VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

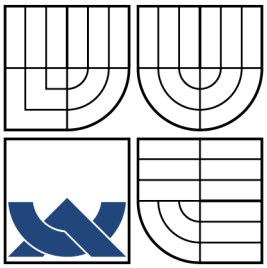
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ELIPTICKÉ KŘIVKY V KRYPTOGRAFII

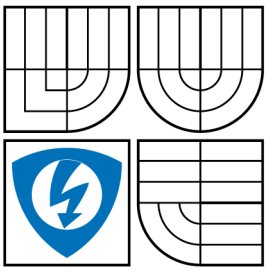
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE LUKÁŠ GEYER
AUTHOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND
COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

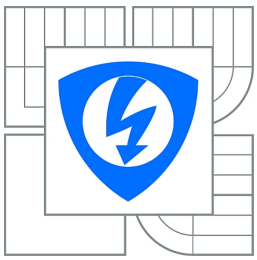
ELIPTICKÉ KŘIVKY V KRYPTOGRAFII

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — LUKÁŠ GEYER
AUTHOR

VEDOUCÍ PRÁCE — Ing. Petra Lambertová
SUPERVISOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Lukáš Geyer ***ID:*** 112044
Ročník: 3 ***Akademický rok:*** 2009/2010

NÁZEV TÉMATU:

Eliptické křivky v kryptografii

POKYNY PRO VYPRACOVÁNÍ:

Nastudujte a popište možnosti využití eliptických křivek v kryptografii. Analyzujte jejich výhody a nevýhody oproti jiným metodám. Zaměřte se především na vužití eliptických křívek pro elektronický podpis. Vytvořte výukovou aplikaci demonstrující jak celý proces probíhá.

DOPORUČENÁ LITERATURA:

[1] HANKERSON, Darrel, MENEZES, Alfred J., VANSTONE, Scott. Guide to Elliptic Curve Cryptography. [s.l.] : Springer, 2004. 311 s. ISBN 978-0387952734.
[2] Elliptic Curve Cryptography [online]. 2009 [cit. 2009-10-13]. Dostupný z WWW: <http://ecc.asp2.cz/>.

Termín zadání: 29.1.2010 ***Termín odevzdání:*** 2.6.2010

Vedoucí práce: Ing. Petra Lambertová

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

ABSTRAKT

Cílem této práce je popsat roli eliptických křivek v moderních kryptosystémech, vysvětlit matematické základy na kterých je tato problematika založena, jejich výhody a nevýhody a následné uplatnění v digitálním podpise. Práce je doplněna o softwarové řešení demonstrující aplikaci eliptických křivek v algoritmu digitálního podpisu ECDSA

KLÍČOVÁ SLOVA

Eliptická křivka, ECDLP, konečné pole, digitální podpis, ECDSA, kryptografie

ABSTRACT

The objective of this bachelor thesis is to decribe the role of the elliptic curves in modern cryptosystems, explain the mathematical fundamentals upon which the elliptic curves are based along with their advantages and disadvantages, followed by application in the digital signature. The project is concluded by a software solution demonstrating the use of elliptic curves in digital signature scheme ECDSA

KEYWORDS

Elliptic curve, ECDLP, finite field, digital signature, ECDSA, cryptography

GEYER, L. *Eliptické křivky v kryptografii*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 34 s. Vedoucí bakalářské práce Ing. Petra Lambertová.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Eliptické křivky v kryptografii“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

(podpis autora)

OBSAH

ÚVOD

Problematika eliptických křivek je v současnosti velice perspektivní oblast moderní kryptografie. Eliptické kryptosystémy umožňují mnohem menší délku šifrovacích/dešifrovacích klíčů než současné asymetrické kryptosystémy při zachování stejné úrovně zabezpečení, což vede ke zvýšení účinosti, miniaturizaci čipů, menšímu zatěžování systémových prostředků atd... Díky rozsáhlému spektru parametrů, které vstupují do procesu generace eliptické křivky, jsme schopni specifikovat úroveň bezpečnosti podle našich potřeb. I přes to, že eliptické kryptosystémy mají mnohé klady, jedná se stále o kryptosystémy relativně mladé ve srovnání s např. RSA, DSA, DH a z důvodu nedostatečného výzkumu do této problematiky v minulých desetiletích jsou tyto starší kryptosystémy stále preferovány.

V 1. kapitole jsou rozebrány základní rozdíly mezi symetrickými a asymetrickými kryptosystémy, základní principy šifrování a dešifrování pomocí eliptických křivek a princip digitálního podpisu.

Ve 2. kapitole je probrána modulární aritmetika a aritmetika konečných polí, které tvoří základní stavební kameny veškerých operací s eliptickýchmi křivkami.

Ve 3. kapitole jsou popsány základní operace na eliptické křivce, zahrnující násobení a sčítání bodů v konečných polích $\mathbb{F}_p$ a $\mathbb{F}_{2^m}$, které jsou v kryptografii eliptických křivek nejčastěji používány, výpočet řádu eliptické křivky, jejího diskriminantu, Weierstrassova rovnice eliptické křivky a její zjednodušené formy.

Ve 4. kapitole jsou vysvětleny algoritmy nezbytné pro šifrování a dešifrování v ECC spolu s generací bezpečné eliptické křivky a klíčového páru soukromého a veřejného klíče.

5. kapitola je věnována teorii digitálního podpisu, jmenovitě jeho implementace v podobě algoritmu ECDSA a jeho propojení s eliptickými křivkami.

V 6. kapitole je popsáno programové řešení bakalářské práce, zahrnující popis jednotlivých obrázků z vypracované výukové animace.

7. kapitola je závěr bakalářské práce, ve kterém je celá problematika eliptických křivek shrnuta.

1 ÚVOD DO PROBLEMATIKY

1.1 Kryptografické základy

Kryptografie je věda zabývající se tvorbou kryptografických algoritmů pro utajení dat před neoprávněnými osobami. Obecně kryptografie spadá do oboru kryptologie, který spolu s kryptografií zahrnuje i kryptoanalýzu, která se zabývá luštěním šifer. Kryptografické algoritmy jsou založené na řešení matematických problémů, které jsou zatíženy vysokou časovou a výpočetní náročností, například faktorizace celých čísel, problém diskrétního logaritmu. V souvislosti s kryptografií je důležité vysvětlit následující pojmy:[5]

1. šifra - šifrou rozumíme, algoritmus, který převádí otevřený text (nešifrovaná data) do zašifrované formy.

2. klíč - jedná se o číselnou hodnotu, která vstupuje do šifrovacího algoritmu za jejíž pomoci se převádí data do šifrované podoby.

3. symetrická šifra - algoritmus využívající pro šifrování a dešifrování stejného klíče.

4. asymetrická šifra - algoritmus využívající dva různé klíče, jeden pro šifrování a druhý pro dešifrování.

5. hašovací funkce - jednocestná funkce, která převádí data na svém vstupu v číselnou hodnotu (otisk) fixní délky na svém výstupu.

6. digitální podpis - zašifrovaný otisk z elektronického dokumentu jednoznačně identifikující odesilatele dokumentu.

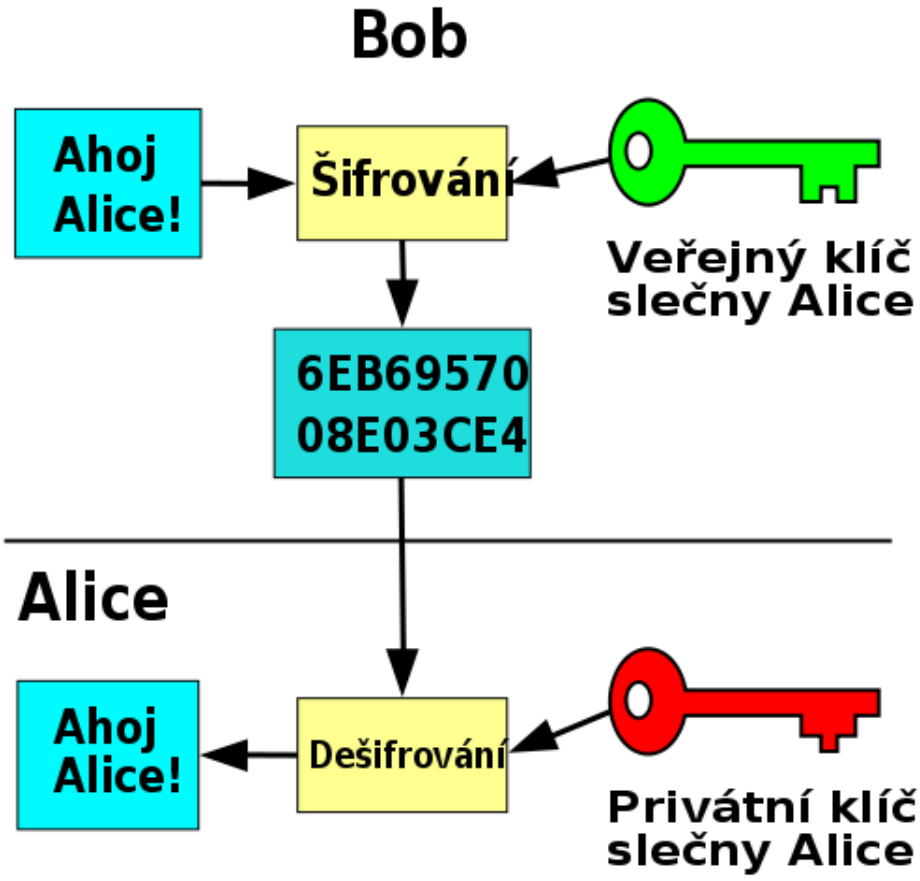
1.2 Asymetrické kryptosystémy

Asymetrické systémy využívají dvou odlišných klíčů, jeden klíč pro šifrování a druhý pro dešifrování. Při implementaci asymetrického kryptosystému jako nástroje pro utajení si musí každá z komunikujících stran vygenerovat jeden pár klíčů, klíč veřejný a klíč soukromý. Soukromý klíč si každá strana uloží na bezpečné místo a veřejné klíče si obě strany vymění přes zabezpečený přenosový kanál (flash karta, počítačová síť). U asymetrických kryptosystému je vyžadováno, aby soukromý klíč nebyl zjistitelný z veřejného klíče v rozumném čase. Tato nezjistitelnost je založena na matematických problémech, které jsou v současnosti neřešitelné v rozumném čase. Těmito problémy jsou následující:[4]

1. Faktorizace čísel (algoritmus RSA) - rozklad celého čísla na součin prvočíselných činitelů tj. $n = p \cdot q$, kde n je celé číslo p, q jsou prvočísla.

2. Problém diskrétního logaritmu - výpočet hodnot x, k je jednoduchý, avšak pro zpětný výpočet hodnoty k při znalosti z, x není znán dostatečně efektivní algoritmus, tj. $z = x^k \bmod p$ je relativně snadné, avšak obrácený postup $k = (\log_x z) \bmod p$ je velice obtížný.

3. Problém diskrétního logaritmu eliptických křivek - výpočet soukromého klíče d ze znalosti veřejného klíče Q a bodu P, tj. výpočet $Q = d \cdot P$ je relativně snadný, ale získání čísla d ze znalosti bodů Q, P je výpočetně velice složitý.



Obr. 1.1: Princip asymetrického šifrování

1.3 Eliptické kryptosystémy

Eliptické kryptosystémy spadají do kategorie asymetrických kryptosystémů aplikujících šifrování a dešifrování za pomoci eliptických křivek. Kryptografie eliptických křivek je založena na obtížnosti řešení problému diskrétního logaritmu eliptických křivek, který lze formulovat následovně $Q = d \cdot P$, výpočtu celého čísla d ze znalosti bodů Q, P se říká problém diskrétního logaritmu eliptických křivek. Mezi nepopiratelné výhody kryptosystémů založených na eliptických křivkách patří menší délka klíčů ve srovnání s ostatními kryptosystémy veřejného klíče (DH, DSA, RSA) při zachování stejné úrovně bezpečnosti jak ukazuje následující tabulka.

