Pedagogická fakulta
Faculty of Education
Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích

Fakulta pedagogická

Katedra matematiky

Diplomová práce

Matematika v moderních šifrovacích metodách

Vypracovala: Bc. Alena Košáková
Vedoucí práce: prof. RNDr. Pavel Tlustý, CSc.

České Budějovice, 2021

Prohlášení

Prohlašuji, že svoji diplomovou práci na téma *Matematika v moderních šifrovacích metodách* jsem vypracovala samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to v nezkrácené podobě, elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích …… …….

Košáková

Poděkování

Tímto bych chtěla poděkovat prof. RNDr. Pavlu Tlustému, CSc. za odborné rady a připomínky během psaní této práce.

Anotace

V diplomové práci se zabývám tématem, které je v dnešním světě velice opomíjeným, přesto se s ním člověk setkává skoro každý den. Jedná se o problematiku matematiky v moderních šifrovacích metodách. Samotné šifrování je široká oblast, proto jsem se zaměřila na nejznámější moderní kryptosystémy. V práci jsou zpracovány jak kryptosystémy symetrické, asymetrické, tak i hybridní. Zájemci si mohou v diplomové práci přečíst o historii, vývoji, ale i výhodách a nevýhodách jednotlivých kryptosystémů. Větší pozornost je také věnována šifrování na bázi eliptických křivek, protože z hlediska matematiky je tato problematika zajímavá. Celá práce je rozdělena do několika důležitých kapitol pro přehlednost a lepší orientaci v textu. Na závěr jsem zařadila konkrétní ukázky praktického využití šifrování pro ucelený pohled čtenáře.

Klíčová slova

šifrování, eliptické křivky, logické operace, zbytek po dělení,

Annotation

In my diploma thesis I deal with a topic that is very neglected in today's world, yet one encounters it almost every day. This is a problem of mathematics in modern encryption methods. Encryption itself is a wide area, so I focused on the most famous modern cryptosystems. The work deals with symmetric, asymmetric and hybrid cryptosystems. Those interested can read in the diploma thesis about the history, development, but also the advantages and disadvantages of individual cryptosystems. Greater attention is also paid to encryption based on elliptic curves, because from the point of view of mathematics, this issue is interesting. The whole work is divided into several important chapters for clarity and better orientation in the text. In conclusion, I included specific examples of practical use of encryption for a comprehensive view of the reader.

Keywords

encryption, elliptic curves, logical operations, remainder after division

Obsah

Úvod

Utajování informací, zpráv i textů je záležitostí, která je stará jako samotné lidstvo. Během staletí se vyvíjelo jak lidstvo, tak i šifrování. V průběhu posledních dvou staletí se tato problematika začala rozvíjet rychlostí blesku. Vždyť prolomení různých šifer je v dnešní době pomocí počítačů, elektroniky a nejrůznějších matematických programů mnohonásobně jednodušší, než tomu bylo v minulosti, kdy se útoky realizovaly pouze ručně a kdy všechny výpočty trvaly delší čas. Každý v dnešním světě si chce udržet co možná největší ochranu svých osobních informací. Proto člověk vymyslel „moderní šifry“, aby byl zajištěn vyšší „stupeň“ ochrany a nedocházelo tak často k dešifrování. Moderní šifrování je dnes používáno i během každodenního života a mnohdy ani sami nevíme, kde se s ním můžeme potkat, ať už se jedná o peněžní převody mezi bankami, o online bankovnictví, o internet či o pouhou bezpečnou elektronickou poštu (email). Novodobá kryptografie představuje matematické algoritmy, ve kterých se skrývají, jak čísla, tak i algebraické elementy.

Tato práce je rozdělena do několika kapitol. V první kapitole si představíme, co je to šifrování, jaké jsou jeho výhody a nevýhody a další pojmy, které jsou s kryptografií spjaty.

Následuje kapitola týkající se matematických operací a jejich vlastností, které se velice často v kryptografii využívají.

Třetí kapitola se zabývá problematikou symetrického šifrování. Zde zdůrazníme jeho hlavní přínos, jeho výhody a nevýhody. Také představíme některé symetrické šifrovací systémy, mezi které můžeme zařadit AES, DES, RC4. Jejich důležité vlastnosti a principy šifrování si ukážeme přímo na konkrétních příkladech.

V další kapitole si můžete přečíst o oblasti kryptografie, která se zabývá asymetrickým šifrováním, které z velké části vychází z kryptografie symetrické. Jedním z hlavních rozdílů mezi asymetrickou a symetrickou kryptografií je počet klíčů, který se u nich využívá. V úvodu této kapitoly je podkapitola zabývající se jednosměrnou funkcí a Diffie-Hellmanovou výměnou klíčů. Další podkapitoly se věnují kryptosystému RSA i kryptosystému El-Gamala. Velké a zajímavé téma, které je součástí asymetrického šifrování, je problematika kryptosystému eliptických křivek. Šifrování pomocí

eliptických křivek existuje jak početně, tak i graficky. Zpracované grafy ke konkrétnímu příkladu jsou také součástí této práce.

V této práci se též nachází kapitola, která se věnuje hybridním kryptosystémům, ve kterých se prolínají vlastnosti symetrického i asymetrického šifrování.

Většina lidí se s kryptosystémy potkává každý den a mnohdy si ani neuvědomují jejich „výskyt“. Z toho důvodu bylo začleněno do poslední kapitoly využití šifrování v reálném každodenním životě, mezi které můžeme zařadit digitální podpis, autentizační protokol Kerberos, ale také platební protokol 3D Secure.

1. Úvod do kryptografie

Kryptografie (z řeckého kryptos – skrytý nebo tajný, gráphien – psát) je věda zabývající se šifrovacími postupy (Hanžl, 2007). Nebo lze říct, že *kryptografie je věda, která zkoumá matematické metody utajování obsahu i prokazování původu přenášených zpráv. Tou se přitom rozumí číselná posloupnost, ve které je veřejně známým kódem zakódována informace* (Burda, 2019). Dnes lze také kryptografii definovat jako vědu, *která se zabývá konstrukcí a aplikací matematických metod pro utajování obsahu a prokazování původu přenášení zpráv (*Burda, 2019). Další z definic kryptografie, kterou si zde uvedeme, je tato: „*Kryptografie je matematická disciplína zabývající se šifrování – převodem zpráv do/z utajené podoby, která je čitelná jen se znalostí šifrovacího klíče“* (Stroukal, 2018). Vondruška ve své knize *Kryptografie, šifrování a tajná písma* z roku 2006 píše: „*Kryptografie se zabývá matematickými metodami se vztahem k takovým prvkům informační bezpečnosti, jako je zajištění důvěrnosti zprávy, integrity dat (neporušenosti), autentizace entit (ověření subjektu) a původ dat (vlastnictví) – včetně zkoumání jejich silných stránek a slabin i odolnosti vůči různým metodám útoků.“*

Kryptografie primárně vznikla k ochraně zpráv během jejich přenosu. V praxi se ukázalo, že *pomocí kryptograficky chráněných zpráv lze velmi efektivně zajistit vysokou úroveň bezpečnosti dalších systémů, například systému řízení přístupu, systémů elektronických plateb atd.* (Burda, 2019). S kryptografií se setkává každý člověk každý den, aniž by si to uvědomil.

V praxi se zpravidla jedná o texty, obrázky i příkazy v podobě posloupnosti dvojkových číslic, tj. bitů (Burda, 2019). Ty mají vždy podobu nul a jedniček, tj. podobu ve dvojkové soustavě. První zmínky o dvojkové soustavě pocházejí od čínského císaře a filozofa Fu-si, který žil 4000 let před německým filozofem a matematikem Gottfriedem Wilhelmem von Leibnizem. Ten o tomto faktu píše v jedné ze svých pracích, která se nazývá *Explication de l´Arithmétique* publikována v roce 1703. Slovo bit jako nejmenší informační jednotka bylo poprvé použito v roce 1948 v článku *A Mathematical Theory of Communication*. Tento článek napsal americký elektronik a matematik Claude Elwood Shannon v časopise *Bell System Technical Journal*. Shannon toto slovo připisuje americkému matematikovi, který se jmenoval John Wilder Tukey a který použil bit jako zkratku dvou slov „binary digit“ v Bellově laboratoři 9. ledna 1947.

Hlavním cílem kryptografie je co nejlépe danou zprávu utajit, čímž vzniká zašifrovaná zpráva. Šifrování je tedy proces k utajení dané informace s pomocí předem připravených pravidel. *Zašifrovaný text je zpráva, která putuje po komunikačním médiu* (Hanžl, 2007), který po přečtení nemusí dávat smysl. Tak to vidí ten, kdo nemá právo daný text rozšifrovat a vidět jeho obsah ve správné formě. Zpravidla se jedná o útočníka. *Útočník je neoprávněná osoba, která může přenosy zpráv buď odposlouchávat (tzv. pasivní útočník), nebo je může modifikovat (tzv. aktivní útočník)* (Burda, 2015).

Informaci, kterou je nutno nějakým způsobem zabezpečit, většinou označujeme jako otevřený text, proces zabezpečování zprávy pak jako šifrování. Zabezpečený otevřený text se stává šifrovaných textem neboli kryptogramem a sada pravidel použitých pro šifrování otevřeného textu se nazývá šifrovacím algoritmem. Operace tohoto algoritmu se běžně odvíjejí od šifrovacího klíče, který společně s textem zprávy představuje vstupní informace pro algoritmus. Chce-li příjemce z kryptogramu obdržet původní zprávu, musí použít dešifrovací algoritmus, který ve spojení s dešifrovacím klíčem převede zašifrovaný text na původní otevřený text (Piper, 2006).

Základním prvkem, který je nutné znát pro šifrování dané zprávy, je správný „typ“ abecedy. Nejpoužívanější je klasická anglická abeceda, která obsahuje 26 písmen. Tato abeceda je také označovaná jako mezinárodní a nevyužívá diakritiku. Při šifrování můžeme používat i jiné druhy abecedy, například rozšířenou anglickou abecedu o české písmeno „ch“, nebo anglickou abecedu, která spojuje písmena „i“ a „j“ pod jeden šifrovací kód, neboť „j“ se v angličtině velice málo používá. Pokud by se jednalo o českou abecedu, tak by bylo výhodné spojit písmena „v“ a „w“, ale z důvodu, aby nedošlo ke zmatkům, se zaměňuje i v české abecedě „i“ za „j“. Poslední variantou je volba plné české abecedy, která obsahuje 42 znaků.

Jako **kryptografický protokol** je označována zabezpečená komunikace mezi původcem a adresátem. Základ, který tvoří daný kryptografický protokol, je datová jednotka, tj. *blok bitů, které si mezi sebou původce s adresátem vyměňují* (Burda, 2019). Existuje více typů kryptografických protokolů jak jednostranný, tak i vícestranný. V praxi se s vícestranným kryptografickým protokolem setkáme u platebního protokolu jak na straně plátce, tak i na straně příjemce.

Pokud je daný text zašifrovaný, musíme ho umět i rozšifrovat. Občas se říká, že daný text musí být schopný příjemce dešifrovat. Ale dešifrováním se jeví proces, který není shodný s procesem rozšifrování. **Rozšifrování** je *proces zpětného použití šifry vůči zašifrovanému textu, kterou provádí zákonný uživatel znající klíč* (Bezpalec, 2015). Ale **dešifrování** je pouhý pokus o přečtení zašifrovaného textu bez znalosti klíče. Během samotného dešifrování dochází k prolomení šifrovaného textu nebo šifry. Avšak často dochází k nerozdělování těchto dvou pojmů. K odhalení správné podoby textu v podobě odkrytého textu musíme použít seznam pravidel, která jsou spojena s daným typem šifrování.

Hlavní role kryptografie je přenos utajených zpráv. Také lze říct, že její povinností je udržení dané zprávy v utajení. Nejtypičtější je utajování v komerčním, státním a lékařském světě.

Ve světě existuje několik způsobů klasifikace šifer, jedním z nich je rozlišení na blokové a proudové šifry.

Bloková šifra je typ šifrování, ve kterém šifrování probíhá v blocích, protože mají stejnou délku. Velikost bloku se pohybuje mezi 64 až 256 bity. Textové zprávy se upravují a transformují na bloky pomocí daného klíče. U této transformace existují principy, jak má správně probíhat. Jedná se o difuzi a o zmatek. Difuze odráží to, jak jednotlivé bity vstupu pronikají do jednotlivých bitů výstupu. Další vlastností blokové šifry je úplnost, což je stav, kdy každý bit výstupu závisí na každém bitu vstupu. Blokové šifry jsou velice podobné v šifrování a rozšifrování, ale liší se pouze v postupu realizace. Kvalitní *n*-bitové blokové šifry se také mohou jevit jako náhodné permutace na množině n-bitových bloků. Z teoreticko-informačního hlediska postačuje k luštění několik dvojic vstupních a výstupních bitů. Z praktického hlediska je bráněno právě složitostí výpočtu. Jako praktický přiklad blokové šifry si můžeme uvést kryptosystém DES.

Druhým typem šifrování je **proudová** neboli **toková šifra**. Ta pracuje s bitovými, ale i bytovými proudy otevřeného textu, který se promění na speciální šifrovaný znak většinou za využití operace XOR (viz matematické logické operace). Tento znak je ale závislý na použitém klíči, ale také na umístění v textu. Generátor proudu klíčů vytváří bitový proud, který je podobný náhodnému, ale ve skutečnosti je determinován a může být obnoven při rozšifrování. Čím blíže je výstup z generátoru

proudu klíčů k náhodnému, tím kryptoanalytikovi zabere více času k prolomení dané šifry. Blokové šifry se využívají k přenosu proudů informací a jsou též vhodné pro šifrování nepřetržitých proudů dat, mezi které se například řadí hovor či video. Proudové šifry nejsou tak náročné jako blokové šifry a jsou mnohem rychlejší. Jejich hlavní nevýhodou je častější „prolomení“ (dešifrování) při špatné implementaci (realizaci). Nejjednodušší varianta proudové šifry je tzv. skramblování, které spočívá v bitové změně proudu dat, které procházejí skrz daný systém. Ve skramblování se nejčastěji používá XOR (viz matematické logické operace). Každý bit výstupní posloupnosti je závislý na jednom vstupním bitu, a to je spojeno se vznikajícími poruchami v přenosovém kanálu. Na základě skramblování dochází k těmto dvěma zásadním problémům, kterými jsou synchronizace a zacyklení, jež vznikají při její dlouhé činnosti.

2. Matematika v šifrování

Matematika se využívá v mnoha oblastech našeho života a je také nedílnou součástí kryptografie. Mezi základní operace využívané v kryptologii patří: logické operace, operace modulo, substituce a rotace. Tyto operace se v kryptografii používají samostatně, ale častěji se mohou kombinovat mezi sebou. Nyní se na některé z nich podrobněji zaměříme a také na pojmy s nimi spojené, které jsou důležité v procesech kryptografie.

2.1. Logické operace

*Logické operace jsou operace s bity, tj. s proměnnými, které mohou nabývat **POUZE** hodnot nula a jedna. V kryptografii jsou nejčastější negace, disjunkce (logický součet), exkluzivní disjunkce a konjunkce (logický součin)* (Burda, 2015).

Logické operace jsou definovány pomocí pravdivostní tabulky, která udává hodnotu logické funkce pro každou možnou kombinaci hodnot jejích argumentů.

Negace je operace s jedním operandem neboli s jednou proměnnou a značí se ¬. Její hodnoty jsou zaznamenány v tabulce 1:

Tabulka 1: Pravdivostní tabulka negace

A	$\neg A$
1	0
0	1

Ostatní zmíněné operace – jedná se o **disjunkci** (značenou ∨), **exkluzivní disjunkce** (označovaná také jako xorování a značená ⊕) a **konjunkce** (značená ∧) – mají již dva operandy. Tyto operace nabývají také hodnot nula a jedna. Jejich výstup si ukážeme v následující pravdivostní tabulce 2:

Tabulka 2: Pravdivostní tabulka pro disjunkci, exkluzivní disjunkci a konjunkci

A	B	$A \vee B$	$A \oplus B$	$A \wedge B$
1	1	1	0	1
1	0	1	1	0
0	1	1	1	0
0	0	0	0	0

Tabulka 2 nám říká, že výrok $A \vee B$ (**disjunkce** neboli **logický součet**) je pravdivý, pokud alespoň jeden z výroků A a B je pravdivý. Jelikož chceme, aby alespoň jeden výrok byl roven jedničce. **Exkluzivní disjunkce** $A \oplus B$ bude pravdivá, bude-li pravdivý pouze jeden výrok, buď výrok A, nebo výrok B. Pro **konjunkci** neboli **logický součin** platí následující definice, výrok $A \wedge B$ je pravdivý právě tehdy, když jsou pravdivé oba výroky, jak výrok A, tak i výrok B.

V kryptografii jsou také důležité *n*-tice bitů, kdy osmice bitů je označována jako **byte.** Tento pojem zavedl německo-americký počítačový specialista Werner Buchholz na konci roku 1956. I výše uvedené matematické logické operace v pravdivostní tabulce lze napsat do uspořádané *n*-tice.

Pro bloky bitů je definována také operace **zřetězení** (symbolicky označována ‖). Také lze zřetězení označit jako operaci, během které dochází ke spojení textových řetězců jednoho k druhému. Zřetězením ze dvou bitových bloků A a B vytvoříme blok C. První část bloku C se sestává z bloku A a druhá část z bloku C tvoří blok B. Zřetězení lze použít i na zřetězení jiných symbolů, než jsou nuly a jedničky, může se jednat i o slova či symboly. Na příkladu uvádíme, jak operace zřetězení funguje: $A = (1, 1),\ B = (0, 1, 1, 0)$. Pak $C = (1, 1, 0, 1, 1, 0)$.

2.2. Operace modulo

Operace modulo *n* se také nazývá zbytek po dělení. Zbytek po dělení lze definovat takto: *Nechť* $a, b > 0$ *jsou celá čísla. Pak existují* $q \in \mathbb{Z}\ a\ r \in \{0, 1, \dots, b-1\}$ *tak, že platí* $a = bq + r, 0 \leq r < b$ (Tlustý, 2006), kde *a* je dělenec, *b* je dělitel, *q* je celočíselná část podílu a *r* je zbytek po dělení.

