

Diffie Hellman protokol v prostředí Mathematica a WebMathematica

Diffie Hellman protocol in Mathematica and WebMathematica environment

Kristýna Němečková



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Kristýna NĚMEČKOVÁ**
Osobní číslo: **A08246**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Informační a řídicí technologie**

Téma práce: **Diffie Hellman protokol v prostředí Mathematica a WebMathematica**

Zásady pro vypracování:

1. Vypracujte literární rešerši na dané téma.
2. Vytvořte základní programovou simulaci generování a výměny klíčů včetně následné šifrované komunikace.
3. Převeďte vytvořenou aplikaci do formátu pro webovou prezentaci pomocí SW WebMathematica.
4. Vytvořte v SW Mathematica a WebMathematica simulaci útoku na tento protokol.
5. Umístěte webovou prezentaci na server UTB.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: tištěná/elektronická

Seznam odborné literatury:

1. HOSTE, Jim. *Mathematica DeMYSTiFied*. McGraw-Hill Professional, 2008. 408 s. ISBN 978-0071591447.
2. RUSKEEPAA, Heikki. *Mathematica Navigator: Mathematics, Statistics and Graphics, Third Edition*. Academic Press, 2009. 1136 s. ISBN 978-0123741646.
3. STEJSKAL, J. *Vytváříme WWW stránky pomocí HTML, CSS a JavaScriptu*. Computer Press, 2006, ISBN: 80-251-0167-3.
4. VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Albatros, 2006. ISBN 80-00-01888-8.
5. KATZ, Jonathan. *Introduction to Modern Cryptography: Principles and Protocols*. Chapman & Hall, 1 edition. 2007. 552 s. ISBN 978-1584885511.
6. MURPHY, Sean. *Kryptografie – Průvodce pro každého . Dokořán*, 2006. 157 s. ISBN 80-7363-074-5.
7. BITTO, O. *Šifrování a biometrika*. BEN, 2005. 168 s. ISBN 80-86686-48-5.
8. KOVÁČOVÁ, M. *webMathematica*. STU Bratislava, 2007. 178 s. ISBN 80-969562-1-3.

Vedoucí bakalářské práce:

Ing. Roman Šenkeřík, Ph.D.

Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce:

25. února 2011

Termín odevzdání bakalářské práce:

7. června 2011

Ve Zlíně dne 25. února 2011

prof. Ing. Vladimír Vašek, CSc.
děkan



prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této bakalářské práce je problematika šifrování. Tato práce je zaměřena na šifrovací protokol Diffie – Hellman. Je zde uvedena historie vývoje protokolu, dále popsán základní princip práce a tvorba sdílených klíčů. Nermalou část bakalářské práce vyplňují též způsoby útoků na zkoumaný protokol. Připomenuta je zde ochrana k zamezení útoků a různé modifikace systému. Pro větší názornost jsou příklady tvorby klíčů názorně ukázány pomocí tabulek a obrázků. K demonstraci slouží také vytvořený projekt v prostředí Mathematica a WebMathematica, jež je detailně popsán v praktické části této práce.

Klíčová slova: kryptologie, Mathematica, WebMathematica, Man In the Middle Attack, Diffie – Hellman protokol.

ABSTRACT

The aim of this bachelor thesis is the issue of encryption. This work is focused on the encryption protocol Diffie - Hellman. In this bachelor thesis, there is introduced the history of the development of protocol, it also describes the basic principle of the work and creation of a shared keys. The significant part of the bachelor thesis also focuses on the ways of attacks on the examined protocol. The protection against the attacks and various modifications of the system is also mentioned. The examples of the key-making are shown in the tables and images in order to be more illustrative. The demonstration project is also created in the environment of Mathematica and WebMathematica, which is in detail described in the practical part of this thesis.

Keywords: cryptology, Mathematica, WebMathematica, Man In the Middle Attack, Diffie – Hellman protocol.

Ráda bych poděkovala především panu Ing. Romanu Šenkeříkovi, Ph.D. za poskytnutí zajímavého tématu a za odborné rady, postřehy a připomínky během řešení mé bakalářské práce. Dále bych ráda poděkovala rodině a přátelům za psychickou podporu během studia.

„Only two things are infinite, the universe and human stupidity, and I'm not sure about the former.“

Albert Einstein

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD.....	9
I TEORETICKÁ ČÁST	10
1 KRYPTOLOGIE.....	11
1.1 HISTORIE.....	12
1.2 SOUČASNOST	12
1.3 ROZDĚLENÍ ŠIFER.....	13
1.3.1 Symetrické šifrování	13
1.3.2 Asymetrické šifrování.....	13
1.4 OBECNÉ ZPŮSOBY ÚTOKŮ.....	14
1.4.1 Určování úrovně bezpečnosti	15
2 PROTOKOL DIFFIE - HELLMAN	16
2.1 PRVOTNÍ VIZE DIFFIEHO A HELLMANA	16
2.2 PRINCIP DOHODY NA KLÍČI	17
2.2.1 Příklad protokolu.....	18
2.3 MATEMATICKÝ POPIS FUNKCE.....	18
2.3.1 Uživatelsky volené hodnoty	19
2.3.2 Generátor grup.....	19
2.3.3 Bezpečnost matematické funkce	20
2.4 VÝHODY	20
2.5 NEVÝHODY.....	21
2.6 MODIFIKACE DH	21
2.7 MOŽNOSTI ÚTOKŮ	22
2.7.1 Podprahový kanál	23
2.7.2 Časový postranní kanál	23
2.8 MAN IN THE MIDDLE ATTACK.....	23
2.8.1 Grafické znázornění útoku	24
2.8.2 Popis útoku	24
2.8.3 Možnosti útočníka	26
2.8.4 Digitální podpis	26
II PRAKTICKÁ ČÁST	29
3 ROZBOR PROGRAMOVÉHO PROSTŘEDÍ.....	30
3.1 MATHEMATICA	30
3.2 WEBMATHEMATICA	31
3.3 ROZDÍL MEZI WEBMATHEMATICOU A MATHEMATICOU.....	31
4 PROGRAMOVÁ SIMULACE – MATHEMATICA	32

4.1	ÚVOD.....	32
4.2	GENERÁTOR PRVOČÍSEL.....	32
4.3	GENERÁTOR GRUP	33
4.4	POTVRZENÍ PRVOČÍSEL.....	34
4.5	DOHODA NA KLÍČI.....	35
4.5.1	Simulace bez útoku	35
4.5.2	Simulace s útokem.....	37
4.6	ZPŮSOB ŠIFROVÁNÍ.....	39
4.7	ZADÁVÁNÍ TEXTU.....	40
4.7.1	Šifrování PlayFair.....	41
4.7.2	Šifrování DES.....	41
4.8	OSTATNÍ ZÁLOŽKY	41
4.8.1	Zašifruj.....	42
4.8.2	Reset.....	42
4.8.3	Další a předchozí	42
5	VIZUALIZACE V PROSTŘEDÍ WEBMATHEMATICA.....	43
5.1	HLAVNÍ STRÁNKA – INDEX.JSP.....	43
5.2	SIMULACE BEZ ÚTOKU	43
5.3	SIMULACE S ÚTOKEM.....	46
	ZÁVĚR.....	49
	ZÁVĚR V ANGLIČTINĚ	50
	SEZNAM POUŽITÉ LITERATURY	51
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	54
	SEZNAM OBRÁZKŮ.....	55
	SEZNAM TABULEK	57
	SEZNAM PŘÍLOH.....	58

ÚVOD

V dnešní době se bez kryptografických systémů jen těžko obejdeme. Ani o tom nemusíme vědět a přesto jsou šifrovací systémy všude kolem nás. Hrozba zcizení důležitých údajů už vedla v historii k jistým krokům, jak tomuto zabránit. Technika ovšem rok co rok postupuje milovými kroky a proto je nutné tyto šifrovací systémy obměňovat a především zlepšovat. To, co platilo před pěti lety, už dnes nemusí platit a proto je důležité vybrat vhodný kryptografický systém k ochraně svých dat. Tato bakalářská práce zabývající se protokolem Diffie – Hellman ukazuje, jak důležitý byl tento objev v asymetrické kryptologii.

Jak již bylo zmíněno, tato bakalářská práce se zabývá především kryptografickým protokolem Diffie – Hellman. Nejdřív je zde ale popsána kryptologie jako celek. Od historických kořenů až po současnost.

Rovněž se zde uvádí rozdělení šifer z hlediska klíčového hospodářství, čili na symetrickou a asymetrickou kryptografii. Větší prostor je kladen pro asymetrickou kryptografii díky zařazení protokolu Diffie – Hellman.

Samotný šifrovací protokol je popsán od počátků jeho vzniku. Jsou zde popsány jeho výhody, nevýhody, matematický popis funkce a to nejdůležitější, rozbor samotného protokolu. V textu je popsán jak teoretický postup vytvoření klíče, tak i praktická ukázka s konkrétními čísly. Jsou využity tabulky a obrázky pro názornější vysvětlení situace.

Rovněž jsou zmíněny modifikace protokolu, ne vždy však jsou lepší než samotný nezměněný protokol.

Poslední kapitola teoretické části je zaměřena na útoky spojené s protokolem. Mezi nejznámější útok patří tzv. Man in the Middle Attack, který je zcela vysvětlen. Je zde popsáno, jak útok vypadá, zda jde útoku předejít, zda druhá strana pozná, že komunikace byla napadena aj. K lepšímu pochopení jsou uvedeny příklady, rovněž jak teoreticky, tak s konkrétními hodnotami i s obrázky. Digitální podpis tento problém z části řeší, jak je uvedeno v další podkapitole.

V praktické části je detailně popsána implementace protokolu v prostředí Mathematica a WebMathematica. Projekt psaný ve WebMathematice lze vyzkoušet na adrese <http://mathematica.fai.utb.cz:8080/webMathematica/Nemeckova/index.jsp>.

I. TEORETICKÁ ČÁST

1 KRYPTOLOGIE

Je věda, která se zabývá šifrováním ze všech úhlů pohledu. Jejími hlavními disciplínami jsou kryptografie, kryptoanalýza a steganografie.[1]

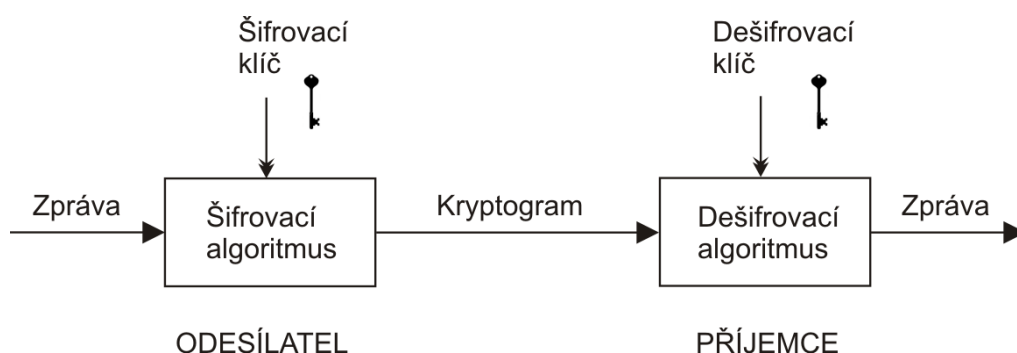
Abychom mohli proniknout do „tajemného“ světa utajené komunikace, je nutné si nejprve tyto pojmy definovat.

Kryptografie neboli šifrování je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí.[2] Často slouží i k ověření, zda v dokumentu nedošlo k neoprávněným zásahům. [6]

Kryptoanalýza je věda zabývající se metodami získávání obsahu šifrovaných informací bez přístupu k tajným informacím, které jsou za normálních okolností potřeba, tzn. především k tajnému klíči. Kryptoanalýza je opakem kryptografie, která šifry vytváří. Člověk zabývající se kryptoanalýzou se nazývá kryptoanalytik.[3]

Steganografie je vědní disciplína (podobor kryptografie) zabývající se utajením komunikace prostřednictvím ukrytí zprávy. Zpráva je ukryta tak, aby si pozorovatel neuvědomil, že komunikace vůbec probíhá. Zachycení skryté zprávy tak prakticky znamená její prolomení. Aby ani v tom případě nedošlo k prozrazení obsahu zprávy, zpravidla se kombinuje s dalšími metodami šifrování.[4]

Tradiční postup šifrování je vidět na obrázku 1. Toto schéma se využívá u všech šifrovacích systémů, jedině, v čem je rozdíl je distribuce klíčů.



Obrázek 1 Základní symetrické šifrovací schéma

V této práci se nadále vyskytují jména Alice, Bob a Eva, kde Alice s Bobem představují pár posílající si tajné zprávy a Eva je považována za útočníka. Tyto osoby se staly typickými účastníky kryptografické komunikace a ve zbytku textu jsou používány.

Kryptografie není jen o šifrování, ale nabízí i ve velké míře řešení, jak nahradit sociální mechanismy jako jsou rozpoznání tváře nebo používání psaného podpisu při přechodu na digitální způsob komunikace. Toto řešení uvedli ve své studii z roku 1976 s názvem Nové postupy kryptografie Whitfield Diffie a Martin Hellman. Představili, jak by mohla být kryptografie využita k vytvoření elektronického ekvivalentu tradičního podpisu.