Symetrické šifry	ECC	DH/DSA/RSA
80	163	1024
128	283	3072
192	409	7680
256	571	15360

Tab. 1.1: Srovnání velikosti klíčů jednotlivých kryptosystémů

Menší délka klíčů u kryptosystémů na bázi eliptických křivek je umožněna větší složitostí matematického problému, na kterém jsou eliptické křivky postaveny tedy řešení problému diskrétního logaritmu (ECDLP). Další výhodou oproti kryptosystémům založených na řešitelnosti diskrétního logaritmu nebo faktorizace celých čísel je rychlost provádění operací s eliptickými křivkami, která je výrazně vyšší a zároveň oproti systémům založených na faktorizaci (RSA) je rychlejší i generace klíčových párů. EC kryptosystémy umožňují detailní nastavení procesu šifrování díky dostupnosti velké škály parametrů (rovnice křivky, řád bodu, řád křivky, velikost podložního pole, reprezentace pole, typ pole), tyto parametry jsou voleny podle úrovně vyžadované bezpečnosti a podle implementačních požadavků. Mezi nevýhody eliptických kryptosystému spadá obtížnost generace bezpečné eliptické křivky a fakt, že spousta eliptických křivek je patentovaných skupinami jako je například NIST (National Institute of Standards and Technology), ANSI X9F1, IEEE P1363, ISO JTC1 SC27 a SECG. I přesto, že eliptické kryptosystémy mají značné přednosti oproti např. RSA, jsou tyto starší kryptosystémy stále využívány více, což je způsobeno zaběhlostí v reálných aplikací a hlavně skutkem, že výzkum do problému faktorizace čísel nebo problém diskrétního logaritmu je výrazně rozsáhlejší než studie problému ECDLP.

1.4 Digitální podpis

Pod pojmem digitální podpis rozumíme šifrovaný otisk z elektronického dokumentu. Jedná o mechanismus, kterým zajišťujeme určité bezpečnostní atributy daného elektronického dokumentu, kterými si přijímající strana je schopna ověřit integritu přenášeného dokumentu, nepopiratelnost a autenticitu dokumentu, popř. timestamp (čas a datum vytvoření digitálního podpisu. Při výpočtu digitálního podpisu se využívá kryptografická hašovací funkce, která přijme na svůj vstup vybraný elektronický dokument a pomocí hašovacího algoritmu skládajícího se z různých matematických funkcí z něj vypočítá otisk fixní délky. Hašovací funkce má následující přednosti:

1. Sebemenší změna vstupních dat vede k diametrálně odlišnému výstupu. Výsledné otisky změněného a nezměněného dokumentu se při změně například jednoho znaku kompletně liší.

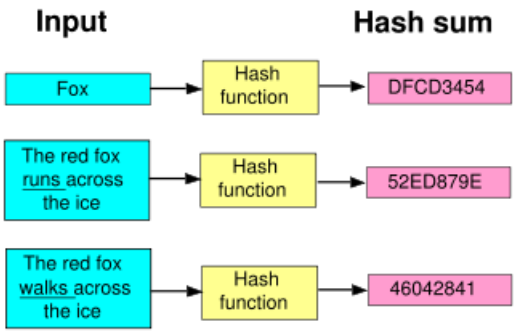
   Př 1.1: Máme 3 vstupní slova: **ahoj, ahoi, ahoy**, na výstupu SHA-1 hašovací funkce obdržíme následující:

   (a) ahoj $\Rightarrow$ EDB433BDD7C13851C7C68CB31A5ACF33A80CD2CC$_{16}$

   (b) ahoi $\Rightarrow$ 16F196E450486F0DB31B7919C5CBCF365E8CA9C9$_{16}$

   (c) ahoy $\Rightarrow$ F1FDF78878CC994E54E8D6476B8E054538E100B9$_{16}$

2. Hašovací funkce generuje otisk fixní délky bez ohledu na velikost vstupu.



Obr. 1.2: Princip hašovací funkce

V technické literatuře se tento otisk také často označuje jako fingerprint, miniatura nebo hash. Výstupem hašovacího algoritmu je tedy celé číslo fixní délky, které tvoří základ digitálního podpisu. V ECDSA algoritmu se jako hašovací funkce využívá SHA-1 (Secure Hash Algorithm), kde výsledný otisk se dále šifruje za pomoci algoritmu eliptických křivek.

2 ARITMETIKA KONEČNÝCH POLÍ

2.1 Úvod do konečných polí

Problematika eliptických křivek se silně opírá o algebraické struktury jako jsou pole, množiny, grupy a aritmetické operace s prvky těchto struktur. Ukázkou nekonečné množiny je například množina reálných čísel $\mathbb{R}$. Pokud na této množině definujeme operace sčítání $(+)$ a násobení $(\cdot)$, vytvoříme tím celočíselné pole. Tyto pole však nejsou vhodné pro kryptografické systémy protože výsledky aritmetických operací s prvky těchto polí jsou postiženy silnou zaokrouhlovací chybou a výpočetní operace jsou sami o sobě velmi pomalé. Proto se v kryptografické literatuře zabývající se eliptickými křivkami setkáváme s označením konečné pole, konečná struktura nebo Galoisovo pole GF (z anglického "*Galois field*"). Všechny tyto označení popisují pole s konečným počtem prvků. Obecně, pole popisuje množinu prvků na které jsou definované určité algebraické operace. V kryptografii jsou těmito operacemi sčítání $(+)$ a násobení $(\cdot)$. Operace odečítání a dělení jsou definovány jako přičítání opačného prvku, operace dělení potom jako násobení inverzním prvkem. Pro konečná pole platí axiomy, které vycházejí ze struktur algebry (grupoid, monoid, pologrupa). Uvažujeme konečné pole $\mathbb{F}$ s operacemi sčítání a násobení, potom platí:

Definice 2.1: Pro každé $(\mathbb{F}, +, \cdot)$, kde $\forall\, a, b, c \in \mathbb{F}$ platí:

Asociativní zákon	$(a + b) + c = a + (b + c)$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Komutativní zákon	$a + b = b + a$ $a \cdot b = b \cdot a$
Distributivní zákon	$a \cdot (b + c) = a \cdot b + a \cdot c$
Existence opačného prvku	$\forall a \in \mathbb{F}$ existuje $-a : a + (-a) = 0$
Existence neutrálního prvku	$a, 0, 1 \in \mathbb{F} : a + 0 = a, a \cdot 1 = a$
Uzavřenost pole vůči sčítání a odčítání	$a + b = c \Rightarrow c \in \mathbb{F}$ $a \cdot b = c \Rightarrow c \in \mathbb{F}$

Struktura definovaná těmito axiomy se nazývá *konečné těleso.* V kryptografii eliptických křivek se pracuje výhradně s tělesy prvočíselnými $\mathbb{F}_p$ a Galoisovými $\mathbb{F}_{p^m}$.

2.2 Prvočíselné těleso $\mathbb{F}_p$

Nechť máme provočíslo pro které platí $p > 3$ pak množina celých čísel $\{0, 1, 2, ..., p-1\}$ spolu s operacemi sčítání a odčítání modulo p tvoří *konečné prvočíselné těleso* $\mathbb{F}_p$. Vzhledem k tomu, že veškeré výpočty jsou výsledkem operace mod p, je zajištěno, že výsledek bude prvkem množiny $\{0, 1, 2, ..., p-1\}$. V prvočíselném tělese je definován jednotkový prvek $1_{\mathbb{F}}$ a prvek nulový $0_{\mathbb{F}}$. Nulový prvek je neutrální vzhledem k operaci sčítání protože platí $a + 0_{\mathbb{F}} = a$ kde $a \in \{0, 1, 2, ..., p-1\}$. Naopak jednotkový prvek je neutrální prvek vzhledem k operaci násobení protože platí $a \cdot 1_{\mathbb{F}} = a$ kde $a \in \{0, 1, 2, ..., p-1\}$. V prvočíselném poli se také setkáme s operací dělení modulo p a odčítání modulo p, avšak jedná se pouze o inverzní operace k násobení a sčítání a proto je nutné také zavést inverzní prvek a^{-1} k násobení pro který platí $a \cdot a^{-1} \equiv 1 \pmod{p}$ a opačný prvek $-a$ k odčítání pro který platí $a + (-a) \equiv 0 \pmod{p}$. Díky inverznímu prvku se elegantně zbavíme zlomků jejichž výsledek často vede k racionálním či iracionálním číslům, které se v kryptografii nepoužívají z důvodu vzniku zaokrouhlovacích chyb. Podle kritérií algebraických struktur je definováno, že konečné těleso má minimálně dva prvky a to prvek nulový $0_{\mathbb{F}}$ a prvek jednotkový $1_{\mathbb{F}}$, například Galoisovo těleso.

2.2.1 Sčítání prvků pole $\mathbb{F}_p$

Při sčítání prvků prvočíselného pole $\mathbb{F}_p$ postupujeme stejně jako při sčítání nad množinou celých čísel $\mathbb{Z}$, pouze s tím rozdílem, že výsledek musí být podroben operaci mod p abychom dodrželi konečnost prvočíselného pole. Protože jak samotné sčítance tak i výsledek operace sčítání musí být kongruentní mod p lze sčítání prvků nad $\mathbb{F}_p$ vyjádřit následující definicí:

Definice 2.2: Nechť $a, b, c \in \mathbb{F}_p$, p je charakteristika pole $\mathbb{F}_p$ pak platí:

$$a + b \equiv c \pmod{p} \tag{2.1}$$

pak rovnice 2.1 je ekvivalentní s následující rovnicí

$$(a + b) \bmod p = c \bmod p \tag{2.2}$$

V literatuře se často mluví o tzv. **aditivní tabulce**[2], která ilustruje operaci sčítání mod p s veškerými prvky množiny $\{0, 1, ..., p-1\}$. Následující tabulka je demonstrací aditivní tabulky pro prvočíselné pole $\mathbb{F}_7$:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Tab. 2.1: Aditivní tabulka provčíselného pole $\mathbb{F}_7$

2.2.2 Odčítání prvků pole $\mathbb{F}_p$

Odčítání je pouze inverzní operace k sčítání za pomoci opačného prvku $-a \in \mathbb{F}_p$ a proto platí:

Definice 2.3: Nechť $a, b, c \in \mathbb{F}_p$ kde $-b \in \mathbb{F}_p$ je inverzní prvek k b pak platí:

$$a - b = a + (-b) \equiv c \pmod{p} \tag{2.3}$$

2.2.3 Násobení prvků pole $\mathbb{F}_p$

Jak sčítání tak i násobení obdobná operace nad $\mathbb{Z}$ pouze s tím rozdílem, že výsledek je podroben operaci mod p. Jako u sčítání mod p nad $\mathbb{F}_p$ existuje aditivní tabulka, tak i pro násobení existuje tzv. **multiplikativní tabulka**[2], která ilustruje operaci $(a \cdot b) \bmod p$ pro včechny $a, b \in \mathbb{F}_p$.