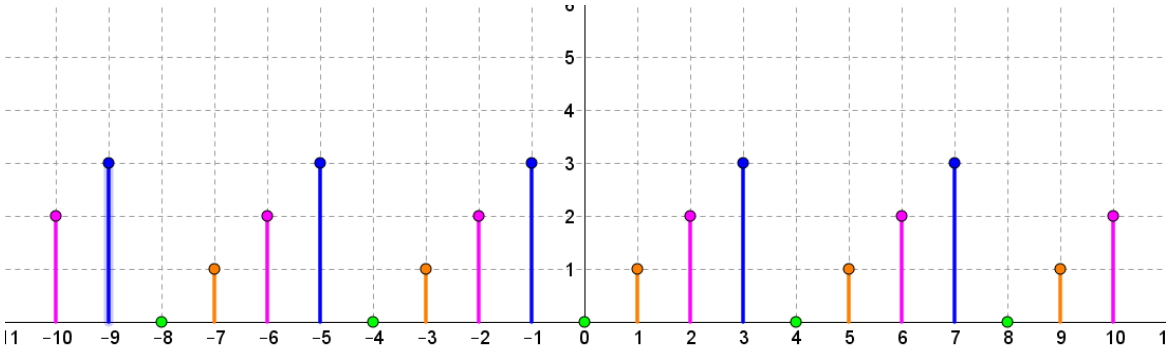
Toto nebylo praktické pro velká čísla, proto lze použít pro operaci zbytek po dělení jinou operaci, kterou je právě operace označována jako operace modulo. Její definice nám říká to samé, jako rovnice $a = bq + r$.

Operace modulo má oproti zbytku po dělení výhodu, kterou je formální zápis, který definuje jak samotnou operaci, tak i všechny další okolnosti, za kterých lze operaci provádět.

Pro operaci *modulo n* platí také následující pravidla: Nechť $x, y, \in \mathbb{Z} - \{0\}, n \in \mathbb{N}$ a pokud platí $D(y, n) = 1$, má operace modulo následující vlastnosti:

- $(x + y)\ mod(n) = [x\ mod\ (n) + y\ mod\ (n)]\ mod\ (n)$,
- $(-x)\ mod\ (n) = (n - x)\ mod\ (n) = n - x\ mod\ (n)$,
- $(x \cdot y)\ mod\ (n) = [x\ mod\ (n) \cdot y\ mod\ (n)]\ mod\ (n)$.

Další zajímavou vlastností operace modulo *n* je rozklad množiny všech celých čísel na tzv. zbytkové třídy. Jedná se o disjunktní množiny čísel a jednotlivé prvky v dané množině budou mít stejný zbytek po dělení daným přirozeným číslem, například číslem 4. Tuto vlastnost si ukážeme na množině celých čísel na intervalu $\langle -10; 10 \rangle$ na následujícím grafu na obrázku 1:



Obrázek 1: Zbytkové třídy po dělení číslem 4 (zdroj: autorka)

Sčítání $modulo\ 2$ pro čísla z množiny $\{0, 1\}$ je ekvivalentní s xorováním. Tuto skutečnost shrneme v tabulce 3:

Tabulka 3: Ekvivalence xorování a sčítání modulo 2 (zdroj: Burda, 2013)

A	B	$A \oplus B$	$(A + B)\ mod\ 2$
1	1	0	$(1 + 1)\ mod\ 2 = 2\ mod\ 2 = 0$
1	0	1	$(1 + 0)\ mod\ 2 = 1\ mod\ 2 = 1$
0	1	1	$(0 + 1)\ mod\ 2 = 1\ mod\ 2 = 1$
0	0	0	$(0 + 0)\ mod\ 2 = 0\ mod\ 2 = 0$

2.3. Permutace

Další operací, se kterou se v této kapitole seznámíme, je permutace. *Permutace je bloková operace, kde vstupem je blok bitů* $V = (v_1, v_2, \dots, v_n)$ *a výstupem je blok bitů* $W = (w_1, w_2, \dots, w_n)$. *Permutace přiřazuje j-tému bitu výstupního bloku hodnotu i-tého bitu vstupního bloku. Přiřazení je dáno pomocí n-tice*

$$P = (p_1,\ p_2, \dots, p_n),$$

kde p_n *je pořadové číslu bitu vstupního bloku, který má být zapsán na n-tou pozici výstupního bloku* (Burda, 2013).

Speciálním typem permutace je rotace a existují dva typy, tj. rotace vlevo nebo rotace vpravo o *k* bitů, *přičemž pro proměnnou k platí, že* $1 \leq k < n$.

2.4. Substituce

Tato operace vstupnímu číslu *x* přiřazuje podle určitého pravidla, nebo tabulky jiné číslo $y = S(x)$. Příklad substituce si nyní ukážeme na následující tabulce 4:

Tabulka 4: Příklad substituční tabulky (zdroj: autorka)

x	0	1	2	3	4	5	6	7	8	9	10
y	5	8	10	7	9	3	0	4	2	6	1

2.5. Algebraická struktura

Následující matematický pojem, který si přiblížíme podrobněji, je algebraická struktura. *Algebraická struktura je množina prvků, na které jsou definovány jedna nebo více binárních operací, přičemž uvedená množina je vzhledem k definovaným operacím uzavřená. Uzavřeností se rozumí, že výsledkem operace s libovolnými prvky dané množiny je vždy také prvek této množiny* (Burda, 2013).

V šifrování se setkáváme s některými typy algebraických struktur s jednou nebo dvěma binárními operacemi. V případě jedné operace jde nejčastěji o grupy. Z algebraických struktur se dvěma binárními operacemi pracujeme obvykle s Galoisovými tělesy.

Galoisovo těleso je algebraická struktura tvořená konečnou množinou T s operacemi sčítání a násobení, kdy všechny prvky a, b, c z množiny T splňují následující podmínky.

Pro operaci sčítání platí:

- algebraická struktura je vůči sčítání uzavřená: $(a + b) \in T$,
- asociativní zákon: $(a + b) + c = a + (b + c)$,
- komutativní zákon: $a + b = b + a$,
- existuje neutrální prvek $0 \in T$, kdy pro každé $a \in T$ platí: $a + 0 = a$.

Pro operaci násobení platí:

- algebraická struktura je vůči násobení uzavřená $(a \cdot b) \in T$,
- asociativní zákon: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- komutativní zákon: $a \cdot b = b \cdot a$,
- distributivní zákon: $a \cdot (b + c) = a \cdot b + a \cdot c$,
- existuje neutrální prvek $1 \in T$, kdy pro každé $a \in T$ platí: $a \cdot 1 = a$,
- pro každé $a \neq 0 \in T$ existuje inverzní prvek a^{-1}, kdy platí $a \cdot a^{-1} = 1$.

3. Symetrické šifrování

Dnes se člověk setkává se šifrováním každý den, přestože si to ani neuvědomuje, že používá šifry. Ke komunikaci s úřady nebo k získání informací z webových stránek využívá například symetrické šifrování, které zajišťuje, že zprávy budou bezpečně předávány jen mezi správným odesílatelem a příjemcem.

Symetrické šifrování je šifrování, které využívá pouze soukromého neboli privátního klíče. Ten znají jak odesílatel, tak i příjemce dané zprávy a musejí ho držet v bezpečí. Přenos informace je proveden ve třech dílčích krocích, které lze takto shrnout: *odesílatel a příjemce se nejprve domluví na klíči (tedy na sekvenci znaků), odesílatel zprávu zašifruje, zašle ji příjemci a ten ji přijme a rozšifruje.* (https://www.napocitaci.cz/33/symetricke-a-asymetricke-sifrovani-uniqueidgOkE4NvrWuNY54vrLeM677jX7sp3Lu-ZpLpGVMy1prA/, 7. 7. 2020) *Symetrická šifra je taková šifra, kde pro každé k, které náleží poli K, lze z transformace zašifrování E_k určit transformaci rozšifrování D_k a naopak* (Klíma, 2007).

Kryptografické symetrické algoritmy se obvykle vytvářejí pomocí jednoduchých a rychle proveditelných příkazů několika typů. Jednou z jejich hlavních nevýhod je nutná domluva obou stran (odesílatele a příjemce) na jednom totožném klíči. Délka klíče je též rozhodující. Pokud klíč prodloužíme o pouhý jeden bit, je větší pravděpodobnost, že klíč je bezpečnější, ale nemusí to platit na sto procent. Klíč lze měnit u každé zprávy, kdy před jejím posláním je vygenerován nový klíč. Takovýto klíč se nazývá „klíč sezení“. Je to bezpečnější verze, neboť hacker prolomí heslo jen na jednu zprávu již poslanou, a ne na všechny. Pokud bude člověk chtít komunikovat s více lidmi, tak bude potřebovat tolik klíčů, kolik bude příjemců, aby s každým komunikoval pomocí jiného privátního klíče.

Výhodou symetrického šifrování je výpočetní nenáročnost, a tím související rychlost šifrování a opětovného rozšifrování. Také u něho najdeme i nevýhody, mezi které můžeme zařadit nutnost domluvy na jednotném klíči, který nemůže být zaslán v nezašifrované komunikaci, neboť by útočník, tj. třetí nepovolaná osoba, mohla dešifrovat nejenom jednu z poslaných zpráv.

Použití symetrických algoritmů představuje způsob, jak zabezpečit důvěrnost transakcí definovaným způsobem s možností přesného stanovení hrozeb, kterým toto zabezpečení odolává. Stěžejní nevýhodou je obtížná distribuce šifrovacích klíčů v rozsáhlých sítích

(počet klíčů roste se čtvercem počtu uživatelů) a jejich složitá logistika (Budiš, 2008). Tyto techniky jsou dnes využívány také v komplexnějších programech. Například můžeme uvést webový prohlížeč či komunikaci s klientem během online služeb.

Mezi nejznámější druhy symetrického šifrování můžeme zařadit kryptosystémy AES, RC4, DES, Akelarre, Anubis, Blowfish a další. Ve světě jsou tyto kryptosystémy nejčastěji používány, a proto jim budeme věnovat větší pozornost v dalších podkapitolách.

3.1. AES

Nejběžnější technikou symetrického šifrování je AES *(= Advanced Encryption Standard*). Můžeme ji též zařadit mezi blokové šifry a v překladu název znamená pokročilý šifrovací standard. Tato *moderní bloková šifra byla původně určená pro státní správu USA, avšak v současné době je celosvětovým de facto standardem* (Burda, 2015). Původní název algoritmu AES zní *Rijndael* a je odvozen ze jmen dvou belgických autorů Vincenta Rijmena a Joana Daelmena. Ti svoji šifru přihlásili na veřejnou soutěž o federálním šifrovacím algoritmu pořádanou Národním institutem standardů a technologie (známou též jako NIST) v lednu 1998. Po pěti letech byla šifra vybrána jako nejvhodnějších z 15 návrhů a dne 26. listopadu 2001 byla schválena Národním úřadem pro standardizaci. Jako federální standard USA začala být využívána dne 26. května 2002. Soutěž vznikla jako reakce na prolomení šifrovacího algoritmu DES. Základy této šifry jsou použity z šifrovacího standardu DES, s tím že tato funkce podporuje obvykle tři stanovené délky klíčů, tj. 128, 192 a 256 bitů.

Tento šifrovací standart se velice liší od šifrovacího kryptosystému DES, ale ve skutečnosti vychází právě ze starých teoretických principů, které byly využívány u kryptosystému DES a během svých 25 let, kdy byl používán, nebyly nikdy principy zpochybněny, a to je jedna z bezpečnostních záruk daného standardu. Druhou zárukou je délka klíčů, neboť podporuje tři klíče o různých délkách, tj. o délkách 128, 192 a 256 bitů.

Data jsou šifrována vícestupňovým postupem, pomocí určitých nástrojů. V případě délky 128 bitů data projdou daným mechanismem desetkrát. Prvním krokem je tzv. **expanze**

AES klíče. Probíhá před samotným šifrováním a rozšifrováním. V této části algoritmus z původního 128bitového AES klíče vypočítá 11 kol klíčů, které jsou také 128 bitů **dlouhé a které se nazývají rundovní klíče**. Počet interakcí závisí na velikosti klíče. V následujícím kroku AES spojí bloky dat bit po bitu (pomocí XOR) s prvním klíčem. Nahrazené byte je označení další etapy, kdy je každý byte nahrazen bytem z tzn. pevně vyhledávací tabulky, která se též označuje jako S-box (je to zkratka tzn. substitučního boxu). Po provedení substituce dojde k cyklickému posouvání byte směrem doleva kromě prvního řádku, který zůstává stejný. Po této záměně dojde k předposlednímu kroku k tzv. míchání sloupců. Kryptosystém AES spočítá ze sloupců a řádků v „pevné" matici nové hodnoty buněk. V některé literatuře je tato část označena jako maticové násobení. V posledním kole je tento krok vynechán. Proces pokračuje přidáním klíče, ve kterém je použit příslušný klíč a data jsou bit po bitu změněna. Toto bude probíhat do té doby, než budou vyčerpány všechny klíče, tj. všech jedenáct klíčů. Na konec kryptosystém AES „položí" zašifrovaný blok znovu k textu. Při rozšifrování se provádí ten samý postup, ale v opačném pořadí.

Šifra AES na rozdíl od většiny starších algoritmů nepracuje s jednorozměrnými bloky, nýbrž s dvourozměrnými bloky (maticemi.) Ústřední datovou jednotkou šifry je matice formátu 4×4 byte, kterou budeme nazývat stavovou maticí. Pro stavovou matici jsou definovány čtyři transformace, tj. substituce byte („SubBytes"), rotace řádků („ShiftRows"), substituce sloupců („MixColumns") a přičtení iteračního klíče („AddRoundKey") (Burda, 2013). **Tato matice se nazývá vnitřní stavba šifry.**

K rozšifrování kryptosystému AES postačí prosté zobrazení, ke kterému existuje inverzní operace. V závislosti na velikosti klíče ho můžeme označovat jako AES-128, AES-192, AES-256. Čísla označují velikost klíče v bitech. Rozšifrování klíče se skládá ze dvou etap.

Tento šifrovací algoritmus vytlačil používanou šifru DES, o které se dozvíte níže, *neboť se jedná o moderní blokovou šifru, která přináší na kryptografii nové pohledy. Inovační je zejména použití dvourozměrných bloků (matice, která dovoluje dosáhnout plnou difuzi a konfuzi relativně nízkých počtem iterací)* (Burda, 2013).

Kryptoanalýza tohoto šifrovacího systému prozatím nevedla k potvrzenému prolomení šifry. Dlužno podotknout, že některé známé typy kryptoanalytických útoků prověřovali autoři algoritmu Rijndael již při jeho návrhu (Jiroušek, 2006).

V dnešní době se tento algoritmus využívá například pro bezdrátové Wi-Fi sítě v rámci zabezpečení WPA2, který byl schválený 24. června 2004. V roce 2018 Wi-Fi Aliance ohlásila, že vydala WPA3 s několika vylepšeními oproti WPA2.

3.2. RC4

Mezi symetrické kryptosystémy také můžeme zařadit RC4 (= Rivest Cipher 4). Jedná se o proudovou symetrickou šifru. Navrhl ji americký kryptograf a matematik Ronald L. Rivest roku 1987. Zdrojový kód byl nejdříve tajný a podléhal ochranné známce.

Postup algoritmu má tři části, které jsou S-box, KSA fáze a PRGA fáze S-box. S-box je pole, které má délku 256 byte s celými čísly vzestupně seřazenými do čísla 255 a hodnota indexu prvku pole bude rovna hodnotě prvku. Druhá část se nazývá KSA fáze, ve které dojde k proházení prvků v poli a poté se k nim přiřadí dané byte z klíče. Jedná se o permutaci, která proběhne dle byte klíče. PRGA fáze nám generuje keystream, který má velikou periodu opakování a měl by teoreticky mít mnoho kombinací jako skutečný náhodný číslicový generátor. KSA a PRGA jsou velice podobné kódy, které se liší v počtu generování keystreamu. Potom zašifrovat a rozšifrovat text je velice jednoduché za použití XOR keystreamu.

Toto je jednoduchá a rychlá šifra, ale má také své nevýhody. V dnešní době již není bezpečná.

Tento proces je bezpečný pouze při jednom použití, nikoliv při opakovaném použití. Problém je ten, že přenosem se také přenáší i klíč. Doba výpočtu pro odvození potřebného klíče je velice krátká, pokud se k tomu použije správný nástroj – například Aircrack.

3.3. DES

Dalším symetrickým kryptosystémem, který je v odborné veřejnosti dobře znám, je kryptosystémů DES. Bloková šifra DES (= Data Encryption Standart) je označení pro pojmenování standardu. Samotný algoritmus je označován jako DEA (=Data Encryption Algorithm). Jde o nejvíce rozšířený algoritmus symetrického šifrování. *Teoreticky tuto myšlenku formuloval již* americký elektronik a matematik *Claude Elwood Shannon (1916-2001) a dále ji rozpracovat Feistel při vytváření kryptosystému LUCIFER firmy IBM* (Jiroušek, 2006). V roce 1977 se stala tato bloková šifra standardem pro bezpečnost NBS (=National Bureau of Standards), později NIST (= National Institute of Standard and Technology). Původní využití šifry DES bylo pro aplikace v oblasti finančnictví.

DES je symetrická bloková šifra s blokem o velikosti 64 bitů. Klíč má délku 56 bitů (+ 8 paritních bitů). Algoritmus se postupně začal využívat na celém světě a stal se jednoznačně nejznámějším a nejpoužívanějším symetrickým blokovým algoritmem. (Vondruška, 2006) *DES poté redukuje výsledný R-blok na 32 bitů a spojí ho bit po bitu s L-blokem. Tento princip se opakuje šestnáctkrát* (Müller, 2009). Moderní technologie se vyvíjejí velice rychlým tempem, a proto už v roce 1995 se na veřejnost dostává informace, že NSA vlastní stroj, který sestrojila firma The Harris Corporation a který je schopný vyluštění kryptosystému DES za pouhou čtvrt hodinu. Tento kryptosystém DES byl považován za bezpečný až do 17.7.1998, kdy superpočítač „Deep Crack“ v ceně cca 130 000 USD jako první hrubou silou „cracknul“ („prolomil“) DES klíč za pouhých 56 hodin. Ve světě jsou známy i další způsoby prolomení tohoto kryptosystému.