1.1 Historie

Kryptografie je dobře zavedený vědní obor, který má na lidskou historii nemalý vliv již více než 2 000 let. Šifrování je zde už odnepaměti. Lze se s ní setkat od starého Egypta přes Mezopotámii, Césarův Řím, 2. světovou válku a s ní spojenou Enigmu a až po současnost.

V Egyptě jsme se mohli setkat s Hieroglyfy, v Římě s Césarovou šifrou (viz dále symetrická kryptografie) a za 2. Světové války to byl proslulý elektromechanický stroj Enigma, který byl využíván od počátku dvacátých let dvacátého století a měl pověst nerozluštitelného stroje.[6]

1.2 Současnost

V dnešní době je velmi důležité chránit si svá soukromá data. K tomuto účelu slouží právě kryptologie. S kryptologií je možno se setkat v podnikatelském sektoru, bankovníctví, vládních organizacích a i pro osobní využití. Rychlý růst technologií umožňuje využívat složitější matematické algoritmy, které dnešní počítače hravě zvládnou. Složité matematické funkce byli v minulosti nepředstavitelné.

Hlavním cílem každého šifrovacího systému je zamaskovat utajovanou zprávu tak, aby byla pro všechny nepovolané osoby zcela nečitelná.

Existují případy, kdy pro obdržení zprávy z kryptogramu není zapotřebí znát šifrovací klíč. Tento fakt, jenž je jedním ze zásadních poznatků zmíněné studie Diffieho a Hellmana, měl výrazný dopad na podobu moderní kryptologie a vedl k rozdělení šifrovacích systémů na dvě skupiny. Tím jsou symetrické a asymetrické šifrovací systémy.[6]

Do současnosti se řadí i kvantová kryptografie využívající poznatků kvantové mechaniky. Výhodou této kryptografie byla spolehlivá detekce odposlechu. Zjistí-li se odposlech, klíč se nepoužije a informace se nezašle.[21] Novější studie ukazují, že lze na tento systém zaútočit, aniž by zůstaly jakékoli stopy.

1.3 Rozdělení šifer

Šifry se dělí do kategorií podle určených kritérií. Jednak jsou to kryptosystémy podle postupu zpracovaného otevřeného textu, jednak dle použitého šifrovacího klíče.

Postup zpracovaného otevřeného textu dělíme na substituční a transpoziční šifry. Substituční znamená náhrada znaku za znak, například Caesarova šifra a transpoziční jednoduché přesouvání znaků podle určitých pravidel a s tím spojená šifra Playfair.

Dále se dělí podle použitého šifrovacího klíče, viz symetrické a asymetrické šifrovací systémy v nadcházející se kapitole 1.3.1 a 1.3.2.

1.3.1 Symetrické šifrování

Potíže spojené se správou klíčů bývají u symetrických a asymetrických systémů rozdílné.[6]

Symetrické šifrovací algoritmy používají tentýž klíč jak pro šifrování, tak i pro dešifrování. Všechny klíče zde musí zůstat utajeny, aby nebylo dovoleno neoprávněné osobě použití klíče k dešifraci tajných zpráv. Klíč má být často střídán a být dostatečně náhodný.[8]

U tohoto šifrování nastává problém, chtějí-li si dva lidé poslat tajnou zprávu. Odesílatel zprávu zašifruje tajným klíčem. Bylo by vhodné, poslat příjemci jak kryptogram, tak klíč. Tajný klíč ovšem nebude ničím chráněn a tak se útočník bez problému může dostat k otevřenému textu. Z toho vyplývá nutnost dostat klíč bezpečným způsobem na druhou stranu a bez obav posílat zašifrované texty. Tento problém řeší asymetrická kryptografie.

1.3.2 Asymetrické šifrování

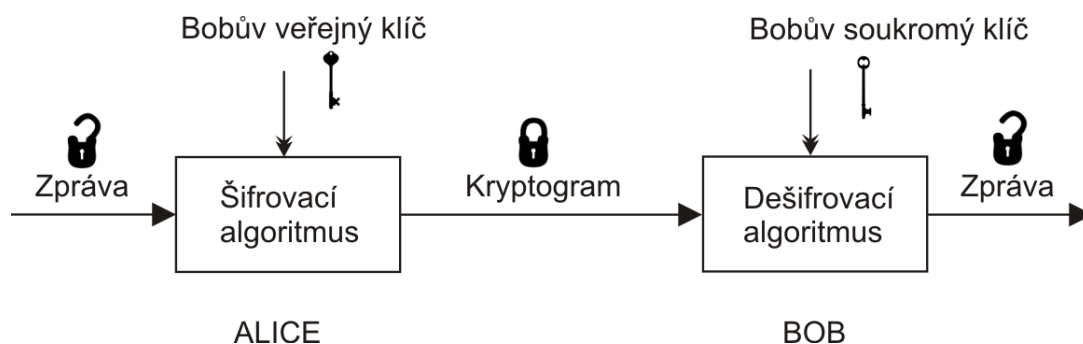
Asymetrické šifrování využívá dvojici klíčů pro šifrování a dešifrování. Tím pádem útočník, který získá klíč k zašifrování, nemůže kryptogram nijak ohrozit.

Používá se zde klíčů veřejných a soukromých. Pro zašifrování slouží klíč veřejný, který je dostupný široké veřejnosti a je spárovatelný pouze k jednomu soukromému klíči. Zatímco klíč soukromý, určený k dešifrování zpráv nesmí být nikým spatřen či odcizen a je utajován. Obrázek 2 napomůže k lepšímu pochopení.

Oba klíče jsou svázány matematickými vztahy, podstatné však je, že ze znalosti veřejného klíče nelze odvodit jeho privátní protějšek.

Princip jak s tímhle systémem pracovat, je následující. Bob má svůj pár klíčů. Jeden soukromý a jeden veřejný. Jeho veřejný klíč znají všichni, soukromý klíč zná jen Bob.

Kdokoliv mu chce poslat tajnou zprávu, zašifruje ji jeho veřejným klíčem. Jediný, kdo tuto zprávu může rozluštit je Bob, dokonce ani odesílatel (Alice) ji nerozšifruje.



Obrázek 2 Schéma asymetrického šifrování

Jak již bylo zmíněno, u symetrických systémů je hlavním úkolem zajistit bezpečnost přenosu klíče od odesílatele k příjemci. Zde, u asymetrických systémů se lze tomu vyhnout rozesíláním pouze šifrovacích (veřejných) klíčů, které není zapotřebí uchovávat v tajnosti. Vzniká zde ovšem jiný problém se zajištěním autenticity šifrovacích klíčů jednotlivých účastníků.[6]

K řešení tohoto problému vznikly certifikační autority a celá oblast, které se říká infrastruktura veřejných klíčů (PKI).[22]

Asymetrické šifry se používají výhradně v rámci takzvaných hybridních šifrovacích schémat. Otevřený text je nejprve zašifrován nějakou ze symetrických metod, poté je symetrický klíč zašifrován asymetrickou metodou. Kryptogram a klíč jsou společně v jednom balíku posláni druhé straně. Důvod hybridního šifrování je především ve využívání obou výhod, tím je rychlost u symetrické metody oproti asymetrické.[9]

1.4 Obecné způsoby útoků

Pokud zašifrovaná zpráva padne do ruky nepříteli, je pro něj odhalení jejího obsahu bez znalosti přesných pravidel použitých k jejímu dešifrování jen velmi obtížné nebo dokonce zcela nemožné.[5]

Je zde mnoho možností, jak šifrovanou zprávu napadnout. Typy útoků jsou následující.

Se znalostí otevřeného textu, se znalostí šifrovaného textu, s možností volby otevřených textů, adaptivní metoda s možností volby otevřených textů, s možností volby šifrovaných textů, s možností volby vybraného klíče, útok hrubou silou, útok postranními kanály, agenturní korupční kryptoanalýza a pendreková kryptoanalýza.[7]

Útok hrubou silou je vždy proveditelný. Schopnost odolat útoku hrubou silou je jednou ze základních vlastností dnešních kryptografických systémů.[8] Lze využít i statickou charakteristiku textu, pomocí frekvenční analýzy, kde se zjišťuje četnost znaků v abecedě. Každý jazyk má své specifika, a proto lze snadno zjistit, zda se jedná o transpoziční nebo substituční šifru.

1.4.1 Určování úrovně bezpečnosti

Jedno slavné kryptografické pravidlo říká, že bezpečnost systému nesmí záviset na utajení kryptografického algoritmu. Bezpečnost by se měla odvíjet pouze od utajení dešifrovacího klíče.

Jedná se vždy jen o předpoklady a odhady nejen co se týče informací, ale ohledně i jeho prostředků. Doporučeným principem v případě jakýchkoli pochyb je vždy očekávat tu horší variantu a řídit se zásadami opatrnosti. Není zde relevantní klást si otázku, zda se jedná o bezpečný systém, ale je tento systém dostatečně bezpečný pro tuto aplikaci? [6]

2 PROTOKOL DIFFIE - HELLMAN

Představitelé protokolu Whitfield Diffie a Martin Hellman začali společně studovat problém distribuce klíče, přičemž ze všech sil hledali alternativu k únavnému úkolu fyzického transportu klíčů na velké vzdálenosti (symetrická kryptografie). Alice i Bob se museli například jednou týdně sejít a předat si všechny možné klíče, se kterými budou v průběhu týdne komunikovat. Způsob předání klíčů je ovšem časově náročný. Pokud se jeden z nich nemohl dostavit, nastával problém, jak doručit příslušné klíče. Jednou z možností je využití kurýra, je to nákladné a navíc se zde objevuje otázka důvěryhodnosti třetí strany. [16]

Tento protokol představili pánové Whitfield Diffie a Martin Hellman, ve své práci z roku 1976 nazvané Nové postupy kryptografie.

Protokol se řadí mezi moderní asymetrické šifry, kde se jedná o algoritmus umožňující odesílateli a příjemci bezpečně ustanovit klíč pro symetrickou kryptografii.[10]

2.1 Prvotní vize Diffieho a Hellmana

Známý příklad o zámcích a kufříku říká: Alice vloží zprávu do kufříku a zamkne svým zámkem. Pošle dál Bobovi, který rovněž na kufřík umístí svůj zámek, a jelikož nemá klíč, nemůže zámek, patřící Alici odstranit. Bob pošle kufřík se dvěma zámky zpět Alici, která sejme svůj zámek a zašle opět Bobovi. Nyní na kufříku zůstává pouze Bobův zámek, který Bob jednoduše sejme a má zprávu od Alice. Zde lze snadno vidět, že zpráva může být bezpečně doručena, aniž by si příjemce a odesílatel museli vyměnit klíč.

Vypadá to, že problém distribuce klíčů je vyřešen, protože toto schéma nepotřebuje výměnu klíčů. Vzniká zde ovšem otázka v implementaci šifrového systému typu Alice zašifruje, Bob zašifruje, Alice dešifruje a Bob dešifruje. Problém je v pořadí šifrování a dešifrování. V našem případě potřebujeme, aby Alice dešifrovala jako první. Pokud se tak stane, už nezískáme původní otevřený text. Je potřeba, aby bylo zachováno pořadí. Kdo šifroval jako poslední, musí dešifrovat jako první. V našem případě Bob. Tuto metodu lze nazvat jako velmi známá metoda LIFO (last in, first out), která vystihuje podstatu věci.

Whitfield Diffie roku 1975 přišel s velkým objevem. Nový typ šifry s asymetrickým klíčem (viz kapitola 1.3.2 Asymetrické šifrování). Diffie tento nový systém formuloval, ale už nevěděl, jak jej realizovat. Ovšem objev to byl revoluční.

Diffie a Hellman si pohrávali s myšlenkou vzniku praktické metody, jež by obešla problém distribuce klíčů. Roku 1976 byla myšlenka dotažena do zdárného konce. Řešením se stala jednosměrná funkce $Y^x \bmod P$, kterou po mnoha pokusech úspěšně představil Martin Hellman. Tímto byl popřen axiom, který platil po staletí. Alice a Bob se nyní nemusí osobně setkat k předání potřebných klíčů pro budoucí komunikaci. Účastníci se dokonce nemusí ani znát. Má se za to, že se jedná o nejméně intuitivní objev v historii přírodních věd.[16]

2.2 Princip dohody na klíči

Veškerý matematický výpočet se točí okolo složitosti výpočtu diskrétního logaritmu (viz 2.3 Matematický popis funkce). Nyní si popíšeme názornou ukázkou protokolu mezi Alicí a Bobem.

Alice s Bobem se dohodnou na veřejných parametrech p a g . Kde p je prvočíslo a g je generátor grupy Z_p^* (viz 2.3.2 Generátor grup).

