru. Pak vlastní číslo λ a jakékoliv $\alpha \in \Gamma$ dávají stejné tvary Jordanových buněk.

Důkaz. Opět využíváme toho, že dle věty 3 existuje matice B.
Máme tedy $|\boldsymbol{T}_g| = p^m$ počet prvků rozkladového nadtělesa polynomu g.
Z teorie konečných těles ([17, Věta 3.10]) víme, že zobrazení σ_i,
$i \in \{0, \ldots, (m-1)\}$ taková, že

$$\sigma_i(\alpha) = \alpha^{p^i},$$

$\alpha \in \boldsymbol{T}_g$, jsou navzájem různá a tvoří automorfismy tělesa $\boldsymbol{T}_g$. Z definice konjugovaných prvků je zřejmé, že se dokonce jedná o Γ-automorfismy tělesa $\boldsymbol{T}_g$ (tedy $\sigma_i(\alpha) \in \Gamma, \forall \alpha \in \Gamma, \forall i \in \{0, \ldots, (m-1)\}$).
Bez újmy na obecnosti zvolme $i = 1$ a označme $\sigma = \sigma_1$. Toto zobrazení σ, které vede z tělesa $\boldsymbol{T}_g$ rozšíříme na zobrazení, které zobrazí i matice a vektory nad tělesem $\boldsymbol{T}_g$. Takto rozšířené zobrazení označíme Σ.
Pro prvek $e \in \boldsymbol{T}_g$ bude

$$\Sigma(e) = \sigma(e),$$

pro matici A nad tělesem $\boldsymbol{T}_g$ stupně b bude platit

$$\Sigma(A) = \begin{pmatrix} \sigma(a_{11}) & \ldots & \sigma(a_{1b}) \\ \vdots & \ddots & \vdots \\ \sigma(a_{b1}) & \ldots & \sigma(a_{bb}) \end{pmatrix}$$

a pro vektor u v prostoru $\boldsymbol{T}_g^c$ bude

$$\Sigma(u) = (\sigma(u_1), \ldots, \sigma(u_c)).$$

Nyní pro λ kořen polynomu g a k němu konjugovaný prvek $\alpha = \Sigma(\lambda) \in \Gamma$, chceme dokázat, že dávají stejné tvary Jordanových buněk.

Z důkazu věty [12, Věta 9.67, str 211-212] víme, že můžeme ekivalentně dokazovat rovnost

$$\dim\Big(\mathrm{Ker}\big((H-\lambda I)^m\big)\Big) = \dim\Big(\mathrm{Ker}\big((H-\alpha I)^m\big)\Big) \tag{3.10}$$

pro každé $m \in \mathbb{N}$, protože $\Big(\dim\Big(\mathrm{Ker}\big((H-\lambda I)^m\big)\Big) - \dim\Big(\mathrm{Ker}\big((H-\lambda I)^{m-1}\big)\Big)\Big)$ určuje počet Jordanových buněk vlastního čísla λ v matici H délky alespoň m (definice $\mathrm{Ker}(A)$, kde A je matice viz [12, Definice 5.7]).
Důkaz rovnosti 3.10 rozdělíme do tří kroků:

1. Dokážeme, že

   $$\Sigma\Big(\mathrm{Ker}\big((H-\lambda I)^m\big)\Big) = \mathrm{Ker}\big((H-\alpha I)^m\big).$$

   Inkluze $\subseteq$: $u \in \mathrm{Ker}\big((H-\lambda I)^m\big) \Leftrightarrow (H-\lambda I)^m u = 0 \Leftrightarrow$
   $\Sigma\big[(H-\lambda I)^m u\big] = 0 \Leftrightarrow (H-\alpha I)^m \Sigma(u) = 0 \Leftrightarrow \Sigma(u) \in \mathrm{Ker}\big((H-\alpha I)^m\big)$.
   Inkluze $\supseteq$: $u \in \mathrm{Ker}\big((H-\alpha I)^m\big) \Rightarrow u = \Sigma\big(\Sigma^{-1}(u)\big) \in \mathrm{Ker}\big((H-\alpha I)^m\big) \Rightarrow$
   $\Sigma^{-1}(u) \in \mathrm{Ker}\big((H-\lambda I)^m\big)$, tedy $u \in \Sigma\Big(\mathrm{Ker}\big((H-\lambda I)^m\big)\Big)$.

2. Dokážeme, že Σ zobrazí množinu $\boldsymbol{T}_g$-lineárně nezávislých vektorů na množinu $\boldsymbol{T}_g$-lineárně nezávislých vektorů.
   Vezmeme-li lineárně nezávislé vektory $u_1, \ldots, u_d$ v $\boldsymbol{T}_g^c$ a $t_1, \ldots, t_d \in \boldsymbol{T}_g$ tak, aby

   $$\sum_{i=1}^{d} t_i \Sigma(u_i) = 0 \qquad\qquad |\Sigma^{-1}$$
   $$\sum_{i=1}^{d} \sigma^{-1}(t_i) u_i = 0.$$

   Z nezávislosti vektorů u_i plyne, že $t_i = 0, \forall i \in \{1, \ldots, d\}$.