Proto byl vyvinut 3DES (čili trojitý DES), který používá tři 56 bitové klíče a který se nyní používá například pro on-line bankovnictví. Tyto tři klíče šifrují bloky dat jeden po druhém, a navíc druhý klíč používá algoritmus obráceně (jakési dekódování). Tento postup se nazývá EDE (Encrypt-Decrypt-Encrypt) (Müller, 2009).

Kryptosystém DES zajišťuje 4 běžné pracovní režimy označené těmito zkratkami: ECB, CBC, CFB, OFB.

Pracovní režim ECB (Electronic Codebook) je nejjednodušší a základní režim a z hlediska chybovosti jednoho souboru nemá vliv na chybné rozšifrování u jiných souborů. Také se může používat pro zabezpečení, pokud bude zajištěna jeho dlouhodobá

jedinečnost bloků, které budou šifrovány stejným klíčem. Tento režim se však v moderní kryptografii prakticky skoro vůbec nepoužívá.

Druhý pracovní režim nese zkratku CBC (= Cipher Block Chaining) a lze ho přeložit jako řetězení šifrovaných bloků. Jak již název napovídá, bude zde šifrování jednoho souboru záviset na souboru, který bude spočívat na jejich předcházejících souborech. Nevýhodou pracovního režimu CBC je, že šifrovaný blok je závislý na všech předcházejících blocích. Při poškození šifrovaného bloku nelze rozšifrovat ani blok, který je přímo následující.

Pracovní režim CFB (= Cipher FeedBack) neboli šifrová zpětná vazba je proces, který je velice podobný předcházejícímu pracovnímu režimu, až na pořadí operací.

Čtvrtou a poslední je pracovní režim OFB (= Output FeedBack) neboli výstupní zpětná vazba, která převádí blokovou šifru na šifru proudovou.

Hlavní kritika DES se od počátku týkala příliš krátkého klíče (Jiroušek, 2006). Neboť již tvůrcům unikla vlastnost komplementarity a tím se velice zúžila, a to až na svou polovinu. Prolomitelnost klíče je potvrzena již od dvou amerických matematiků z roku 1975. V roce 1977 zavedla americká vláda tuto šifru, která je založena na Luciferově algoritmu, jako první veřejný standard pro symetrické šifrování.

Je známo, že existují útoky na kryptosystém DES tzv. hrubou silou. Zároveň ve světě bylo publikováno několik kryptoanalytických metod, které jsou založeny na rozboru slabých míst tohoto šifrovacího algoritmu. Spory o jeho odolnosti se vedou již od let, kdy byl tento algoritmus přijat ve standardu. Podrobné popsání těchto diskusí je možné si přečíst v mnoha pracích, které se týkají kryptografie. Později bylo jasné, že všechny tyto zápory vedou k jedné jediné věci, a to k velikosti klíče. Toto se jevilo jako největší slabina algoritmu DES, a proto na něj byly uskutečněny útoky. Slabina byla zřejmá až v devadesátých letech minulého století.

3.4. Akelarre

Následující symetrický kryptosystém, na který se zaměříme, je Akelarre.

Algoritmus Akelarre je bloková šifra, která byla vypracována kolektivem španělských kryptografů v roce 1996, ale ihned o rok později holandský kryptograf Niels T. Ferguson a americký odborník na kryptografii Bruce Schneier popsali útok na Akelarre. Další útok na tento algoritmus provedl dánský kryptograf Lars Ramkilde Knudsen a Vincent Rijmen. Vývojáři přepracovali původní kryptosystém Akelarre, avšak nová verze z roku 1997 byla také velice slabá.

Tento algoritmus v sobě představuje dva již známé algoritmy, tj. IDEA a RC5. Šifruje text v blocích o 128 bitech.

Struktura algoritmu je vcelku podobná struktuře algoritmu IDEA. Rozdíl je v tom, že v každém kole používá 32 bitů 16bitového slova, ale IDEA má šifrovací blok o velikosti 128 bitů ve čtyřech subblocích.

3.5. Anubis

Další blokovou šifrou, která je z roku 2000 je Anubis. Byla speciálně vytvořena na soutěž NESSIE. Vymyslel ji belgický kryptograf Vincent Rijmen a brazilský kryptograf Paulo Sérgio Licciardi Messeder Barreto. Šifra byla pojmenována na počest egyptské boha smrti Anubise. Tato šifra nebyla zahrnuta do konečného portfolia soutěže NESSIE, není ani patentována a je určena pro bezplatné veřejné použití.

Kryptosystém Anubis šifruje po 128 bitech s použitím klíče, který může mít velikost od 128 do 320 bitů.

Tento algoritmus pokračuje v řadě algoritmů, na kterých se podílel Vincent Rijmen, který již na svém kontě má šifrovací systémy Square, SHARK a Rijndael. Všechny tyto algoritmy spojuje jejich struktura čtvercového typu s velmi podobnou sadou provedených transformací.

Algoritmus Anubis představuje blok šifrovaných dat ve formě 16bitového pole, které je pro usnadnění popisu reprezentováno jako čtverec. V každém kole algoritmu jsou prováděny typické kroky.

Na soutěži NESSIE bylo zveřejněno několik verzí algoritmu Anubis, ale rozdíly byly v zápisu jedné z operací, která se v tomto kryptosystému využívá. Byl také považován jako nejrychleji pracující algoritmus. Jeden z problémů tohoto algoritmu byla totožnost s algoritmem Rijndael, který byl již znám a který byl stanoven jako nový standard šifrování USA pod názvem AES a který též byl účastníkem této soutěže. Experti soutěže se rozhodli kryptosystém Anubis neposlat do druhé etapy této soutěže.

3.6. Blowfish

Ve 20. století byl vymyšlen další algoritmus, který byl nazván Blowfish. Tento algoritmus byl vypracován v roce 1994 americkým kryptografem Brucem Schneierem. Ten ho navrhl jako náhradu místo již známého standardu DES, z důvodu jeho krátkého klíče, který mohl být již v této době prolomitelný. Podle kryptografa Schneiera nebyly žádní jiní kandidáti jako náhrada místo standardu DES z těchto důvodů:

- mnoho algoritmů, které jsou již známy, jsou patentovány a jsou tím pádem omezené ve svém využití,
- podle Schneiera není algoritmus „Gost 28147-89“ popsán úplně, neboť neobsahuje hodnoty tabulek náhrad,
- algoritmus Skipjack byl ještě v této době tajný.

Kryptosystém Blowfish byl velice široce realizován v různých šifrovacích prostředcích. O všech jeho využitích se můžeme dočíst na webových stránkách samotného autora, kde je uvedeno okolo 150 typů využití tohoto kryptosystému.

Svou strukturou je v principu velice podobný kryptosystému DES, ale šifruje v 64bitových blocích. Velikost klíče je v rozmezí mezi 32 až 448 bity.

Jednou z výhod kryptosystému Blowfish je velká rychlost šifrování, pokud se pomocí jednoho klíče šifruje soubor o větším množství dat. Pokud se však mění klíč po každém šifrování, je jeho rychlost katastroficky nízká. Tento kryptosystém se nedoporučuje používat v „smart kartách“.

3.7. Další symetrické kryptosystémy

Následující symetrické kryptosystémy nejsou tak známé, významné a detailně popsané.

Kryptosystém **Twofish** je symetrická bloková šifra o délce 128 bitů, která vznikla v roce 1995. Za jejího autora je považován především americký kryptograf Bruce Schneier, přestože byla vyvinuta kolektivem šesti Američanů, z nichž čtyři byli pracovníci firmy Conterpane Systems Bruce Schneiera. Tato symetrická šifra je nepatentovaná, ale je volně k dispozici.

Jako další symetrické kryptosystémy můžeme uvést algoritmy **Bear**, **Lion** a **Lioness**. Všechny tři algoritmy vymyslel známý kryptograf a profesor univerzity v Cambridgi Ross John Anderson spolu s izraelským kryptografem Elim Bihamem. Algoritmus Bear je kombinací dvou kryptografických funkcí, tj. hash funkce a generátoru posloupností.

4. Šifrování s veřejným klíčem (= asymetrické šifrování)

Člověk se nikdy nespokojí jen s jedním řešením, proto se neomezí pouze na jeden typ šifrování. Tak vymýšlel další typy a druhy kryptografie, které byly lepší, vyspělejší a bezpečnější, proto se v této kapitole zaměříme na šifrování, které se označuje jako šifrování s veřejným klíčem neboli asymetrické šifrování. Tento typ šifrování má tři fáze: generace klíče, šifrování a rozšifrování. Šifrování s veřejným klíčem se ale liší od šifrování symetrického, tzn. bez veřejného klíče tím, že nevyužívá pouze jeden klíč, ale klíče dva, tj. klíč soukromý a klíč veřejný. Tyto klíče jsou rozdílné a odlišují se. Je důležité vědět, že soukromý klíč není dostupný všem, ale je viditelný pouze pro svého majitele. Opakem je veřejný klíč, který je dostupný všem. Jedná se o velké číslo, které vzniklo vynásobením dvou prvočísel a používá se pro zašifrování daného textu. Důležité pro šifrování s veřejným klíčem je znát základní fakta o tomto šifrování, pochopit šifrování RSA a jeho význam v praxi.

Toto šifrování má své výhody i nevýhody. Mezi výhody můžeme zařadit možnost svobodně se podělit o svůj veřejný klíč s jakýmkoliv člověkem, který nám bude chtít poslat tajnou zprávu. Jedná se o nezasílání prvního typu klíče, tzn. soukromého neboli privátního klíče, neboť se tento klíč nevyřazuje ze seznamu klíčů, které jsou momentálně k dispozici. Z tohoto důvodu existuje druhý typ klíče, tzn. veřejný klíč, který je k dispozici všem uživatelům. Každá strana účastníků konverzace musí mít svoji kopii soukromého klíče. Veřejný klíč může být publikován v seznamu se jménem svého majitele a ve výsledku může pomocí daného klíče kdokoliv cokoliv zašifrovat a poslat tajnou informaci majiteli daného soukromého klíče. Rozšifrovat danou zprávu může tedy pouze ten, kdo je vlastník konkrétního soukromého klíče. Přesněji řečeno dochází k následujícímu schématu:

zpráva + VEŘEJNÝ KLÍČ ALISY = ZAŠIFROVANÝ TEXT

ZAŠIFROVANÝ TEXT + soukromý klíč Alisy = zpráva.

Tímto způsobem může Alise kdokoliv poslat tajnou informaci, pokud má k dispozici její veřejný klíč. Pouze Alisa však může danou zprávu rozšifrovat, pokud u ní bude odpovídající soukromý klíč.

Mezi nevýhody šifrování s veřejným klíčem, které se objevují při používání v asymetrické digitální kryptografii, patří rychlost šifrování anebo rozšifrování; požadované ověření pravosti klíče, tj. stoprocentní identifikace majitele veřejného klíče. Z toho vyplývá, že pokud k této identifikaci nedojde, zpráva nebude majiteli ukázána a tím si ji majitel nemůže přečíst. K zajištění správné identifikace slouží certifikační úřady, jejichž hlavním úkolem je dohlížet na databázi osob a na ověřování jejich totožnosti na základě daných veřejných klíčů. Tyto klíče jsou delší než u symetrických algoritmů, což ale nemusí znamenat, že budou vždy silnější. Tento fakt lze považovat za další nevýhodu asymetrického šifrování, které je dáno jeho matematickou podstatou. Další nevýhodou asymetrického šifrování je získání pokaždé stejného kryptogramu.

Důvodem fungování takových kryptosystémů je jednoznačný matematický vztah. Vztah existující mezi oběma klíči, při kterém informace o veřejném klíči nepomáhají stanovit klíč soukromý. Na druhou stranu vlastnictví soukromého klíče dává možnost rozšifrovat zprávu, která byla zašifrována veřejným klíčem. Na první pohled se tento vztah zdá velice zvláštní a pro jeho používání je nutný čas a spousta úsilí.

Šifrování s veřejným klíčem obsahuje tři dílčí procesy: vytváření klíčů, šifrování a rozšifrování. Algoritmus pro získávání klíčů G je veřejně dostupný, což znamená, že každý uživatel může podat náhodný řetězec r požadované délky, a tak obdržet dvojici klíčů (K_1, K_2). K_1 je označení pro veřejný klíč, který je publikovatelný a K_2 označuje soukromý klíč a spolu s řetězcem r budou tajné.

V roce 1973 jako první objevil algoritmus založený na šifrování s veřejným klíčem britský kryptograf Clifford Christopher Cocks. Jeho algoritmus byl následně označen za algoritmus s netajným klíčem, neboť v sobě zahrnoval složitost rozkladu celého čísla na prvočísla. V prosinci roku 1977 společnost Communications Services Electronic Security Group tento algoritmus odtajnila.

Myšlenka asymetrické kryptografie byla uveřejněna v červnu v roce 1976 v publikaci *New Directions in Cryptography (tj. Nové směry v kryptografii)* amerického informatika Whitfielda Diffieho a amerického kryptologa Martina Hellmana. Na tomto článku také spolupracoval i počítačový vědec Ralph C. Merkle. V tomto článku byla představena metoda distribuce šifrovacích klíčů. V prosinci 1987 byl zveřejněn na internetu na toto téma také článek britského inženýra a kryptografa Jamesa H. Elissa. Během roku byla

vydána první kryptografie s veřejným klíčem, která je dodnes označována RSA. Více než pět let před publikací jejich práce, britský inženýr a kryptograf James Henry Ellis rozpracoval koncept kryptografie s veřejným klíčem. Stejně jako Ellis, tak ani Diffie s Hellmanem nedokázali do detailů rozpracovat daný kryptosystém.

Bezpečnost používaných asymetrických kryptosystémů spočívá v tom, že v současné době nejsou známy dostatečně efektivní algoritmy k řešení matematických problémů, na nichž tyto kryptosystémy spočívají (Burda, 2013). Pokud tvrdí, že nejsou známy, neznamená to, že neexistují. Zatím matematici nezjistili algoritmy, které by byly k řešení vhodné. Do budoucna se předpokládá, že budou nalezeny algoritmy o polynomiální složitosti, které překonají složitost kryptosystému s veřejným klíčem, to by však přineslo definitivní konec asymetrického šifrování.

Asymetrické šifry mají i řadu problémů např. autentizace, kterou si ukážeme na příkladu: *Alice chce poslat zprávu Bobovi, ale aby Bob získal zprávu, musí Alice sehnat Bobův veřejný klíč a pak pomocí něho zprávu pro Boba zašifrovat. Avšak Alice nemá 100 % jistotu, že je to klíč Bobův. Netuší, že klíč byl Evou změněn a zprávu tím pádem posílá Evě, ne Bobovi. K Bobovi se, bohužel, tato zpráva nedostane.* Proto je výhodné v těchto případech použít certifikačních autorit, které uchovávají seznam osob a jejich veřejné klíče a tím garantují jejich platnost a správnost. Avšak problémů je mnohem více.

Šifry s veřejným klíčem se používají ve spojení se symetrickými šiframi pro domluvení klíče při jednorázovém použití. Jinak jsou asymetrické šifry příliš složité, a proto se v praxi používají spíše šifry symetrické.

Bezpečnost asymetrických kryptosystémů může být definována na základě matematické složitosti problému, která představuje rozklad násobku dvou velkých prvočísel. To je však pouze matematické vyjádření pojmu bezpečnost kryptosystému. Existují i jiné definice, které určují, za jakých podmínek můžeme dané šifrování považovat za bezpečné. Je zřejmé, že tedy žádné asymetrické šifrování není bezpečné, pokud se použije neomezeně velký výpočetní výkon. O bezpečnosti algoritmu lze hovořit jen s ohledem na velikost reálně použitého výpočetního výkonu.

Mezi šifry s veřejným klíčem řadíme například šifry RSA, DSA, El-Gamal a šifrování pomocí eliptických křivek, ale také Diffie-Helmannovu výměnu klíčů, která navíc využívá jednosměrnou funkci a hash funkci.

4.1. Jednosměrná funkce

Jak již bylo zmíněno, jednosměrná funkce je využívána v šifrovacím systému Diffie-Hellmanově výměně klíčů, kde zaujímá důležité místo v systému tohoto šifrování.

V asymetrické kryptografii je nejdůležitější jednosměrná funkce. Jednosměrná funkce je funkce, která je definována na množině X a množina Y je obor hodnot funkce tak, že $f: X \rightarrow Y$ se dvěma vlastnostmi: Existuje polynomiální výpočet algoritmu $f(x)$, anebo neexistuje žádný polynomiální výpočet algoritmu $f(x)$, tím pádem existuje vztah $f(x) = y$.

Jednosměrné funkce jsou funkce, které se dají snadno vypočítat jedním směrem, ale výpočet opačného směru je velice složitý (Pelánek, 2012). Také lze říct, že *jednosměrná funkce je funkce, pro jejíž libovolný vzor x lze snadno vypočítat obraz* $y = f(x)$*, avšak pro daný obraz y je prakticky nemožné vypočítat jeho vzor* $x = f^{-1}(y)$ (Burda, 2015), proto se právě tyto funkce s danými vlastnostmi využívají v kryptologické praxi.

Nejznámějším příkladem jednosměrné funkce je násobení, které je momentálně považováno za prakticky jednosměrnou funkci (*Hanžl*, 2007). Vynásobení dvou libovolných čísel je jednoduché, ale jejich součin rozložit na součin prvočísel je velice složité.

Proto může říct, že tento algoritmus využívá vlastnosti rozkladu čísla na součin prvočísel neboli na prvočíselný rozklad. Prvočíselný rozklad je pojem z oboru matematiky, který vyjadřuje přirozená čísla jako součin mocnin prvočísel.