Alice si zvolí libovolné číslo x takové, že $1 \leq x < p-1$, a vypočítá X , které zašle Bobovi (viz vztah 1).

$$X = g^x \bmod p \quad (1)$$

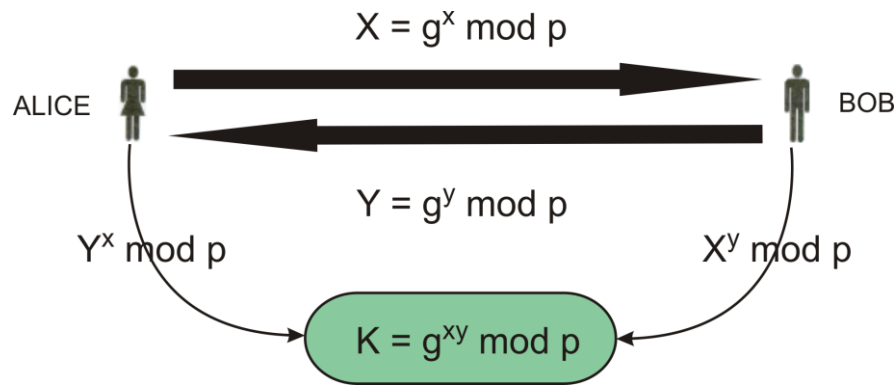
Bob si zvolí libovolné číslo y takové, že $1 \leq y < p-1$, a vypočítá $Y = g^y \bmod p$, které pošle Alici.

Alice vypočítá $Y^x \bmod p$ a Bob vypočítá $X^y \bmod p$ k získání klíče.

Jak Alice, tak Bob nyní vlastní tajný šifrovací klíč K pro symetrickou kryptografii, protože

$$K = Y^x \bmod p = (g^y)^x \bmod p = g^{xy} \bmod p = (g^x)^y \bmod p = X^y \bmod p = K. \quad \text{Grafické}$$

znázornění na Obrázku 3 napomůže k lepšímu pochopení.



Obrázek 3 Schéma protokolu Diffie Hellman

2.2.1 Příklad protokolu

Dosazení konkrétních čísel pro názornější představu.

p		31
g		11
x		22
$X = g^x \bmod p$	$X = 5^6 \bmod 23$	18
y		19
$Y = g^y \bmod p$	$Y = 5^{15} \bmod 23$	22
$K = Y^x \bmod p$	$K = 19^6 \bmod 23$	10
$K = X^y \bmod p$	$K = 8^{15} \bmod 23$	10

Tabulka 1 Princip Diffie Hellman protokolu

V Tabulce 1 lze jasně vidět, že vypočítaný klíč pro obě komunikující strany je stejný a má hodnotu 10.

2.3 Matematický popis funkce

Diffieho a Hellmana zajímaly především jednosměrné funkce. Tzn. jednoduché zašifrování a složité rozšifrování. Pro lepší představu, máme dvě barvy červená a modrá. Je jednoduché smícháním obou barev dostat fialovou, ovšem už mnohem obtížnější je dostat zpět barvu červenou a modrou. Na ukázce je jasné, že jednosměrné funkce nejsou vratné, oproti funkcím obousměrným.[16]

Bezpečnost Diffie - Hellmanova systému je založena na obtížnosti řešení úlohy tzv. diskretního logaritmu.[11] Jedná se o jednosměrnou funkci.

Je dáno $Y = g^k \bmod m$, kde k je nazýváno diskretním logaritmem o základu g z čísla Y vzhledem k modulu m . Jak lze zde vidět, jednoduché na spočítání pro libovolné k , ovšem

pokud se strana obrátí a máme zjistit inverzní funkci a hodnotu k , úloha je mnohem obtížnější.[19]

Pro srovnání normální a modulární aritmetika (viz Tabulka 2), kde je možnost vidět nepředvídatelnost chování modulární aritmetiky.

x	1	2	3	4	5	6
5^x	5	25	125	625	3125	15625
$5^x \pmod{7}$	5	4	6	2	3	1

Tabulka 2 Srovnání normální a modulární aritmetiky

2.3.1 Uživatelsky volené hodnoty

Uživatelé si zvolí velké prvočíslo p , často se volí $p = 2q + 1$, kde q je rovněž prvočíslo (tzv. prvočíslo Sophie Germainové nebo také bezpečné prvočíslo) a číslo g , které je generátorem grupy Z_p^* . Toto bezpečné prvočíslo má za úkol znesnadnit řešení diskretního logaritmu.[19]

Další zdroje naopak uvádějí jako veřejný parametr k prvočíslo p rovněž prvočíslo q . Zmínka o rozdílu mezi těmito parametry není v žádných z uvedených zdrojů. K rozdílu mezi generátorem grup g a prvočíslem q nejsou uváděny ani žádné spory, tudíž je pouze na uživateli, co se rozhodne použít. Ve vytvořeném projektu v Mathematice si uživatel stejně tak může vybrat.

Pokud prvočíslo p bude alespoň o 300 bitech a hodnoty a , b o 100 bitech, protokol DH bude zcela bezpečný. U generátoru g se volí menší číslo.

$$Z_p^* = \{1, 2, \dots, p-1\} \quad (2)$$

$$(1 < g < p)$$

$$Z_p^* = \{1, g^1, g^2, \dots, g^{p-2}\} \pmod{p} \quad (3)$$

Například, pokud je zvoleno prvočíslo $p = 11$, Z_{11}^* se rovná cyklické grupě (má v sobě generátor). $Z_{11}^* = \{1, 2, \dots, 10\}$ podle vztahu 2 a 3, kde generátor grup je číslo 2. $Z_{11}^* = \{1, 2, 2^2, \dots, 2^9\} \pmod{11} = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\}$. Čísla 3, 4 a 5 nejsou generátory grup, ale čísla 6 a 7 generátory rovněž jsou.[18]

2.3.2 Generátor grup

Máme celé číslo a a nejmenší celé číslo n takové, kde

$$1 = a^n \bmod p,$$

a kde n se nazývá řádem $a(\bmod p)$. Jestliže řádem je číslo $p-1$ ($1 = a^{p-1} \bmod p$) a pokud současně neplatí $1 = a^n \bmod p$ pro $(1 \leq n < p-1)$, pak celé číslo a je generátorem Z_p^* . [23]

Lze dokázat, že číslo 4 není generátorem. $Z_{11}^* = \{1, 4, 4^2, \dots, 4^9\} \bmod 11 = \{1, 4, 5, 9, 3, 1, \dots\}$. Vidíme, že $p-1$ (10) není nejmenší řád, je jím číslo 5 ($4^5 \bmod 11 = 1$).

2.3.3 Bezpečnost matematické funkce

Pro RSA (resp. Rabin-Williamsovo schéma) je základem bezpečnosti možnost protivníka faktorizovat velké číslo. Pro schémata, jejichž bezpečnost je založena na úloze diskretního logaritmu (El-Gamalovo schéma, Diffie-Hellmanův systém pro výměnu klíčů) je možnost spočítat tento diskretní logaritmus téměř nereálný, pokud se jedná o velká čísla. Je známo, že se jedná o vysoce složitý problém. Obecně se považuje za nemožné, pokud prvočíslo $p > 10^{300}$. Analogicky pro systémy na bázi eliptických křivek to jsou protivníkovy možnosti spočítat eliptický diskretní logaritmus. [12][15]

2.4 Výhody

- Narozdíl od symetrické kryptografie se neposílá přes komunikační kanál samotný klíč a odpadá jejich značné množství. Účastníci by nejlépe měli při každé komunikaci používat jiný klíč. Používání stále stejného klíče napomáhá kryptoanalytikům v jejich práci.
- Další výhodou je rozdíl ve zveřejnění čísel p a g . V šifře RSA, musí být čísla utajena (bezpečnost závisí na faktorizaci $p \cdot g$), na rozdíl od DH, kde čísla utajena být nemusejí.
- Za další je výhoda spočívající zejména v matematické funkci, jež protokol disponuje. Pokud by Eva odposlouchávala linku Alice a Boba, bezpečnost systému by neovlivnila, obzvlášť jedná-li se o velmi velké čísla. Je uveden příklad, co by se stalo při úspěšném odposlechu (viz níže).

Máme veřejně známé prvočíslo p , číslo g a jednosměrná funkce ($g^a \bmod p = A$). Eva odposlechem zjistí pouze číslo A , které Alice zasílá Bobovi nebo obráceně číslo B . Aby Eva zjistila klíč, musí udělat to stejné, co Bob/Alice a tím je $A^b \bmod p = K$ nebo

$B^a \bmod p = K$. Eva ovšem nezná ani číslo a , ani číslo b , které si oba účastníci nechávají v tajnosti. Evě v takovémto případě nezbyvá nic jiného, než řešit jednosměrnou funkci. Jak už sám název napovídá, touto cestou to bude velmi obtížné, dá se říci, pro velmi velká čísla zcela nemožné.[16]

2.5 Nevýhody

- Jedním z největších nevýhod patří bezpochyby útok Man in the Middle, který je popsán v kapitole 2.8 Man in the Middle Attack.
- Mezi další problémy se řadí zdlouhavost celého procesu předání klíče. Je nutné si vzájemně zaslat dílčí výpočty a z nich pak dopočítat společný klíč pro symetrickou komunikaci. Naproti tomu klasická šifra se posílá jen jednou, ovšem toto je vykoupeno složitým způsobem zajišťující bezpečnost pro příslušný dešifrovací klíč. V dnešní přetechizované době tento problém nepředstavuje žádné obtíže.[5]
- Za další nevýhodu lze považovat nutnost přímé komunikace účastníků na dohodě klíče. Jestliže se účastníci chtějí dohodnout na klíči, musí vzájemně komunikovat při posílání dílčích výpočtů, ze kterých pak vzejde klíč K pro symetrickou kryptografii. Chce-li Alice poslat tajnou zprávu Bobovi, musí obdržet jeho část výpočtu, pokud ji nemá, nemůže začít tajně komunikovat.

Existuje menší modifikace, kde účastníci na sebe nemusejí čekat. Postačí, když Bob zašle Alici vypočítané Y . Zde jeho úloha prozatím končí. Alice si z došlých údajů spočítá klíč K ($Y^x \bmod p = K$) a zašifruje zprávu. Nyní už nemusí na nic čekat a posílá kryptogram společně s X (může být veřejně) Bobovi. Příjemce kdykoli rovněž může spočítat klíč K a zprávu přečíst.[17]

2.6 Modifikace DH

Diffie – Hellman protokol byl od svého počátku již několikrát zmodifikován. Ve stručnosti představíme El Gamalův systém s veřejným klíčem, Diffie – Hellman s využitím eliptických křivek a s využitím digitálního podpisu.

El Gamalův postup je obdobný jak u klasického DH protokolu. Bob si zvolí čísla p a g , z nichž následně vypočítá svůj veřejný klíč B . Alici zašle veřejné parametry (B, g, p) . Alice si

zvolí náhodné celé číslo k a provede následující výpočty. Nejdřív si zprávu m převede do číselného tvaru a vypočítá $c = g^k \bmod p$ a $d = m \cdot (Y^k \bmod p) \bmod p$, které následně zašle Bobovi jako řetězec (c, d) . Nyní si už Bob může rozšifrovat zprávu podle vztahu
$$\frac{d}{c^y} = \frac{m(Y^k)}{(g^k)^y} = \frac{m(g^{yk})}{g^{ky}} = m.$$
 Nevýhoda systému je taková, že šifrovaná data jsou dvakrát tak velká. Z tohoto důvodu není El Gamal příliš rozšířený.[18]

Dalším vylepšením DH je **využití eliptických křivek** poskytující větší bezpečnost a používají výrazně kratší délku klíčů. Účastníci se musí dohodnout na parametrech vztahující se k eliptickým křivkám, které se využívají při výpočtu. Jsou považovány jako nástupci modulární aritmetiky. Bezpečnost rovněž závisí na řešení problému diskrétního logaritmu u eliptických křivek.[20]

Digitální podpis je probrán v kapitole 2.8.4 Digitální podpis.

2.7 Možnosti útoků

V kryptologii se od pradávna snažili útočníci získat různými způsoby tajné informace. Mezi útoky patří útoky postranními kanály proti kryptografickým modulům, s nimiž vznikla nová kategorie útočných metod.[13] Ukázalo se, že z kvalitně zabezpečeného systému, který implementuje ty nejlepší šifry, bezpečnostní normy a systémové ochrany, lze postranními kanály získávat právě ty senzitivní informace (šifrovací klíče, podepisovací klíče, aj.), které měly zůstat utajené. Do jejich příchodu bývalo velmi neobvyklé, aby se i na těch nejprestižnějších konferencích objevovaly útoky vedoucí k totálnímu prolomení napadaného systému. Ukazuje se, že riziko prolomení nedbale navrženého systému je vysoké.[14] Kryptografické moduly (čip, bankomat, server, knihovna apod.) pracují s tajnými klíči a zajišťují operace šifrování, ověřování aj.

Postranní kanály vznikají většinou nevědomky, jsou nezamýšlené a bývají nejcitlivější součástí systému. Proto jsou vyhledávaným místem útoků. Postranní kanál se dá definovat jako nežádoucí způsob výměny informací mezi kryptografickým modulem a jeho okolím. Tyto kanály většinou mají měřitelné fyzikální veličiny, které jsou závislé na průběhu výpočtů napadeného modulu. Zařazeny jsou kanály proudové, napětíové, časové...