3. Dokážeme, že $\Sigma(\langle u_1, \ldots, u_t \rangle) = \langle \Sigma(u_1), \ldots, \Sigma(u_t) \rangle$.
   Z předchozího kroku víme, že se lineární kombinace zobrazením Σ převede na lineární kombinaci s jinými koeficienty, odkud už tento krok plyne.

Dokázali jsem tedy rovnost 3.10 a tím i tvrzení.

❑

Máme-li tedy $u_1, \ldots, u_k$ Jordanův řetízek délky k s počátkem u_1 příslušným k vlastnímu číslu λ, pak pro u_1 platí

$$Gu_1 = \lambda^a u_1.$$

Z tohoto vztahu spočítáme stejně jako v případě diagonalizovatelných matic a_0 takové, že $\lambda^{a_0} = \lambda^a$.

V předchozím případě by zde výpočet končil. V případě nediagonalizovatelných matic však pro Jordanovu buňku J

$$J = \begin{pmatrix} \lambda & 1 & 0 & & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 0 & \lambda & & 0 & 0 \\ & \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}$$

máme dle [12, Tvrzení 9.65], že

$$J_a = \begin{pmatrix} \lambda^a & \binom{a}{1}\lambda^{a-1} & \binom{a}{2}\lambda^{a-2} & \dots & \binom{a}{k-1}\lambda^{a-k+1} \\ 0 & \lambda^a & \binom{a}{1}\lambda^{a-1} & \dots & \binom{a}{k-2}\lambda^{a-k+2} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^a & \binom{a}{1}\lambda^{a-1} \\ 0 & 0 & \dots & 0 & \lambda^a \end{pmatrix}. \tag{3.11}$$

Vidíme tedy, že nestačí aby si výrazy matic J^b a J_a odpovídaly pouze hlavní diagonále (což zaručuje volba $b = a_0 + m \cdot \mathrm{ord}(\lambda), m \in \mathbb{N}_0$), ale potřebujeme, aby byly stejné i výrazy nad hlavní diagonálou. To zaručíme následujícím postupem. Již víme, že pro hledané b platí

$$b = a_0 + m \cdot \mathrm{ord}(\lambda).$$

Dále máme, že

$$\lambda^{a_0} = \lambda^a \Rightarrow \lambda^{a_0 - s} = \lambda^{a-s},$$

pro $s \leq a$.
Označme jednotlivé členy nad hlavní diagonálou buňky J_a takto:

$$\binom{a}{t}\lambda^{a-t} = c_t$$

a odpovídající člen v matici J^b označme d_t. Pak chceme docílit, aby

$$c_t = d_t \tag{3.12}$$

pro všechna t.
Pro $t = 1$ máme:

$$c_1 = \binom{a}{1}\lambda^{a-1} = a\lambda^{a_0-1} = d_1 = b\lambda^{b-1}.$$

Odtud pak

$$b \bmod 7 = (\lambda^{a_0-1})^{-1} \cdot c_1 = \beta$$

a se znalostí β a $\mathrm{ord}(\lambda)$ vypočítáme a označíme

$$m \bmod 7 =: \alpha_0.$$

Rovnosti $c_t = d_t$ pro $t \in \{2, \dots, 6\}$, protože výrazy $\binom{b}{2}\lambda^{b-2}$, … , $\binom{b}{6}\lambda^{b-6}$ závisí pouze na hodnotách a_0 a b mod 7.

Poznámka 20. $\binom{x}{y} = 0$ pro $x < y$.

Otázkou tedy zůstává, co nastane případě $t = 7$.
Pro $t = 7$ dostaneme

$$d_7 = \binom{b}{7}\lambda^{b-7} = \frac{b(b-1)\dots(b-\beta)\dots(b-6)}{7\cdot 6\cdot\dots\cdot 1}\lambda^{a_0-7},$$

odkud společně s 3.12

$$\frac{b-\beta}{7} \bmod 7 = c_7 \frac{6\cdot\dots\cdot 1}{b(b-1)\dots(b-\beta+1)(b-\beta-1)\dots(b-7)}(\lambda^{a_0-7})^{-1}.$$

Označíme-li

$$\beta_1 = \frac{b-\beta}{7} \bmod 7,$$

máme

$$b \bmod 49 = 7\beta_1 + \beta,$$

odkud spočteme a označíme

$$m \bmod 49 =: \alpha_1.$$

Dosazením $b = 7\beta_1 + \beta$ do výrazů d_t pak už dostaneme rovnosti $c_t = d_t$ pro $t \in \{7, \dots, 18\}$ (stupeň Jordanovy buňky J je maximálně 18 (viz tabulka 3.3)).
Pak máme

$$b = a_0 + (\alpha_0 + 7\cdot\alpha_1)\mathrm{ord}(\lambda)$$

hledané b pro Jordanovu buňku J.