Existuje několik metod pro součin čísel z oboru přirozených čísel. Mezi nejznámější metody pro součin patří metoda eliptických křivek a také kvadratické síto, které nám určuje, jak rychlým způsobem lze zjistit rozklad daného přirozeného čísla na součin čísel, které leží mezi 10^{80} a 10^{100}.

Existují i další způsoby ve formě složitějších zadání, které jsou propojeny s rozkladem na prvočísla a které se používají k vývoji kryptosystému s veřejným klíčem. Musíme si uvědomit, že i když známe přirozené číslo, nemusíme znát ani jeden z jeho prvočíselných dělitelů.

Jednosměrné funkce používané v kryptografii můžeme klasifikovat na funkce s pevnou délkou výstupu a na funkce s volitelnou délkou výstupu (Burda, 2013). Délka u jednosměrné funkce s volitelnou délkou může být buď kratší, stejná, nebo delší. Pokud se jedná o funkci s kratší délkou, hovoříme o tzv. **kompresní** funkci, pokud se jedná o funkci se stejnou délkou, hovoříme o funkci **ekvivalentní**. Je-li funkce s volitelnou délkou delší, máme na mysli funkci **expanzní**.

Jednosměrná funkce s pevnou délkou výstupu přiřazuje danému vzoru určitý obraz o určité bitové délce a setkáváme se s ní jako s funkcí **hash.**

Jako konkrétní příklad jednosměrné funkce si uvedeme Diffie-Hellmanovu výměnu klíčů.

4.1.1. Diffie-Hellmanova metoda výměny klíčů

Diffie-Hellmanovu metodu výměny klíčů lze také označit zkratkou D-H nebo také DHF. Jak již bylo zmíněno, Diffie-Hellmanova funkce byla poprvé představena v roce 1976 na Národní počítačové konferenci a následně během několika měsíců byla vydána v díle „*New Directions in Cryptography*“ (viz kapitola 4). Byla vyvinuta americkými kryptografy Whitlfieldem Diffiem a Martinem Hellmanem, podle kterých je metoda výměny klíčů pojmenována. Tato metoda výrazně změnila kryptografii, ale také vedla k rychlému rozvoji nových směrů v matematice. Na vývoji se podíleli i američtí kryptografové Ralph Merkle a John Gill, kteří navrhli praktické využití metody diskrétního logaritmu. Z tohoto důvodu se tento algoritmus označuje také jako schéma Diffie-Hellman-Merkle.

Diffie-Hellmanova metoda výměny klíčů byla vytvořena již v roce 1974 britským matematikem a kryptografem Malcolmem Johnem Williamsonem, ale tajná instituce GCHQ (= Government Communications Headquarters = Vládní komunikační ústředí) se rozhodla protokol utajit a poprvé zveřejnit až v roce 1997. Protokol, který vznikl v roce

1974, již neměl žádný velký význam, ale dodnes je považován za algoritmus využívaný v Diffie-Hellmanově metodě výměny klíčů.

Jde o to, že účastníci komunikace si prostřednictvím veřejného kanálu vymění informace, které jim umožní sestavit společný tajný klíč pro šifrování vzájemné výměny zpráv (Jiroušek, 2006).

Tento princip je realizován pomocí matematických funkcí, konkrétně pomocí operace zvané diskrétní logaritmus (Hanžl, 2007). *Nechť p, g, k, Y jsou přirozená čísla, pro něž platí* $Y \equiv g^k \, mod(p)$. *Potom každé číslo k odpovídající uvedené rovnici nazveme diskrétní logaritmus o základu g z Y vzhledem k modulu p. Tato definice nedefinuje číslo k jednoznačně, proto se někdy upravuje tak, že ze všech možných diskrétních logaritmů ve smyslu předchozí definice se vybere ten nejmenší* (https://cs.wikipedia.org/wiki/Diskrétní_logaritmus, 6. 5. 2020).

Dva jedinci, které budeme považovat za účastníky, se musí domluvit na nějakém dostatečně velkém prvočíslu p a také na primitivním prvku g, který bude z Galoisova tělesa, to je takový prvek, který vygeneruje $GF(q)$ ve smyslu, že mocniny $g^k mod(q)$ pro libovolná k nabývá všech hodnot z $GF(q)$. Galoisovo těleso je takové těleso, které má konečný počet prvků a též se označuje jako konečná grupa.

Uvedený postup si nyní ukážeme na konkrétních číslech: $g = 15$, $p = 13$. Víme, že účastník Alice si vybrala přirozené číslo 7 a že druhý účastník Bob si vybral nezávisle na výběru Alice své přirozené číslo, kterým bylo číslo 5. Tyto čísla byla jejich soukromá a museli je udržet v tajnosti před okolním světem i před sebou samém. To, co si budou mezi sebou předávat, jsou hodnoty, které si nyní vypočteme.

Hodnota funkce daná předpisem $F(x) = g^a \, mod(p)$, kde g je primitivní číslo, p je zvolené prvočíslo, a je přirozené číslo zvolené Alicí. Výsledek, ke kterému se výpočtem Alice dostane, označíme jako A.

$$A = g^a \, mod(p)$$

$$A = 15^7 \, mod(13)$$

$$A = (13 + 2)^7 \, mod(13)$$

$$A = 2^7 \, mod(13)$$

$$A = 128\ mod(13)$$

$$A = (9 \cdot 13 + 11)\ mod(13)$$

$$A = (9 \cdot 13)\ mod(13) + 11\ mod(13)$$

$$A = 11$$

Obdobným způsobem si hodnotu své funkce vypočte i Bob. Pro něho je předpis funkce velice podobný jako u Alice, až na horní exponent, kde bude mít pouze písmenko b, tj. $F(x) = g^b\ mod(p)$. Svůj výsledek si označí B. Nyní si zde vypočteme hodnotu B.

$$B = g^b\ mod(p)$$

$$B = 15^5\ mod(13)$$

$$B = (13 + 2)^5\ mod(13)$$

$$B = 2^5\ mod(13)$$

$$B = 32\ mod(13)$$

$$B = (2 \cdot 13 + 6)\ mod(13)$$

$$B = (2 \cdot 13)\ mod(13) + 6\ mod(13)$$

$$B = 6$$

Nyní si Alice a Bob mohou hodnoty, které vypočetli (A a B), mezi sebou vyměnit. K tomu, aby získali příslušný klíč, který potřebují pro rozšifrování daného textu a tím, aby zjistili, jaký text si navzájem poslali, potřebují si spočítat jeho hodnotu klíče. Ta bude pro oba stejná, ale my si zde ukážeme, jak bude vypočet provádět Alice, tak i Bob. Začneme výpočtem Alice, pro kterou platí následující předpis:

$$klíč_a = B^a\ mod(p),$$

kde B je hodnota, kterou jí poslal Bob, a je přirozené číslo zvolené jí samotnou, p je prvočíslo.

$$klíč_a = 6^7\ mod(13)$$

$$klíč_a = 279\,936\ mod(13)$$

$$klíč_a = (13 \cdot 21\,533 + 7)\ mod(13)$$

$$klíč_a = 7$$

Pro kontrolu, zda naše tvrzení platí a zda Bob i Alice počítali dobře, si vypočteme i klíč, který by získal Bob pomocí předpisu

$$klíč_b = A^b\ mod(p),$$

kde A je hodnota získaná od Alice, b je přirozené číslo zvolené jím, p je prvočíslo.

$$klíč_b = A^b\ mod(p)$$

$$klíč_b = 11^5\ mod(13)$$

$$klíč_b = 161\,051\ mod(13)$$

$$klíč_b = (12\,388 \cdot 13 + 7)\ mod(13)$$

$$klíč_b = 7$$

Tímto jsme si ověřili, že Alice i Bob počítali dobře. Získali jsme $klíč_a = klíč_b$.

Významnou úlohu u tohoto kryptosystému představuje bezpečnost a ochrana dat před nepovolanou osobou. *Největší hrozbou pro Diffie-Hellmanův protokol je tzv. útok mužem uprostřed („man-in-the-middle attack" – MITM attack). Předpokladem pro tento typ útoku je skutečnost, že útočník C má komunikační kanál mezi stranou A i B pod svou kontrolou a přenášené zprávy tak může modifikovat* (Burda, 2013). *Bezpečnost algoritmu spočívá v obtížné řešitelnosti problému diskrétního logaritmu, pro Galoisova tělesa $GF(q)$ totiž neexistuje efektivní algoritmus* (Jiroušek, 2006).

Případný útočník může sice odposlechem kanálu snadno zjistit hodnoty veřejných klíčů A a B, avšak k určení tajného klíče potřebuje zjistit hodnotu buď soukromého klíče, anebo b. Tyto klíče může teoreticky získat jako diskrétní logaritmus čísel A a B avšak, jak jsme již uvedli, pro vhodně zvolené parametry je to prakticky nemožné (Burda, 2015).

Ochranou proti útoku třetí osoby slouží metoda certifikátů. *Certifikát je v tomto případě veřejný klíč dané strany, který je digitálně podepsán nějakou důvěryhodnou třetí stranou, tzv. certifikační autoritou.* Zároveň si *obě strany navzájem sdělí a vymění certifikáty svých*

veřejných klíčů a také ověří platnost digitálního podpisu certifikátu protější strany (Burda, 2015).

4.1.2. Hash funkce

Hash funkce, také označována jako hashovací funkce, je *kryptografická funkce, která číselnému argumentu D (neboli vzoru) o prakticky libovolné délce (jednotky bitů až trilióny triliónů bitů) přiřazuje tzv. hash H, což je číselná hodnota o pevně stanovené délce (typicky o délce 256 až 512 bitů)* (Burda, 2019). *Hash funkcí rozumíme způsob, jak z uceleného textu (obecně dat) vytvořit krátký řetězec (číslo) identifikující původní obsah* (Koláček, 2009). Hash funkce je matematická funkce, která zmenšuje vstupní data do velmi malých čísel. Využívá se k rychlému prohlížení tabulky (například v antivirových programech k hledání malware). Označuje se také jako HSF. Formálně tato funkce se zapisuje:

$$H = HSF(D).$$

Základní princip hashovacích funkcí spočívá v tom, že výsledná hashovací funkce je zhuštěným otiskem, který zastupuje původní zprávu (Piper, 2006).

Hashovací funkce je obvykle funkce, od které se požaduje, aby byla odolná vůči získání vzoru, odolná vůči modifikaci vzoru a také aby byla odolná vůči kolizím (Burda, 2013).

Hash funkce má dvě vlastnosti: jednosměrnost a bezkoliznost. *Jednosměrnost znamená, že určení hodnoty hash H je pro zadaný vzor D výpočetně snadné, určit hodnoty vzoru D ze znalosti jeho hash H je prakticky nemožné.* (K argumentu *D* lze najít *H*, ale k *H* nelze najít *D*.) (Burda, 2019).

Bezkolizností se rozumí, že je prakticky nemožné nalézt nějakou dvojici různých vzorů D_1 a D_2 takovou, aby jejich hash byly stejné (Burda, 2019).

Také se požaduje, aby výstup této funkce (hash) byl neprolomitelný, aby ho nebylo možné najít. *Kvantita vstupních dat nemá žádný vliv na délku výstupního otisku (hash) této funkce. Je třeba si uvědomit, že sebemenší změna vstupního řetězce způsobí zcela odlišný hash* (Koláček, 2009).

Funkce hash je prazáklad pro několik dalších aplikací a je důležitá v autentizačních asymetrických kryptosystémech. Primární účel tohoto kryptosystému je zajistit nepopíratelnost informace o původci zprávy. Můžeme za něj považovat systémy digitálního podpisu.

Hlavním úkolem těchto funkcí je vytvářet reprezentanty zpráv o konstantní délce, tzv. hash (Burda, 2013). *Hash hodnota přestavuje zhuštěnou hodnotu dlouhé zprávy, ze které byla vypočtená, ve významu „digitálního otisku prstu" velkého dokumentu. Opačný proces je nemožný – díky požadavku jednosměrnosti hash funkce* (Budiš, 2008).

Hash funkce má tři základní atributy, které by měla plnit. Jedná se o *odolnost vůči získání vzoru („preimage resistence"), odolnost vůči modifikaci vzoru („2nd-preimage resistence) a odolnost vůči kolizím („collision resistence)* (Burda, 2015). Pokud bude jedna z těchto části nenaplněna, anebo naplněna částečně, omezuje se tím použitelnost samotné hash funkce v praxi.

Ke konstrukci hashovací funkce se nejčastěji používá Merkle-Damagårdova konstrukce. Vzor je zde chápán jako řetězec bitů, který se nejprve zarovná výplňovými bity D a na konci se doplní polem L o stanovené délce, v němž je uvedena bitová délka vzoru V. Počet výplňových bitů se volí tak, aby bylo možné výsledný řetězec $X = (V \parallel D \parallel L)$ *rozdělit na bloky* X_i *o délce r bitů* (Burda, 2015).

Historie hash funkce sahá do roku 1953, kdy výzkumný pracovník v oblasti počítačové vědy Hans Peter Luhn položil její základy. Donald Ervin Knuth si myslí, že byl Hans Peter Luhn prvním, kdo vyvinul první systematickou myšlenku pro hash funkci. V roce 1956 Arnold Dumey ve své práci *Computers and automation* popsal poprvé hash funkci tak, jak ji známe dnes. Díval se na ni jako na řešení problému ve slovníku, prezentoval ji v roli hash adresy jako zbytek po rozkladu na prvočísla. V roce 1957 v časopise *IBM Journal of Research and Development* byl otisknut článek amerického matematika Williama Wesleyho Petersona, ve kterém se zmiňuje o hledání textu ve velkém obsahu dat. Tato stať je považována za první skutečnou práci v problematice hash šifrování a hash funkce. O šest let později byl zveřejněn článek německo-amerického počítačového vědce Wernera Buchholze, ve kterém podrobně napsal o hash funkci. Během posledních let nebyl publikovaný žádný odborný článek v rámci žádné významné práce.

4.1.2.1. Konkrétní příklady hash funkcí

Mezi jednu z nejdůležitějších hash funkcí patří **MD5**, která se prosadila například v kontrole integrity souborů nebo v ukládání hesel. Tuto hash funkci navrhl americký matematik Ronald L. Rivest v roce 1991 a po drobných úpravách ji zveřejnil v dubnu 1992. MD5 má 128bitový vstup. Existovala také verze označována jako **MD4**, ale byla považována za nedostatečně bezpečnou, a proto byla vymyšlena nová verze MD5. B. den Boer a. Bosselaers přinesli v roce 1993 „pseudo-kolize" v této hash funkci. Nalezli dva odlišné inicializační vektory, které ovšem produkovaly stejný výsledek. O dva roky později byla oznámena kolize, která však nebyla útokem na MD5, ale měla vliv na kryptografy, kteří raději doporučili přechod na SHA-1 a RIPEMD-160. V roce 1996 v návrhu MD5 byla nalezena chyba, která však nebyla tak zásadní, ale kryptografům bylo doporučeno používat jiné algoritmy. Od roku 2004 se nedoporučuje používat MD5, protože velikost chyb se stále zvětšovala.

Další hash funkce, která se v současnosti také používá, se nazývá **SHA**. SHA (= Secure Hash Algoritmus) je *hashovací funkce vytvářející ze vstupních dat výstup fixní délky.* (https://cs.wikipedia.org/wiki/Secure_Hash_Algorithm, 15. 3. 2021) Má podobné principy, které byly využity R. R. Riversem při tvorbě MD4 i MD5. Tento standard počítá zmenšenou reprezentaci zprávy nebo hash délky 160 bitů. Zveřejněna byla v roce 1993 ve Spojených státech amerických Národním institutem standardů a technologií jako oficiální standard kryptografie. První verze z roku 1993 je označována jako SHA-0, ale zanedlouho byla vyměněna za verzi označovanou jako SHA-1, která byla publikována již o dva roky později. Avšak obě tyto hash funkce mají své nedostatky, které byly brzy objeveny. Novější verze obsahuje méně nedostatků a je o trochu odolnější. SHA-1 se používá v aplikacích a protokolech, které se využívají v bezpečnosti, například TLS and SSL, SSH a IPsec. Tyto novější hash funkce SHA nebyly doposud tak dobře otestovány jako SHA-0 a SHA-1, ale v praxi stále nebyly nalezeny jejich slabiny. *SHA-256 byla naposledy standardizována v roce 2012 a náleží do rodiny funkcí SHA-2* (Burda, 2015). Tato funkce je prakticky neprolomitelná. Pracuje se též na SHA-3, která by v budoucnu nahradila stávající hash funkce.

Nesmíme zapomenout uvést ani na další hash funkci **RIPEMD**, která vznikla ve 20. století. Toto slovo v sobě skrývá anglickou zkratku RACE Integrity Primitives Evaluation Message Digest. Tuto hash funkci vymysleli německý kryptograf Hans

Dobbertin, Antoon Bosselaers a belgický kryptograf a kryptoanalytik Bart Preneel. Ve své konečné podobě byla publikována až v roce 1996. Podle velikosti výstupů se označuje RIPEMD-128, RIPEMD-160, RIPEMD-256 a RIPEMD-320.

Hash funkce, která má kontrolní součet neboli hash o délku 192 bitů, je označována jako **Tiger**. Tuto hash funkci navrhli v roce 1995 Ross Anderson a Eli Biham. Využívá se ke kontrole integrity souboru a ukládání hesel. Existuje také varianta Tiger2, která je ve svém používání totožná s MD5 a SHA-1. Specifika hash funkce Tiger2 nebyla dodnes veřejně publikována.

Hlavní využití hash funkce Tiger je v hash stromě, který je také označován jako **Merkleův strom**, který má v „listech" data a ve všech ostatních vrcholech má hodnotu odpovídající výsledku kryptografické hash funkce. Jedná se o datovou strukturu používanou v šifrování a informatice, ve které je možno ověřit integritu listu v logaritmickém čase vzhledem k počtu datových uzlů. Hash stromy vymyslel v roce 1979 Ralph Merkle, aby rozšířil Lamportovo podpisové schéma, čímž vytvořil Merkleovo podpisové schéma.