Definice 2.4: Nechť $a, b, c \in \mathbb{F}_p$, p je charakteristika pole $\mathbb{F}_p$ pak platí:

$$a \cdot b \equiv c \pmod{p} \tag{2.4}$$

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tab. 2.2: Multiplikativní tabulka provčíselného pole $\mathbb{F}_7$

2.2.4 Výpočet inverzního prvku v $\mathbb{F}_p$

V mnoha situacích při výpočtech násobků bodu nebo při sčítání bodů se dostaneme do situace, kdy nám vyjde vzorec ve tvaru zlomku a proto je zapotřebí definovat inverzní prvek, kterým se elegantně zbavíme operace dělení a nahradíme ji operací násobení. Inverzním prvek se vyhneme zavedení zaokrouhlovacích chyb do početních operací. Pro výpočet inverzního prvku se využívá rozšířený Euklidův algoritmus:[4]

Algoritmus 2.5: Postup při výpočtu inverzního prvku.
Vstup: Modulus n, proměnná x
Výstup: Inverzní prvek $x^{-1} = b \bmod n$

1. Provedeme výpočet největšího společného dělitele proměnných n, x tak aby platilo $gcd(n, x) = 1$
2. Za pomoci proměnných z toho algoritmu vyjádříme $gcd(n, x)$ jako lineární kombinaci n, x následovně: $gcd(n, x) = 1 = a \cdot n + b \cdot x$

$$(1 \bmod n) = (a \bmod n) \cdot (n \bmod n) + (b \bmod n) \cdot (x \bmod n) \tag{2.5}$$

3. Pro inverzní prvek platí $x^{-1} = b \bmod n$

Př 2.6: Při výpočtu inverzního prvku postupujeme tak, že si vypočítáme gcd(n,x)=1 jako lineární kombinací zbytků mod x. Máme-li například číslo $x = 12$ a potřebujeme k němu vypočítat inverzní prvek nad podložním polem GF(15), pak postupujeme následovně:

1. Nyní si vyjádříme $z_2 = 1$ jako lineární kombinaci zbytků po dělení mod 23

$$z_3 = 48 - 2 \cdot 23$$

$$z_2 = 23 - 2 \cdot 11 = 1 \cdot 23 - 11 \cdot (48 - 2 \cdot 23) = 22 \cdot 23 - 11 \cdot 48$$

$$z_2 = 1 = (22 \bmod 23) \cdot (23 \bmod 23) - (11 \bmod 23) \cdot (48 \bmod 23)$$

Dělenec n	Dělitel x	n div x	n mod x
48	23	2	$z_3 = 2$
23	2	11	$z_2 = 1$
2	1	2	$z_1 = 0$

2. Inverzním prvkem pro $x = 48$ je tedy číslo 12 protože platí $(48 \cdot 12) \bmod 23 = 1$

2.2.5 Dělení prvků pole $\mathbb{F}_p$

Dělení prvků pole $\mathbb{F}_p$ je nahrazeno operací násobení za pomoci inverzního prvku x^{-1}.

Definice 2.7: Nechť $a, b \in \mathbb{F}_p$ a prvek b je invertibilní tzn. existuje k němu inverzní prvek b^{-1} pak pro operaci dělení platí:

$$\frac{a}{b} = a \cdot b^{-1} \bmod p \tag{2.6}$$

2.3 Galoisovo těleso

Označíme-li konečné těleso $\mathbb{F}_{p^m}$, kde $p = 2$ potom se jedná o takzvané **Galoisovo těleso**, v literatuře označované $\mathrm{GF}(\mathbb{F}_{p^m})$ z anglického "*Galois field*". Elementy Galoisova tělesa jsou reprezentovány jako polynomy, o stupni maximálně $m - 1$, kde jednotlivé koeficienty nabývají hodnot $z_i \in \{0, 1\}$:

$$f(x) = z_{m-1}x^{m-1} + z_{m-2}z^{m-2} + ... + z_2x^2 + z_1x + z_0 \tag{2.7}$$

Celkové množství prvků v $GF(\mathbb{F}_{p^m})$ je p^m. Pro počítačové zpracování veškerých aritmetických operací mezi jednotlivými prvky se polynomy reprezentují jako m-bitové vektory koeficientů z_i:

$$(z_{m-1}z_{m-2}...z_2z_1z_0) \tag{2.8}$$

Vzhledem k tomu, že pracujeme s binárními posloupnostmi je počítačové zpracování velmi rychlé a efektivní.

2.3.1 Sčítání prvků pole $\mathbb{F}_{2^m}$

Protože prvky Galoisova pole $\mathbb{F}_{p^m}$ jsou polynomy, které se dají vyjádřit vektorovou notací $(a_{m-1}a_{m-2}a_{m-3}...a_1a_0)$ kde $a_i \in \{0, 1\}$, přechází sčítání polynomů ve sčítání

vektorů, při kterém se vždy sčítají odpovídající hodnoty prvků na odpovídající pozici ve vektoru a výsledek se opět podrobí operaci mod 2.

Definice 2.8: Nechť $a = (a_4a_3a_2a_1a_0), b = (b_4b_3b_2b_1b_0)$ jsou prvky pole $\mathbb{F}_{2^5}$ vyjádřené vektorovou notací koeficientů polynomu pak pro součet $a + b = c$ platí:

$$\begin{aligned} a_4 + b_4 &= c_4 \bmod 2 \\ a_3 + b_3 &= c_3 \bmod 2 \\ a_2 + b_2 &= c_2 \bmod 2 \\ a_1 + b_1 &= c_1 \bmod 2 \\ a_0 + b_0 &= c_0 \bmod 2 \end{aligned} \tag{2.9}$$

Výsledkem je tedy vektor $c = (c_4c_3c_2c_1c_0)$. Protože při sčítání se nemění řád polynomu platí, že $c \in \mathbb{F}_{2^5}$. Další možností sčítání nad $\mathbb{F}_{2^m}$ je využití logické funkce XOR. Funkce XOR se tedy aplikuje jak tomu je i v předchozí metodě na dvojici hod-

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Tab. 2.3: Pravdivostní tabulka funkce XOR

not na odpovídající pozici vektorů a, b. Výhodou této metody je, že na místo dvou výpočetních operací využijeme pouze jednu čímž přispíváme k urychlení výpočtu.

$$\begin{aligned} a_4 \oplus b_4 &= c_4 \\ a_3 \oplus b_3 &= c_3 \\ a_2 \oplus b_2 &= c_2 \\ a_1 \oplus b_1 &= c_1 \\ a_0 \oplus b_0 &= c_0 \end{aligned} \tag{2.10}$$

2.3.2 Odčítání prvků pole $\mathbb{F}_{2^m}$

Všechny prvky Galoisova pole $\mathbb{F}_{2^m}$ jsou svojí vlastní aditivní inverzí protože platí:[6]

$$(a_{m-1}a_{m-2}a_{m-3}...a_1a_0) + (a_{m-1}a_{m-2}a_{m-3}...a_1a_0) = (000...00) \tag{2.11}$$

rovnice 2.11 vyjadřuje takzvanou aditivní identitu. Protože platí aditivní identita je operace sčítání a odčítání nad $\mathbb{F}_{2^m}$ ekvivalentní matematická operace.

Definice 2.9: Nechť $a = (a_4a_3a_2a_1a_0), b = (b_4b_3b_2b_1b_0)$ jsou prvky pole $\mathbb{F}_{2^5}$ vyjádřené vektorovou notací koeficientů polynomu pak díky existenci aditivní identity operace odčítání platí:

$$(a_4a_3a_2a_1a_0) - (b_4b_3b_2b_1b_0) = (a_4a_3a_2a_1a_0) + (b_4b_3b_2b_1b_0) = (c_4c_3c_2c_1c_0) \tag{2.12}$$

2.3.3 Redukční polynomy f(x)

Redukční polynomy tvoří nedílnou součást operace násobení s prvky pole $\mathbb{F}_{2^m}$ kde jednotlivé prvky jsou reprezentovány jako polynomy stupně nejvýše $m-1$. V operacích sčítání a odčítání není zapotřebí redukční polynom používat protože výsledkem těchto operací nikdy není polynom stupně větší než $m-1$. Jinak je tomu u operace násobení kdy součinem dvou polynomů vzniká polynom stupně větší než $m-1$, který již není prvkem pole $\mathbb{F}_{2^m}$ proto je zapotřebí tento výsledek nějakým způsoben redukovat tak, aby patřil do množiny prvků pole $\mathbb{F}_{2^m}$. Zavádí se proto redukční polynom $f(x)$, kterým se pomocí $\mathrm{mod} f(x)$ upravují veškeré operace součinu s prvky pole $\mathbb{F}_{2^m}$ tak, aby stupeň výsledného polynomu byl menší než $m-1$, tedy aby patřil do množiny prvků pole $\mathbb{F}_{2^m}$. Pro využití v kryptografii eliptických křivek se využívají dva typy redukčních polynomů:

1. Trinomiální tvar redukčního polynomu nad polem $\mathbb{F}_{2^m}$:

$$x^m + x^k + 1 \tag{2.13}$$

   pro k platí $1 \leq k \leq m-1$

2. Pentomiální tvar redukčního polynomu nad polem $\mathbb{F}_{2^m}$:

$$x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1 \tag{2.14}$$

   platí $1 \leq k_1 < k_2 < k_3 \leq m-1$

Redukční polynom je tedy každý polynom, který odpovídá triominálnímu nebo pentominálnímu tvaru a platí, že je nad polem $\mathbb{F}_{2^m}$ nerozložitelný, tj. nejde zapsat jako součin dvou polynomů o stupni menší než m.

3 ARITMETIKA ELIPTICKÝCH KŘIVEK

Kryptosystémy na bázi eliptických křivek (ECC) jsou založeny na řešení problému diskrétního logaritmu (ECDLP). Veškeré aritmetické operace zahrnují sčítání nebo násobení bodů z konečného pole nad kterým je elitptická křivka zkonstruována. Z hlediska matematického zařazení jsou eliptické křivky podmnožinou kubických křivek. V souvislosti s kryptografií eliptických křivek je důležité vysvětlit si několik pojmů. Prvním takovým pojmem je diskriminant Δ eliptické křivky. Před samotným počítáním s prvky polí nad kterými je eliptická křivka zkonstruovaná se musí vždy vypočítat hodnota diskriminantu, která poskytuje informaci o nevhodných deformacích eliptické křivky. Pokud je tedy diskirminant nulový jedná se o singulární eliptickou křivku která je deformovaná buď do podoby hrotové nebo uzlové singularity. Pokud je diskriminant eliptické křivky nenulový jedná se o nesingulární eliptickou křivku. Rovnice 3.1 vyjadřuje výpočet diskriminantu z parametrů $a_1, a_2, ..., a_6$.

$$\begin{aligned} \Delta &= -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6 \\ d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + a_1 a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \end{aligned} \tag{3.1}$$

Definice 3.1: Máme-li eliptickou křivku E definovanou nad $\mathbb{F}_p$, kde $1_{\mathbb{F}}$ je jednotkový prvek pole $\mathbb{F}_p$ a $0_{\mathbb{F}}$ je nulový prvek pole $\mathbb{F}_p$, pak charakteristika pole $\mathbb{F}_p$ je definována následovně:[2]

$$1_{\mathbb{F}} + 1_{\mathbb{F}} + ... + 1_{\mathbb{F}} + 1_{\mathbb{F}} = 0_{\mathbb{F}} \tag{3.2}$$

Definice 3.2: Máme-li eliptickou křivku E, potom řád křivky $\#E$ je definován jako počet bodů na křivce. Protože se pohybujeme ve kartézské soustavě souřadnic jednotlivé body jsou ve tvaru $[x, y]$, a vyhovují jedné ze zjednodušených forem Weierstrassovy rovnice, podle typu konečného pole nad kterým je E zkonstruována. K přibližnému výpočtu řádu křivky $\#E$ slouží **Hasseův interval**:[1]

$$\#E : q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q} \tag{3.3}$$

Definice 3.3: Eliptická křivka E definovaná nad konečným polem F, v literatuře označováno E/F, kde $a_1, a_2, a_3, a_4, a_6 \in F$, je reprezentovaná pomocí tzv. **Weierstrassovy rovnice**[1]:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.4}$$