Nalezení $\overline{b}$. Máme již b_j taková, že $J_j^{b_j} = J_j^a$, pro $j \in \{1, \dots, l\}$ a hledáme $\overline{b}$ takové, že $J_j^{\overline{b}} = J_j^a, \forall j$. Lehce nahlédneme, že takové $\overline{b}$ bude splňovat

$$\overline{b} = b_1 + k_1\mathrm{per}(J_1) = \dots = b_l + k_l\mathrm{per}(J_l)$$

pro $k_j \in \mathbb{N}_0$, což nám opět dává soustavu diofantických rovnic (jejich řešení viz 3.8). Se znalostí period jednotlivých Jordanových buněk tedy umíme pro matici M_i spočítat příslušné $a_i = \overline{b}$.

Perioda Jordanovy buňky. Označme p hledanou periodu Jordanovy buňky J. Je zřejmé, že p bude tvaru

$$p = k\cdot\mathrm{ord}(\lambda),$$

pro $k \in \mathbb{N}$.
Tím, že p bude násobkem řádu vlastního čísla λ zajistíme, aby se prvky na diagonále matice J shodovaly s prvky na diagonále matice J^p. Volbou vhodného k pak zajistíme, aby všechny prvky nad diagonálou J^p byly nulové. Pak tedy bude $J = J^p$.
Řád vlastního čísla λ již zjistit umíme (viz sekce 3.4.1). Inicializujme $p = \mathrm{ord}(\lambda)$ hledané p.
Při hledání čísla k rozdělme situaci na několik případů.

Poznámka 21. Připomeňme, že počítáme nad tělesem $\mathbb{Z}_7$, tedy všechny operace probíhají modulo 7.

(a) 7 dělí p a stupeň matice J je nejvýše 7.
V tomto případě 7 dělí všechna kombinační čísla vyskytující se v matici J^p a tedy $k = 1$ a $\mathrm{per}(J) = p$.

(b) 7 dělí p a stupeň matice J je větší jak 7.
Označme $c = p/7$. Problém v tomto případě nastane ve chvíli, kdy budeme pracovat s kombinačním číslem $\binom{p}{7}$. Víme, že 7 dělí p, tedy bude

$$\begin{aligned}\binom{p}{7} &= \frac{p \cdot (p-1)(p-2) \cdot \ldots \cdot (p-6)}{7 \cdot 6 \cdot 5 \cdot \ldots \cdot 1} \\ &= \frac{c \cdot (p-1)(p-2) \cdot \ldots \cdot (p-6)}{6 \cdot 5 \cdot \ldots \cdot 1}.\end{aligned}$$

Pro vynulování tohoto členu modulo 7 je tedy potřeba, aby $7|c$ (jelikož 7 nedělí čísla $(p-1), \ldots, (p-6)$). Pokud 7 nedělí c, tak zvolíme $k = 7$, což nám dá $\mathrm{per}(J) = 7p$.
Zdá se, že by mohl opět nastat problém pro $\binom{\mathrm{per}(J)}{14}$. V tomto případě však máme ve jmenovateli číslo 7 pouze dvakrát, zato v čitateli je třikrát (přibyde člen $(p-7)$) a tedy opět dostáváme nulový člen modulo 7.

(c) 7 nedělí $\mathrm{ord}(\lambda)$ a stupeň J je alespoň 2.
Pokud 7 nedělí $\mathrm{ord}(\lambda)$, pak inicializujeme $p = 7 \cdot \mathrm{ord}(\lambda)$ a případ je tím převeden na předchozí dva.

Poznámka 22. Připomeňme, že z tabulky 3.3 víme, že budeme pracovat s Jordanovymi buňkami do stupně maximálně 18, tedy postup výše zahrnuje všechny možnosti, které mohou v naší situaci nastat.

3.5 Nalezení a'

Máme tedy prvky $a_1, \ldots, a_7$ nejmenší takové, že $M_i^{a_i} = N_i$, s jejichž pomocí najdeme a' takové, aby $M^{a'} = N$. Označme p_i velikost periody každé matice M_i (postup pro jejich určení viz sekce 4.1). Pak existují l_i,$i \in \{1, \ldots, 7\}$ taková, že platí

$$a' = a_1 + l_1 p_1 = a_2 + l_2 p_2 = \ldots = a_7 + l_7 p_7. \tag{3.13}$$

Rovnici 3.13 můžeme chápat jako soustavu diofantických rovnic

$$a_1 + l_1 p_1 = a_2 + l_2 p_2 = \ldots = a_7 + l_7 p_7,$$

s neznámými $l_1, \ldots, l_7$, které umíme najít (viz 3.8). Po zpětném dosazení jakéhokoliv $l_i, i \in \{1, \ldots, 7\}$ do rovnice 3.13 dostaneme hledané a' tvaru

$$a' = x + my, \tag{3.14}$$

$x, y, m \in \mathbb{Z}$, kde čísla x a y budou vypočítaná a m značí parametr.