4.2. RSA

Další metodou, která je algoritmem pro šifrování s veřejným klíčem, je metoda označována zkratkou RSA. Toto schéma je pojmenováno podle prvních písmen příjmení autorů, jimiž jsou Američan Ron Rivest, Izraelec Adi Shamir a Američan Leonard Adleman. RSA kryptosystém je nejznámější kryptosystém s veřejným klíčem. Algoritmus byl vypracován v roce 1977 a publikován o rok později. Na tomto algoritmu také pracoval britský matematik Clifford Cocks, který se o něm zmiňuje ve svém dokumentu z roku 1973, *ale jeho systém nebyl uznán jako použitelný z důvodu nutnosti použití relativně drahé výpočetní techniky pro uvedení algoritmu do praxe. Jeho výzkum nebyl až do roku 1997 prozrazen z důvodu označení jako „přísně tajné".* (http://www.kryptografie.wz.cz/uk.htm, 4. 8. 2020). V roce 1983 byl kryptosystém RSA v USA patentován, ale patent byl zrušen již v roce 2000, neboť algoritmus byl publikován dříve, než proběhlo jeho patentování. V srpnu 2001 na konferenci Crypto'2001 James Manger ukázal, že v té době nejnovější verze, která nestačila proniknout do masového použití, obsahovala již chybu.

Šifra RSA náleží do kategorie asymetrických kryptosystémů typu IF, což jsou kryptosystémy, jejichž bezpečnost spočívá v obtížnosti řešení problému faktorizace velkých čísel (Burda, 2015). Bezpečnost RSA šifrování se také opírá o časovou složitost problému faktorizace prvočísel. Aby šifrování RSA bylo bezpečné, musí být použita kvalitní šifra, která bude použita správným způsobem a také musí být správně realizována.

V několika modifikacích je schéma aktivně používáno pro šifrování dat na internetu a je zahrnuto v různých mezinárodních a národních normách v oblasti informační bezpečnosti, mezi které můžeme zařadit standarty IEEE P1363 a EKCS#1.

Přenos utajených zpráv mezi k účastníky tak vyžaduje výměnu $\frac{k(k-1)}{2}$ *klíčů, nebo vedení utajené komunikace prostřednictvím jednoho důvěryhodného centra* (Jiroušek, 2006). I tento kryptosystém, stejně jako všechny asymetrické kryptosystémy, poskytuje pouze důvěrnost. *Útočník zná veřejný klíč, může si zvolit nějakou zprávu Z, a tu veřejným klíčem zašifrovat do podoby kryptografu C* (Burda, 2013). Potom může pomocí „pokus omyl" zkoušet všechny možné rozšiřovací klíče, aby nalezl soukromý klíč. Tento systém je prakticky neproveditelný, neboť možných rozšifrovacích klíčů je velice mnoho. Dodnes nejsou známy efektivní algoritmy pro řešení dvou matematických problémů, jimiž jsou *problém výpočtu e-té odmocniny čísla C v aritmetice modulo n a druhým problémem je problém faktorizace velkého čísla n* (Burda, 2013).

Velkou výhodou kryptosystémů RSA oproti ostatním typům asymetrických kryptosystémů je skutečnost, že jej lze efektivně využít jak pro zajištění důvěrnosti, tak i autentičnosti zpráv (Burda, 2015).

Slabinou všech asymetrických kryptosystémů je skutečnost, že šifrováním stejné zprávy získáme pokaždé stejný kryptogram. K eliminaci této slabiny se u RSA používá technika OAEP (= Optimal Asymmetric Encryption Padding) (Burda, 2015). Metoda OAEP je založena na tom, že šifrovaná zpráva je modifikována semenem. Tím se rozumí náhodný a tajný řetěz bitů. Odesílatel nejdříve zprávu převede pomocí této techniky na zprávu, která je poté pomocí asymetrického kryptosystému RSA zašifrována. Tato zpráva je označena Z. Zpráva je poté přepsána na bajt 01_{16}, výplň p a konstantu c, která závisí na

hash funkci a která byla sjednána. Tento řetězec je označen následně jako db. Pro každou novou zprávu je vygenerováno nové semeno.

Toto asymetrické šifrování využívá Fermatovu větu a modulární aritmetiku. Nyní si ukážeme na jednom konkrétním příkladu všechny tři etapy – etapu generování klíče, etapu šifrování a etapu rozšifrování. Pokud budou u etapy generování klíče použity velice malá čísla (například čísla 3 a 7), během opětovného rozšifrování budou v rozšifrovaném textu chyby.

4.2.1. Etapa generování klíče

První etapou, která je nutná k šifrování a následnému rozšifrování, je etapa označována jako etapa generování klíče. Ta v sobě skrývá několik dílčích na sebe navazujících kroků a operací, které si na konkrétních číslech ukážeme nyní.

1. Určíme si dvě prvočísla p, q (čísla dělitelná pouze jedničkou a sami sebou), která musí být náhodná a rozdílná:

$$p = 11,$$

$$q = 7.$$

2. Vypočítáme jejich násobek, který označíme n:

$$n = p \cdot q = 11 \cdot 7 = 77$$

3. Vypočítáme vztah $(p-1) \cdot (q-1)$, který označíme n_1:

$$n_1 = (p-1) \cdot (q-1) = (11-1) \cdot (7-1) = 60$$

4. Vybereme si nyní hodnotu čísla e:

$$e = 7.$$

5. Vypočteme hodnotu čísla d podle následujícího vztahu: $(e \cdot d)\ mod(n_1) = 1$. Také pro číslo d musí platit, že největší společný dělitel čísla d a čísla n_1 bude roven 1, tj. číslo d a číslo n_1 budou nesoudělná, a zároveň číslo d bude menší než číslo n.

   Tento matematický problém se řeší pomocí Euklidovy věty:

$$(e \cdot d)\ mod\ (n_1) = 1$$

$$(7 \cdot d)\ mod(60) = 1$$

$$d = 43.$$

6. Nyní již víme, jak bude vypadat veřejný a soukromý klíč. Veřejný klíč je $(e, n) = (7, 77)$ a soukromý klíč je roven $(d, n) = (43, 77)$.

4.2.2. Etapa šifrování

Druhou etapou je etapa šifrování, která slouží k zašifrování daného textu či symbolů. Etapa šifrování pracuje se substitucí daných písmen a znaků do číslic. Proto jako první krok, než se pustíme do samotného šifrování, si musíme vytvořit tabulku, ve které jednomu písmenu bez diakritiky bude odpovídat pouze jedno číslo.

Tabulka 5: etapa šifrování – přiřazení čísla k daným písmenům (zdroj: autorka)

a	0	n	13
b	1	o	14
c	2	p	15
d	3	q	16
e	4	r	17
f	5	s	18
g	6	t	19
h	7	u	20
i	8	v	21
j	9	w	22
k	10	x	23
l	11	y	24
m	12	z	25

Budeme šifrovat slovo $matematika$ pomocí tohoto šifrovacího kryptosystému.

Nejprve si převedeme jednotlivá písmena pomocí předchozí tabulky na čísla.

Tabulka 6: převod slova matematika do šifrovacího kryptosystému (zdroj: autorka)

m	a	t	e	m	a	t	i	k	a
12	0	19	4	12	0	19	8	10	0

Dalším krokem pro šifrování je určení hodnoty M_i^e pro jednotlivá čísla. Hodnota M_i^e je rovna hodnotě přiřazeného na hodnotu čísla e.

Tabulka 7: určení hodnoty (zdroj: autorka)

M_i	12	0	19	4	12	0	19	8	10	0
M_i^e	12^7	0^7	19^7	4^7	12^7	0^7	19^7	8^7	10^7	0^7

Následuje výpočet hodnoty čísla C_i, který je dán předpisem $C_i = M_i^e \ mod(n)$. Výpočty budou také znázorněné v následující tabulce.

Tabulka 8: výpočet hodnoty C_i (zdroj: autorka)

M_i^e	Výpočet	Hodnota C_i
12^7	$C_i = 12^7 \ mod(77) = (77 \cdot 465\,348 + 12) \ mod(77)$	12
0^7	$C_i = 0^7 \ mod(77)$	0
19^7	$C_i = \ 19^7 \ mod(77) = (11\,608\,723 \cdot 77 + 68) \ mod(77)$	68
4^7	$C_i = 4^7 \ mod(77) = (212 \cdot 77 + 60) \ mod(77)$	60
12^7	$C_i = 12^7 \ mod(77) = (77 \cdot 465\,348 + 12) \ mod(77)$	12
0^7	$C_i = 0^7 \ mod(77)$	0
19^7	$C_i = 19^7 \ mod(77) = (11\,608\,723 \cdot 77 + 68) \ mod(77)$	68
8^7	$C_i = \ 8^7 \ mod(77) = (27\,235 \ \cdot 77 + 57) \ mod(77)$	57
10^7	$C_i = \ 10^7 \ mod(77) = (129\,870 \cdot 77 + 10) \ mod(77)$	10
0^7	$C_i = 0^7 \ mod(77)$	0

Bloky C_i jsou zašifrované zprávy, které je možno v klidu předávat otevřeným kanálem, protože operace umocnění podle modulu prvočísla je nevratná matematická úloha.

4.2.3. Proces rozšifrování

Rozšifrování je opačný proces k šifrování. Nyní si prakticky ukážeme, jak rozšifrovat daný text, pokud známe všechny potřebné údaje k tomuto procesu. Budeme využívat hodnot C_i z předchozího procesu šifrování (viz kap. 4.2.2.).

Prvním z dílčích kroků je zapsání hodnoty C_i^d.

Tabulka 9: rozšifrování krok č. 1 (zdroj: autorka)

C_i	12	0	68	60	12	0	68	57	10	0
C_i^d	12^{43}	0^{43}	68^{43}	60^{43}	12^{43}	0^{43}	68^{43}	57^{43}	10^{43}	0^{43}

Dalším krokem (č. 2) je výpočet hodnoty M_i, která se vypočte podle předpisu: $M_i = C_i^d \; mod(n)$. K těmto výpočtům byla použita online matematická kalkulačka na výpočet hodnot, když je znám modul.

Tabulka 10: rozšifrování krok č. 2 (zdroj: autorka)

C_i^d	Výpočet	M_i
12^{43}	$M_i = 12^{43} \; mod(77)$	12
0^{43}	$M_i = 0^{43} \; mod(77)$	0
68^{43}	$M_i = 68^{43} \; mod(77)$	19
60^{43}	$M_i = 60^{43} \; mod(77)$	4
12^{43}	$M_i = 12^{43} \; mod(77)$	12
0^{43}	$M_i = 0^{43} \; mod(77)$	0
68^{43}	$M_i = 68^{43} \; mod(77)$	19
57^{43}	$M_i = \; 57^{43} \; mod(77)$	8
10^{43}	$M_i = 10^{43} \; mod(77)$	10
0^{43}	$M_i = 0^{43} \; mod(77)$	0

Jako poslední krok (č. 3) je náhled do tabulky 11 a přiřazení danému M_i daného písmene.

Tabulka 11: rozšifrování krok č. 3 (zdroj: autorka)

M_i	12	0	19	4	12	0	19	8	10	0
	m	a	t	e	m	a	t	i	k	a

Během šifrování i rozšifrování nedošlo ke ztrátě dat, ani chybě během jejich přenosu.

4.3. Kryptosystém El-Gamal

Další z kryptosystémů, který spatřil světlo světa v minulém století je kryptosystém, který se nazývá El-Gamal. Tento kryptosystém vymyslel v roce 1984 americký kryptograf původem z Egypta, Dr. Taher Elgamal. Jedná se o kryptosystém s otevřeným klíčem, který je kvůli své obtížnosti výpočtu diskrétních logaritmů na konečné množině složitý k vyřešení. Byl prvním asymetrickým algoritmem, který fungoval.

Skládá se ze šifrovacích a podpisových schémat, která jsou základem bývalých elektronických digitálních podpisů v USA (DSS) a v Rusku (ГОСТ Р 34.10-94 – „Gost R 34.10-94“).

U systému El-Gamal jsou velikosti klíčů obdobné jako u RSA, ale jeho bezpečnost se odvíjí od obtížnosti jiného matematického problému. (Piper, 2006) *Bezpečnost je založena opět na obtížné řešitelnosti problému diskrétního logaritmu* (Jiroušek, 2006).

Ke konstrukci tohoto kryptosystému si potřebujeme jako u Diffie-Hellmanovy metody nejdříve libovolně určit velké prvočíslo q a primitivní prvek g Galoisova tělesa $GF(q)$, tj. číslo nesoudělné s q, které generuje Galoisovo těleso v tom smyslu, že jeho mocniny $g^i \, mod(q)$ pro různá i nabývají všech hodnot z Galoisova tělesa. Poté musíme zvolit nenulový prvek s, který bude pocházet z Galoisova tělesa jako soukromý klíč a následně vypočítáme p, pro které bude platit následující vztah:

$$p = g^s \, mod(q).$$

Hodnoty písmen g, p, q zveřejníme jako veřejný klíč, pouze hodnotu písmene s ponecháme utajenou pro rozšifrování, neboť s je součástí soukromého klíče.

Podstatné je to, že pro nalezení s z čísel p, q, g neexistuje rychlý algoritmus, takže vzniklý kryptosystém má vlastnosti asymetrického šifrování (Jiroušek, 2006).

4.4. Kryptografie na bázi eliptických křivek

Šifrování s veřejným klíčem se stále zdokonaluje, neustále se vymýšlejí nové způsoby a techniky, jak ušetřit čas. Z tohoto důvodu vznikla v roce 1985 kryptografie na bázi eliptických křivek. Označuje se také jako nejmladší šifrování s veřejným klíčem. Kryptografie na bázi eliptických křivek se také značí pomocí zkratky ECC. Tato zkratka pochází z anglického označení Elliptic Curve Cryptography. *Eliptická křivka je rovinná křivka a každý její bod P_i je dán kartézskými souřadnicemi. Platí tedy, že $P_i = (x_i, y_i)$, kde x_i je souřadnice bodu v ose x a y_i je souřadnice bodu v ose y* (Burda, 2013).

Na tomto asymetrickém šifrování se podíleli dva vědci, kteří pracovali nezávisle na sobě, profesor matematiky Neal Koblitz z Washingtonské univerzity a americký matematik Victor Saul Miller z Centra pro komunikační výzkum a Institutu pro obranné analýzy v Princetonu v New Jersey.

Přibližně v roce 2005 byl tento kryptosystém prosazen do technické praxe. Má také tu výhodu, že pokud bychom chtěli šifrovat pomocí šifrování RSA, potřebujeme klíč o délce 3 072 bitů, ale k šifrování na bázi eliptických křivek nám postačí klíč o délce pouze 256 bitů. V budoucnosti šifrování na bázi eliptických křivek bude velmi používáno díky své malé délce bezpečnostních klíčů, ale i rozumné výpočetní složitosti, například *v telekomunikačních systémech s promělnlivou přenosovou kvalitou, v chytrých telefonech a tabletech, ve vestavěných systémech, v internetu* (Oulehla, 2017).

V dnešní době kryptografie na bázi eliptických křivek pronikla i do šifrování RSA a DSA. *Kryptografie eliptických křivek je moderní a nadějný směr, přinášející výsledky v řadě ukazatelů lepší než stávající kryptosystémy* (Klíma, 9/2002).

Tento typ asymetrického šifrování se liší od všech ostatních v rychlosti, v menší náročnosti na hardware a software a také tím, že má také geometrickou interpretaci a nemá pouze číselnou interpretaci.

4.4.1. Geometrická interpretace eliptických křivek nad polem T

Eliptická křivka $\mathcal{E}$ představuje množinu všech bodů o souřadnicích $[x, y]$, které vyhovují Weierstrassově rovnici, a zároveň x a y jsou prvky pole T. Mezi body eliptické křivky zahrneme i bod $\mathcal{O}$, kterým nazýváme bod v nekonečnu (Ouhlehla, 2017).

Eliptickou křivkou $\mathcal{E}$ nad polem T rozumíme algebrackou křivku třetího stupně s rovnicí

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

kde $a_1, a_2, a_3, a_4, a_6 \in T$. *Chybí koeficient a_5 z důvodu „zachování kompatibility" s historickým značením koeficientů* (Ouhlehla, 2017).

Diskriminant Δ eliptické křivky $\mathcal{E}$ je nenulový. Pokud by byl nulový, funkce by nebyla hladká a neexistovala by k ní derivace a ani tečna. Pro diskriminant Δ platí následující vztah:

$$\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6,$$

kde:

$$d_2 = a_1^2 + 4a_2$$

$$d_4 = 2a_4 + a_1a_3$$

$$d_6 = a_3^2 + 4a_6$$

$$d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 + a_4^2.$$

Výpočty pomocí obecné formy Weierstrassovy rovnice

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

jsou velice složité, proto se pro jednoduchost používá zjednodušená verze Weierstrassovy rovnice, která má tvar:

$$y^2 = x^3 + ax + b,$$

kde *a, b* jsou koeficienty, které jsou součástí pole T a pro kterou počítáme diskriminant Δ následujícím způsobem:

$$\Delta = -16(4 \cdot a^3 + 27 \cdot b^2).$$

Pro diskriminant jak obecné formy Wierstrassovy rovnice, tak i pro její zjednodušenou verzi platí, že se nesmí rovnat nule. Pro diskriminant tedy nastanou dvě situace - záporná a kladná. Pro obě situace musí platit, že funkce bude hladká.

Pokud diskriminant bude kladný, je eliptická křivka rozdělena do dvou spojitých částí. Je-li diskriminant záporný, je eliptická křivka spojitá a tvořená jedinou částí. Schopnosti eliptických křivek se záporným i kladným diskriminantem jsou shodné.

Nejdříve si ukážeme, jak bude vypadat graf eliptické křivky, která je dána předpisem:

$$y^2 = x^3 - 4x + 1$$

pro $a = -4, b = 1$.

