Bankovní institut vysoká škola, a.s.

Katedra matematiky, statistiky a informačních technologií

Kryptografie v ICT

Bakalářská práce

Autor: **Michal Novák**

Informační technologie, MPIS

Vedoucí práce: **Ing. Vladimír Beneš**

Strakonice **Leden 2012**

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a v seznamu uvedl veškerou použitou literaturu.

Svým podpisem stvrzuji, že odevzdaná elektronická podoba práce je identická s její tištěnou verzí, a jsem seznámen se skutečností, že se práce bude archivovat v knihovně BIVŠ a dále bude zpřístupněna třetím osobám prostřednictvím interní databáze elektronických vysokoškolských prací.

V Strakonicích dne 11. ledna 2012 Michal Novák

Poděkování:

Na tomto místě bych rád poděkoval svému vedoucímu bakalářské práce, Ing. Vladimíru Benešovi za pomoc, cenné rady a veškerý čas, který mi věnoval.

Anotace

Bakalářská práce se zabývá základními principy kryptografie a definuje základní pojmy. Rozsahem zasahuje na začátky vzniku až do dnešních moderních trendů. Zabývá se hlavně kryptografií v ICT a vybraných aplikací, s kterými se můžeme v tomto oboru setkat.

Klíčová slova: kryptografie, klíč, algoritmus, šifra, autorizace, protokol

Annotation

The bachelor work deals with basic principles of cryptography and defines basic terms of it. It includes the development of cryptography from beginnings to modern trends. The main topic is cryptography in ICT and in selected applications that we can find in this discipline.

Keywords: cryptography, key, algorithm, code, authorization, protocol

Obsah

1. Úvod

V posledních letech, hlavně s příchodem internetu a potřeby stálého zlepšování produktů a služeb, začal velký rozmach informačních technologií. S příchodem informačních technologií, které nám pomáhají a ulehčují práci, přichází také odvrácená strana tohoto odvětví a to strach z odcizení a neoprávněnému použití informací. Ke zneužívání informačních technologií většinou dochází v konkurenčním boji nebo ve snaze někoho poškodit.

Lidé, kteří pracují v oboru IT či alespoň trochu se o IT zajímají, určitě vědí o možné hrozbě odcizení dat. Tento problém pořád narůstá, hlavně od doby, kdy se rozšířil internet, který pospojoval většinu informačního světa, do jednoho velkého celku. Bohužel s rozmachem tohoto oboru se objevila již zmíněná odvrácená strana, kterou představují většinou lidé, kteří chtějí odcizením dat dokázat svoje nadání či získat výhodu pro svoji společnost a tím i lepší postavení v dnešním konkurenčním boji. Objevila se tedy velká potřeba chránit svoje osobní informace, jak před cizím zrakem, tak i před neoprávněným používáním či odcizením těchto informací. Tento problém v oblasti informačních technologií se snaží řešit obor Kryptografie. Kryptografie se rozvíjí od doby, kdy člověk dostal potřebu chránit nějakou informaci, před cizími zraky a považoval danou informaci za soukromou. V dnešní době je již kryptografie skrytá a implementována do většiny programů či služeb, aniž by o tom neznalý člověk tohoto oboru věděl. V dnešní době se s kryptografií a způsobem jejího použití na ochranu svého soukromí setkáváme v mnoha různých situacích každodenního světa, např. při komunikaci se svým účtem přes internet komunikujeme přes šifrované spojení, které ostatním lidem znemožní, nebo hodně ztíží dané informace získat. Obor kryptografie se nenachází, ale jen v oboru bankovnictví, ale můžeme se s ním setkat také např. při ověřování totožnosti, či posílání zpráv nebo souborů, u kterých chceme zajistit ochranu před neoprávněným použitím.

2. Historie kryptografie

Věda o kryptografii se vyvíjela po celá století a hlavně ve spojení se skrýváním strategických vojenských operací, politických událostí, ale i např. přípravy atentátů atd. Samozřejmě s rozvojem kryptografie, která se zabývá zašifrováním tajných informací, se stále více začala také vyvíjet kryptoanalýza, která se zabývá dešifrování tajných informací a prolomením šifer. S postupně lepší a vyvinutější kryptoanalýzou se samozřejmě musí dále vyvíjet a stávat složitější i kryptografie, aby byla schopná zachovat danou informaci tajnou před nežádoucím prolomením šifry.

První zaznamenaná zmínka použití kryptografie byla popsána řeckým historikem Plutarchem v 5 století př.n.l., kde popisuje transpoziční šifrovací systém Scytale. Scytale začali používat spartští vojevůdci a tím získali výhodu tajných zpráv oproti svým protivníkům. Tento transpoziční šifrovací systém je velmi jednoduchý a je založen, jak už samotný název systému uvádí, na transpozičním řešení zprávy, které představuje s přeházením jednotlivých symbolů zprávy. Systém Scytale je založen na pásce pergamenového papíru a dvou dřevěných holích stejného průměru. Na první hůl navine odesílatel pásku pergamenového papíru ze shora dolů a napíše tajnou informaci. Po odmotání pásky je zpráva ve formě nesrozumitelného zpřeházení symbolů. Pro dešifrování zprávy musíme pásek namotat opět na hůl stejného průměru, kde se nám po navinutí objeví tajná informace. Navinutí pásky na jiný průměr hole nám opět dá nesrozumitelný text, proto jen osoba se správným průměrem hole dokáže rozluštit zašifrovanou zprávu. [1]