Pomocí transformací proměnných x, y Weierstrassovy rovnice vznikají tzv. zjednodušené formy Weistrassovy rovnice, se kterými se počítá v kryptografické praxi. U prvočíselných polí s charakteristikou $p > 3$ se provádí následující transformace[1]:

$$(x, y) \rightarrow \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24} \right) \tag{3.5}$$

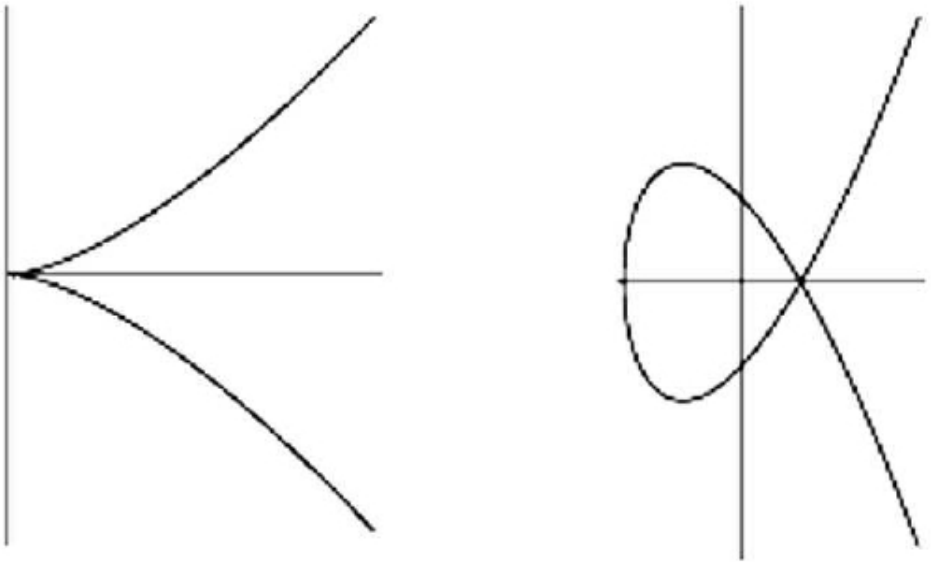
Výsledkem této transformace je pak zjednodušená forma Weistrassovy rovnice pro eliptickou křivku nad prvočíselným polem $\mathbb{F}_p$:

$$E/\mathbb{F}_p : y^2 = x^3 + ax + b \tag{3.6}$$

Máme-li tedy zadanou křivku podle rovnice 3.6 nad $\mathbb{F}_p$ pak všechny body $[x, y]$ v kartézské soustavě souřadnic spolu s bodem v nekonečnu ∞ tvoří množinu bodů, které leží na eliptické křivce E. Porovnáním obecné Weistrassovy rovnice 3.4 a zjednodušené formy 3.6 je zřejmé, že určité parametry a_i jsou nulové a proto vlivem transformace Weistrassovy rovnice dojde i k transformaci diskriminantu Δ. Protože a_1, a_3 a a_4 jsou nulové, pro diskriminant platí:

$$\Delta = -16(4a^3 + 27b^2) \tag{3.7}$$

kde a, b jsou koeficienty eliptické křivky v rovnici 3.6. Důležitou podmínkou je aby platilo $\Delta \neq 0$, což znamená, že daná eliptická křivka může tvořit grupu nad tělesem $\mathbb{F}_p$. Pokud je diskiminant nulový tak křivka je nevyhovujícně zdeformovaná do formy uzlové nebo hrotové singularity, a nemůže být použita v ECC.



Obr. 3.1: Deformované eliptické křivky do formy hrotové a uzlové singularity

V případě Galoisových polí, kde charakteristika pole $p = 2$ se provádí dva typy transformací v závislosti na hodnotě parametru a_1.

1. Pokud $a_1 \neq 0$

$$(x, y) \rightarrow \left(a_1^2 x + \frac{a_3}{a_1}, a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} \right) \tag{3.8}$$

   Výsledkem této transformace je tak zjednodušená forma Weistrassovy rovnice odpovídající eliptické křivce, která je nesupersingulární z anglického *"non-supersingular"* nad Galoisovým polem $\mathbb{F}_{2^m}$:

$$E/\mathbb{F}_{2^m} : y^2 + xy = x^3 + ax^2 + b \tag{3.9}$$

   kde $a, b \in \mathbb{F}_{2^m}$ a $\Delta = b$

2. Pokud $a_1 = 0$

$$(x, y) \rightarrow (x + a_2, y) \tag{3.10}$$

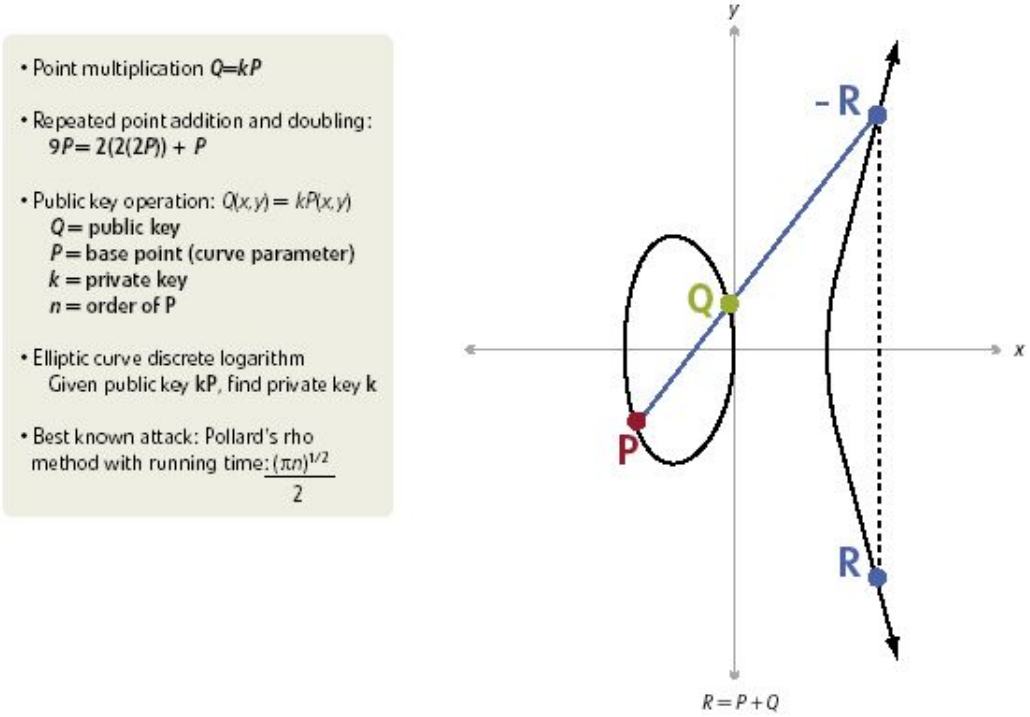
   Výsledná křivka je supersingulární z anglického *"supersingular"*. Zjednodušená forma Weistrassovy rovnice odpovídající této křivce má tvar:

$$E/\mathbb{F}_{2^m} : y^2 + cy = x^3 + ax + b \tag{3.11}$$

   kde $a, b, c \in \mathbb{F}_{2^m}$ a $\Delta = c^4$.

3.1 Sčítání bodů eliptické křivky

Operace sčítání bodů je základním kamenem šifrování v kryptografii eliptických křivek. Díky sčítání bodů jsme schopni definovat samotné šifrování/dešifrování a dále pak i využití eliptických křivek v digitálním podpise. Protože ve veškerých výpočtech počítáme s konečným polem, množina bodů se kterou počítáme je také omezená a z toho plynoucí diskretizace eliptické křivky. Vzhledem k tomu, že jsme odkazání na práci s konečnou množinou prvků nad konečným polem, odpadají nám starosti se zaokrouhlováním, vlivem toho, že každý výsledek je podroben operaci mod p nebo mod $f(x)$ kde p je charakteristika prvočíselného pole a $f(x)$ je redukční polynom v případě Galoisových polí. Mezi aritmetickými operacemi nad prvočíselnými poli a poli Galoisovými existují jemné rozdíly ať už mezi samotným sčítaním, násobením, opačným prvkem či výše zmíněnou operaci mod p resp. mod $f(x)$ tak i například jiný souřadnicový systém (binární vektory versus skaláry). Rozvedeme tedy jako první sčítání bodů nad prvočíselným polem $\mathbb{F}_p$.



Obr. 3.2: Sčítání bodů eliptické křivky nad $\mathbb{F}_p$

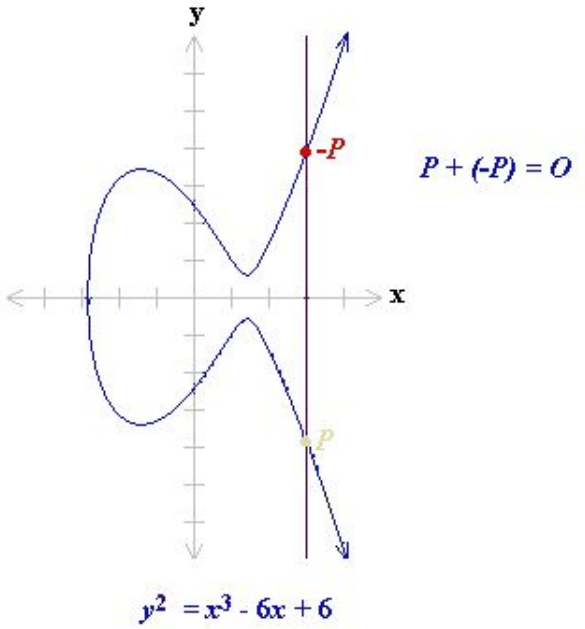
3.1.1 Sčítání nad $\mathbb{F}_p$

Protože se pohybujeme v kartézské soustavě kde každému bodu je přiřazena jedna x-ová a jedna y-ová souřadnice, tak z algebraického pohledu není sčítání dvou bodů

ležících na křivce nad $\mathbb{F}_p$ nic jiného než sčítání a odčítání dvou dekadických čísel.

Definice 3.4: Máme-li zadán bod $P[x_P, y_P] \in E$ a bod O_∞ označován také jako bod v nekonečnu tak platí:

1. Pro všechny body $P[x_P, y_P] \in E$ existuje opačný bod $-P[x_P, -y_P \bmod p] \in E$
2. Pro všechny body P platí $P + (-P) = O_\infty$
3. Pro všechny body P platí $P + O_\infty = P$ tzv. "'aditivní identita"'
4. Opačný bod k $O_\infty = -O_\infty = O_\infty$



Obr. 3.3: Součet bodů $P + O_\infty = P$

Je důležité si uvědomit zda-li sčítáme dva různé body, dva stejné body nebo dva vzájemně opačné body. Máme tedy tři možnosti:

Definice 3.5: Uvažujeme tedy body $P[x_P, y_P], Q[x_Q, y_Q] \in E$

1. Pokud platí, že $P[x_P, y_P] \neq Q[x_Q, y_Q] \wedge P[x_P, y_P] \neq -Q[x_Q, y_Q]$, sčítáme tedy dva různé body jejichž součtem je bod P+Q=R. Pro bod $R[x_R, y_R]$ platí následující:

$$\begin{aligned} s &= \frac{y_Q - y_P}{x_Q - x_P} \\ x_R &= s^2 - x_P - x_Q \\ y_R &= s(x_P - x_R) - y_P \end{aligned} \tag{3.12}$$

kde s je směrnice přímky spojující body P a Q.