Poznámka 23. Rozeberme podrobněji otázku nulových vlastních čísel.
Změřme se opět na jednu z matic $(M_1, \ldots, M_7)$ a označme $H = M_i, G = M_i^a = N_i, i \in \{1, \ldots, 7\}$ a U bázi, vzhledem ke které má matice H Jordanův kanonický tvar

$$U^{-1}HU = \begin{pmatrix} J_1 & 0 & \ldots & 0 \\ 0 & J_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & J_l \end{pmatrix}.$$

Jak v diagonalizovatelném případě (stupeň J_j je roven 1 pro všechna $j \in \{1, \ldots, 7\}$), tak v nediagonalizovatelném případě, jsme hledali $b_j, j \in \{1, \ldots, 7\}$ taková, aby

$$J_j^{b_j} = J_j^a. \tag{3.15}$$

Z těchto b_j jsme pak spočítali $\overline{b}$ takové, že $H^{\overline{b}} = G$.
Dle 3.11 víme, že umocnění matice H na exponent $k \in \mathbb{N}$ se v jejím Jordanově kanonickém tvaru projeví jako umocnění každé Jordanovy buňky na exponent k.
Označme L Jordanovu buňku stupně l příslušnou vlastnímu číslu 0 a hledané b_j označme b_0. Pak k-tá mocnina Jordanovy buňky

$$L = \begin{pmatrix} 0 & 1 & 0 & & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ 0 & 0 & 0 & & 0 & 0 \\ & \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix},$$

bude

$$L^k = \begin{pmatrix} \overbrace{0 & \ldots & 0}^{(k+1)\text{-krát}} & 1 & \overbrace{0 & 0 & \ldots}^{(l-k-1)\text{-krát}} & 0 \\ 0 & \ldots & 0 & 0 & 1 & 0 & \ldots & 0 \\ & & & & & \ddots & & \\ 0 & & & & \ldots & 0 & 1 & 0 \\ 0 & & & & \ldots & & 0 & 1 \\ 0 & & & & \ldots & & & 0 \\ \vdots & & & & & & & \vdots \\ 0 & & & & \ldots & & & 0 \end{pmatrix}.$$

Vidíme tedy, že jedničky nad hlavní diagonálou ustupují do pravého horního rohu a zřejmě L^k bude nulová matice pro $k \geq l$.
Máme tedy, že Jordanova buňka nulového čísla nebude nulová pouze pro $b_0 < l$ a tedy i pro $\overline{b} < l$. Z 3.14 vidíme, že výsledné a' je tvaru $x + ym$ a vhodnou volbou parametru $m \in \mathbb{Z}$ zajisté umíme zaručit, aby $a' \geq 18$.
Je zřejmé, že problémem nebudou ani vícenásobná nulová vlastní čísla.

Kapitola 4

Baby-step giant-step

V dnešní době je známo několik algoritmů pro řešení diskrétního logaritmu. Jedním z nich je algoritmus Baby-step giant-step.
Tento postup, který se pro cyklickou grupu $\boldsymbol{G} = \langle a \rangle$ řádu n a $b \in \langle a \rangle$ snaží najít $x \in \mathbb{N}$ takové, aby $b = a^x$ využívá toho, že se toto x dá přepsat jako

$$x = im + j, \tag{4.1}$$

pro $m = \lceil \sqrt{n} \rceil$, $i, j \in \{0, \ldots, m-1\}$.
Z 4.1 pak plyne

$$b = a^{im+j} \Leftrightarrow ba^{-im} = a^j.$$

Algoritmus baby-step giant-step pak provede tzv. *baby-steps* spočítáním a uložením hodnot (j,a^j) pro $j \in \{0, \ldots, m-1\}$, po kterých následují tzv. *giant-steps*, které postupně počítají hodnoty ba^{-im}, pro $i \in \{0, \ldots, m-1\}$ a porovnávají je s již spočtenými a^j. Ve chvíli, kdy nastane rovnost

$$ba^{-im} = a^j$$

pro nějaké $i, j \in \{0, \ldots, m-1\}$, dostáváme výsledek $x = im + j$, pro který platí $a^x = b$.
Převeďme celou situaci v souladu s [2] do řeči matic. Pracujeme tedy s maticemi $M, N \in M_3\left(\mathbb{Z}_7[\boldsymbol{S}_5]\right), n = |M_3\left(\mathbb{Z}_7[\boldsymbol{S}_5]\right)|$ takovými, že $M^a = N$, pro nějaké $a \in \mathbb{N}$ a hledáme $x \in \mathbb{N}$, které splňuje

$$M^x = N.$$

Hledané číslo x můžeme opět přepsat stejně jako v 4.1.
V [2] je použita obdoba algoritmu baby-step giant-step, která vychází z rovnice