Jako první si spočítáme diskriminant, kdy hodnoty *a, b* dosadíme do rovnice, pro výpočet diskriminantu:

$$\Delta = -16(4 \cdot a^3 + 27 \cdot b^2)$$

$$\Delta = -16(4 \cdot (-4)^3 + 27 \cdot 1^2)$$

$$\Delta = -16(-4^4 + 27)$$

$$\Delta = 4\,096 - 432$$

$$\Delta = 3\,664$$

Hodnota diskriminantu je kladná a z toho plyne, že grafem této eliptické křivky bude graf, který bude rozdělen na dvě spojité části.

Tvorbu grafu musíme rozdělit na dvě části, první z nich bude pro:

$$y = \sqrt{x^3 - 4x + 1}.$$

Tato funkce je definována pro *x*, která leží na intervalu, který vypočteme pomocí průsečíků předpisu funkce s osou *x*, tzn. za hodnotu *y* dosadíme nulu

$$0 = \sqrt{x^3 - 4x + 1}.$$

Tuto funkci již můžeme dát na druhou a tím spočítat kořeny dané funkce. K tomu musíme využít Cardanovy vzorce. Jejich odvozením se v této práci nebudeme zaobírat, protože je to další zajímavý matematický problém, který vyžaduje znalost komplexních čísel a rozsáhlé znalosti matematiky. Pro jednoduchost jsme využili elektronické kalkulačky, která nám určila požadované kořeny zaokrouhlené na čtyři desetinná čísla (https://www.hackmath.net/cz/kalkulacka/kubicka-rovnice?a=1&b=0&c=-4&d=1&eq3=&submit=Vyřeš, 25. 3. 2021).

Kořeny naší kubické rovnice jsou:

$$x_1 = 1{,}8608$$

$$x_2 = -2{,}1149$$

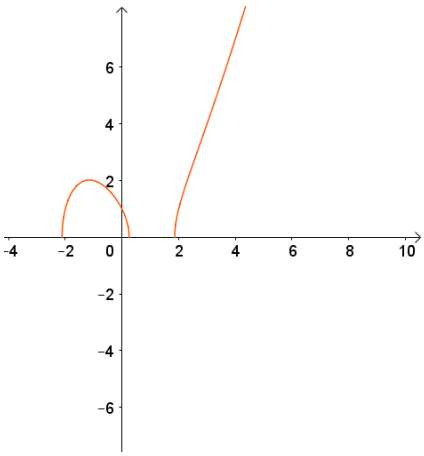
$$x_3 = 0{,}2541.$$

Nyní již víme, že kubickou rovnici $x^3 - 4x + 1 = 0$ lze rozložit na

$$(x - 1{,}8608) \cdot (x + 2{,}1149) \cdot (x - 0{,}2541) = 0.$$

Tím jsme zjistili všechny průsečíky s osou *x*.

Pro znázornění následujících grafů využijeme program GeoGebra.

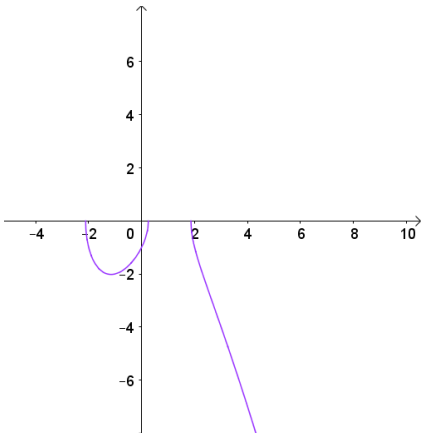


Obrázek 2: 1. část grafu eliptické křivky s kladným diskriminantem (zdroj: autor)

Druhou část bude tvořit graf, který bude definovaný na stejném intervalu jako první část, ale bude pouze osově souměrný podle osy *x* a bude mít předpis:

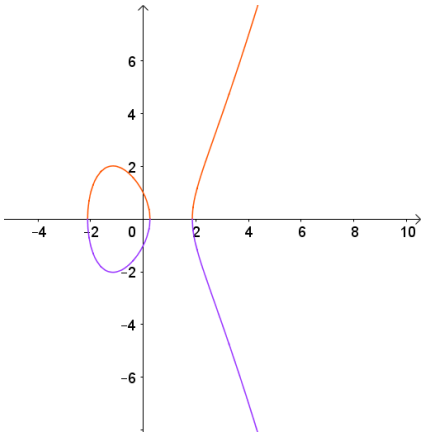
$$y = -\sqrt{x^3 - 4x + 1}.$$

O této funkci víme, že bude osově souměrná podle osy x a bude mít totožné průsečíky s osou x jako první část, která předpisově byla shodná až na záporné znaménko před odmocninou. Graf opět vytvoříme v programu GeoGebra.



Obrázek 3 část grafu eliptické křivky s kladným diskriminantem (zdroj: autorka)

Pokud tyto dva grafy spojíme do jednoho grafu, dostaneme graf pro eliptickou křivku s kladným diskriminantem. Jeho výsledná podoba je na následujícím obrázku:

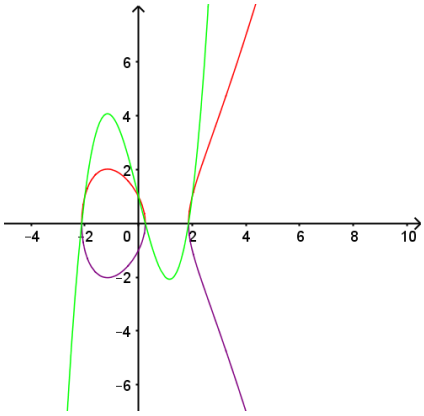


Obrázek 4: spojení dvou grafů s kladným diskriminantem (zdroj: autorka)

Tuto eliptickou křivku můžeme ještě proložit funkcí:

$$y = x^3 - 4x + 1.$$

Tím si ukážeme, že opravdu graf celé eliptické křivky se nachází na kladné části této kubické funkce.



Obrázek 5: proložení grafu eliptické křivky s grafem kubické funkce (zdroj: autorka)

Následujícím příkladem pro eliptické křivky, bude opačné znaménko diskriminantu, tj. záporné znaménko. To bude platit pro funkci s předpisem

$$y^2 = x^3 - 2x + 9$$

pro $a = -2, b = 9$.

Jako první si spočítáme diskriminant, kdy hodnoty a, b dosadíme do rovnice, pro výpočet diskriminantu:

$$\Delta = -16 \cdot (4 \cdot a^3 + 27 \cdot b^2)$$

$$\Delta = -16 \cdot (4 \cdot (-2)^3 + 27 \cdot 9^2)$$

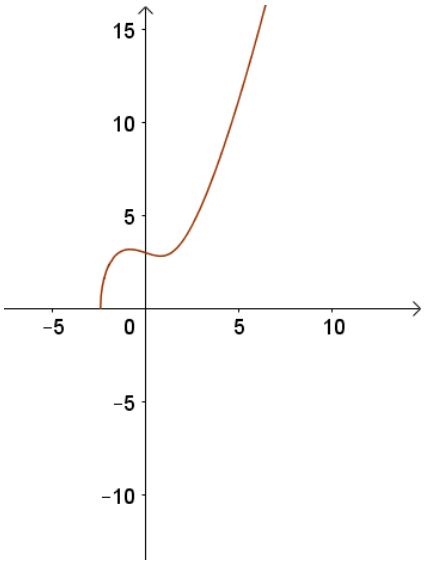
$$\Delta = -34\,480.$$

Hodnota diskriminantu je záporná a z toho lze usoudit, že graf eliptické křivky bude spojitý a tvořen jedinou částí.

Tvorbu grafu si rozdělíme na dva kroky. Prvním z nich bude, kdy se y bude rovnat odmocnině kubické funkce, tj.

$$y = \sqrt{x^3 - 2x + 9}.$$

To bude znázorňovat následující obrázek.

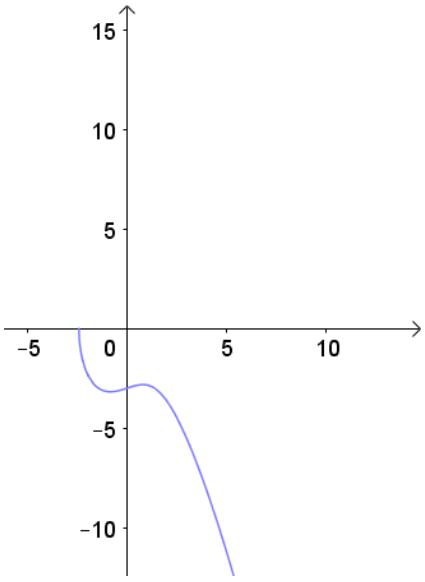


Obrázek 6: 1. část grafu eliptické křivky se záporným diskriminantem (zdroj: autorka)

Jelikož předpis rovnice pro eliptickou křivku byl $y^2 = x^3 - 2x + 9$, musíme graf vyřešit i pro hodnoty y, které se budou rovnat hodnotám odmocniny a které budou mít opačné hodnoty, tzn. opačná znaménka.

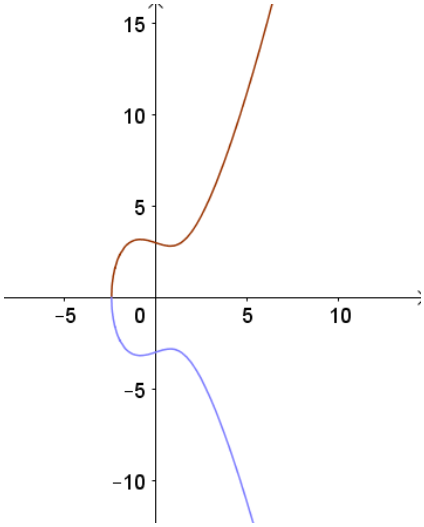
Budeme tedy řešit výraz daný předpisem:

$$y = -\sqrt{x^3 - 2x + 9}$$



Obrázek 7: 2. část grafu eliptické křivky se záporným diskriminantem (zdroj: autorka)

Pokud tyto dvě části sloučíme do jednoho grafu, vznikne nám graf pro eliptickou křivku se záporným diskriminantem. Tyto dvě části jsou osově souměrné podle osy *x*. Toto lze také vidět na obrázku 8.



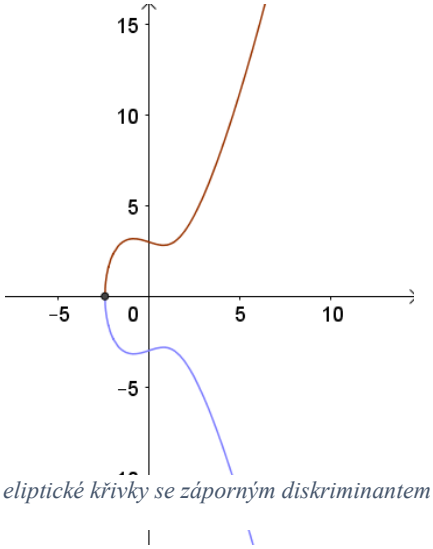
Obrázek 8: spojení dvou grafů eliptické křivky se záporným diskriminantem (zdroj: autorka)

Daná funkce je definována na intervalu, který je z jedné strany ohraničen průsečíkem s osou *x* a na druhé straně jde do nekonečna. Průsečík s osou *x* vypočteme tak, že za ypsilonovou souřadnici dosadíme nulu:

$$y^2 = x^3 - 2x + 9$$

$$0 = x^3 - 2x + 9.$$

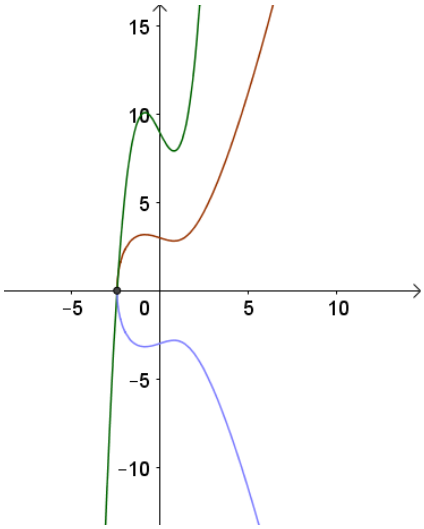
Poté buď pomocí vzorců na rozklad kubické rovnice, nebo pomocí online elektronických kalkulaček zjistíme hodnoty. Jediný kořen, který není v oboru komplexních čísel, je kořen $x = -2{,}398$, který je zároveň také bodem styku obou částí grafu.



Obrázek 9: průsečík grafu eliptické křivky se záporným diskriminantem s osou x (zdroj: autorka)

Nyní si ukážeme graf eliptické křivky rovnice $y^2 = x^3 - 2x + 9$ a výrazu pod odmocninou $x^3 - 2x + 9$.

Vidíme zde, že tyto dvě funkce se setkávají v jednom bodě, v průsečíku na ose *x* (viz obrázek 10).



Obrázek 10: proložení grafu eliptické křivky s výrazem pod odmocninou (zdroj: autorka)

4.4.2. Operace na eliptických křivkách nad polem *T*

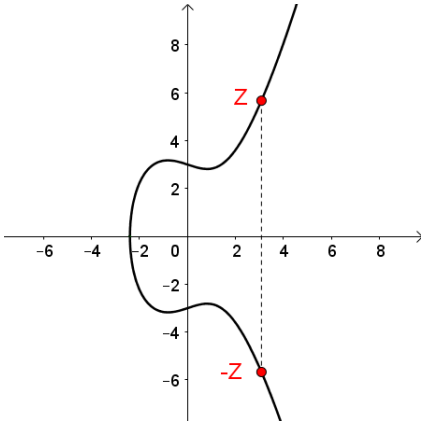
Nyní si společně představíme základní operace probíhající na eliptických křivkách. Bude se jednat o operace, které jsou následně využity při šifrování na bázi eliptických křivek. Tyto jevy si ukážeme na eliptické křivce o rovnici $y^2 = x^3 - 2x + 9$. Jako první operaci, kterou si uvedeme, bude negace bodu na eliptické křivce.

4.4.2.1. Negace bodu na eliptické křivce

Jak se v definici uvádí, negace bodu na eliptické křivce je: *Ke každému bodu* $Z[x, y]$, *jenž leží na eliptické křivce* $\mathcal{E}$ *a který není bodem v nekonečnu* $\mathcal{O}$, *lze sestrojit opačný bod* $-Z\ [x, -y]$*:*

$$\forall Z[x, y] \epsilon\ \mathcal{E} \wedge Z \neq \mathcal{O} \qquad \exists - Z[x, -y].$$

Z definice, kterou jsme nyní napsali, vyplývá, že *negaci bodu Z provedeme prostým otočením znaménka u y-ové souřadnice. Bod Z a jeho negace $-Z$ jsou symetrické podle osy x.* (Oulehla, 2017) Tento jev je naznačen na následujícím obrázku 11.



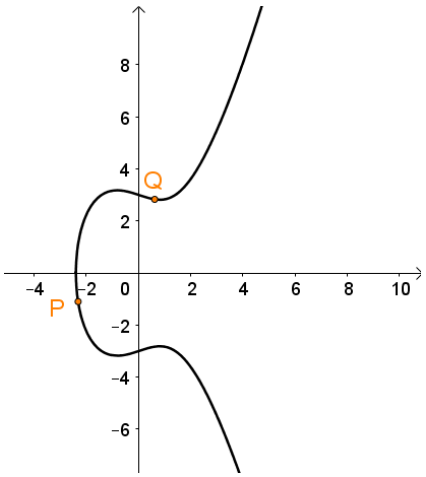
Obrázek 11: negace bodu na eliptické křivce (zdroj: autorka)

4.4.2.2. Operace sčítání na eliptické křivce $\mathbf{P + Q = R}$

Sčítání dvou různých bodů *P*, *Q* na eliptické křivce není pouhé sečtení *x*-ové a *y*-ové složky, tj.

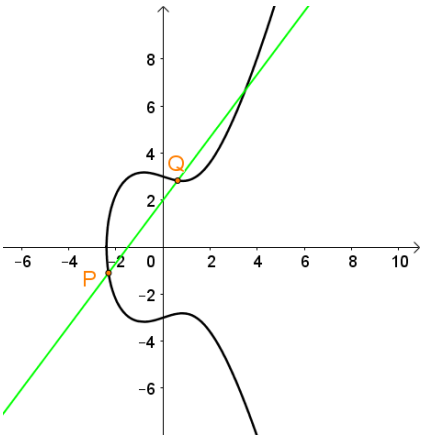
$$P[x_p, y_p] + Q[x_q, y_q] \neq R[x_p + x_q, y_p + y_q].$$

Při sčítání dvou bodů musíme brát v úvahu body, které nejsou opačné a které zároveň leží na eliptické křivce (viz obrázek 12).



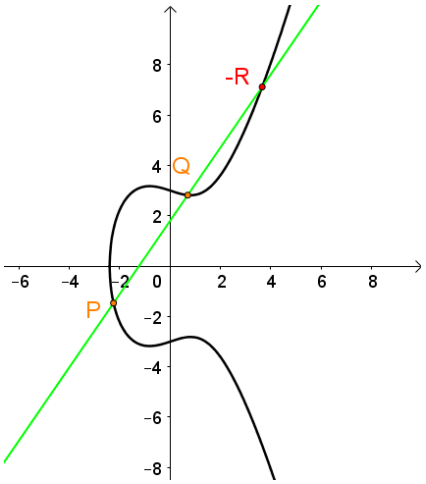
Obrázek 12: pozice bodů P a Q na grafu eliptické křivky (zdroj: autorka)

Následně oba body proložíme přímkou. Proložení můžeme vidět na následujícím obrázku (viz obrázek 13).



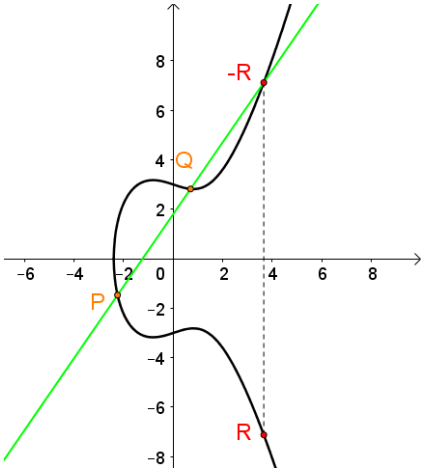
Obrázek 13: proložení bodu P a Q přímkou (zdroj: autorka)

Tato přímka nám protne danou eliptickou křivku v bodě, který označíme $-R$ (viz obrázek 14).