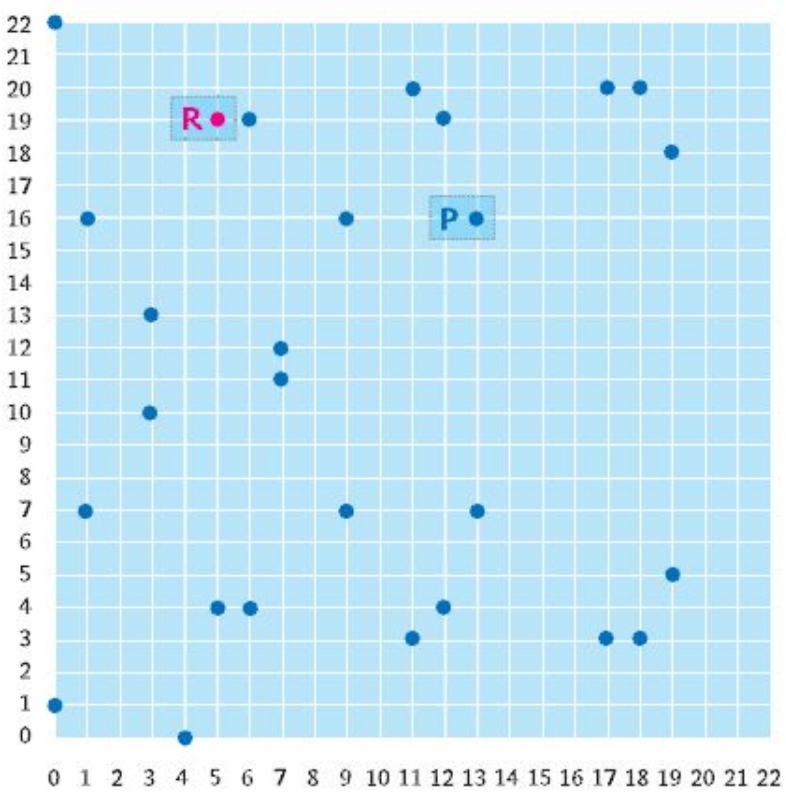
2. Pokud platí, že $P[x_P, y_P] = Q[x_Q, y_Q]$ pak sčítáme dva stejné body. V aditivní notaci se toto zapíše jako $P + Q = P + P = R$ jinými slovy $2P = R$, tato druhá notace se nazývá multiplikativní. Je tedy vidět, že násobení lze zapsat jako sčítání téhož prvku. Pro sčítání totožných prvků platí následující:

$$\begin{aligned} s &= \frac{3x_P^2 + a}{2y_P} \\ x_R &= s^2 - 2x_P \\ y_R &= s(x_P - x_R) - y_P \end{aligned} \tag{3.13}$$

kde s je křivky E v bodě P a a je parametr ze zjednodušené formy Weierstrassovy rovnice 3.6.

3. Pokud jsou body P a Q vzájemně inverzní tzn. $P = -Q$ pak podle 2. bodu v definici 3.4 platí:

$$P + Q = -Q + Q = O_\infty \tag{3.14}$$



Obr. 3.4: Eliptická křivka E: $y^2 = x^3 + x + 1$ nad podložním polem GF(23)

Př 3.6: Máme zadány body $R = (6, 19)$, $P = (13, 16)$ a eliptickou křivku $E : y^2 = x^3 + x + 1$. Počítáme jejich součet, tedy $Q = R + P$:

1. Výpočet směrnice přímky spojující body R a P, $s = \frac{16-19}{13-6} = \frac{-3}{7} \bmod 23 = \frac{20}{7} \bmod 23$. Abychom se zbavili zlomku vypočítáme pomocí Euklidova algoritmu inverzní prvek k číslu 7.

Dělenec n	Dělitel x	n div x	n mod x
7	23	0	$z_3 = 7$
23	7	3	$z_2 = 2$
7	2	3	$z_1 = 1$
2	1	2	$z_0 = 0$

$$z_3 = 7 = 7 - 0 \cdot 23$$

$$z_2 = 2 = 23 - 7 \cdot 3 = 23 - 3 \cdot z_3 = 23 - 3 \cdot (7 - 23 \cdot 0) = 23 - 3 \cdot 7$$

$$z_1 = 7 - 3 \cdot 2 = z_3 - 3 \cdot z_2 = (7 - 23 \cdot 0) - 3 \cdot (23 - 3 \cdot 7)$$

$$z_1 = (10 \bmod 23) \cdot (7 \bmod 23) - (3 \bmod 23) \cdot (23 \bmod 23)$$

2. Inverzním prvkem k číslu 7 je tedy číslo 10. Směrnice přímky spojující body R a P je $s = \frac{20}{7} \bmod 23 = 20 \cdot 10 \bmod 23 = 16$

3. Výpočet souřadnice x_Q

$$x_Q = s^2 - x_R - x_P = 16^2 - 6 - 13 = 237 \bmod 23 = 7$$

4. Výpočet souřadnice y_Q

$$y_Q = s \cdot (x_R - x_Q) - y_R = 16 \cdot (6 - 7) - 19 = -35 \bmod 23 = 11$$

5. Bod $Q = R + P = (6, 19) + (13, 16) = (7, 11)$ a platí $Q \in E$

$$E : y^2 = x^3 + x + 1 \Rightarrow 11^2 \bmod 23 = (7^3 + 7 + 1) \bmod 23$$

$$121 \bmod 23 = 351 \bmod 23$$

$$6 = 6 \pmod{23}$$

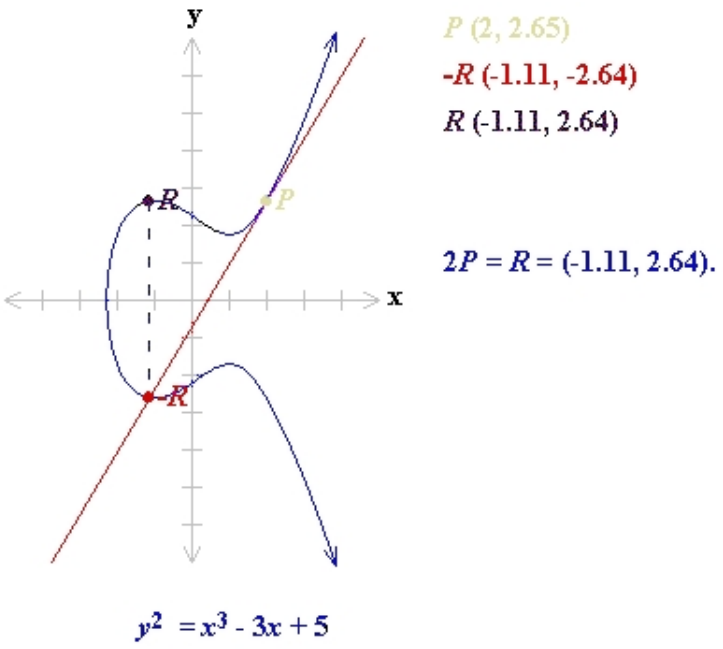
3.1.2 Násobení bodu skalárem nad $\mathbb{F}_p$

Násobení bodu $P \in E$ skalárem k se provádí jako k-násobný součet bodu P a proto k násobek bodu P v multiplikativní notaci je vyjádřen jako $P + P + ... + P + P = k \cdot P$ v aditivní notaci. Máme-li tedy vypočítat $Q = 2 \cdot P$ převedeme si tuto operaci do aditivní notace $Q = P + P$ a postupujeme podle rovnice 3.13. Pokud bychom počítali větší k násobek bodu P například $Q = 6 \cdot P$ mohli bychom postupovat tak,

že bychom spočítali $Q_{1,2} = P + P + P + P + P + P$ například jako $Q_1 = 3 \cdot P + 3 \cdot P$ nebo $Q_2 = 4 \cdot P + 2 \cdot P$. Pro výpočet bodu Q_1 bychom postupovali podle rovnice 3.13 protože sčítáme dva stejné body naopak pro výpočet Q_2 použijeme rovnici 3.12 protože sčítáme dva různé body, avšak výsledek je v obou případech stejný.

(0, 1)	(6, 4)	(12, 19)	(0, 22)
(6, 19)	(13, 7)	(1, 7)	(7, 11)
(13, 16)	(1, 16)	(7, 12)	(17, 3)
(3, 10)	(9, 7)	(17, 20)	(3, 13)
(9, 16)	(18, 3)	(4, 0)	(11, 3)
(18, 20)	(5, 4)	(11, 20)	(19, 5)
(5, 19)	(12, 4)	(19, 18)	*O*

Obr. 3.5: Body eliptické křivky E: $y^2 = x^3 + x + 1$ nad GF(23)



Obr. 3.6: Násobení bodů na eliptické křivce

Př 3.7: Máme zadány bod $P = (9, 7)$ a eliptickou křivku $E : y^2 = x^3 + x + 1$, bod $Q = 2 \cdot P = P + P$ vypočítáme následovně:

1. Vypočítáme tečnu eliptické křivky v bodě $P = (9, 7)$, $s = \frac{3 \cdot 9^2 + 1}{2 \cdot 7} = \frac{244}{14} \bmod 23$. Abychom se zbavili zlomku musíme opět pomocí Euklidova algoritmu vypočítat inverzní prvek k číslu 14.

Dělenec n	Dělitel x	n div x	n mod x
14	23	0	$z_5 = 14$
23	14	1	$z_4 = 9$
14	9	1	$z_3 = 5$
9	5	1	$z_2 = 4$
5	4	1	$z_1 = 1$
4	1	4	$z_0 = 0$

$$z_5 = 14 - 0 \cdot 23$$

$$z_4 = 23 - 1 \cdot 14 = 23 - 1 \cdot z_5 = 23 - 14 + 0 \cdot 23$$

$$z_3 = 14 - 1 \cdot 9 = z_5 - z_4 = 14 - 0 \cdot 23 - 23 + 14 = 2 \cdot 14 - 1 \cdot 23$$

$$z_2 = 9 - 1 \cdot 5 = z_4 - z_3 = (1 \cdot 23 - 1 \cdot 14) - (2 \cdot 14 - 1 \cdot 23) = 2 \cdot 23 - 3 \cdot 14$$

$$z_1 = 5 - 1 \cdot 4 = z_3 - z_2 = (2 \cdot 14 - 1 \cdot 23) - (2 \cdot 23 - 3 \cdot 14) = 5 \cdot 14 - 3 \cdot 23$$

$$z_1 = (5 \bmod 23) \cdot (14 \bmod 23) - (3 \bmod 23) \cdot (23 \bmod 23)$$

2. Inverzním prvkem k číslu 14 je tedy číslo 5. Směrnice tečny protínající eliptickou křivku v bodě P je $s = \frac{244}{14} \bmod 23 = 244 \cdot 5 \bmod 23 = 1220 \bmod 23 = 1$

3. Výpočet souřadnice x_Q

   $$x_Q = s^2 - x_P - x_P = 1^2 - 9 - 9 \bmod 23 = -17 \bmod 23 = 6 \bmod 23 = 6$$

4. Výpočet souřadnice y_Q

   $$y_Q = s \cdot (x_P - x_Q) - y_P = 1 \cdot (9 - 6) - 7 \bmod 23 = 19 \bmod 23 = 19$$

5. Bod $Q = 2 \cdot P = (9, 7) + (9, 7) = (6, 19)$ a platí $Q \in E$

   $$E : y^2 = x^3 + x + 1 \Rightarrow 19^2 \bmod 23 = (6^3 + 6 + 1) \bmod 23$$

   $$361 \bmod 23 = 223 \bmod 23$$

   $$16 = 16 \pmod{23}$$

4 ALGORITMY V ECC

4.1 Generování náhodné eliptické křivky

Generace klíčových párů a samotné šifrování předchází generace náhodné eliptické křivky. Z důvodů zvýšení bezpečnosti a odolnosti eliptické křivky vůči různým druhům útoků mířených na zjištění soukromého klíče se do generačního algoritmu náhodné eliptické křivky zavádí bitový řetězec *seed*, který vnáší do generace určitou náhodnost, aby nedošlo k vygenerování "slabé" eliptické křivky. V kryptografických algoritmech pracujících s eliptickými křivkami se využívají eliptické křivky nad prvočíslným polem nebo nad polem Galoisovým. Vzhledem k tomu, že v dnešní době se veškeré výpočetní operace provádějí na počítačích, které využívají binární reprezentaci dat je postup generace náhodné eliptické křivky vysvětlen pro Galoisovo pole. U binární reprezentance bodů nám odpadá nutnost převodu z dekadické do binární soustavy, navíc u aritmetických operací v některých případech lze nahradit operaci mod p operací XOR, čímž snížíme počet výpočetních operací.