$$N = M^{im+j} \Leftrightarrow NM^{-j} = M^{im},$$

pro M regulární.
Kroky *baby-steps* pak spočívají v počítání a uložení hodnot (j, NM^j), pro $j \in \{1, \ldots, m-1\}$, zatímco kroky *giant-steps* postupně počítají hodnoty M^{im}, pro $i \in \{1, \ldots, \lceil n/m \rceil\}$ a porovnávají je s již spočtenými NM^j. Je-li splněna rovnost

$$NM^j = M^{im}$$

pro nějaké $i \in \{1, \ldots, \lceil n/m \rceil\}$, $j \in \{1, \ldots, m-1\}$, dostáváme výsledek $x = im - j$, pro který platí $M^x = N$.
Samotný algoritmus pro modifikovaný Difieho Hellmanův protokol vypadá dle [2] takto:

Algoritmus 5: Baby-step giant-step

Vstup: $M, N \in M_3\left(\mathbb{Z}_7[\boldsymbol{S}_5]\right), n = \left|M_3\left(\mathbb{Z}_7[\boldsymbol{S}_5]\right)\right|$
Výstup: $x \in \mathbb{N}$ takové, že $M^x = N$

$m = \lceil \sqrt{n} \rceil$;
$t = \lceil n/m \rceil$;
for $j = 1, \ldots, m-1$ **do**
    Vypočítej NM^j;
    Ulož (j, NM^j);
for $i = 0, \ldots, t$ **do**
    Vypočítej $M_i = M^{im}$;
    if existuje j takové, že $M_i = NM^j$ **then**
        return $im - j$.

Výše popsaný algoritmus vyžaduje, aby platila implikace

$$M^{im} = NM^j \Rightarrow N = M^{im-j}.$$

Jelikož matice M nemusí být regulární a tedy invertibilní, tak se zdá, že by důkaz této implikace mohl být problém. Podíváme-li se ale na Jordanovy kanonické tvary (viz 3.4), pak pro bázi U dostaneme rovnost

$$(U^{-1}MU)^{im} = U^{-1}NU\left(U^{-1}MU\right)^j, \tag{4.2}$$

která může být znázorněna jako

$$\begin{pmatrix} \boxed{\textbf{sing}} & 0 \\ 0 & \boxed{\textbf{reg}} \end{pmatrix}^{im} = \begin{pmatrix} \boxed{\textbf{sing}} & 0 \\ 0 & \boxed{\textbf{reg}} \end{pmatrix}^{a} \begin{pmatrix} \boxed{\textbf{sing}} & 0 \\ 0 & \boxed{\textbf{reg}} \end{pmatrix}^{j},$$

kde **reg** značí část příslušnou nenulovým vlastním číslům a **sing** značí část příslušnou nulovým vlastním číslům. Bude-li ale matice $N = M^a$ dostatečně velká mocnina matice M a bude-li m dostatečně velké, pak můžeme rovnost 4.2 znázornit takto:

$$\begin{pmatrix} \boxed{0} & \\ & \boxed{\textbf{reg}^{im}} \end{pmatrix} = \begin{pmatrix} \boxed{0} & \\ & \boxed{\textbf{reg}^{a}} \end{pmatrix} \begin{pmatrix} \boxed{?} & \\ & \boxed{\textbf{reg}^{j}} \end{pmatrix}.$$

A tedy

$$\begin{aligned} M^{im} &= NM^j \\ &\Updownarrow \\ \textbf{reg}^{im} &= \textbf{reg}^a\textbf{reg}^j \\ &\Updownarrow \\ \textbf{reg}^{im-j} &= \textbf{reg}^a. \end{aligned}$$

Tedy pokud je $im - j$ velké natolik, aby $\textbf{sing}^{im-j} = 0$, pak $M^{im-j} = N$.

Poznámka 24. Je zřejmé, že se rovnají stupně jednotlivých regulárních i singulárních částí.

Podle [2] není algoritmus Baby-step giant-step použitelný pro modifikovaný Diffieho-Hellmanův protokol a to především proto, že má příliš velkou paměťovou náročnost, pokud by pracoval nad prostorem matic nad $\mathbb{Z}_7[\boldsymbol{S}_5]$.
Autoři [2] také okrajově zmínili, že by mohla při tomto útoku pomoci znalost periody matice M. Tuto možnost nyní probereme hlouběji.

4.1 Baby-step giant-step se znalostí periody matice M

Je zřejmé, že pokud bychom znali periodu matice M, tak se problém mnohonásobně zjednodušší. Nebudeme totiž muset prohledávat celou pologrupu $M_3\left(\mathbb{Z}_7[\boldsymbol{S}_5]\right)$, ale omezíme se pouze na prostor velikosti $\mathrm{per}(M)$. Otázkou zůstává, jak zjistit periodu matice M.
Máme-li opět matici M zobrazenou izomorfismem ψ jako sedmici matic $(M_1, \ldots, M_7)$, pak platí

$$\mathrm{per}(M) = \mathrm{NSN}(\mathrm{per}(M_1), \ldots, \mathrm{per}(M_7)).$$

Stačí tedy umět spočítat periody jednotlivých matic M_i. Situaci rozdělíme stejně jako v 3.4 na případ, kdy je matice M_i diagonalizovatelná a kdy není.