Chybové kanály se rovněž řadí mezi postranní kanály. Výsledky vzniklé při chybě nebo výpadku části systému, jsou vynášeny pomocí chybových hlášení a jsou zdrojem cenných informací o citlivých datech uvnitř modulu. Chyba může být jak neúmyslná, tak i záměrně

způsobená působením na modul. Útočník příslušný postranní kanál vytváří nebo jej aktivuje invazivními i neinvazivními metodami.[13][14]

2.7.1 Podprahový kanál

Podprahový kanál je záměrně vytvořen útočníkem, k vynášení citlivých informací, který má poměrně blízko ke steganografii. Pokud je takový kanál implementován do kryptografického zařízení bez vědomí jeho uživatele, potom se z něho stává zvláštní druh postranního kanálu, který označujeme jako kleptografický.

Kryptografické moduly integrují s okolím nejrůznějšími způsoby jako je elektromagnetické, akustické a jiné vyřazování. Projevují se rovněž spotřebou proudu, času, paměti a chybovými hlášeními.[13]

2.7.2 Časový postranní kanál

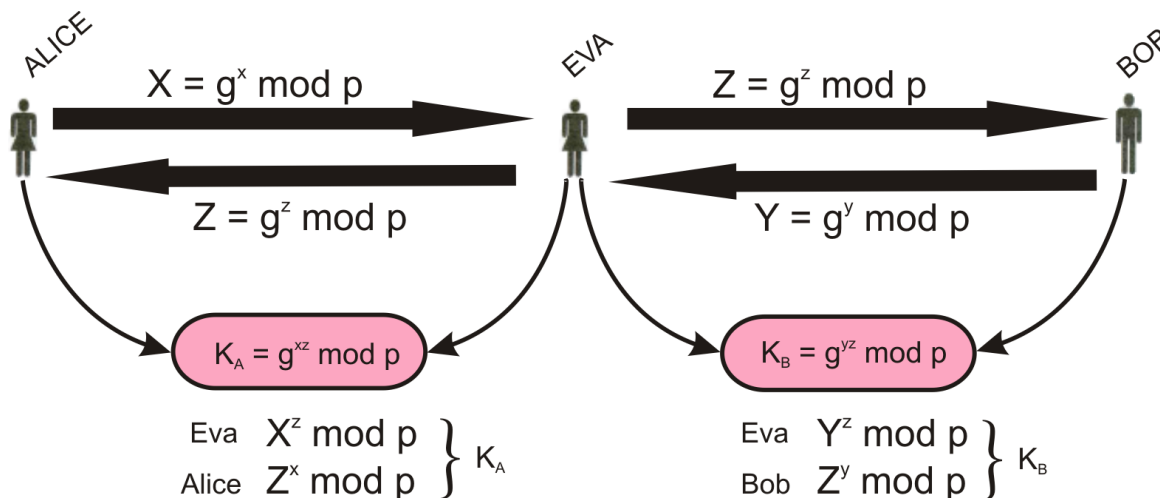
Časový postranní kanál využívá toho, že určité operace závislé na tajném klíči trvají krátce nebo déle v závislosti na konkrétních hodnotách jednotlivých bitů klíče. Útoky, založené na tomto principu využívají různá místa příslušného kryptografického modulu a různé nástroje na vyhodnocování získaných časových údajů. Doba každého průchodu smyčkou závisí na tom, zda daný bit klíče je nula nebo jedna. Je-li nula, výpočet je rychlejší, je-li jedna, výpočet trvá déle. Útočník zná vstupní hodnotu, tudíž si může každý krok uvedené smyčky simulovat, pokud zná daný algoritmus.

Mezi další útoky patří známé schéma Man in the Middle viz dále.

2.8 Man in the Middle Attack

Laicky řečeno útočník, který stojí uprostřed a zachytává komunikaci. Tento útok je nebezpečný v tom, že jak příjemce, tak odesílatel za určitých okolností nemusí o útočnickovi vůbec vědět. Útočník nejenže si může zprávu, která mu nepatří přečíst, ale může i komunikaci či dokument svým vlastním způsobem pozměnit, což může vést k nežádoucím následkům, probíhá-li komunikace například v obchodní sféře. Na obrázku 4 je uvedeno, jak komunikace probíhá.

2.8.1 Grafické znázornění útoku



Obrázek 4 Schéma útoku man in the middle

Útok Man in the middle spočívá v zachycení, překryptování a zaslání dále uživateli v domnění, že se jedná o zprávu od sjednaného komunikujícího, nikoli od útočníka.

2.8.2 Popis útoku

Jak lze vidět na obrázku 4 Alice známým způsobem vypočítá X a pošle Bobovi. Ovšem tuto část zachytí Eva a Bobovi zašle své vypočítané Z . Bob nemá žádné podezření, jedná se o podvrh. Je stále v domnění, že přijal X poslané Alicí. Stejným způsobem postupuje i Bob. Posílá vypočítané Y , kde Eva znovu zachytí toto číslo a Alici podstrčí svoje. Nyní komunikující žijí v domnění, že mají čísla toho druhého, a kde již můžou v bezpečí spočítat svůj tajný klíč k pozdějšímu šifrování. V takovémto případě Alice i Bob mají společný klíč s Evou. Pokud tedy Eva nechce, aby kdokoli pojal podezření, že je hlavním článkem v komunikaci, musí každou zprávu, kterou si budou Alice s Bobem vyměňovat, překryptovat a poslat určenému příjemci. Bez toho, aby to Eva udělala, by komunikující ihned nabyli podezření, že mají nezvaného hosta.

Po krocích jsou ukázány dílčí výpočty k snadnějšímu pochopení.

1. Krok: Alice i Bob si zvolí tajné číslo a a b . Podle vztahu 1, kam dosadí své údaje spočítají veřejné A a B . Následně zašlou druhé straně.
2. Krok: Eva odposlouchávající na lince, zachytí komunikaci (A a B) a zašle Alici i Bobovi své veřejné C , rovněž vypočítáno dle vztahu 1, z tajného čísla c .

3. Krok: Alice s Bobem spočítají tajné klíče (viz vztah 2). V tomto kroku již oba účastníci mají různé klíče spojené s Evou.
4. Krok: Eva si spočítá zvlášť klíč pro Alici a zvlášť klíč pro Boba ze vztahu 2.

Doplnění konkrétních čísel k jednotlivým krokům níže.

Legenda grafického značení.

	veřejné	tajné	společné
--	---------	-------	----------

Je zvoleno prvočíslo p a generátor grup g .

p	17
g	5

1. Krok: Volba tajného čísla Alice i Boba se současným výpočtem veřejných čísel.

	a	7
	b	3
A	$g^a \bmod p = 5^7 \bmod 17$	10
B	$g^b \bmod p = 5^3 \bmod 17$	6

2. Krok: Tajné číslo c s výpočtem veřejného C .

	c	2
C	$g^c \bmod p = 5^2 \bmod 17$	8

3. Krok: Výpočet klíče Alice a Boba s podstrčeným číslem C od Evy.

K_{AC}	$C^a \bmod p = 8^7 \bmod 17$	15
K_{BC}	$C^b \bmod p = 8^3 \bmod 17$	2

4. Krok: Výpočet Evy obou klíčů ze zachycených údajů.

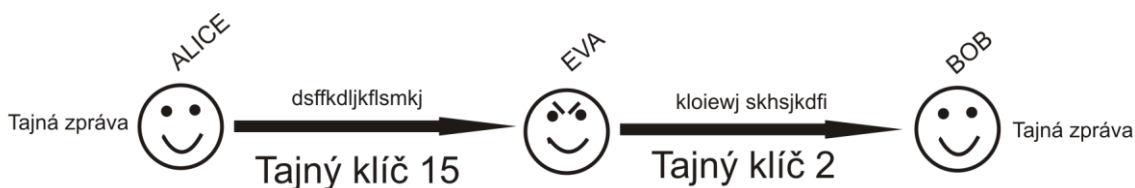
K_{AC}	$A^c \bmod p = 10^2 \bmod 17$	15
K_{BC}	$B^c \bmod p = 6^2 \bmod 17$	2

Jde vidět, že Alice i Bob mají různé klíče (K_{AC} a K_{BC} by měly mít stejné hodnoty), čili přímá komunikace by nebyla možná. Jediná možnost je přes Evu, která musí překryptovávat zprávy.

Co se děje, když Eva překryptovává zprávy a co se stane, kdyby Eva v každém směru komunikace zprávy nepřekryptovávala je popsáno níže (kapitola 2.8.3).

2.8.3 Možnosti útočníka

V prvním případě, pokud Eva zprávy překryptovává, druhá strana nepozná (Bob), že zpráva se nacházela v nesprávných rukou. Eva si zprávu u sebe přečte a překryptuje na stejný symetrický klíč s Bobem, se kterým si jej dříve vytvořila (v našem případě klíč 2, viz obrázek 5).



Obrázek 5 Ukázka s překryptování útočníka

Tímto způsobem může Eva bez problému libovolně měnit text, aniž by o tom kdokoli věděl. I na tento problém bylo myšleno a lze jej snadno vyřešit tzv. digitálním podpisem.

V případě druhém (obrázek 6) si Eva zprávu rovněž přečte, ale ponechá jej tak jak je a do zašifrovaného textu putující Bobovi již nezasahuje. Bob nemá společný klíč s Alicí, a proto není možné, aby zprávu rozšifroval na smysluplný text. Zpráva byla zašifrována klíčem 15 a Bob má klíč 2.



Obrázek 6 Bez překryptování útočníka

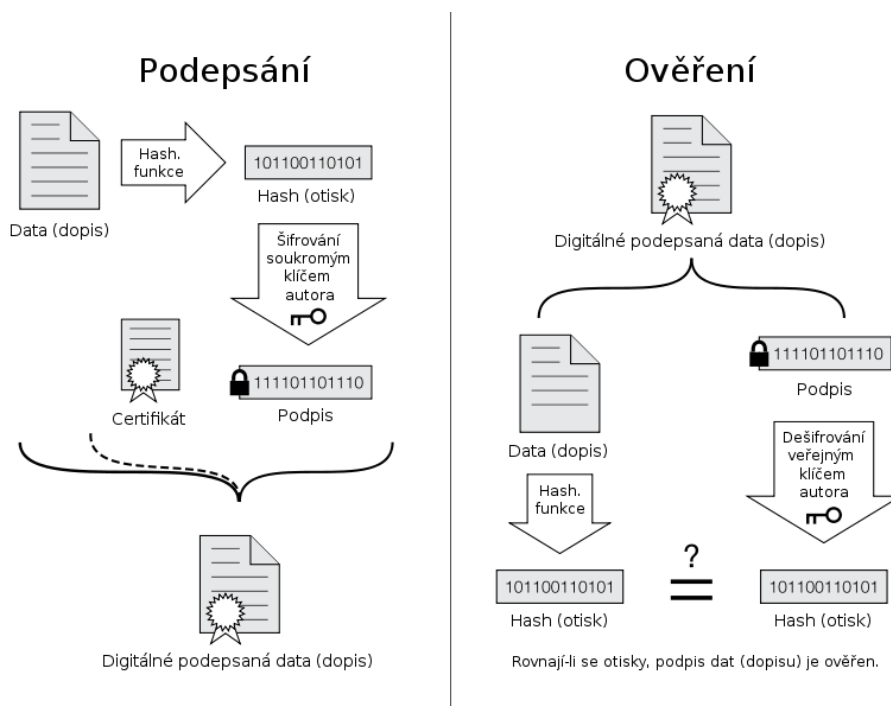
2.8.4 Digitální podpis

Digitální podpis zaručuje autentizaci zpráv, díky nimž si je Bob plně jist o přijetí originální zprávy od Alice.

Digitální podpis se provádí pomocí soukromého klíče, kde soukromý klíč je šifrovací a veřejný dešifrovací. Vychází rovněž z koncepce Diffie - Hellman.

Využití digitálního podpisu je vhodné, pokud chce Alice zaslat zprávu Bobovi a dbá na tom, aby zpráva dorazila v nepozměněném tvaru. Alice zprávu nejprve zašifruje svým soukromým klíčem a poté šifruje veřejným klíčem Boba. Bob po přijetí zprávy potřebuje dva klíče na plné dešifrování. Nejprve svůj soukromý klíč, a poté veřejný klíč Alice, který je dostupný široké veřejnosti. Bob si je jist původem zprávy, protože Alice jako jediná zná svůj soukromý klíč k digitálnímu podpisu.

Jako druhou metodou se může použít hashovací funkce. Jedná se rovněž o jednosměrnou funkci. Alice otevřený text prožene hash. funkcí, kde výsledkem je náhodná posloupnost číslic (tzv. hash), kterou posléze zašifruje svým soukromým klíčem. Je to rychlejší, než aby podepisoval celý otevřený text. Otevřený text se zašifruje předem dohodnutým klíčem DH protokolu a zašle Bobovi jak kryptogram, tak hash. Bob klasicky dešifruje kryptogram a na otevřený text použije rovněž hashovací funkci. Poté veřejným klíčem Alice dešifruje podepsaný dokument. Nyní, pokud vše proběhlo v pořádku, má Bob dva identické dokumenty. Alicinu hashovanou zprávu a svoji. Pokud by ve zprávě byl změněn pouze jeden jediný bit, hash by byl úplně jiný (obrázek 7).