Algoritmus 4.1: Generace definujících parametrů a, b eliptické křivky E nad Galoisovým polem $\mathbb{F}_{p^m}$[1]
Vstup: Galoisovo pole typu $q = 2^m$
Výstup: Parametry $a, b \in \mathbb{F}_{p^m}$ z rovnice 3.9 a bitový řetězec seed potřebný pro zpětnou verifikaci dostatečné bezpečnosti parametrů a, b.

1. Vygenerujeme seed, aby délka $g \geq 160$ bitů
2. Vypočteme $H = \text{SHA-1}(seed)$ a nechť b_0 je bitový řetězec obsahující v LSB bitů získaných z H
3. Nechť z je celé číslo jehož binární rozvoj je dán $g-$bitovým řetězcem seed
4. Pro všechny i od 1 do s provedeme následující:
   (a) Nechť s_i je g-bitový řetězec, který odpovídá binárnímu rozvoji celého čísla $(z + i) \bmod 2^g$
   (b) Spočítáme $b_i = \text{SHA-1}(s_i)$
5. Nechť b je element pole $\mathbb{F}_{2^m}$ získaný spojením řetězců $b_1, b_2, b_3, ..., b_s$ následovně $b = b_1 \parallel b_2 \parallel b_3 \parallel ... \parallel b_s$
6. Jestliže $b = 0$ pak opakujeme celý algoritmus od bodu 1.
7. Nechť a je libovolný prvek z pole $\mathbb{F}_{2^m}$
8. Eliptická křivka nad polem $\mathbb{F}_{2^m}$ odpovídá rovnici $E : y^2 + xy = x^3 + ax^2 + b$

4.2 Generování klíčových párů

Protože kryptosystémy na bázi eliptických křivek spadají do kategorie asymetrických kryptosystémů je nezbytné aby si každá entita X před samotným šifrováním/dešifrováním dat vygenerovala platný soukromý a veřejný klíč. Pro potřeby generace klíčového páru jsou nezbytné platné doménové parametry, kterými je charakteristika pole q , reprezentace pole FR, definující parametry eliptické křivky a a b, bod G, řád bodu n a kofaktor h. Z těchto parametrů se vypočítájí dvě hodnoty, bod Q, který slouží jako veřejný klíč pro šifrování v eliptických kryptosystémech ECC a celé číslo d, které slouží jako soukromý klíč pro dešifrování dat.

Algoritmus 4.2: Výpočet veřejného a soukromého klíče pro šifrování za pomoci eliptických křivek.[1]
Vstup: Doménové parametry $D = (q, FR, a, b, c, G, n, H)$
Výstup: Soukromý klíč d, veřejný klíč Q.

1. Vybereme náhodné celé číslo d z intervalu $[1, n-1]$.
2. Vypočítáme bod $Q = d \cdot G$.
3. Bod Q je veřejný klíč, celé číslo d je soukromý klíč.

4.3 Šifrování v ECC

Základní princip šifrování spočívá v převodu textu (dat) do číselným bloků[10], které na základě problému diskrétního logaritmu eliptických křivek převedeme na bod eliptické křivky. Do šifrovacího algoritmu vstupuje veřejný klíč tj. bod Q, otevřený (nešifrovaný) text T a bod $P \in \mathbb{F}_{p^m}$ jehož řád je $\#E(P) = n$. Znaky nešifrovaného textu se převedou do ASCII formátu a spojí se dohromady. Vytvořené číslo se rozdělí do bloků jejichž velikost nesmí přesáhnout velikost řádu bodu P. Vybere se soukromý klíč d z intervalu $(1, n-1)$ a vypočítá se bod $A = d \cdot Q$, dále se vypočítá bod $B = d \cdot P$ a číslo $C = (A_x \cdot b_1) \bmod f(x)$ resp. mod$p$, které reprezentuje zašifrovaný blok b_1. Tento postup se provede pro všechny bloky, převedeného textu do ASCII formátu.

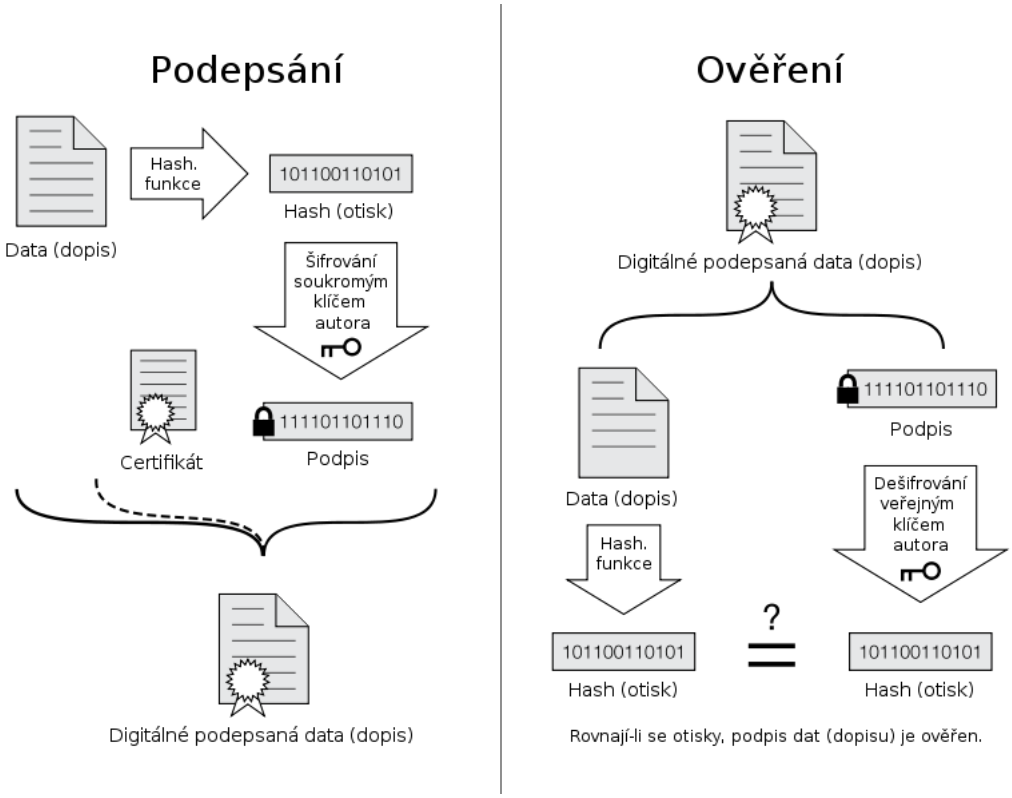
4.4 Dešifrování v ECC

Dešifrování textu se provede následovně[10], nejdříve se vypočte bod $D = d \cdot R$ a poté se dešifrují veškeré bloky b_i následovně $b_1 = C \cdot B_x^{-1} \bmod f(x)$ resp. mod$p$.

5 DIGITÁLNÍ PODPIS

Elektronický podpis je identifikační údaj odesilatele, kterým zajišťujeme integritu a nepopiratelnost dat, autenticitu odesilatele a volitelně i časový údaj indikující datum a čas kdy byl digitální podpis vytvořen.

Integrita dat je ochrana proti neoprávněné modifikaci daného dokumentu, jinými



Obr. 5.1: Princip digitálního podpisu

slovy tato vlastnost digitálního podpisu umožňuje přijímající straně ověřit zda-li dokument byl nebo nebyl při přenosu pozměněn, tato možnost je uskutečněna za pomoci jednocestné hašovací funkce, která na vstup přijme dokument v binární formě a pomocí binárních operací z něj vypočítá otisk, jakákoliv změna v dokumentu (záměna pořadí znaků, změna znaků, smazání znaků) má za následek jiný otisk na výstupu použité hašovací funkce. Otiskem je myšlena číselná hodnota fixní délky.

Protože výše zmíněný otisk vypočítaný z přenášeného dokument se šifruje soukromým klíčem odesílající strany, a protože soukromý klíč je pouze ve vlastnictví odesilatele, zajišťujeme digitálním podpisem nejen autenticitu odesilatele ale i nepopiratelnost dat. Nepopiratelností dat se míní ten fakt, že po odeslání dokumentu

druhé straně, se odesilatel nemůže najednou rozhodnout a říct, že daný dokument od něj nebyl odeslán protože ho usvědčuje soukromý klíč, kterým byl digitální podpis vytvořen. Pod autenticitou odesilatele se rozumí, že digitální podpis jedinečně určuje odesilatele podle soukromého klíče.

Mechanismus digitálního podpisu lze shrnout do následujících pěti bodů:

1. Za pomoci hašovací funkce se vytvoří otisk dokumentu, který chceme odeslat.
2. Tento otisk se zašifruje pomocí soukromého klíče odesilatele a vytvoří se tím digitální podpis.
3. Přijímající strana nezávisle na přijatém digitálním podpise vypočítá otisk dokumentu stejnou hašovací funkcí jako odesílající strana.
4. Přijímající strana rozšifruje přijatý digitální podpis veřejným klíčem odesilatele.
5. Přijímající strana porovná přijatý otisk s lokálně vypočítaným. Pokud se oba otisky rovnají má přijímací strana potvrzeno, že dokument byl digitálně podepsán vlastníkem soukromého klíče.

Autenticita dokumentu se provádí na základě vlastnictví soukromého klíče, a proto je nezbytné, aby tento klíč byl střežen popř. umístěn mimo dosah neoprávněných osob (externí disk, čipová karta, hardwarový klíč, flash karta). Pokud dojde k odcizení nebo ke ztrátě klíčového páru, který se používá k šifrování otisku z příslušného dokumentu, musí být co nejdřív vygenerován nový klíčový pár jinak se může stát, že třetí osoba která se zmocní onoho odcizeného soukromého klíče začne podvrhovat digitální podpisy z důležitých dokumentů v neprospěch odesilatele.

5.1 ECDSA

ECDSA je algoritmus definující procedury a pravidla při tvorbě digitálního podpisu za pomoci šifrování pomocí eliptických křivek. Jedná se o analogický algoritmus k DSA. DSA byl poprvé navrhnut v srpnu roku 1991 americkou organizací NIST a dále specifikován ve standardu FIPS 186 vydaný federální vládou Spojených Států Amerických pod názvem DSS. Bezpečnost algoritmu ECDSA závisí stejně tak jako šifrování za pomoci eliptických křivek na řešení problému diskrétního logaritmu. Hlavní rozdíly mezi algoritmem ECDSA a DSA jsou následující:

5.1.1 DSA (Digital Signature Algorithm)

- Grupa: Z_P^*
- Prvky grupy: celá čísla, $\{1, 2, 3, ..., p-1\}$
- Operace grupy: násobení mod p
- Matematické operace:

  Násobení: $g \cdot h$

  Inverze: g^{-1}

  Dělení: g/h

  Umocňování: g^a
- Problém diskrétního logaritmu: Pro dané $g \in \mathbb{Z}_P^*$ a $h = g^a \bmod p$ je cílem nalézt a.