4.1.1 Diagonalizovatelná matice M_i.

Vzhledem k tomu, že matice M_i je diagonalizovatelná, máme dobrou představu o tom, jak vypadají jednotlivé mocniny matice M_i. Pro Jordanův kanonický tvar matice M_i

$$J = \begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda_k \end{pmatrix}$$

(všechny Jordanovy buňky mají stupeň 1) dostaneme

$$J^m = \begin{pmatrix} \lambda_1^m & 0 & \ldots & 0 \\ 0 & \lambda_2^m & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda_k^m \end{pmatrix}.$$

Tedy pro matici M_i a pro $\{\lambda_1, \ldots, \lambda_s\} \subseteq \{\lambda_1, \ldots, \lambda_k\}, s \leq k$ její nenulová vlastní čísla bude platit

$$\mathrm{per}(M_i) = \mathrm{NSN}(\mathrm{ord}(\lambda_1), \ldots, \mathrm{ord}(\lambda_s)),$$

přičemž řád vlastního čísla již umíme zjistit viz. 3.4.1.

4.1.2 Nediagonalizovatelná matice M_i.

Pro nediagonalizovatelnou matici M_i platí

$$\mathrm{per}(M_i) = \mathrm{NSN}(\mathrm{per}(J_1), \ldots, \mathrm{per}(J_l)),$$

kde J_j jsou Jordanovy buňky nenulových vlastních čísel matice M_i, jejichž periody umíme zjistit dle 3.4.2.

Kapitola 5

Implementace útoku

V této části se krátce věnujeme implementaci výše popsaného útoku.
Pro implementaci jsme zvolili vývojové prostředí Wolphram Mathematica 8 a Microsoft Visual C++ 2012. Z popisu útoku je patrné, že bylo potřeba zvládnout polynomiální aritmetiku a počítání s velkými čísly. Pro počítání s polynomy jsme zvolili knihovnu NTL a pro velká čísla knihovnu Empire.
Třída *MatrixM* obsluhuje operace nad maticemi z pologrupy $M_3(\mathbb{Z}_7[\boldsymbol{S}_5])$. Pomocí této třídy můžeme vygenerovat jak náhodnou matici z dané pologrupy, tak matici, která odpovídá specifikům zmíněným ke konci kapitoly 2. Dále můžeme pro matici M spočítat M^a pomocí algoritmu *binární mocnění*.
Projekt *Representations* vytvoří izomorfismus ψ specifikovaný v kapitole 3 a zobrazí matici M na sedmici matic.
V neposlední řadě pak třída *AthPower* spočítá pro matice $M^a = N$ a' takové, že $M^{a'} = N$.

Příklad 13. Zde uvedeme některé výsledky testování implementace daného útoku.
Pracovali jsme s maticí $M = M_1 S$, kde matice S a M_1 jsou stejné jako v příkladě 11.
Tajný exponent $a = 387060858948298925000441656 41$.
Matice M byla zobrazena izomorfismem ψ (stejně jako v 3.3) na sedmici matic $(M_1, \ldots, M_7)$ (číslování opět odpovídá očíslování v tabulce 3.2). Všechny matice M_i vyšly diagonalizovatelné, tedy postup probíhal podle postupu v 3.4.1. Budeme se tedy držet značení z této části.
Pro matici $M_i, i \in \{1, \ldots, 7\}$ označme p_i její charakteristický polynom. Tyto charekteristické polynomy vypadaly následovně:

$$p_1 = 6(2+x)(1+4x+x^2);$$
$$p_2 = x^3(4+x)(2+5x^4+6x^5+6x^6+3x^7+x^8);$$
$$p_3 = 6x^3(5+x)(2+6x+x^3)(6+5x+4x^2+2x^3+x^4+5x^5+3x^6+4x^7+x^8);$$
$$p_4 = 6x^3(1+5x+4x^2+3x^3+6x^4+3x^5+4x^6+4x^7+3x^8+2x^9+3x^{10}+x^{12});$$
$$p_5 = x^3(5+5x+4x^2+x^3+3x^5+5x^7+2x^8+2x^9+5x^{10}+6x^{11}+x^{12}+ 5x^{13}+6x^{14}+x^{15});$$
$$p_6 = (1+x)(4+4x+x^2+5x^3+x^4)(6+5x^2+5x^4+5x^5+x^6+x^7);$$
$$p_7 = 6(1+x)(3+x)(6+x).$$

Výsledky z postupu pro hledání b_j shrnuje následující tabulka.