Obrázek 7 Digitální podpis

Pokud by Eva přece jen odposlouchávala linku (Man In the Middle), zprávu by si mohla přečíst, má s Alicí a Bobem své klíče a zná veřejný klíč Alice, ale i přesto by nemohla zprávu/hash pozměnit. Nezná již soukromý klíč Alice. Pokud by Eva zprávu i tak podepsala

svým soukromým klíčem, Bob by zprávu dešifroval Aliciným veřejným klíčem k ověření integrity. Zde Bob pozná, že se stal obětí podvodu, neboť by se nedočetl ničeho zajímavého. Místo smysluplného textu by viděl pouze chaotický změt' písmenek. V případě hashe by byla zpráva zcela jiná.

II. PRAKTICKÁ ČÁST

3 ROZBOR PROGRAMOVÉHO PROSTŘEDÍ

Předchozí část bakalářské práce se zabývala pouze teoretickými vlastnostmi a principy šifrování. Hlavním tématem je protokol Diffie – Hellman. Vysvětleno bylo především, na jakém principu protokol pracuje, jaké jsou jeho klady a zápory a rovněž teoreticky rozebraný útok. Zde v praktické části je ukázána demonstrace protokolu DH od generování veřejných údajů, přes tvorby klíče, až po výsledný zašifrovaný text.

Ukázkový projekt je vytvořen v prostředí Mathematica a webMahtematica. U Mathematicy je nutné tento produkt vlastnit. Ostatní zájemci zde mají možnost využít službu webMathematica, kde si kdokoli může jednoduše nastavit své tajné a veřejné hodnoty a jen sledovat výpočet klíče a zašifrovaný text viz kapitola 4 a 5.

3.1 Mathematica

Software Mathematica je výpočetní software, který dokáže řešit složité matematické úkony, vykreslovat funkce, grafy. Dokáže si poradit i s interaktivními prvky, různými tlačítky, přepínači a dokonce i posuvníky.

Nyní jej používají miliony uživatelů - od studentů na svých studentských projektech, přes obchodníky až po vědce, kteří jej využívají k odborným činnostem. Umožňuje řešit projekty libovolného rozsahu od rutinních výpočtů až po velkosystémová řešení.[24]

Mathematica nachází široké uplatnění zejména v oblasti vědecko-technických výpočtů, statistickém zpracování dat, finančním managementu, univerzitách, v lékařských institucích, astronomii atp.[24] Hlavní síla výpočetních dovedností spočívá v modelování a simulacích.

Univerzity a zaměstnanci po celém světě po 20 let používají Mathematicu od učení jednoduchých pojmů až po ohromné výzkumy v celosvětových skupinách. Mathematica angažuje studenty převážně v interaktivním cvičení k hlubšímu pochopení a přípravě pro budoucí zaměření. Akademičtí vědci můžou využívat Mathematicu pro rychlou a přesnou analýzu dat a testování hypotéz.[26]

Výhoda softwaru, oproti jiným, je v alokaci a dealokaci místa v paměti. O všechno se stará program sám. Další výhoda je v technické podpoře a bravurně zvládnuté nápovědě. Nápověda činní kolem 10 000 stránek s matematickými funkcemi a tutoriály a více než 100 000 příkladů.[25]

3.2 WebMathematica

WebMathematica slouží především pro ty, kteří nemají tu možnost spouštět klasické mathematické soubory. Uživatelé nemusí mít nainstalovanou Mathematicu a přitom mu vytvořený program bezproblémově půjde. Všechny údaje, co uživatel zadá, se posílají na server. Server je specializovaný Mathematicou, kde se provedou dané výpočty, které uživateli navrátí zpět.

WebMathematica dokáže přidat dynamické prvky na stránku, jako jsou posuvníky a ostatní zařízení. Dokáže interaktivně počítat a zobrazovat grafické prvky, přes webové servery s nejnovějšími technologiemi. Po změně dynamického prvku zajišťuje novým parametrům přepočítání na serveru a nově vrátit.

WebMathematica využívá webové Java technologie jako Java Servlet, JavaScript a Java applety. Umožňuje výstup na webové stránky nebo vytvoření stáhnutelného PDF dokumentu, notebooku nebo do jiných formátů.

3.3 Rozdíl mezi webMathematicou a Mathematicou

WebMathematica a Mathematica mají stejné vlastní jádro, ale poskytují odlišný uživatelský interface a jsou zaměřené na různé typy uživatelů.

WebMathematica nabízí přístup ke specifickým Mathematickým aplikacím skrz webový prohlížeč nebo webové klienty. Standardní interface vyžaduje menší znalosti k efektivnímu používání. V mnoha případech, uživatelé ani nemusí být obeznámeni s Mathematicou nebo ani nemusí vědět, že ji používají.

Podobně, vývojáři WebMathematicy potřebují pouze základní znalosti HTML kódu a Mathematicy k vytvoření kompletní, plně funkční webové stránky. Ostatní odborné programy vyžadují znalosti programování Javy a dovolují pouze tvorbu menších appletů. Výhodou WebMathematicy je přístup k plnému rozsahu výpočetních Mathematických možností. Díky této dovednosti vývojáři nepotřebují pracovat s knihovnami.

Dá se říci, že Mathematica je vývojovým prostředím pro stránky WebMathematicy. Například lze pracovat s kódem v Mathematice, který je umístěn do stránky WebMathematicy a přístupný ostatním k prohlížení a spuštění.[27]

4 PROGRAMOVÁ SIMULACE – MATHEMATICA

V této kapitole je uvedena vytvořená simulace programu protokolu Diffie - Hellman. Uvedeny jsou části programu, které jsou využívány k celkovému generování tajných čísel společně s veřejnými uživatelskými údaji i se zašifrováním.

4.1 Úvod

V úvodu je menší shrnutí, co tato programová simulace přináší a co nabízí jednotlivé záložky.

Celé okno, kde si uživatel vybírá z nabídnutých možností je vytvořeno pomocí záložek, jak lze vidět na obrázku 8. Nejlepší způsob, jak simulovat protokol Diffie-Hellman je procházet záložky popořadě.

Protokol Diffie Hellman	
<p><i>Tato programová simulace má za úkol ukázat postup vytvoření klíče. Niže jsou popsány jednotlivé funkce. Uživatel si v pravo vybírá z daných voleb. Je doporučeno procházet položky popořadě. V dolní části je v krátkosti popsáno, co která záložka nabízí.</i></p>	
Prvočíslo	Záložka prvočíslo umožňuje uživateli vytvořit si prvočíslo dle libosti. Může si zvolit, kterou proměnnou chce generovat a může přímo určit počet desetinných míst.
Potvrzení	Uživatelská volba simulace s útokem nebo bez útoku se současným potvrzením prvočísel. Tento krok je důležitý pro další pokračování tvorby klíče.
Dohoda na klíči	Podle výběru simulace se zadávají veřejné údaje obou zúčastněných, popřípadě třetího účastníka Evy. V této části se vygeneruje klíč k šifrování.
Způsob šifrování	Výběr dat k zašifrování ze souboru a uložení vytvořeného kryptogramu do souboru nebo do textového pole v simulaci. Uživatel si zde vybírá typ šifry a zda chce šifrovat či dešifrovat.
Text	Text, který se bude šifrovat nebo dešifrovat. Je-li zvolena simulace s útokem, uživatel si může v horní části vybrat, zda chce šifrovat s klíčem Alice-Eva nebo Bob-Eva.
Zašifruj	Tato záložka slouží jako tlačítko. Po této volbě se provede zašifrování vytvořeným klíčem a současně se vrátí na přechodí položku Text.
Reset	Opět slouží jako tlačítko ke smazání všech proměnných. Po tomto stisku může uživatel znovu vybírat prvočísla a tvořit nové klíče. Stávající kryptogram se smaže.
Další Předchozí	Přepínání mezi záložkami tam a zpět.

Předchozí
Zvolte jednu z hodnot v pravo
Další

Obrázek 8 Prostředí pro uživatele

Nejdřív si ukážeme tvorbu prvočísla p a g/q .

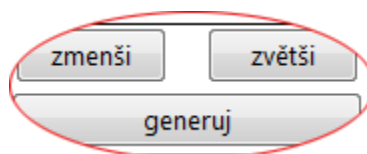
4.2 Generátor prvočísel

Generátor prvočísel má za úkol vygenerovat prvočísla v rozsahu zvoleného počtu cifer. Čím větší prvočíslo, tím silnější klíč. Program je náchylný na setkání příliš dlouhých čísel prvočísla a tajného čísla (kapitola 4.4).

Obrázek 9 Generování prvočísel

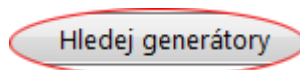
Jak lze vidět na obrázku 9, prvočíslo p je zvoleno trojmístné. Horní přepínač mezi p a q umožňuje vybrat, pro jakou proměnnou je právě vybíráno prvočíslo. Přepínač jiné se využívá v případě, pokud uživatel bude chtít například 100místné prvočíslo.

Prvek zmenši a zvětši, ubírá a přidává desetinné místo. Tlačítko generuj, generuje ve zvoleném desetinném místě prvočíslo k naší plné spokojenosti (Obrázek 10).



Obrázek 10 Tlačítka k volbě vhodného prvočísla

Spodní tlačítko „Hledej generátory“ na obrázku 11, vyhledá všechny generátory grup Z_p^* (viz 2.3.2 Generátor grup). Tato funkce je omezena pouze do velikosti prvočísla 700. Je to dáno matematickou náročností výpočtu.



Obrázek 11 Tlačítko pro vyvolání generátoru grup

4.3 Generátor grup

Po stisku tlačítka na obrázku 11 se objeví tabulka (Obrázek 12) s vypsányými všemi generátory grup daného prvočísla. V našem případě má prvočíslo hodnotu 541.

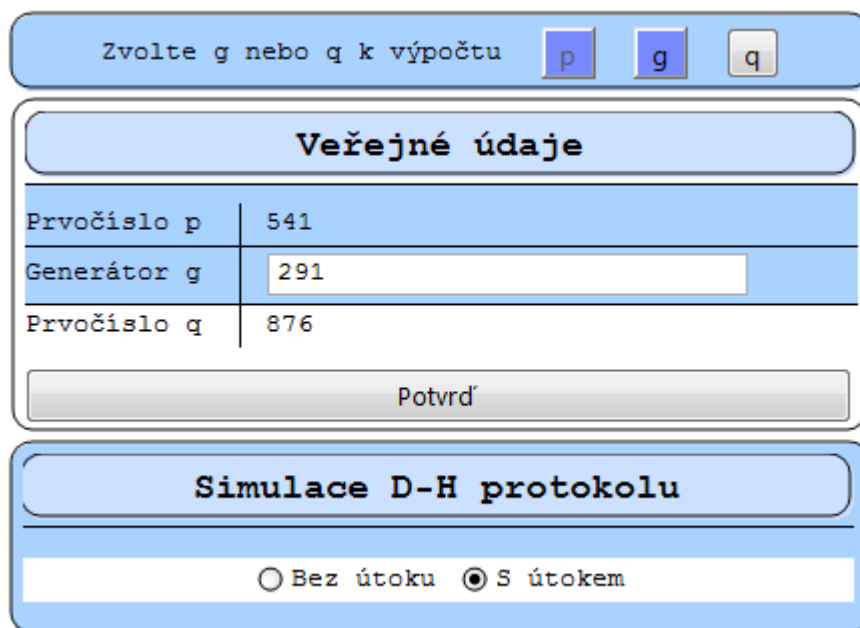
Generátor grup	
Prvočíslo	541
Generator	{2, 10, 13, 14, 18, 24, 30, 37, 40, 47, 51, 54, 55, 59, 62, 65, 67, 68, 72, 73, 77, 83, 86, 87, 91, 94, 96, 98, 99, 107, 112, 113, 114, 116, 117, 126, 127, 128, 131, 132, 138, 146, 150, 152, 153, 156, 158, 163, 166, 176, 181, 183, 184, 195, 197, 199, 206, 208, 210, 213, 218, 220, 223, 224, 235, 242, 244, 248, 250, 255, 257, 258, 259, 260, 261, 263, 267, 269, 270, 271, 272, 274, 278, 280, 281, 282, 283, 284, 287, 291, 293, 297, 305, 317, 318, 321, 323, 326, 328, 331, 333, 335, 342, 344, 346, 357, 358, 360, 365, 377, 378, 382, 383, 385, 388, 389, 391, 397, 403, 409, 410, 413, 414, 415, 424, 425, 427, 428, 434, 442, 443, 445, 447, 450, 454, 455, 458, 464, 468, 469, 473, 474, 476, 479, 482, 486, 487, 490, 496, 501, 504, 511, 517, 523, 527, 528, 531, 536, 539}
Rychlost výpočtu	1.419
OK	

Obrázek 12 Výpis všech generátorů zvoleného prvočísla

Uživatel si v tomto případě může vybrat jedno z výše uvedených čísel. Toto číslo zapíše do kolonky „Generátor g “ (Obrázek 13). Pakliže tohoto způsobu nevyužije, vybere si prvočíslo q místo g . Toto prvočíslo se volí stejně jako prvočíslo p , viz 4.1.