5.1.2 ECDSA (Elliptic Curve Digital Signature Algorithm)

- Grupa: $E(Z_P)$
- Prvky grupy: body eliptické křivky E o souřadnicích (x, y) + bod v nekonečnu O_∞
- Matematické operace:

  Sčítání: $P + Q, P + P, P + O_\infty$

  Negace: $-P$

  Odčítání: $P - Q$

  Násobení: $d \cdot Q$
- Problém diskrétního logaritmu: Pro daný bod $P \in E(\mathbb{Z}_P)$ a $Q = d \cdot P$ je cílem nalézt d.

5.1.3 ECDSA doménové parametry

Generace potřebných parametrů zahrnutých ve všech použitých algoritmech spojených s ECDSA.[9]

1. Velikost pole q, kde $q = p$ (liché prvočíslo) pro prvočíselné pole $\mathbb{F}_p$ nebo $q = 2^m$ pro Galoisovo pole $\mathbb{F}_{2^m}$.
2. Reprezentace prvků pole, normálová báze nebo polynomální báze.

3. Parametry $a, b \in \mathbb{F}_q$, definující rovnici eliptické křivky E podle rovnice 3.6 resp. 3.9

4. Souřadnice bodu $G \in E$, kde $x_G, y_G \in \mathbb{F}_q$

5. Řád n bodu G, pro který platí $n > 2^{160}$ a $n > 4\sqrt{q}$

6. Kofaktor $h = \#E(\mathbb{F}_q)/n$

7. Bitový řetězec seed o délce $l > 160$ bitů

5.1.4 Generace a ověření eliptické křivky

Druhým krokem v generaci digitálního podpisu pomocí ECDSA algoritmu je zvolení vhodné eliptické křivky, jinými slovy pomocí algoritmu 5.1 vygenerování vhodných parametrů a, b zjenodušené formy Weierstrassovy rovnice 3.6 resp. 3.9 tak, aby si uživatel využívající danou eliptickou křivku byl schopen ověřit, zda entita která křivku vygenerovala vytvořila nebo nevytvořila úmyslně "slabou" eliptickou křivku náchylnou k některým z útoku vedoucí k získání soukromého klíče. K tomuto ověření právě slouží náhodně vygenerovaný bitový řetězec seed o délce 160-ti bitů či více, zároveň tento binární řetězec zavádí určitou náhodnost do procesu generování eliptické křivky.

Algoritmus 5.1: Generace definujících parametrů a, b eliptické křivky E nad prvočíselným polem $\mathbb{F}_p$.[9]
Vstup: Charakteristika prvočíselného pole p, kde p je liché prvočíslo.
Výstup: Parametry $a, b \in \mathbb{F}_p$ z rovnice 3.6 a bitový řetězec seed potřebný pro zpětnou verifikaci dostatečné bezpečnosti parametrů a, b.

1. Vygenerujeme seed tak, aby délka $g \geq 160$ bitů

2. Vypočteme $H = \text{SHA-1}(seed)$ a nechť c_0 je bitový řetězec obsahující v LSB bitů získaných z H

3. Nechť W_0 je bitový řetězec délky v, získaný nastavením MSB bitu na 0

4. Nechť z je celé číslo dané binárním rozvojem g-bitového řetězce seed

5. Pro všechny i od 1 do s proveď následující:

   (a) Nechť s_i je g-bitový řetězec, který odpovídá binárnímu rozvoji celého čísla $(z + i) \bmod 2^g$

   (b) Vypočti $W_i = \text{SHA-1}(s_i)$

6. Bitový řetězec W obdržíme spojením řetězců $W_1, W_2, W_3, ..., W_s$ následovně $W = W_1 \parallel W_2 \parallel W_3 \parallel ... \parallel W_s$

7. Nechť r je celé číslo jehož binární rozvoj je dán W

8. Jestliže $r = 0$ nebo $4r + 27 \equiv 0 \pmod{p}$ pak jdi do bodu 1

9. Vybereme libovolná celá čísla $a, b \in \mathbb{F}_p$ tak, aby obě nebyly nulové a aby platilo $r \cdot b^2 \equiv a^3 \bmod p$

10. Eliptická křivka nad polem $\mathbb{F}_p$ odpovídá rovnici $E : y^2 = x^3 + ax + b$

Algoritmus 5.2: Generace definujících parametrů a, b eliptické křivky E nad Galoisovým polem $\mathbb{F}_{p^m}$[9]
Vstup: Galoisovo pole typu $q = 2^m$
Výstup: Parametry $a, b \in \mathbb{F}_{p^m}$ z rovnice 3.9 a bitový řetězec seed potřebný pro zpětnou verifikaci dostatečné bezpečnosti parametrů a, b.

1. Vygenerujeme seed, aby délka $g \geq 160$ bitů

2. Vypočteme $H = \text{SHA-1}(seed)$ a nechť b_0 je bitový řetězec obsahující v LSB bitů získaných z H

3. Nechť z je celé číslo jehož binární rozvoj je dán $g-$bitovým řetězcem seed

4. Pro všechny i od 1 do s provedeme následující:

   (a) Nechť s_i je g-bitový řetězec, který odpovídá binárnímu rozvoji celého čísla $(z + i) \bmod 2^g$

   (b) Spočítáme $b_i = \text{SHA-1}(s_i)$

5. Nechť b je element pole $\mathbb{F}_{2^m}$ získaný spojením řetězců $b_1, b_2, b_3, ..., b_s$ následovně $b = b_1 \parallel b_2 \parallel b_3 \parallel ... \parallel b_s$

6. Jestliže $b = 0$ pak opakujeme celý algoritmus od bodu 1.

7. Nechť a je libovolný prvek z pole $\mathbb{F}_{2^m}$

8. Eliptická křivka nad polem $\mathbb{F}_{2^m}$ odpovídá rovnici $E : y^2 + xy = x^3 + ax^2 + b$

5.1.5 Generování klíčového páru

Nezbytnou součástí při tvorbě digitálního podpisu je generace klíčového páru určeného pro šifrování a dešifrování vypočítaného otisku funkcí SHA-1. Narozdíl od šifrování dat při kterém se zajišťuje pouze nečitelnost dat pro neoprávněnou osobu, která nevlastní soukromý klíč pro dešifrování zašifrovaných dat, se v digitálním podpise šifruje soukromým klíčem a dešifruje klíčem veřejným čímž se zajistí autenticita a nepopiratelnost dat.

Algoritmus 5.3: Výpočet veřejného a soukromého klíče pro šifrování za pomoci eliptických křivek.[9]
Vstup: Doménové parametry $D = (q, FR, a, b, G, n, H)$
Výstup: Soukromý klíč d, veřejný klíč Q.

1. Vybereme náhodné celé číslo d z intervalu $[1, n-1]$.
2. Vypočítáme bod $Q = d \cdot G$.
3. Bod Q je veřejný klíč, celé číslo d je soukromý klíč.

Př 5.4: Před samotnou generací digitálního podpisu máme zadány tyto doménové parametry eliptickou křivku E: $y^2 = x^3 + x + 1$ tedy $a = 1$ a $b = 1$, bod $P = (13, 16)$ a řád bodu $n = 7$. Pro reálné aplikace je z důvodu ochrany proti Pollard-rho a Pohlig-Hellman útokům doporučována hodnota $n > 2^{160}$ (viz. ANSI X9.62), pro naše demonstrativní účely je hodnota triviálně nízká.

1. Vybereme statisticky jedinečné číslo d v rozsahu $< 1, n-1 >$, číslo d slouží jako soukromý klíč.

   $d \in < 1, 6 > \Rightarrow d = 4$

2. Vypočítáme bod $Q = d \cdot P$, bod Q slouží jako veřejný klíč.

   $Q = 4 \cdot (13, 16)$. Nejdříve si podle rovnice 3.13 vypočítáme $2 \cdot P = P + P$ a poté $4 \cdot P = 2 \cdot P + 2 \cdot P = (17, 3)$

3. Výstupem je tedy veřejný klíč daný parametry (E, G, n, Q) a soukromý klíč d, v našem případě $Q = (13, 16)$ a $d = 4$.

5.1.6 Generace a ověření digitálního podpisu

Po vygenerování dostatečně bezpečné eliptické křivky, doménových parametrů a klíčového páru určeného pro zašifrování digitálního podpisu, se vypočítá otisk ze vstupního dokumentu m, který je zašifrován soukromým klíčem Q vysílající strany.

Algoritmus 5.5: Generace digitálního podpisu A.[9]
Vstup: Dokument k podepsání m, doménové parametry $D = (q, FR, a, b, G, n, h)$ podepisující entity a klíčový pár (d, Q) kde d je soukromý klíč a Q je veřejný klíč
Výstup: Digitální podpis dokumentu m

1. Vybereme náhodné nebo pseudonáhodné celé číslo k z intervalu $< 1, n-1 >$
2. Vypočítej $k \cdot G = (x_1, y_1)$
3. Vypočítej $r = x_1 \bmod n$. Pokud $r = 0$ pak jdi do bodu 1. Pokud $r = 0$ pak by digitální podpis nebyl závislý na soukromém klíči jak je vidno z podpisové rovnice v bodě 6.
4. Vypočítej $k^{-1} \bmod n$
5. Vypočítej SHA-1(m) a výsledný binární hash převeď na celé čislo e
6. Vypočítej $s = k^{-1}(e + dr) \bmod n$. Pokud $s = 0$ pak jdi do bodu 1
7. Digitálně podepsaný dokument m entity A $= (r, s)$

Př 5.6: Před generací podpisu máme k dispozici, dokument m k podepsání, soukromý klíč d a veřejný klíč Q.

1. Vybereme číslo $k \in < 1, n-1 >$

   $k = 5$ platí $k \in < 1, 6 >$

2. Vypočítáme bod $Q = k \cdot G = 5 \cdot (13, 16)$ pomocí rovnic 3.12 a 3.13, $Q = (x_Q, y_Q) = (5, 4)$ a číslo $r = x_Q \bmod n = 5 \bmod 7 = 5$
3. Výpočet $k^{-1} \bmod n$, tzn. pomocí Euklidova algoritmu vypočítáme inverzní prvek k prvku $k = 5 \Rightarrow k^{-1} = 3$ platí $k \cdot k^{-1} \bmod 7 = 1$
4. Výpočet digitálního podpisu $s = k^{-1}(h(m) + d \cdot r) \bmod n$, kde h reprezentuje hashovací funkci SHA-1 jejíž výstupem je 160-bit hash daného dokumentu m. Pro naše účely budeme využívat zkrácenou hash $h(m) = \text{EDB433B}_{16} = 249250619_{10}$

   $s = 3 \cdot (249250619 + 4 \cdot 5) \bmod 7 = 747751917 \bmod 7 = 3$

5. Výstup algoritmu je digitální podpis $(r, s) = (5, 3)$

Algoritmus 5.7: Ověření digitálního podpisu A.[9]
Vstup: Digitální podpis A $= (r, s)$, dokument m
Výstup: Pravost či nepravost přijatého digitálního podpisu.