Tabulka 5.1: Mezivýsledky

Polynom	Vlastní čísla	Řád vlastního čísla	b_i	Řád Dlog
p_1	5	6	3	6
	λ	8	1	7^2-1
p_2	3	6	3	6
	λ	2882400	1328841	7^8-1
p_3	2	3	3	6
	λ	342	249	7^3-1
	ω	1921600	1328841	7^8-1
p_4	λ	88726200	12509241	$7^{12}-1$
p_5	λ	2373780754971	907694003535	$7^{15}-1$
p_6	6	2	1	6
	λ	60	21	7^4-1
	ω	137257	102910	7^7-1
p_7	1	1	1	6
	4	3	3	6
	6	2	1	6

První sloupec tabulky 13 obsahuje charakteristické polynomy a poslední sloupec obsahuje řády grup, ve kterých byly počítány diskrétní logaritmy (před Pohligovou-Hellmanovou redukcí).
Následovalo vypočítání $\overline{b}$, kde jsme pro všechna vlastní čísla $\lambda_1, \ldots, \lambda_k$ polynomu $p_i, i \in \{1, \ldots, 7\}$ spočítali $\overline{b}$ ze soustavy diofantických rovnic

$$\overline{b} = b_j - \mathrm{ord}(\lambda_j)h_j, \tag{5.1}$$

kde $h_j \in \mathbb{Z}, j \in \{1, \ldots, k\}$.
V následující části ukážeme, jak se taková soustava diofantických rovnic vyřeší pro polynom p_7.

Řešení diafantických rovnic Pracujeme se soustavou diofantických rovnic

$$\overline{b} = b_1 - \mathrm{ord}(\lambda_1)h_1, \tag{5.2}$$
$$\overline{b} = b_2 - \mathrm{ord}(\lambda_2)h_2, \tag{5.3}$$
$$\overline{b} = b_3 - \mathrm{ord}(\lambda_3)h_3. \tag{5.4}$$

Vzájemným odečtením dostaneme

$$(5.2) - (5.3) \qquad b_2 - b_1 = \mathrm{ord}(\lambda_2)h_2 - \mathrm{ord}(\lambda_1)h_1, \tag{5.5}$$
$$(5.2) - (5.4) \qquad b_3 - b_1 = \mathrm{ord}(\lambda_3)h_3 - \mathrm{ord}(\lambda_1)h_1. \tag{5.6}$$

Dosazením do rovnice 5.5 budeme mít

$$\begin{aligned} 3 - 1 &= 3h_2 - 1h_1 \\ 2 &= 3h_2 - 1h_1. \end{aligned} \tag{5.7}$$

Dále rozšířeným Eukleidovým algoritmem spočítáme čísla h_1' a h_2', pro která platí

$$\mathrm{NSD}(\mathrm{ord}(\lambda_1),\mathrm{ord}(\lambda_2)) = \mathrm{NSD}(1,3) = -1h_1' + 3h_2'.$$

Pro NSD(1,3) = 1 dostaneme $h'_1 = -1$ a $h'_2 = 0$.
Pak platí

$$\text{NSD}(1,3)g = 3h'_2g - 1h'_1g,$$

a tedy $g = 2$ a označme

$$\begin{aligned} x_0 &= h'_2g = 0, \\ y_0 &= h'_1g = -2, \end{aligned}$$

pro která platí

$$2 = 3x_0 - y_0.$$

Pak víme, že rovnice 5.7 má minimální řešení

$$h_1 = x_0 + \frac{-1}{\text{NSD}(1,3)}t = -T, \tag{5.8}$$

$$h_2 = y_0 + \frac{3}{\text{NSD}(1,3)}t = -2 - 3T, \tag{5.9}$$

kde $T \in \mathbb{Z}$ je parametr (minimalita je zaručena dělením NSD(1,3)).
Dosazením h_1 do rovnice 5.6 dostaneme

$$\begin{aligned} 1 - 1 &= 2h_3 - 1(-2 - 3T), \\ 2 &= -2h_3 - 3T, \end{aligned}$$

odkud stejně jako výše spočítáme

$$\begin{aligned} h_3 &= 2 - 3t, \\ T &= -2 + 2t, \end{aligned}$$

kde $t \in \mathbb{Z}$ je parametr.
Dosazením takto vyjádřeného T do 5.8 a 5.9 dostaneme

$$\begin{aligned} h_1 &= 4 - 6t, \\ h_2 &= 2 - 2t, \\ h_3 &= 2 - 3t. \end{aligned}$$

Odtud pak

$$\begin{aligned} \overline{b} &= 1 - 1(4 - 6t) = -3 + 6t, \\ \overline{b} &= 3 - 3(2 - 2t) = -3 + 6t, \\ \overline{b} &= 1 - 2(2 - 3t) = -3 + 6t, \end{aligned}$$

je hledané $\overline{b}$ a tedy hledané a_7 pro matici M_7 (pracovali jsme s polynomem p_7).
V následující tabulce je možno nalézt $a_i, i \in \{1, \ldots, 7\}$, která byla spočtena metodou popsanou výše, avšak bez toho, aby se v rovnicích 5.8 a 5.9 dělilo NSD(1,3).
Máme tedy správná řešení, ne však zaručeně minimální.