4.4 Potvrzení prvočísel

Další krok uživatele je potvrzení zadaných prvočísel (Obrázek 13). Bez potvrzení nemůže uživatel dál pokračovat a ještě se může vrátit k předchozímu kroku, ke změně čísla p , g/q . Po potvrzení už jej měnit nemůže a postupuje dál v simulaci.



Zvolte g nebo q k výpočtu p g q

Veřejné údaje

Prvočíslo p	541
Generátor g	291
Prvočíslo q	876

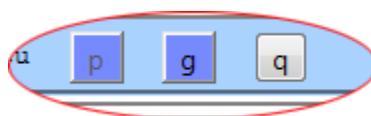
Potvrd

Simulace D-H protokolu

☐ Bez útoku ☒ S útokem

Obrázek 13 Potvrzení zvolených prvočísel

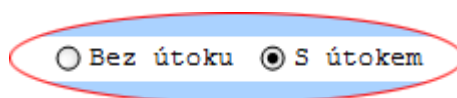
Jako první si uživatel vybere nabídku g nebo q .



Obrázek 14 Volba proměnných k výpočtu

Dle této volby program bude počítat s vybranou proměnnou. Na obrázku 14 je vybrána proměnná p , která je nastavená implicitně a uživatelem vybraná druhá proměnná g .

Dále je vidět, že byl vybrán jako „Generátor g “ číslo 291. Po potvrzení již v tomto kroku zbývá vybrat, zda využít simulaci s útokem nebo bez útoku (Obrázek 15).



Obrázek 15 Volba simulace

4.5 Dohoda na klíči

Podle výběru na obrázku 15 následují dvě situace.

4.5.1 Simulace bez útoku

V této situaci nefiguruje útočník. Pouze obvyklí účastníci Bob a Alice. Na obrázku 16 jsou vidět potřebné úkony, které musí uživatel splnit.

Alice	Bob
Zadejte tajné číslo x 665	Zadejte tajné číslo y 434
Vypočítané veřejné X 760	Vypočítané veřejné Y 2062
Zašli Bobovi ->	<- Zašli Alici
Tajný klíč 1509	Tajný klíč Výsledek K
Zaslané druhou stranou: 2062	Zaslané druhou stranou: X
Vypočítej klíč	Čekej na X od Alice
x = 665 X = 760.	y = 434 Y = 2062.

Obrázek 16 Generace čísel bez útoku

Každý uživatel zadá do kolonky „Zadejte tajné číslo“ své tajné číslo, které zůstává v tajném držení dotčené osoby. Současně se vypočítá veřejné X a Y, které se zašlou druhé straně pomocí tlačítka „Zašli Bobovi/Alici“. Jak lze vidět na obrázku 16 i 17, Alice zadala tajné číslo 665 a její veřejné číslo je 760.

Zadejte tajné číslo x

665

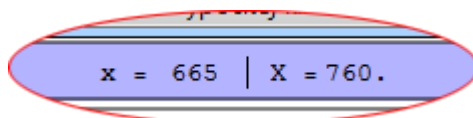
Vypočítané veřejné X

760

Obrázek 17 Zadané tajné číslo prvního účastníka

Bez zaslání veřejného čísla druhé komunikující osobě nepůjde vypočítat tajný klíč, který je závislý jak na veřejném čísle toho druhého, tak na zadaném tajném čísle (viz kapitola 2.2). Spodní tlačítko ukazuje, jaká akce je ještě potřeba. Pokud jakákoli strana stále nedostala všechny potřebné informace, tlačítko zůstává neaktivní, společně s upozorňujícím popiskem.

Na obrázku 16 si lze povšimnout že, Bob stále čeká na veřejné číslo X zaslané od Alice. Samotný klíč je podbarven červenou barvou. Spodní řádek pouze signalizuje, veřejné a tajné číslo v jednom (Obrázek 18).



Obrázek 18 Tajné a veřejné číslo

Barevné označení tlačítek vybízí a současně upozorňuje uživatele k provedení akce. Obrázek 16 ukazuje, že veřejné číslo Boba již bylo zasláno Alici, ale Alice stále nezaslala svůj veřejný parametr k výpočtu klíče.

4.5.2 Simulace s útokem

Zde následuje ukázka tvorby klíčů s útokem. Figurují zde všichni tři účastníci (Obrázek 19).

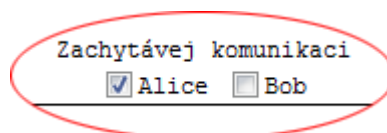
The screenshot shows a simulation interface with three main panels for Alice, Eva, and Bob.

- Alice Panel:**
 - Header: Alice
 - Input: "Zadejte tajné číslo x" with value 65.
 - Output: "Vypočítané veřejné X" with value 2799.
 - Button: "Zašli Bobovi ->" (disabled).
 - Section: "Tajný klíč" with "Výsledek K" (red box).
 - Text: "Zaslané druhou stranou: 1903".
 - Button: "Vypočítej klíč" (cyan).
 - Footer: "x = 65 | X = 2799."
- Eva Panel:**
 - Header: Eva
 - Section: "Zachytávej komunikaci" with checkboxes for Alice (checked) and Bob (unchecked).
 - Input: "Zadej tajné číslo z" with value 33.
 - Output: "Vypočítané útočnickovo Z" with value 1903.
 - Table:

Zachyceno X:	2799	[?]
Zachyceno Y:	Y	[?]
 - Buttons: "Zašli 'Z'" (disabled), "Alicí" (disabled), "Bobovi" (disabled).
 - Text: "Tajný klíč s Alicí" (2615, red box) and "Tajný klíč s Bobem" (Výsledek KB, red box).
 - Buttons: "Vypočítej klíč" (disabled), "Potřeba Y" (cyan).
 - Footer: "z = 33 | Z = 1903."
- Bob Panel:**
 - Header: Bob
 - Input: "Zadejte tajné číslo y" with value 98.
 - Output: "Vypočítané veřejné Y" with value 6967.
 - Button: "<- Zašli Alici" (disabled).
 - Section: "Tajný klíč" with "Výsledek K" (red box).
 - Text: "Zaslané druhou stranou: 1903".
 - Button: "Vypočítej klíč" (disabled).
 - Footer: "y = 98 | Y = 6967."

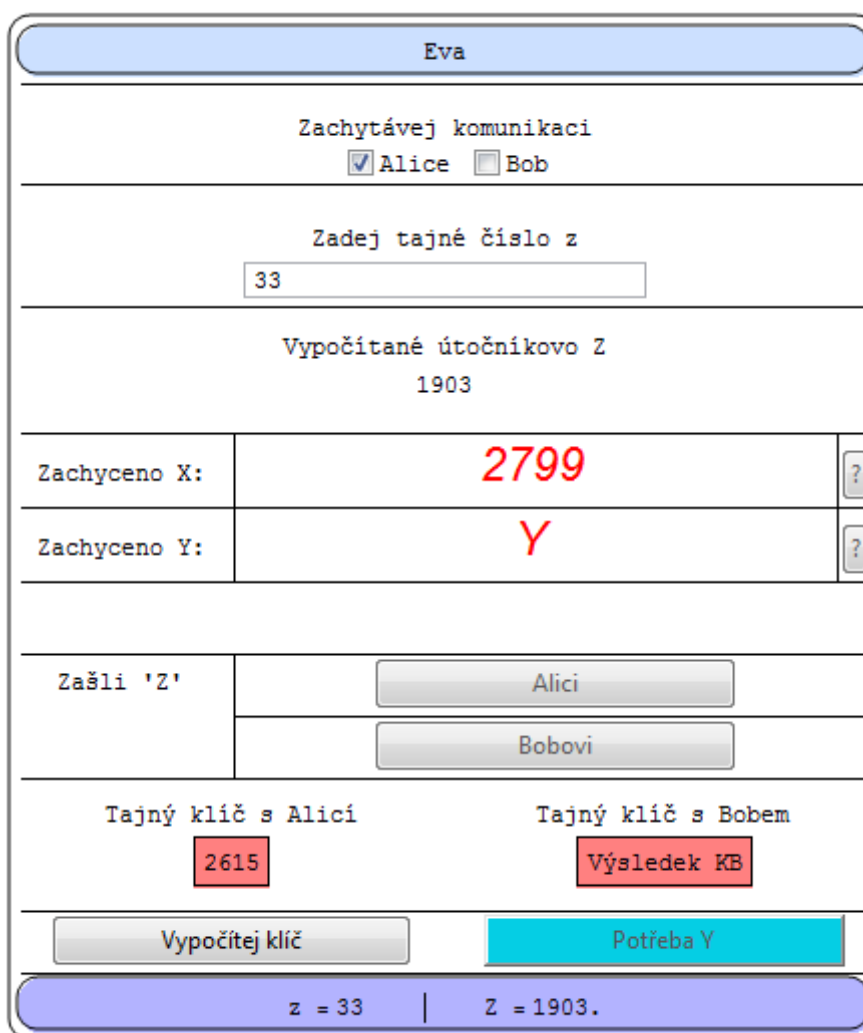
Obrázek 19 Simulace s útokem

Políčko „Zachytávej komunikaci“ značí, zda zachycené číslo dorazí oprávněnému příjemci (Obrázek 20). Zatřené políčko, viz Alice, získá pouze Eva, Bob nikoli, naopak odznačené políčko (Bob) způsobí, že číslo poslané Bobem dojde jak Evě, tak požadovanému příjemci Alici. Druhý případ je pro Evu méně žádoucí, tudíž je lepší, pokud budou políčka zatřené. Implicitně zatřené jsou.



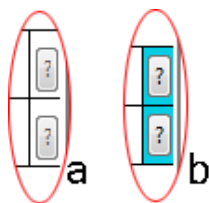
Obrázek 20 Volba k zachyvení komunikace

Obrázek 21 ukazuje červeně zvýrazněná zachycená čísla, tlačítka k rozeslání veřejného Z jak Alici, tak Bobovi a tlačítka k výpočtu klíče. Spodní řádek opět udává veřejné a tajné číslo v jednom, stejně jako v předchozích případech.



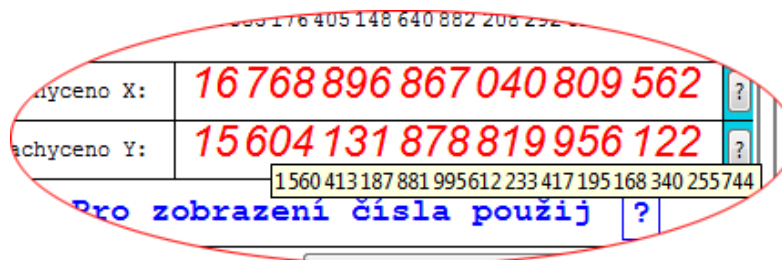
Obrázek 21 Simulace útočníka

Tlačítka v podobě otazníků (Obrázek 22) slouží pro zobrazení celého zachyceného čísla.



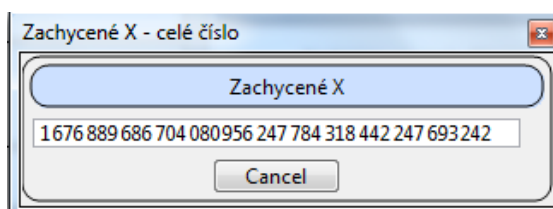
Obrázek 22 Tlačítka pro zobrazení celých čísel a) neaktivní, b) aktivní

Do políčka se pouze vejde dvacetimístné číslo. Pokud bude mít číslo více jak 20 cifer, tlačítka se stanou aktivní a objeví se výrazné modré upozornění (Obrázek 23).



Obrázek 23 Zobrazení u víc jak 20místného čísla

Po stisknutí tlačítka otazníku se objeví menší okno s vypsáním celým číslem (Obrázek 24). Je možné si rovněž zobrazit celé číslo najetím kurzorem nad zkrácené číslo, jak lze vidět na obrázku 23.



Obrázek 24 Okno s vypsáním celým číslem

4.6 Způsob šifrování

V další části si uživatel vybírá, zdali chce šifrovat do souboru, či ze souboru, jaký typ šifry použije a zda se bude šifrovat, či dešifrovat. Na výběr jsou dvě šifry, šifra PlayFair a šifra DES, přičemž šifra DES je převzata ze stránky <http://www.cs.bc.edu/~straubin/crypto2011/381.html>. Jádru této šifry zůstalo stejné, pouze jsou upravené vstupy a výstupy. Na obrázku 25 je vybrána šifra DES s šifrováním a výsledný kryptogram se uloží do souboru zasifrovane.txt.