Obrázek 14: průsečík přímky a eliptické křivky (zdroj: autorka)

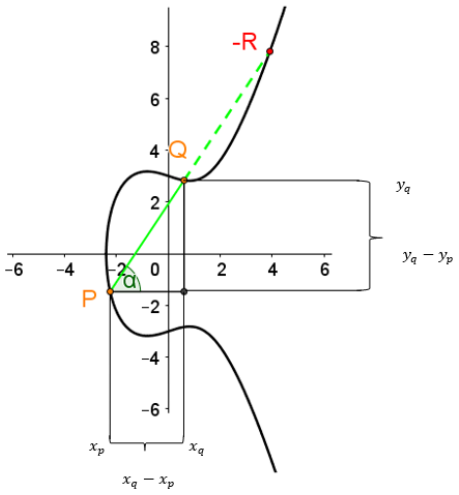
Nakonec musíme provést negaci daného bodu, to znamená, že u bodu $-R$ otočíme y-ovou souřadnici a tím získáme bod R. Můžeme říci, že provedeme osovou souměrnost podle osy x (viz obrázek 15).



Obrázek 15: promítnutí bodu -R na eliptické křivce (zdroj: autorka)

Tento postup lze zapsat též matematicky, čímž si můžeme spočítat dané souřadnice bodu, aniž bychom museli využívat speciální matematický program, který nám danou křivku vykreslí. Tento výpočet má několik kroků, se kterými se seznámíme. Prvním krokem je

výpočet směrnice přímky vedené body P a Q. Směrnice přímky se vypočte pomocí goniometrické funkce tangens. Do obrázku 16 doplníme souřadnice daných bodů a úhel u bodu P.



Obrázek 16: graf eliptické křivky obohacený o souřadnice (zdroj: autorka)

Směrnice přímky, jak již bylo řečeno, se vypočítá pomocí funkce tangens úhlu alfa. Pro tento případ je předpis následující:

$$tg(\alpha) = \frac{protilehlá}{přilehlá} = \frac{y_q - y_p}{x_q - x_p}.$$

U eliptických křivek je zvykem směrnici označovat s. Písmeno s z důvodu anglického označení pro směrnici neboli slope

$$s = \frac{y_q - y_p}{x_q - x_p}.$$

Na příkladu si ukážeme, jak provést součet $P + Q = R$ během několika kroků. Nechť je dána eliptická křivka o předpisu $y^2 = x^3 - 3x + 6$. Známe také x-ovou souřadnici bodů P a Q:

$$x_p = -2,$$

$$x_q = 0{,}96.$$

Kroky k výpočtu součtu $P + Q$:

1. Dopočítat ypsilonové souřadnice bodu P:

$$y_p{}^2 = x^3 - 3x + 6$$

$$y_p = \sqrt{x^3 - 3x + 6}$$

$$y_p = \sqrt{(-2)^3 - 3(-2) + 6}$$

$$y_p = \sqrt{4}$$

$$y_p = \pm 2.$$

V tomto případě jsme si vybrali zápornou variantu.

2. Dále vypočteme ypsilonové souřadnice bodu Q:

$$y_q{}^2 = x_q{}^3 - 3x_q + 6$$

$$y_q = \sqrt{0{,}96^3 - 3 \cdot 0{,}96 + 6}$$

$$y_q = \sqrt{4{,}004\,7}$$

$$y_q \doteq \pm 2.$$

V tomto případě jsme volili kladnou variantu čísla.

3. Nyní známe souřadnice bodu $P[-2;\ -2]$ i bodu $Q\ [0{,}96;\ 2]$.

4. Určit směrnici přímky podle vzorce $s = \frac{y_q - y_p}{x_q - x_p}$:

$$s = \frac{2 - (-2)}{0{,}96 - (-2)}$$

$$s = \frac{50}{37}.$$

5. Vyjádříme neznámou m (posunutí) z rovnice přímky, neboť využijeme skutečnosti, že námi známé dva body leží na jedné přímce, známe také směrnici a souřadnice dvou bodů:

$$y = s \cdot x + m$$

$$m = y - s \cdot x.$$

6. Vypočteme hodnotu daného posunutí, pro jednoduchost výpočtu si vybereme bod $P[-2; -2]$ a dosadíme ho do rovnice $m = y - s \cdot x$:

$$m = -2 - \frac{50}{37} \cdot (-2)$$

$$m = \frac{26}{37}.$$

7. Vypočtenou směrnici a hodnotu posunutí dosadíme do rovnice pro přímku, na které se budou nacházet body $P, Q, -R$:

$$y = \frac{50}{37} \cdot x + \frac{26}{37}.$$

8. Nyní určíme vzájemnou polohu přímky a eliptické křivky. Tímto vypočteme jejich společné průsečíky:

$$\left(\frac{50}{37} \cdot x + \frac{26}{37}\right)^2 = x^3 - 3x + 6$$

$$\frac{2\,500}{1\,369} \cdot x^2 + 2 \cdot \frac{50}{37} \cdot x \cdot \frac{26}{37} + \frac{676}{1\,369} = x^3 - 3x + 6$$

$$2\,500 \cdot x^2 + 2\,600 \cdot x + 676 = 1\,369 \cdot x^3 - 4\,107 \cdot x + 8\,214$$

$$1\,369x^3 - 2\,500x^2 - 6\,707x + 7\,538 = 0.$$

K vyřešení této kubické rovnice využije online kalkulačku pro kubické rovnice (https://www.hackmath.net/cz/kalkulacka/kubicka-rovnice?a=1369&b=-2500&c=-6707&d=7538&eq3=&submit=Vyřeš, 28. 3. 2021). Průsečíky přímky a eliptické křivky mají tyto x-sové souřadnice:

$$x_1 = -2$$

$$x_2 \doteq 0{,}96$$

$$x_3 \doteq 2{,}865.$$

Hodnota *x*-sové souřadnice x_1 odpovídá *x*-sové souřadnice bodu *P*, *x*-sová souřadnice x_2 odpovídá *x*-sové souřadnici bodu Q. Poslední *x*-sová souřadnice je právě *x*-sová souřadnice bodu $-R$.

9. Zjistit *y*-ovou souřadnici bodu $-R$. Existují dvě varianty. Můžeme dosadit do rovnice eliptické křivky nebo do rovnice přímky, neboť víme, že leží na jejich průsečíku. My si zde vybereme dosazení do rovnice přímky, kde za x dosadíme hodnotu x_3:

$$y = \frac{50}{37} \cdot 2{,}865 + \frac{26}{37}$$

$$y \doteq 4{,}57.$$

Bod $-R$ má souřadnice $-R[2{,}865; 4{,}57]$.

10. Posledním krokem pro zjištění hodnoty součtu na eliptické křivce je provedení negace bodu $-R$. Bod R bude mít souřadnice $R[2{,}865, -4{,}57]$.

Výsledkem je bod $R[2{,}865; -4{,}57]$, který odpovídá součtu bodů P a Q na eliptické křivce $y^2 = x^3 - 3x + 6$.

4.4.2.3. Operace sčítání $\mathbf{P + P = 2P = R}$

Tato operace je v angličtině označována slovem doubling. V češtině je tento pojem pojmenováván jako zdvojení, neboť se jedná o sčítání jednoho stejného bodu P na eliptické křivce.

Než přejdeme k této problematice, musíme si uvědomit, že pokud sčítáme dva odlišné body, tak je musíme nejdříve proložit přímkou a teprve pak hledat průsečík přímky s danou eliptickou křivkou. Avšak v tomto případě máme bod jen jeden. Z toho lze usoudit, že se bude jednat o tečnu, protože tečna je přímka, která se dotýká daného grafu pouze v jednom místě. Tečna ke grafu funkce v bodě dotyku P, který má souřadnice $P = [x_p, y_p]$ je dána rovnicí:

$$y - y_p = y'_p \cdot (x - x_p),$$

kde y'_p představuje první derivaci a také hledanou směrnici, kterou si nyní odvodíme. Vycházíme z předpokladu, že výpočet y-ové souřadnice funkce se počítá podle definice eliptické křivky, podle následujícího předpisu:

$$\mathrm{y} = \sqrt{x^3 + ax + b}.$$

Jelikož nás zajímá bod dotyku, tak můžeme souřadnice bodu P dosadit do předchozího předpisu. Vznikne nám následující rovnice:

$$y_p = \sqrt{x_p^3 + ax_p + b}.$$

Tento předpis si ještě upravíme, aby se nám lépe derivoval, tj. odmocninu si přepíšeme jako mocninu. Druhá odmocnina se může přepsat jako mocnina ½:

$$y_p = (x_p^3 + ax_p + b)^{\frac{1}{2}}.$$

Před samotným derivováním je ještě dobré připomenout, že písmena a, b budeme považovat za konstanty, nikoli za proměnné.

Derivace složené funkce se skládá ze dvou dílčích kroků, které jsou mezi sebou vynásobené. V prvním kroku se jedná o derivaci vnější funkce a druhým krokem je derivace samotné vnitřní funkce (vnitřní funkce je funkce, která se v našem případě nachází uvnitř závorky).

Nyní provedeme samotnou derivaci funkce:

$$y_p = (x_p^3 + ax_p + b)^{\frac{1}{2}}$$

$$y'_p = \frac{1}{2 \cdot (x_p^3 + ax_p + b)^{\frac{1}{2}}} \cdot (3 \cdot x_p^2 + a)$$

$$y'_p = \frac{1}{2\sqrt{x_p^3 + ax_p + b}} \cdot (3 \cdot x_p^2 + a)$$

$$y'_p = \frac{3 \cdot x_p^2 + a}{2\sqrt{x_p^3 + ax_p + b}}.$$

Po důkladném prozkoumání vzniklé první derivace můžeme zjistit, že se ve druhé odmocnině ve jmenovateli nachází výraz, který je roven y_p. Z toho důvodu výraz pod mocninou nahradíme y_p a vznikne nám předpis, který bude roven

$$y'_p = \frac{3 \cdot x_p^2 + a}{2 \cdot y_p}.$$

Tento výraz je také roven směrnici tečny dané eliptické křivky. Jelikož se směrnice tečny dané eliptické křivky označuje písmenem *s*, tak i rovnice $y'_p = \frac{3 \cdot x_p^2 + a}{2 \cdot y_p}$ bude rovna písmenu *s*. Vznikne nám předpis, který má následující tvar:

$$s = \frac{3 \cdot x_p^2 + a}{2 \cdot y_p}.$$

Nyní již známe předpis směrnice, teď stačí jen upravit rovnici pro výpočet *x*-ové souřadnice. K tomu použijeme vzorec pro součet dvou různých bodů:

$$x_r = s^2 - x_p - x_q.$$

V našem případě sčítáme stejný bod, z toho důvodu přechozí vztah ještě upravíme:

$$x_r = s^2 - x_p - x_p = s^2 - 2 \cdot x_p.$$

Pro výpočet *y*-ové souřadnice máme dvě varianty výpočtu. První z nich je prosté dosazení do předpisu $y^2 = x^3 + ax + b$, kde *a, b* jsou libovolné konstanty. Pokud za *x* dosadíme,

spočítáme *y*-ovou souřadnici. Druhým způsobem je dosazením do vzorce, pro *y*-ovou souřadnici, který můžeme nechat beze změny, neboť se v této rovnici nenachází žádné souřadnice bodu *Q:*

$$y_r = -y_p + s(x_p - x_r).$$

Pak už stačí jen napsat souřadnice bodu R.

Tento postup si nyní ukážeme na konkrétní eliptické křivce, která je dána předpisem $y^2 = x^3 - 2x + 5$ a chceme provést operaci sčítání $P + P = 2P = R$, kdy víme, že bod P má souřadnice $P[-2, -1]$. Postup je uveden v jednotlivých krocích.

Kroky k výpočtu $P + P$:

1. Výpočet směrnice tečny:

$$s = \frac{3 \cdot x_p^2 + a}{2 \cdot y_p} = \frac{3 \cdot (-2)^2 - 2}{2 \cdot (-1)} = -5$$

2. Výpočet *x*-ové souřadnice bodu R:

$$x_r = s^2 - 2 \cdot x_p = (-5)^2 - 2 \cdot (-2) = 29$$

3. Výpočet y_r:

$$y_r = -y_p + s(x_p - x_r) = -(-1) + (-5)(-2 - 29) = 156$$

Souřadnice bodu R jsou $R = [29; 156]$.

4.4.2.4. Operace násobení bodu skalárem

Poslední operace, o které se v této práci zmíníme, bude násobení bodu skalárem. Tuto operaci lze chápat jako postupné sčítání. Například 3P, lze provést jako postupné sčítání. Nejdříve provedeme 2P a poté k tomu přičteme ještě jednou P.

4.4.3. Geometrická interpretace eliptických křivek nad konečným polem

Interpretace eliptických křivek není jenom nad polem *T*, ale existuje i další varianta interpretace eliptických křivek, kterou můžeme nazvat druhou variantou. Jedná se o geometrickou interpretaci eliptických křivek nad tzv. konečným polem. Tím se rozumí, že budeme brát v úvahu všechny eliptické křivky, které mají na poli konečně mnoho prvků. Pro tuto interpretaci platí, že všechny principy a výpočetní techniky jsou v geometrické interpretaci eliptických křivek nad Galoisovým polem totožné s geometrickou interpretací eliptických křivek nad polem T.

Eliptické křivky lze také v kryptografii napsat pomocí rovnice:

$$y^2 \, mod(p) \equiv (x^3 + ax + b) \, mod(p),$$

kde p je prvočíslo, pro které musí platit $p > 3$ a pro koeficienty a, b platí podmínka

$$(4 \cdot a^3 + 27 \cdot b^2) \, mod(p) \neq 0.$$

Diskriminant D se v tomto případě nad Galoisovým tělesem vypočítá podle vztahu:

$$D = -16 \cdot (4 \cdot a^3 + 27 \cdot b^2),$$

pro který platí podmínka, že se nesmí rovnat nule.

Rovnici eliptické křivky $y^2 \, mod(p) \equiv (x^3 + ax + b) \, mod(p)$ za předpokladu, že Galoisovo těleso splňuje podmínku, že char $T \neq 2, 3$ lze pomocí vhodné změny souřadnic transformovat na rovnici:

$$y^2 = x^3 + ax + b.$$

Rovnici eliptické křivky $y^2 \, mod(p) \equiv (x^3 + ax + b) \, mod(p)$ lze pak za předpokladu, že existuje konečné pole s charakteristikou, která je rovna 2, transformovat vhodnou změnou souřadnic na rovnici označovanou jako nesupersingulární eliptickou křivku

$$y^2 + xy = x^3 + ax + b$$

nebo jako tzv. supersingulární eliptickou křivku, která bude mít rovnici

$$y^2 + cy = x^3 + ax + b$$

a která bude mít diskriminant roven c^4.

Eliptická křivka nad konečným polem je tvořena konečnou množinou bodů $P[x, y]$*, jejichž souřadnice* $x, y \in GF(p)$ *splňují rovnici* $y^2 mod(p) \equiv (x^3 + ax + b)\, mod(p)$*. Do množiny bodů eliptické křivky rovněž zahrnujeme i bod v nekonečnu* $\mathcal{O}$ (Oulehla, 2017).

4.4.4. Využití eliptických křivek v šifrování

Jedním z důležitějších využití eliptických křivek v kryptografii je Diffie-Hellmanův protokol na eliptické křivce, který v odborné literatuře můžeme najít pod zkratkou ECDH. Tato zkratka v sobě skrývá anglický název jednoho z nejznámějších algoritmů v oblasti eliptických křivek, tj. Elliptic Curve Diffie Hellman. Existují i další algoritmy, které jsou známy pod svými zkratkami, např. ECIES (= Elliptic Curve Integrated Encryption Scheme).

5. Hybridní šifrování

Ve světě kryptosystémů se nepoužívá jen jeden druh šifrování, ale můžeme se setkat se šifrováním, které je přechodem mezi symetrickým a asymetrickým šifrováním. Označuje se jako hybridní šifrování.

Hybridní metody šifrování se skládají ze symetrické části s pouze jedním klíčem a z asymetrické části s párem klíčů, jak s veřejným, tak i se soukromým. Z obou těchto šifrování se využívají jejich pozitiva, ze symetrického šifrování rychlost a z asymetrického šifrování jeho „použitelnost“.

Odesílatel si volí klíč, kterým symetricky zašifruje zprávu. Tento klíč je následně zašifrován veřejným klíčem adresáta a pošle ho spolu se zprávou adresátovi, Ten obdrží asymetricky zašifrovaný klíč a symetricky zašifrovanou zprávu. Klíč se musí rozšifrovat soukromým klíčem a následně využije ten klíč, který byl zašifrován, k rozšifrování samotného textu.

Tento typ šifrování je výhodnější, protože se nemusí posílat klíč jako při symetrickém šifrování a zároveň je tento princip šifrování rychlejší.

5.1. PGP

Mezi hybridní šifrování patří PGP systém, jehož první verze byla zveřejněna v roce 1991 Philem Zimmermannem ze společnosti Pretty Good Software. Avšak v roce 1997 byl tento PGP systém prodán samotným autorem firmě NAI.

Název PGP skrývá v sobě anglickou zkratku Pretty Good Privacy. *PGP je šifrovací program, který používal pro šifrování symetrickou šifru IDEA a pro přenos klíčů asymetrickou šifru RSA. Dnes patří mezi nejrozšířenější šifrovací programy používané internetovou komunitou. Pro soukromé účely je zadarmo* (Vondruška, 2006).

Používá se pro bezpečnou elektronickou poštu a umožňuje správu klíčů, šifrovat a rozšifrovat zprávy, digitálně je podepisovat nebo ověřovat identitu odesilatelů (Koláček, 2009).