Tabulka 5.2: a_i

i	a_i
1	$9 + 48t$
2	$1328841 + 8647200t$
3	$227218993789641 - 1971561600t$
4	12509241
5	907694003535
6	$663745170141 - 16470840t$
7	$-3 + 6t$

V dalším kroku se z těchto a_i sestavilo a' jako řešení rovnice 3.13 (postup pro nalezení period matic M_i je uveden v 4.1). Vyřešili jsme tedy soustavu diofantických rovnic (pro volbu parametru $t = 0$)

$$\begin{aligned}
a' &= 9 + 24l_1, \\
a' &= 1328841 + 2882400l_2, \\
a' &= 227218993789641 + 328593600l_3, \\
a' &= 12509241 + 88726200l_4, \\
a' &= 907694003535 + 2373780754971l_5, \\
a' &= 663745170141 + 8235420l_6, \\
a' &= -3 + 6l_7,
\end{aligned}$$

postupem uvedeným výše a vypočítali

$a' = 350310065731473567845307248788215993519556264585853249124127858504 41+$
$4872873390037779882720801600\tau,$

kde $\tau \in \mathbb{Z}$ je parametr.
Pro takto vypočítané a' jsme dostali rovnost $M^{a'} = N$ pro několik různých voleb parametru τ.

Závěr

V této práci jsme popsali útok na modifikovaný Diffieho-Hellmanův protokol, který publikovali D. Kahrobaei a spol. v [2]. Nejprve jsme zavedli potřebné definice především z teorie reprezentací a část práce jsme věnovali samotnému Diffieho-Hellmanově protokolu jak v původní, tak v modifikované verzi. V další kapitole jsme se zabývali samotným popisem útoku na modifikovaný protokol, který jsme v některých částech rozdělili na případ diagonalizovatelných a nediagonalizovatlných matic. Další část je věnována útoku *baby-step giant-step* a především prohlášení z článku [2], že tento útok nebude při dané modifikaci protokolu fungovat. Součástí této práce je i programová implementace útoku, kterou jsme stručně zmínili v poslední kapitole.

Literatura

[1] M.E. Hellman W. Diffie. New directions in cryptography. *IEEE Transaction on Information Theory*, IT-22.

[2] V. Shpilrain D. Kahrobaei, C. Koupparis. Public key exchange using matrices over group rings. *Groups, Complexity and Cryptology 5*, pages 97–115, 2013. `http://arxiv.org/pdf/1310.7903.pdf`.

[3] A. Ushakov A. Myasnikov. Quantum algorithm for discrete logarithm problem for matrices over finite group rings. *Quantum algorithm for discrete logarithm problem for matrices over finite group rings*, 2012. `http://eprint.iacr.org/2012/574.pdf`.

[4] B. Tsaban M. Banin. A reduction of semigroup DLP to classic DLP. *IACR Cryptology ePrint Archive*, 2013. `http://arxiv.org/pdf/1310.7903.pdf`.

[5] M. D. Neusel Ch. Monico. Cryptanalysis of a system using matrices over group rings. 2014. Preprint.

[6] B. Steinberg. *Representation Theory of Finite Groups*.

[7] G.D James. *The Representation Theory of the Symmetric Group*. Springer-Verlag, lecture notes in math., vol. 682 edition, 1978.

[8] D. Stanovský. *Základy algebry*. Matfyzpress, Praha, 2010.

[9] D. R. Stinson. *Cryptography: Theory and Practice*. CRC Press, Inc., 2005.

[10] J. F. Humphreys. *A Course in Group Theory*. Oxford University Press, 1996.

[11] J. J. Rotmen. *An Introduction to the Theory of Groups*. Springer, 4 edition, 1994.

[12] J. Tůma L. Barto. *Lineární algebra*. `http://www.karlin.mff.cuni.cz/~barto/linalg1213/skripta_la3.pdf`.

[13] Barto L. Stanovský D. *Počítačová algebra*. Matfyzpress, Praha, 2011.

[14] S. H. Weintraub. *Representation Theory of Finite Groups: Algebra and Arithmetic (Graduate Studies in Mathematics)*, volume 59. Amer Mathematical Society, 2003.

[15] A. Kerber G.D. James. *The Representation Theory of the Symmetric Group*. Cambridge University Press, 2009.

[16] L. Bican. *Lineární algebra a geometrie*. Academia, Praha, 2000.

[17] J. Tůma L. Barto. *Konečná tělesa*. `http://www.karlin.mff.cuni.cz/~barto/student/SkriptaKonTel.pdf`.

[18] J. Buchmann. *Introduction to Cryptography*. Springer, 2004.

[19] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer.

Seznam algoritmů

Seznam tabulek