Uložení do souboru

<input type="checkbox"/>	D:\mathematica\	zasifrovane	.txt
Prohodit			
<input type="checkbox"/>	ze souboru <input type="checkbox"/>		
Vhodný pouze pro text psaný v uvozovkách!!			
<input type="checkbox"/>	D:\mathematica\	Zadejte název souboru	.txt

Způsob šifrování

<input type="radio"/> PlayFair	<input checked="" type="radio"/> Šifrování
<input checked="" type="radio"/> DES	<input type="radio"/> Dešifrování

Obrázek 25 Výběr typu šifry

Tlačítko prohodit umožňuje vyměnit soubory z pozice do souboru na ze souboru a naopak. Zaškrťovací tlačítka vlevo (Obrázek 26), nabízí uživateli změnit adresář vyhledávání a ukládání souborů. Implicitně je nastaven jako adresář umístění spustitelného „.nb“ souboru.



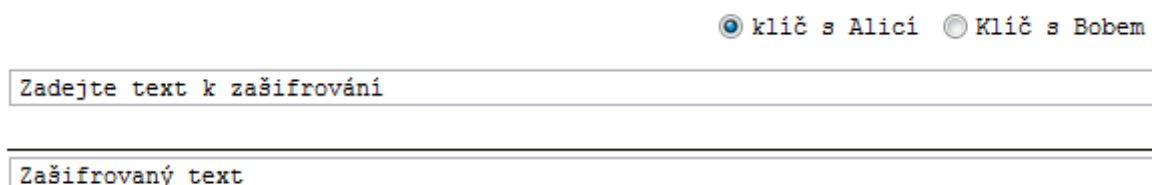
Obrázek 26 Tlačítka pro editaci adresáře

Jak je napsáno na obrázku 25 (Vhodný pouze pro text psaný v uvozovkách!!), je nutné, aby textový obsah psaný v souborech typu .txt byl v uvozovkách. Program by jiný text bez uvozovek nevzal. Jestliže soubor, ze kterého se má číst neexistuje, program nás na to upozorní modrým nápisem v témže záložce. Pokud naopak neexistuje soubor, do kterého chceme výsledný text uložit, program si jej sám vytvoří.

4.7 Zadávání textu

Do horního vstupního pole se zadává text, který bude zašifrován, spodní udává daný kryptogram. Naopak při dešifrování se do dolního vstupního pole zadává zašifrovaný text a

v horním poli se objeví otevřený text. Na obrázku 27 lze nahoře vidět výběr klíče s Alicí nebo Bobem, tato volba se objeví pouze v případě, je-li zvolena simulace s útokem. Pokud je zvolena simulace bez útoku, vygeneruje se pouze jeden klíč a uživatel nemá z čeho vybírat, tím pádem žádná nabídka není.

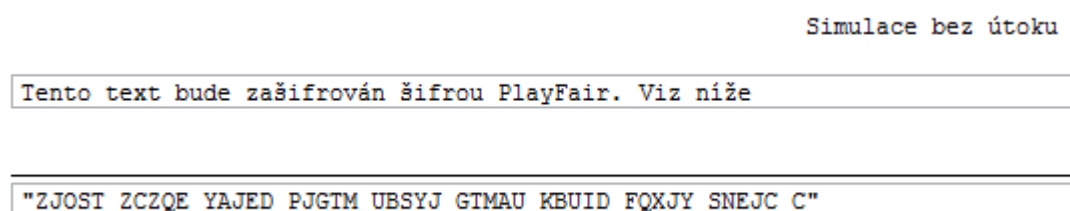


The image shows a web interface for a simulation. At the top right, there are two radio buttons: the first is selected and labeled 'klíč s Alicí', and the second is labeled 'Klíč s Bobem'. Below this is a text input field containing the placeholder text 'Zadejte text k zašifrování'. At the bottom, there is another text input field containing the placeholder text 'Zašifrovaný text'.

Obrázek 27 Textové pole pro text

4.7.1 Šifrování PlayFair

Na obrázku 28 je ukázka kryptogramu zašifrovaného šifrou PlayFair.

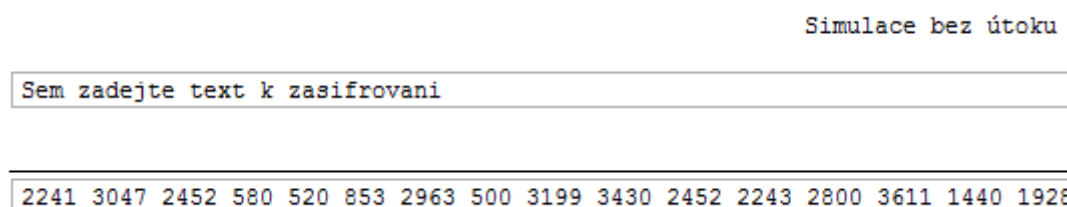


The image shows a web interface for a PlayFair encryption simulation. At the top right, it says 'Simulace bez útoku'. Below this is a text input field containing the text 'Tento text bude zašifrován šifrou PlayFair. Viz níže'. At the bottom, there is a text input field containing the encrypted text '"ZJOST ZCZQE YAJED PJGTM UBSYJ GTMAU KBUID FQXJY SNEJC C"'. The text is displayed in a monospaced font.

Obrázek 28 Šifra PlayFair

4.7.2 Šifrování DES

Ukázka šifry DES, viz obrázek 29.



The image shows a web interface for a DES encryption simulation. At the top right, it says 'Simulace bez útoku'. Below this is a text input field containing the text 'Sem zadejte text k zasifrovani'. At the bottom, there is a text input field containing the encrypted text '2241 3047 2452 580 520 853 2963 500 3199 3430 2452 2243 2800 3611 1440 1928'. The text is displayed in a monospaced font.

Obrázek 29 Šifra DES

4.8 Ostatní záložky

Mezi další záložky, které ještě nebyly zmíněny patří záložka Zašifruj, Reset, Další a Předchozí.

4.8.1 Zašifruj

Tato záložka je dynamicky měnící, je – li v záložce „Způsob šifrování“ zvolena možnost šifrovat, tato záložka má název „Zašifruj“, opačně „Dešifruj“

Po kliknutí na tuto záložku mění otevřený text na zašifrovaný. Funguje jako tlačítko, které po stisku současně kontroluje, zda jsou potvrzené hodnoty v proměnných p a g/q a zda je vygenerován klíč. Samozřejmostí je testování existence souboru, pokud je vybráno šifrování ze souboru.

4.8.2 Reset

Záložka opět funguje jako tlačítko. Po jejím stisknutí se smažou všechny hodnoty proměnných a uživatel může znovu vybírat z prvočísel a generovat nové klíče

4.8.3 Další a předchozí

Posouvání vpřed a vzad v záložkách.

V dolní části okna se nachází měnící se text, podle toho, kam kurzor aktuálně ukazuje. Dávají menší nápovědu, jak záložky fungují a co obsahují.

5 VIZUALIZACE V PROSTŘEDÍ WEBMATHEMATICA

Projekt v tomto prostředí nedisponuje takovými možnostmi jako projekt v Mathematice. Je to dáno omezením WebMathematicy. Ovšem splňuje své účely jako simulace protokolu Diffie – Hellman, kde uživatelé si volí svá tajná a veřejná čísla a proměňují otevřený text v kryptogram.

5.1 Hlavní stránka – index.jsp

Stránka, která se objeví ihned po zadání adresy. Návštěvník má možnost ve výběru dvou typů simulace. Simulace bez útoku a s útokem (Obrázek 30).



Obrázek 30 Hlavní stránka index.jsp

5.2 Simulace bez útoku

Pro tuto simulaci byl vytvořen soubor s názvem protokolDHbez.jsp. I zde si můžou uživatelé zadávat svá čísla ke generování tajných klíčů. Jak v Mathematice, tak i v tomto provedení je možnost s výběru dvou šifer. Tím jsou PlayFair a DES. Na obrázku 31 lze vidět vrchní polovinu stránky, kam do formulářových políček zadává uživatel své hodnoty.

Simulace protokolu bez útoku

Index Simulace bez útoku Simulace s útokem

Zadejte prvočíslo p:

Zadejte prvočíslo q: Musí být prvočíslo

Alice

Tajné číslo x:

Bob

Tajné číslo y: Pouze čísla

☐ PlayFair ☐ DES

☐ Šifrování ☐ Dešifrování

Zadejte text v uvozovkách

VYHODNOTIT

Obrázek 31 WebMathematika - bez útoku

Po vyhodnocení se zkontrolují veškeré údaje ve formulářových políčkách. Na obrázku 31 chybí prvočíslo q a tajné číslo y je rovněž špatně zadáno. Červené vyznačení vedle políčka dává najevo chybu. V tomto případě se zadání nevyhodnocují a čeká se, až bude zadání korektní.

Pomocí označovacích tlačítek se vybírá typ šifry a šifrování či dešifrování (Obrázek 32).

☐ PlayFair ☐ DES

☐ Šifrování ☐ Dešifrování

Obrázek 32 Výběr šifry a způsobu

Bez toho označení program rovněž čeká a neprovádí žádné výpočty.

Na dalším obrázku 33, je znázorněn plnohodnotný výpočet s již korektně zadanými údaji.

Výsledky:

Otevřený text:

Zvolila jsem takovy normalni text

Zašifrovaný text:

402 997 99 2016 1697 1158 1214 2802 1697 2286 2683
586 614 3563 1697 1027 2597 3270 2367 863

Veřejné údaje p a q	
Prvočíslo p	13
Prvočíslo q	11

Tajné údaje	
Tajné x	45
Tajné y	3422

Obrázek 33 První část výpočtu – s útokem

Dle údajů v tabulce lze vidět zadané hodnoty. Bylo zvoleno šifrování a šifra DES. V další části, na obrázku 34 jsou znovu zopakovány zadané údaje Alice i Boba s uvedeným vztahem pro výpočet veřejných X a Y . Vztah pro výpočet klíče je rovněž uveden.

Alice	Bob
Zadané tajné číslo x 45	Zadané tajné číslo y 3422
Vypočítané veřejné X $X = q^x \bmod p$ 8 ----->	Vypočítané veřejné Y $Y = q^y \bmod p$ 4 <-----
Tajný klíč $Y^x \bmod p$ 12	Tajný klíč $X^y \bmod p$ 12
Přijaté Y druhou stranou: 4	Přijaté X druhou stranou: 8

Obrázek 34 Druhá část výpočtu – bez útoku

5.3 Simulace s útokem

Simulace s útokem se nachází v souboru protokolDHs.jsp. Obsahuje formulářová políčka jako v předchozím případě, doplněná o výzvu k zadání tajného čísla „z“ pro útočníka. Tato simulace způsobuje v konečném důsledku vznik dvou klíčů spojující oba účastníky s Evou. V tomto případě má uživatel na výběr, jaký klíč použije k šifrování či dešifrování. Názornější ukázka na obrázku 35,36.

Simulace protokolu s útokem

Simulace bez útoku Simulace s útokem Index

Zadejte prvočíslo p: Zvolte první prvočíslo Musí být prvočíslo

Zadejte prvočíslo q:

Alice Bob

Tajné číslo x: Tajné číslo y: Pouze čísla

Eva

Tajné číslo z: Pouze čísla

☐ PlayFair ☐ DES

☐ Šifrování ☐ Dešifrování

☐ Klíč s Alicí ☐ Klíč s Bobem

Zadejte text v uvozovkách

VYHODNOTIT

Obrázek 35 Simulace s útokem- WebMathematika

Opět jsou ošetřeny vstupy zadané do políček. Z nabídky na obrázku 36 musí být zvolen alespoň jedna možnost pro každý pár. Pokud tak nebude, šifrování/dešifrování se neprovede.



Obrázek 36 Možnosti voleb s útokem

Pokud je vše korektně zadáno, program provede úplný výpočet i s šifrováním. Obrázek 37 a 38 jsou toho důkazem.

Výsledek:

Otevřený text:

Teto text se bude šifrovat

Zašifrovaný text:

QCZTQ CZRQB FYGFY NAPLZ CRAAA A

Veřejné údaje p a q	
Prvočíslo p	101
Prvočíslo q	13

Tajné údaje	
Tajné x	344
Tajné y	555 656
Tajné z	198

Obrázek 37 První část výpočtu - s útokem

Na obrázku 37 lze vidět zadané prvočísla a zvolená tajná čísla x , y a z . Dle těchto údajů se provádí výpočty k nalezení obou klíčů.

Obrázek 38 ukazuje zadaná čísla každého z účastníků společně s vypočítanými veřejnými hodnotami X , Y a Z . Hodnoty X a Y se zašlou druhé straně, Alice posílá Bobovi a obráceně. Ale jelikož zde figuruje Eva, zachytí veřejné údaje obou účastníků a rozešle svoji veřejnou hodnotu. Z došlých údajů se vypočítají dva klíče, které si uživatel, může zvolit.

Alice	Eva	Bob
Zadané tajné číslo x 344	Zadané tajné číslo z 198	Zadané tajné číslo y 555656
Vypočítané veřejné X $X = q^x \bmod p$ 16 ----->	Vypočítané veřejné Z $Z = q^z \bmod p$ 52 <----->	Vypočítané veřejné Y $Y = q^y \bmod p$ 19 <----->
Tajný klíč $Y^x \bmod p$ 58	Tajný klíč KA $X^z \bmod p$ 58	Tajný klíč KB $Y^z \bmod p$ 54
Přijaté Y (Z) druhou stranou: 52	Zachycené X od Alice: 16 Zachycené Y od Boba: 19	Přijaté X (Z) druhou stranou: 52

Obrázek 38 Druhá část výpočtu - s útokem

ZÁVĚR

Cílem práce bylo vysvětlit základní principy protokolu DH, demonstrovat jak funguje, jaké jsou jeho přednosti a nedostatky.