1. Ověříme, že $r, s \in [1, n-1]$
2. Vypočítáme SHA-1(m) a převedeme výsledek z binární podoby na celé číslo e
3. Spočítáme $w = s^{-1} \bmod n$
4. Spočítáme $u_1 = ew \bmod n$ a $u_2 = rw \bmod n$
5. Spočítáme $X = u_1 G + u_2 Q$
6. Pokud $X = O_{inf}$ pak je pravost přijatého podpisu zamítnuta, v opačném případě se x-ová souřadnice x_1 bodu X převede na celé číslo x_1' a vypočítáme $v = x_1' \bmod n$
7. Pouze pokud platí $v = r$ pak je pravost přijatého digitálního podpisu ověřena

Př 5.8: Při ověřování digitálního podpisu (r, s) provede přijímající strana následující:

1. Přijme přes zabezpečený komunikační kanál od vysílající strany kopii veřejného klíče (E, G, n, Q) a ověří, že čísla $r, s \in < 1, n-1 >$

   $r = 5 \Rightarrow r \in < 1, 6 >$

   $s = 3 \Rightarrow s \in < 1, 6 >$

2. Výpočet hashe z přijatého dokumentu a čísla $w = s^{-1} \bmod n$

   $w = 5 \bmod 7 = 5$

   $h(m) = \text{EDB433B}_{16} = 249250619_{10}$

3. Výpočet koeficientů $u_1 = h(m) \cdot w \bmod n$ a $u_2 = r \cdot w \bmod n$

   $u_1 = 249250619 \cdot 5 \bmod 7 = 1246253095 \bmod 7 = 3$

   $u_2 = 5 \cdot 5 \bmod 7 = 25 \bmod 7 = 4$

4. Ověření digitálního podpisu

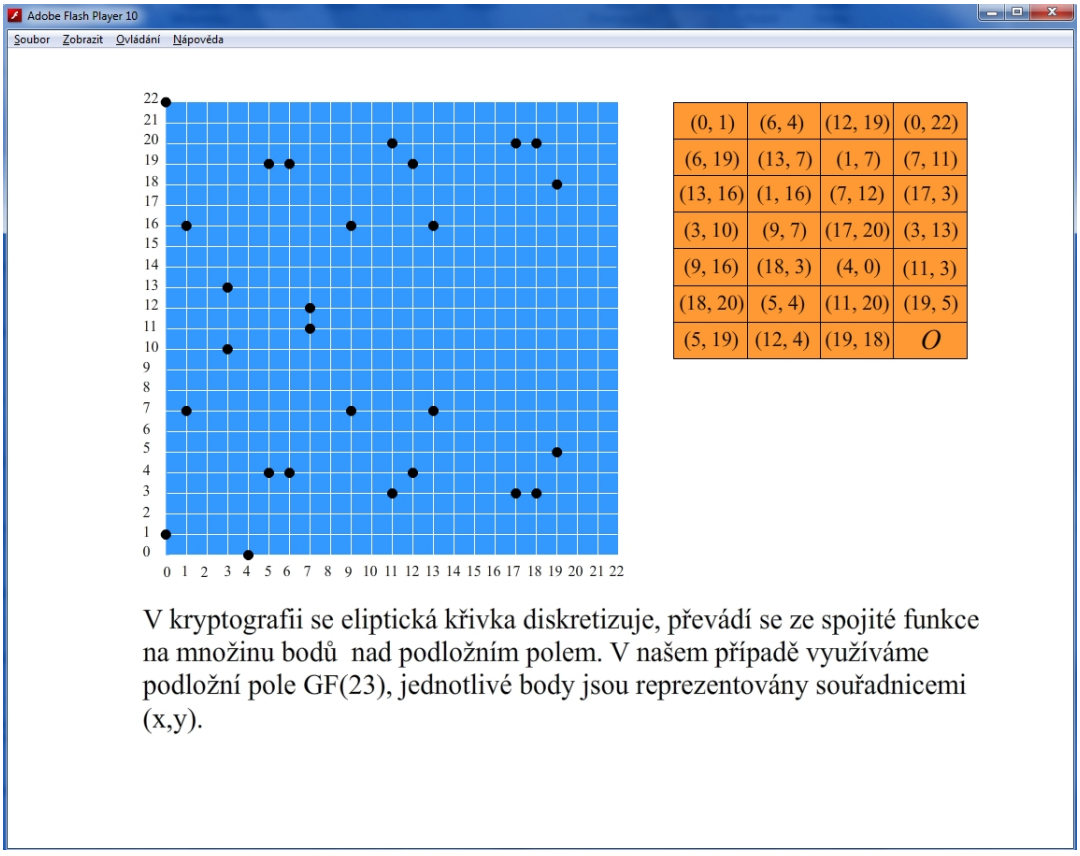
   $u_1 \cdot G + u_2 \cdot Q = (x_0, y_0) = 3 \cdot (13, 16) + 4 \cdot (5, 4) = (17, 20) + (13, 7) = (5, 19)$

   $v = x_0 \bmod n = 5 \bmod 7$

Verifikace digitálního podpisu se odvíjí od porovnání hodnot čísel v a r pokud platí $v = r$ pak nebyl digitální podpis změněn.

6 SOFTWAROVÉ ŘEŠENÍ BP

Součásti bakalářské práce je výuková animace, demonstrující využití eliptických křivek v digitálním podpise (algoritmus ECDSA). Animace je vytvořena v programu Adobe Flash CS4 Professional. Algoritmus generace digitálního podpisu využívá eliiptickou křivku $E : y^2 = x^3 + x + 1$ nad podložním polem GF(23) a bod $G = (13, 16)$ o řádu $n = 7$. Z důvodu velikosti výstupu hashovací funkce SHA-1 je při generaci a verifikaci digitálního podpisu využita pouze část hashe. Animace je navrhnuta tak aby si uživatel byl krokovat jednotlivé algoritmy stisknutím tlačítka šipka doprava pro krok dopředu, šipka doleva pro krok zpátky. Celá animace je rozdělena do tří částí, v první částí je popsána diskretizace eliptické křivky do množiny bodů nad podložním polem ohraničeným prvočíslem. Ve zbylých třech částech jsou popsány algoritmy ECDSA, generace klíčového páru, generace digitálního podpisu ECDSA a jeho verifikace. Pro spuštění animace je zapotření mít nainstalovaný Adobe Flash Player, při programování byla animace zobrazována za pomoci Adobe Flash Player verze 10.0 r2.



Obr. 6.1: Diskretizace eliptické křivky nad GF(23)

1. Výběr čísla $\boldsymbol{k}$ z intervalu (1, n - 1)

$$\text{Např. } \boldsymbol{k} = 5, \text{ z intervalu } (1, 6)$$

2. Výpočet bodu $\boldsymbol{k} * \boldsymbol{P}$ a čísla $\boldsymbol{r}$
   - pokud $\boldsymbol{r} = 0$ pak podpisová rovnice není závislá na soukromém klíči $\boldsymbol{d}$ a je nutné vygenerovat nové číslo $\boldsymbol{k}$ a tedy opakovat krok 1 a krok 2

$$\text{Např. } k * P = (x_1, y_1) = 5 * (13, 16) = (5, 4)$$
$$r = x_1 \bmod n = 5 \bmod 7 = 5$$

3. Výpočet digitálního podpisu
   - pokud $\boldsymbol{s} = 0$, pak při ověřování digitálního podpisu neexistuje inverzní prvek $\boldsymbol{s^{-1}}$ v tomto případě se opakují kroky 1, 2 a 3
   - funkce $\boldsymbol{h}$ reprezentuje hashovací funkci SHA-1, jejíž výstupem je 160-bit hash pro naše demonstrativní účely bude výstupem hashovací funkce $\boldsymbol{h}$ hodnota $\boldsymbol{0xEDB433B = 249250619_{10}}$

$$\boldsymbol{s} = k^{-1} * \{h(m) + d * r\} \bmod n$$
$$\boldsymbol{s} = 3 * \{249250619 + 4 * 5\} \bmod 7$$
$$\boldsymbol{s} = 747751917 \bmod 7 = 3$$

Obr. 6.2: Demonstrativní ukázka výpočtu digitálního podpisu

7 ZÁVĚR BAKALÁŘSKÉ PRÁCE

Cílem bakalářské práce bylo uvedení do problematiky kryptografie eliptických křivek a jejich aritmetiky. V první polovině bakalářské práce jsou vysvětleny aritmetické operace s konečnými poly a operace sčítání bodů a násobení bodů skalárem, které tvoří podstatu matematického problému na jehož neřešitelnosti je založena bezpečnost eliptických křivek, tedy problém diskrétního logaritmu (ECDLP). Druhá polovina bakalářské práce je soustřeďena na využití eliptických křivek v digitálním podpise. Vysvětleny jsou dva druhy polí nad kterými je eliptická křivka konstruována a to pole prvočíselné $\mathbb{F}_p$ a pole Galoisovo $\mathbb{F}_{2^m}$. Galoisovo pole je pro počítačové zpracování ideální protože jeho prvky jsou reprezentovány jako binární posloupnosti a nemusí tedy docházet k žádným konverzím mezi číselnými soustavami což urychluje výpočetní operace. V souvislosti s poli jsou vysvětleny operace sčítání a násobení vzhledem k jejich převážnému použití v bodové aritmetice, inverzní prvek, kterým se elegantně zbavíme operace dělení převodem na operaci násobení a redukční polynomy, které jsou nezbytné pro výpočetní operace nad Galoisovým polem. V další kapitole je vysvětlen výpočet diskriminantu ke zjišťení nevhodných transformací eliptické křivky, řád bodu, který hraje významnou roli v problému diskrétního logaritmu a řád eliptické křivky. Popsána je obecná Weierstrassova rovnice eliptické křivky a její zjednodušenné formy používané v kryptografii pro křivky nad polem $\mathbb{F}_p$ a pro supersingulární a nesupersingulární křivku nad polem $\mathbb{F}_{2^m}$. Dále jsou popsány rozličné algoritmy pro generaci náhodných elitpických křivek nad poli $\mathbb{F}_p$ a $\mathbb{F}_{2^m}$, generaci klíčového páru pro šifrování (veřejný klíč) a dešifrování (soukromý klíč) a v páté kapitole, která se kompletně věnuje teorii digitálního podpisu, jsou rozvedeny algoritmy generace a verifikace digitálního podpisu. Praktickou částí bakalářské práce je tvořena animací vytvořenou v programu Adobe Flash CS4 Professional, která demonstruje proces generace a verifikace digitálního podpisu spolu s generací klíčového páru.

LITERATURA

[1] HANKERSON, D. MENEZES, A. J. VANSTONE, S.: *Guide to Elliptic Curve Cryptography.* Springer, 2004. 311 s. ISBN 978-0387952734.

[2] KUREŠ, M.: *Eliptické křivky a kryptografie.* Dostupné z URL: `http://ecc.asp2.cz/`.

[3] COHEN, H. FREY, G.: *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* Chapman & Hall/CRC, 2006. 843 s. ISBN 978-1-1-58488-518-4

[4] BURDA, K.: *Aplikovaná kryptografie - DTK2.* Dostupné z URL: `http://www.vutbr.cz/elearning/`.

[5] *Kryptografie* Dostupné z URL: `http://cs.wikipedia.org/wiki/Kryptografie/`.

[6] PŘIBYL, J.: *Informační bezpečnost a utajování zpráv.* Česká technika - nakladatelství ČVUT, 2005. 82s. ISBN 80-01-03347-3

[7] *ECC Tutorial.* Dostupné z URL: `http://www.certicom.com/index.php/ecc-tutorial`.

[8] OCHODKOVÁ, E.: *Přínos teorie eliptických křivek k řešení moderních kryptografických systémů.* Katedra informatiky, FEI, VŠB. 12s.

[9] JOHNSON, D. MENEZES A. VANSTONE S.: *The Elliptic Curve Digital Signature Algorithm (ECDSA).* Certicom Research, Canada, 2001. 54s.

[10] DOBEŠ, J.: *Algoritmy v konečných geometriích a kryptografii.* ZMVŠ Třebíč, 2006. 79s.