6. Využití šifrování

Šifrování nepatří jen do světa vědců a matematiků, kteří se tímto tématem zabývají. Málokdo si uvědomí, že kryptologie se stává běžnou součástí našeho života, protože ji často využíváme, aniž si to uvědomujeme. V této kapitole se seznámíme s využitím kryptosystémů, se kterými se můžeme setkat v běžném životě, v zaměstnání, při platbě v obchodech, nebo přes internet, při sledování filmů, a to v podobě digitálního elektronického podpisu, ochrany autorských dat, ale také v problematice optických discích (systém AACS), v systému pro řízení přístupu ke službám (Kerberos) a v platebním protokolu 3D Secure. Dalším praktickým využitím šifrování jsou například elektronické volby, elektronické peníze atd.

6.1. Digitální podpis

Jednou z mnoha aplikací šifrování s veřejným klíčem je problematika digitálního podpisu. *V legislativě se namísto pojmu digitální podpis často používá pojem elektronický podpis (Burda, 2015).* Lze říct, že *digitální podpis je velmi složitý, zašifrovaný číselný kód, který je pro každého uživatele ojedinělý obdobně jako otisk prstu a který je právně ověřitelný* (Bezpalec, 2015). U digitálního podpisu se používá hash funkce s technikou šifrování s veřejným klíčem. *Cílem zde není utajení obsahu dokumentu, ale ověření jeho autenticity (tedy ověření identity autora dokumentu) a integrity (tedy prokázání, že se dokument cestou nezměnil). Odesílatel vytvoří hash dokument a svým soukromým klíčem ho zašifruje. Dokument a zašifrovaný hash pošle příjemci.* (https://www.napocitaci.cz/33/symetricke-a-asymetricke-sifrovani-uniqueidgOkE4NvrWuNY54vrLeM677jX7sp3Lu-ZpLpGVMy1prA/, 7. 7. 2020)

Nutná je i znalost certifikační autority, která má za úkol ověření autenticity. Odesílatel si nechá na začátku vygenerovat dva klíče, veřejný a soukromý. Veřejný si nechá zkontrolovat certifikační autoritu. Ověření si může udělat i příjemce.

Úkolem elektronického podpisu není utajit obsah zprávy, ale zajistit průkaznost toho, že po podpisu nebyl obsah otevřeného textu změněn a že elektronický podpis mohla vytvořit jen konkrétní osoba, která to nemůže popřít. Pracuje se s dvojicí klíčů jiným odlišným způsobem než při šifrování (Vondruška, 2006).

Transformaci, kterou provede vlastník soukromého klíče s otevřeným textem, nazýváme elektronickým podpisem. Každý, kdo má přístup k veřejnému klíči, může pomocí něj ověřit, že byl opravdu elektronický podpis vytvořen pomocí odpovídajícího soukromého klíče.

U elektronického podpisu se využívá RSA šifrování a *vyhláška k zákonu o elektronickém podpisu umožňuje podepisovat i pomocí eliptických křivek* (Klíma, 9/2002).

Bezpečnost hashovací funkcí je jedním z klíčových parametrů bezpečnosti elektronického podpisu (Budiš, 2008). Hash funkce se podílí na tvorbě elektronického podpisu svou hash hodnotou, která se dá vypočítat. Ta bývá o něco kratší než samotná zpráva, která je podepisovaná a následně zašifrována pomocí asymetrického šifrování.

Výhodou elektronického podpisu je, že splňuje stejná bezpečností kritéria jako autorizace celého dokumentu, provedení však trvá nesrovnatelně kratší dobu (Budiš, 2008).

Základní vlastností elektronického (digitálního) podpisu je autentičnost, kdy pouze odesílatel zná soukromý klíč a je skutečným autorem dokumentu. Vytvoření takového klíče je různé, protože můžeme použít nejrůznější asymetrické kryptografické algoritmy s veřejným klíčem, například RSA, DSA, nebo bezpečné hash funkce, například MD5.

Elektronický podpis může být také šifrován pomocí eliptických křivek, a pak ho známe pod zkratkou ECDSA (= Elliptic Curve Digital Signature Algorithm). Tento princip elektronického podpisu zmiňuje i vyhláška k zákonu o elektronickém podpisu České republiky.

6.2. Systém AACS

Nejenom u digitálního podpisu se využívá šifrování, ale také je možné ho nalézt u záznamů na optický disk. Jedná se o s*ystém AACS (= Advanced Access Content System), který je určen k ochraně audiovizuálního obsahu optických disků před neoprávněnou prezentací obsahu a před neoprávněným kopírováním tohoto obsahu* (Burda, 2013). *Optický disk je typ moderního paměťového média diskového tvaru* (https://www.sprava-site.eu/opticky-disk/, 10.8.2020). Jedná se o disky typu CD, DVD, HD DVD a Blu-Ray.

Z hlediska šifrování je tento systém jednosměrným přenosovým systém, kde jsou zprávy svým původcem odeslány na optické disky. *Oprávněnými příjemci obsahu jsou majitelé přehrávačů, kteří obsah disků prezentují a disky kopírují s pravidly vyžadovanými výrobcem disků* (Burda, 2013). Ti, kteří nejsou majiteli přehrávače, jsou považovány za útočníky.

Techniky šifrování v systému AACS zajišťují důvěrný přenos chráněného obsahu na disku a také aktualizaci oprávněných příjemců obsahu. Důvěrný přenos chráněného obsahu na disku je realizován jeho šifrováním. Může se také jednat o samostatné jednotky, které jsou označovány jako tituly. Tím může být buď film, část nějakého filmu nebo seriálu, film o filmu, upoutávka na film. Každý titul *T* je zašifrován svým klíčem titulu *K* za použití blokové šifry AES o délce 128 bitů. Během šifrování jsou použité vždy klíče, které jsou odlišné a *iniciační vektor IV je konstanta určená standardem* (Burda, 2013).

Kryptografické klíče se v tomto systému odvozují pomocí úplných binárních stromů.

6.3. Standard SSL

Šifrování proniklo i do elektronické komunikace, a proto slouží také k zabezpečení komunikace po internetu. Mezi nejpokrokovější techniky v dnešní době můžeme zařadit i standard SSL (Secure Sockets Layer), který vymezí univerzální bezpečnostní protokol využívaný zejména pro ochranu komunikace s webovými servery, a tudíž i využití pro e-business a internetové bankovnictví.

Tento standard byl vyvinut ve 20. století, v roce 1994, firmou Netscape Communication. *Je podporován populárními klientskými aplikacemi (např. Netscape, Navigator, Microsoft a Internet Explorer), serverovými aplikacemi (např. Netscape, Microsoft a Apache) a certifikačními autoritami* (Bezpalec, 2015).

Základem pro zajištění bezpečného spojení pomocí tohoto standardu jsou certifikáty, které obsahují údaje o svém majiteli, o jeho veřejném klíči a také údaje o certifikační autoritě. Každá strana, která se účastní komunikace, si pomocí veřejného klíče ověří digitální podpis certifikátu a z něj zjistí údaje o druhé straně komunikace, tzv. protistraně.

K šifrování jsou použity klíče, které jsou automaticky generovány na základě náhodně zvolených dat. Také je brán ohled na to, aby dané klíče nezískala nepovolaná osoba, nebo aby je nemohl tak snadno získat. Proto hlavním cílem tohoto standardu je zajištění vysoké úrovně bezpečnosti a nezávislosti klienta na určitém počítači a jeho maximálním pohodlí, neboť *ověření identity serveru, se kterým klient komunikuje, zajišťuje automaticky internetový prohlížeč* (Bezpalec, 2015).

Standard SSL využívá kryptografii s veřejným klíčem pro výměnu klíče sezení mezi klientem a daným serverem pokaždé s novým unikátním klíčem.

6.4. Autentizační protokol Kerberos

Kerberos je v řecké mytologii bájné zvíře o dvou či třech hlavách, jehož úkolem je hlídat říši mrtvých, ale v oblasti šifrování je Kerberos autentizační protokol.

Protokol Kerberos je síťový autentizační protokol, který na základě úvodní autentizace uživatele zajišťuje jeho následující autentizace v síti zcela automaticky (Burda, 2013).

Tento protokol je definovaný na základě standardu RFC-4120 a na jeho činnosti se podílejí čtyři strany (klient, autentizační server, správní server, server), které jsou mezi sebou propojené.

Tento autentizační protokol Kerberos vychází z Needham-Schroederova protokolu a je založen na znalosti tajných klíčů symetrického systému.

Kerberos vychází na principu dvou navazujících středisek distribuce klíčů, přičemž použité klíče jsou použité jak k šifrování, tak i k autentizaci. Prvním střediskem distribuce klíčů je autentizační server AS, který na žádost klienta vygeneruje klíč (Burda, 2013). Druhým střediskem je správa klíčů serverů, která je označována SS.

6.5. Platební protokol 3D Secure

Dalším praktickým využitím šifrování, které si uvedeme, je platební protokol 3D Secure označovaný také jako protokol pro internetové platby kartou. *Přesněji řečeno se jedná o obecný rámec pro tento druh plateb, neboť nestanovuje žádný závazný způsob komunikace mezi zúčastněnými stranami* (Burda, 2013). K autentizaci zákazníka je většinou nutná metoda principu tajného hesla. Kryptografické zabezpečení VISANet není veřejné.

Jedná se o pětistranný protokol, jehož aktéři jsou *zákazník, obchodník, banka zákazníka, banka obchodníka a prostředník* (Burda, 2013). Jako prostředníka si můžeme uvést specializovaný server finanční asociace VISA, který tento protokol podporuje. Ke komunikaci mezi sebou jednotlivé strany používají internet na základě protokolu HTTP s funkcí přesměrování stránky.

Označení 3D Secure vyžaduje skutečnost, že v rámci protokolu existují tři domény, které jsou spravovány třemi různými správci. Toto řešení má tu výhodu, že každý správce si může spravovat svou doménu podle svých vlastních potřeb.

Nyní si stručně popíšeme princip samotné komunikace v několika krocích. Jako první krok je výběr zboží zákazníkem na e-shopu libovolného obchodu, kdy po ukončení výběru odešle zákazník seznam své objednávky obchodníkovi. Platební protokol 3D Secure přesměruje objednávku zákazníka na internetovou stránku obchodníka. Pak s příkazem k platbě pošle přes zákazníka také údaje o své bance, které jsou potřebné pro další zpracování objednávky. Po řádném vyplnění údajů si banka ověří správnost informací o elektronické transakci peněz. Banka obchodníka si ověří, zda banka zákazníka využívá požadovaný protokol 3D Secure a také si zjistí webovou adresu banky zákazníka. Na webové stránce banky zákazníka se objeví následující údaje o transakci, tj. název obchodníka a cenu nákupu. Zákazník zde vyplní po zkontrolování osobních údajů své heslo. Tímto procesem zákazník schválí provedení úhrady dané částky. Po uskutečnění převodu banka obchodníka pošle zákazníkovi informaci o převedení dané částky a odešle zákazníkovi jeho již objednané i zaplacené zboží na požadovanou adresu.

Výše popsaný princip, není jediný, který je v elektronickém bankovnictví využívaný.

6.6. Smart karty

I v současné době lidé za zboží a služby stále platí mincemi a bankovkami, ale z důvodu bezpečnosti častěji platí pomocí kreditních karet a ani si neuvědomují, že i zde se vyskytuje šifrování. Můžeme tedy říct, že další využití kryptosystémů v praxi jsou smart karty a bankovní aplikace realizované na nich za použití symetrického algoritmu šifrování DES a asymetrického šifrovacího algoritmu RSA.

Smart karty slouží jako prostředek pro zajištění požadované úrovně bezpečnosti. Za posledních pár let se technologie právě zmíněných smart karet velice rychle začala rozvíjet a tím dosáhla úrovně snadné integrace do veřejných infrastruktur. Dnes tyto karty disponují objemem paměti až 65 kB pro uložení nejrůznějších certifikátů, klíčů, ale i dalších informací, které v sobě skrývají kryptografické procesory sloužící ke generování digitálního podpisu pomocí RSA a DES s délkou klíčů 1 024 bitů.

Jsou využívány pomocí mobilního komunikačního systému pro identifikaci uživatele a následné poskytování služeb a jejich ověření. Také jsou používány pro samotné bankovnictví. Kreditní karty existují jak pro zákazníky, zaměstnance firem nebo pouze pro občany.

Samotné smart karty jsou opatřeny také čipovými kartami, které zvyšují bezpečnost bezhotovostních plateb.

Existuje několik typů smart karet. Jako příklady můžeme uvést jednoduché smart karty (ty se orientují na systém souborů bez veřejného klíče, zápis souborů může být chráněn různorodými podmínkami přístupu a podporují pouze kryptografický algoritmus DES nebo 3DES) a pokročilé smart karty (ty se zaměřují na systém souborů s veřejným klíčem)

Závěr

Cílem diplomové práce bylo seznámit zájemce i širokou veřejnost s problematikou šifrování a využití matematiky v této oblasti. Práci o kryptologii jsem rozdělila do několika důležitých kapitol podle jednotlivých druhů šifrování na základě využívaných klíčů. U každé zmíněné šifry je uvedena stručná historie, jak se tvoří a jaká je její bezpečnostní úroveň. Nezapomněla jsem ani na vysvětlení základních pojmů, které se týkají kryptosystémů a šifer, tak aby byly srozumitelné. Vše je doplněno o názorné příklady s konkrétními čísly, která čtenářům pomohou problematiku šifrování ještě hlouběji pochopit. K některým příkladům byly vytvořeny tabulky, rovnice a barevné grafy, které slouží jako vizuální podpora. Zajímavou částí práce je šifrování na bázi eliptických křivek, kde je grafické řešení známější než početní. Z tohoto důvodu je zde zpracováno hodně eliptických křivek, které jsou zajímavé a poučné. Při psaní diplomové práce jsem si stanovila jako poslední úkol, seznámit všechny čtenáře o praktickém využití kryptosystémů v běžném životě. V současném světě totiž používáme kryptografii čím dál víc častěji, aniž bychom si to uvědomovali a vnímali. Kryptosystémy dneška budou v blízké budoucnosti překonány a budou vymyšleny jiné, které budou lepší a dokonalejší, ale největší šifrovací systém bude stále náš mozek a jeho myšlenky.

Zdroje

Knihy a časopisy – české:

- Bezpalec, P. (2015): *Nové trendy v elektronických komunikacích. Kryptografie*, Praha: České vysoké učení technické v Praze
- Budiš, P. (2008): *Elektronický podpis a jeho aplikace v praxi*, Olomouc: ANAG
- Burda K. (2013): *Aplikovaná kryptografie*, Brno: Vutium
- Burda K. (2015): *Úvod do kryptografie*, Brno: akademické nakladatelství Cerm
- Burda K. (2019): *Kryptografie okolo nás*, Praha: edice CZ.NIC
- Jiroušek R. a kol. (2006): *Principy digitální komunikace*, Voznice: LEDA
- Klíma V. (9/2002): *Eliptické křivky a šifrování (1.)*. Chip, 134-136
- Klíma V. (10/2002). *Eliptické křivky a šifrování (2.)*. Chip, 160-162
- Koláček, M. (2009): *Šifrování a biometrie pod drobnohledem*, 2009 online článek dostupný https://www.svethardware.cz/sifrovani-a-biometrie-pod-drobnohledem/25723 (cit. 2. 7. 2020)
- Oulehla M. a Jašek R. (2017): *Moderní kryptografie. Průvodce světem šifrování*, Praha: IFP Publishing s. r. o.
- Pelánek R. (2012): *Programátorská cvičebnice. Algoritmy v příkladech*. Praha: Computer Press
- Piper F. a Murphy, S. (2006), *Kryptografie. Průvodce pro každého*. Praha: Dokořán
- Pop T., *Kryptografie a její použití při zabezpečeném přenosu datových souborů*, Praha, 2006, Bakalářská práce, Univerzita Karlova v Praze, Matematicko-fyzikální fakulta
- Stroukal, D. a Skalický, J. (2018): *Bitcoin a jiné kryptopeníze budoucnosti*: *historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Grada Publishing a. s.
- Tlustý, P. (2006): *Obecná algebra pro učitele.* České Budějovice: Jihočeská univerzita
- Vondruška P. (2006): *Kryptologie, šifrování a tajná písma*. Praha: Albatros

Knihy – cizojazyčné:

- Музагафаров А. (2018) *Шифрованный мир: азы криптографии. Просто, понятно и увлекательно*. Издательские решения
- Панасенко, С. П. (2009): *Алгортимы шифрования. Специальный справочник*. Санкт-Петербург: БХВ-Петербург

Internetové zdroje (k 20.4.2021)

- https://intsystem.org/security/asymmetric-encryption-how-it-work/
- https://infedu.ru/2017/05/05/kto-pridumal-bit/
- http://www.kryptografie.wz.cz/uk.htm
- https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7029
- https://cs.wikipedia.org/wiki/Secure_Hash_Algorithm#SHA-0_a_SHA-1
- https://utmagazine.ru/posts/21195-kriptograficheskaya-hesh-funkciya
- https://www.sites.google.com/site/kriptografics/kriptosistema-s-otkrytym-klucom
- https://www.sites.google.com/site/kriptografics/simmetricnye-kriptosistemy
- https://www.sites.google.com/site/kriptografics/home
- https://cs.wikipedia.org/wiki/Provozní_režim_blokových_šifer
- http://r3al.ru/bezopasnost/simmetrichnoe_shifrovanie.htm
- https://www.napocitaci.cz/33/symetricke-a-asymetricke-sifrovani-uniqueidgOkE4NvrWuNY54vrLeM677jX7sp3Lu-ZpLpGVMy1prA/
- https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7026
- https://www.soselectronic.cz/articles/sos-supplier-of-solution/symetricke-sifry-2140
- https://pctuning.tyden.cz/software/ochrana-soukromi/4711-moderni_metody_sifrovani
- https://www.itnetwork.cz/navrh/algoritmy/algoritmy-ostatni/pod-poklickou-algoritmu-rc4
- http://crypto-world.info/klima/2005/cryptofest_2005.htm#_Toc98987052
- https://sifrovani.fd.cvut.cz