V první kapitole jsou objasněny základní pojmy, se kterými se pracuje v celé bakalářské práci. Ve zkratce je zde popsána kryptografická historie až po současnost. Rovněž je zmíněno rozdělení šifer na symetrické a asymetrické.

V druhé kapitole se uvádí samotný protokol Diffie – Hellman. Oba představitelé jej uvedli ve své práci z roku 1976, kde se zabývali tímto tématem. Protokol patří mezi moderní asymetrickou kryptografii. Šifrování tímto protokolem spočívá ve vygenerování bezpečného klíče pro symetrickou kryptografii.

V další kapitole jsou k vidění útoky na tento šifrovací protokol. Mezi nejznámější patří útok nazývaný Man in the Middle Attack. Jedná se o útočníka, který vystupuje jako druhá komunikující strana, ale jde o nežádoucí článek uprostřed. Útočník musí zprávy překryptovávat, díky odlišným klíčům od obou zúčastněných. Pokud by tak neudělal, druhá strana ihned pozná přítomnost narušitele. K řešení problémů může zčásti pomoci digitální podpis popsany dále.

Praktická část nahlíží na rozbor simulace v programu Mathematica a WebMathematica. Jsou zde popsány kroky, jak by měl uživatel postupovat při simulaci protokolu.

Pouze uživatelé, kteří vlastní software Mathematica si jej můžou v tomto prostředí otestovat. Tato verze poskytuje i uložení kryptogramu do textového souboru. Pro ostatní zájemce slouží WebMathematica, běžící na webu a používající jádro Mathematicy. Tato verze je zájemcům kdykoli k dispozici.

Tato aplikace slouží všem zájemcům o kryptologii a pro studijní účely k předmětu Kryptologie na fakultě aplikované informatiky.

Na přiloženém CD jsou k nahlédnutí .nb soubory z Mathematicy se zdrojovými kódy a soubory .jsp s dalšími potřebnými daty pro webovou prezentaci a pro zobrazení obsahu WebMathematicy.

ZÁVĚR V ANGLIČTINĚ

The aim of the bachelor thesis was to explain the basic principles of the DH protocol, to demonstrate how it works, what are its strengths and weaknesses.

The first chapter shows the explanation of the basic concepts that are used within the whole bachelor thesis. In short, there is a description of the cryptological history from past to the present. The distribution of ciphers to symmetric and asymmetric is also mentioned.

The second chapter contains description of Diffie-Hellman protocol. Both leaders introduced it in their work from 1976, which dealt with this issue. The protocol is the part of the modern asymmetric cryptography. The encryption of this protocol consists in generating a secure key for the symmetric cryptography.

In the next chapter, there are shown the attacks against this encryption protocol. I would like to mention the most famous one, called Man in the Middle Attack. It is a Mallory that appears as the second communicating side, but it is an undesirable element in the middle. The Mallory must re-encrypt messages and it is because of different keys of both participants. If he does not, the other side immediately identifies the presence of an intruder. To solve the problems the digital signature described below may help.

The practical part of the thesis looks at the analysis simulation in Mathematica and WebMathematica programs. There are the steps described in order to show the user how to proceed in the protocol simulation.

Only the users who own software Mathematica can test it in this environment. This version also provides saving of a cryptogram as a text file. The WebMathematica, running at the website and using the Mathematica core, serves to the others interested persons. This version is always available.

This application is for anyone interested in cryptology and also for study purposes at Cryptology Course at the Faculty of Applied Informatics.

On the enclosed CD there are available .nb Mathematica files with the source codes and .jsp files with other necessary data for web presentation and for screening the content of WebMathematica.

SEZNAM POUŽITÉ LITERATURY

- [1] BITTO, Ondřej. Fi.muni [online]. 2003 [cit. 2011-04-25]. Historie kryptologie. Dostupné z WWW: <<http://www.fi.muni.cz/usr/jkucera/pv109/2003/xbitto.htm>>.
- [2] Kryptologie. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, 31. 12. 2008, last modified on 5. 4. 2011 [cit. 2011-04-25]. Dostupné z WWW: <<http://cs.wikipedia.org/wiki/Kryptologie>>.
- [3] Kryptoanal%C3%BDza. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, 5. 6. 2006, last modified on 7. 4. 2011 [cit. 2011-04-25]. Dostupné z WWW: <<http://cs.wikipedia.org/wiki/Kryptoanal%C3%BDza>>.
- [4] Steganografie. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, 29. 12. 2007, last modified on 18. 4. 2011 [cit. 2011-04-25]. Dostupné z WWW: <<http://cs.wikipedia.org/wiki/Steganografie>>.
- [5] Security-portal [online]. 2. Prosinec, 2004 [cit. 2011-04-25]. Praktické základy Kryptologie a Steganografie. Dostupné z WWW: <<http://www.security-portal.cz/clanky/praktické-základy-kryptologie-steganografie>>.
- [6] PIPER, Fred; MURPHY, Sean. Kryptografie : Průvodce pro každého. Praha : Dokořán, 2006. 157 s. ISBN 80-7363-074-5.
- [7] VONDRUŠKA, Pavel. Kryptologie, šifrování a tajná písma. Praha : Albatros, 2006. 340 s. ISBN 80-00-01888-8.
- [8] PINKAVA, Jaroslav. Crypto-world [online]. 1998 [cit. 2011-04-28]. Úvod do kryptologie. Dostupné z WWW: <<http://www.crypto-world.info/pinkava/uvod/uvod98.pdf>>.
- [9] KLÍMA, Vlastimil; ROSA, Tomáš. Kryptologie pro praxi : protokol D-H. Sdělovací technika [online]. 2004, č. 5, [cit. 2011-04-28]. Dostupný z WWW: <http://crypto-world.info/klima/2004/st_2004_05_16_16.pdf>.
- [10] BITTO, Ondřej. Šifrování a biometrika : aneb tajemné bity a dotyky. Kralice na Hané : Computer Media, 2005. 168 s. ISBN 80-86686-48-5.

- [11] PINKAVA, Jaroslav. Crypto-world [online]. 1998 [cit. 2011-04-28]. Základy kryptografie IV. Dostupné z WWW: <<http://www.crypto-world.info/pinkava/uvod/bulletin4.pdf>>.
- [12] PINKAVA, Jaroslav. Crypto-world [online]. 1998 [cit. 2011-04-28]. Základy kryptografie I. Dostupné z WWW: <<http://www.crypto-world.info/pinkava/uvod/bulletin1.pdf>>.
- [13] KLÍMA, Vlastimil; ROSA, Tomáš. Vybrané aspekty moderní kryptoanalýzy. Sdělovací technika [online]. 2003, č. 3, [cit. 2011-04-28]. Dostupný z WWW: <http://crypto.hyperlink.cz/files/ST_2003_03_str_03_07.pdf>.
- [14] KLÍMA, Vlastimil; ROSA, Tomáš. Na kanálu se pracuje aneb O revolučním objevu v kryptoanalýze [online]. 2003 [cit. 2011-04-29]. Dostupné z WWW: <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.85.9913&rep=rep1&type=pdf>>.
- [15] CHURCHHOUSE, Robert. Codes and ciphers : Julius Caesar, the Enigma and the internet. England : Cambridge University Press, 2001. 252 s.
- [16] SINGH, Simon. Kniha kódů a šifer : Utajování od starého Egypta po kvantovou kryptografii. Praha : Dokořár, Argo, 2003. 382 s. ISBN 80-86569-18-7, ISBN 80-7203-499-5.
- [17] WOBST, Reinhard. Cryptology Unlocked. England : Willey, 2001. 540 s.
- [18] YUEN, P. K. Practical Cryptology and Web Security. England : Pearson Education, 2006. 879 s.
- [19] VLČEK, Martin. ElGamal, Diffie-Hellman : Asymetrické šifrování. Praha, 2010. 27 s. Skripta. FJFI ČVUT Praha. Dostupné z WWW: <<http://kmlinux.fjfi.cvut.cz/~balkolub/Vyuka/Vlcek.pdf>>
- [20] Diffie-Hellman protokol s využitím eliptických křivek. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, 30. 10. 2010, last modified on 24. 12. 2010 [cit. 2011-04-28]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Diffie-Hellman_protokol_s_vyu%C5%BEit%C3%ADm_eliptick%C3%BDch_k%C5%99ivek>.

- [21] DUŠEK, Miloslav. Kvantová kryptografie: aneb šifrování pomocí fotonů. Olomouc, 2004. 126 s. Skripta. Universita Palackého, Olomouc. Dostupné z WWW: <<http://kaleidoskop.upol.cz/old/kal2004/Dusek/Dusek.pdf>>
- [22] KLÍMA, Vlastimil; ROSA, Tomáš. Kryptologie pro praxi. Sdělovací technika : symetrická a asymetrická kryptografie [online]. 2003, č. 7, [cit. 2011-04-28]. Dostupný z WWW: <http://crypto-world.info/klima/2003/st_2003_07_16_16.pdf>.
- [23] ZLATOŠ, Pavol. Lineárna algebra a geometria : Úvod do teórie grúp. Bratislava, 2006. 663 s. Skripta. FMPH Bratislava. Dostupné z WWW: <<http://thales.doa.fmph.uniba.sk/zlatos/la/LAG.pdf>>.
- [24] Mathematica [online]. 2011 [cit. 2011-04-29]. Wolfram Mathematica. Dostupné z WWW: <http://www.mathematica.cz/produkty.php?p_mathematica>.
- [25] Reference.wolfram [online]. 2011 [cit. 2011-04-29]. Wolfram Mathematica. Dostupné z WWW: <<http://reference.wolfram.com/mathematica/guide/Mathematica.html>>.
- [26] Wolfram [online]. 2011 [cit. 2011-04-29]. Solutions for Higher Education. Dostupné z WWW: <<http://www.wolfram.com/solutions/education/higher-education/>>.
- [27] Wolfram [online]. 2011 [cit. 2011-04-29]. What is webMathematica. Dostupné z WWW: <<http://www.wolfram.com/products/webmathematica/whatis.html>>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DH Diffie - Hellman

RSA Rivest, Shamir, Adleman

DES Data Encryption Standard

SEZNAM OBRÁZKŮ

Obrázek 1 Základní symetrické šifrovací schéma	11
Obrázek 2 Schéma asymetrického šifrování.....	14
Obrázek 3 Schéma protokolu Diffie Hellman	18
Obrázek 4 Schéma útoku man in the middle.....	24
Obrázek 5 Ukázka s překryptování útočníka	26
Obrázek 6 Bez překryptování útočníka	26
Obrázek 7 Digitální podpis	27
Obrázek 8 Prostředí pro uživatele.....	32
Obrázek 9 Generování prvočísel.....	33
Obrázek 10 Tlačítka k volbě vhodného prvočísla	33
Obrázek 11 Tlačítko pro vyvolání generátoru grup.....	33
Obrázek 12 Výpis všech generátoru zvoleného prvočísla	34
Obrázek 13 Potvrzení zvolených prvočísel.....	35
Obrázek 14 Volba proměnných k výpočtu	35
Obrázek 15 Volba simulace.....	35
Obrázek 16 Generace čísel bez útoku	36
Obrázek 17 Zadané tajné číslo prvního účastníka.....	36
Obrázek 18 Tajné a veřejné číslo	37
Obrázek 19 Simulace s útokem	37
Obrázek 20 Volba k zachyvení komunikace.....	38
Obrázek 21 Simulace útočníka.....	38
Obrázek 22 Tlačítka pro zobrazení celých čísel a) neaktivní, b) aktivní.....	39
Obrázek 23 Zobrazení u víc jak 20místného čísla	39
Obrázek 24 Okno s vypsáním celým číslem.....	39
Obrázek 25 Výběr typu šifry	40
Obrázek 26 Tlačítka pro editaci adresáře.....	40
Obrázek 27 Textové pole pro text	41
Obrázek 28 Šifra PlayFair	41
Obrázek 29 Šifra DES	41
Obrázek 30 Hlavní stránka index.jsp	43
Obrázek 31 WebMathematika - bez útoku	44
Obrázek 32 Výběr šifry a způsobu	44

Obrázek 33 První část výpočtu – s útokem.....	45
Obrázek 34 Druhá část výpočtu – bez útoku	45
Obrázek 35 Simulace s útokem- WebMathematika.....	46
Obrázek 36 Možnosti voleb s útokem	47
Obrázek 37 První část výpočtu - s útokem.....	47
Obrázek 38 Druhá část výpočtu - s útokem	48

SEZNAM TABULEK

Tabulka 1 Princip Diffie Hellman protokolu	18
Tabulka 2 Srovnání normální a modulární aritmetiky.....	19

SEZNAM PŘÍLOH

PŘÍLOHA P I: Zdrojový kód – Mathematica

PŘÍLOHA P II: Zdrojové kódy – WebMathematica