Další známou šifrou, která byla používaná v historii je Ceasarova šifra. Ceasarova, protože byla používána právě nejznámějším římským vojevůdcem Juliem Ceasarem pro šifrování komunikace mezi jeho legiemi. Caesarova šifra je substituční systém, tedy systém kdy je každý symbol zprávy nahrazen za jiný. Konkrétně používaná šifra Juliem Ceasarem znamenala posunutí každého symbolu o 3 znaky v abecedě. Ale za Ceaserovu šifru označujeme také jakýkoliv jiný prostý posun v abecedním seznamu o konstantní velikosti. Pro dešifrování takovéto zprávy musí příjemce znát, že se jedná o tento kryptografický systém a hodnotu, o kterou posouváme abecední seznam. [2]

Roku 1499 n.l. byla napsána první kniha o kryptografii s názvem Steganographia. Autorem byl Johannes Trittheim, teoretik kryptografie a steganografie. Téměř po vydání se kniha dostala na černou listinu zakázaných knih, protože zveřejňovala příliš mnoho tajných informací, které znepokojovaly tehdejší panovnické rody. Stenografická šifra je založena na substitučním systému, kdy nahrazujeme každé písmeno abecedního seznamu daným slovem z předem napsané tabulky. Trittheim dále doporučoval používat takzvané „klamače“, který znesnadňovali rozluštit šifru díky vložením nadbytečných znaků do textu, které stěžovaly rozluštění šifry. [3]

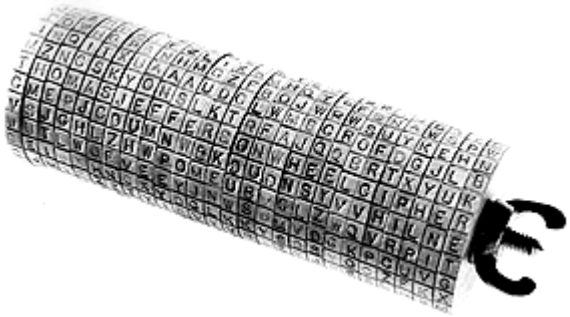
Jako poslední šifru používanou v naší historii bych rád uvedl šifru, jejímž autorem je Armand Jean du Plessis, známý spíše jako kardinál Richelieu, který byl prvním ministrem Ludvíka XIII. Kardinál Richelieu údajně vytvořil šifrovací oddělení, které mělo za úkol šifrovat zprávy, ve kterých se jednalo o královský trůn, komunikace s nepřáteli jeho panovníka a další intriky. Šifra používaná kardinálem Richelieu je jednoduchý transpoziční systém, založený na přeskupení písmen ve větě na základě domluveného hesla stejné délky. [4]

2.1. Šifrovací stroje

S přibývající potřebou používání kryptografie na ochranu citlivých informací se začaly vyvíjet mechanické či elektrické šifrovací a dešifrovací stroje, které nám výrazně usnadní práci se šifrováním a dešifrováním těchto informací.

Jedním z prvních těchto strojů, byl Jeffersonův válec, který sestrojil americký ministr pro zahraniční věci Thomas Jefferson v roce 1790. Tento válec se skládá z 26 stejných kol, které jsou na stejné ose a tím představují válec, jak je vidět na obr. 1. Na obvodu jednotlivých kol jsou poskládané všechny znaky abecedy, ale v rozházeném pořadí. Při šifrování se kola otáčejí tak, abychom měli na jednom řádku poskládanou požadovanou citlivou informaci, ale za šifrovaný text této informace se považuje řádek následující a nebo jiný vybraný. Jednotlivá kola jsou ještě samostatně číslována, čímž při s přeházením jednotlivých kol, dosáhneme další stupeň zašifrování.

Obrázek 1 - Jeffersonův válec



Zdroj: [5]

Za první světové války nastal další výrazný vývoj v oboru kryptografie. Jedním ze zásadních objevů této doby byl polyalfabetický šifrovací stroj, který sestrojil Gilbert S. Vernam. Do jeho stroje se vkládaly dvě děrné pásky. Jedna s otevřeným textem a druhá s náhodným klíčem. Stroj provedl za pomoci sčítání bitů obou pásek otevřený text do zašifrované zprávy. Používaný systém je tak bezpečný, že ho můžeme bez obav nějaké hrozby používat i v dnešní době. [5]

Nejznámější z elektromechanických rotorových strojů je Enigma, kterou vidíme na obr. 2. Enigma je šifrovací stroj, který byl původně vyvinut k civilním účelům a v roce 1918 si ho nechal patentovat německý inženýr Arthur Scherbius. Enigma byla využívaná mnoha firmami po celém světě, ale opravdu známou se stala až při častém používání v německé armádě. Enigma je složena z mnoha důmyslných součástí, které dohromady dávají působivý a složitý stroj. Při rozebrání na jednotlivé části je ale princip enigmy poměrně jednoduchý. Enigma je tvořena ze 3 hlavních částí a to klávesnice, šifrovacího mechanismu a výstupní jednotky, která je tvořena žárovkami, později tiskem. Nejdůležitější částí je šifrovací mechanismus, který se skládá se vzájemně propojených rotorů a jejich vzájemného otáčení po stisku kláves. K šifrování docházelo tak, že v případě zmáčknutí daného písmena stroje na klávesnice, začal vést proud mezi jednotlivými kontakty rotoru, až rozsvítil žárovku, která prosvítila již zašifrované písmeno.

Obrázek 2 - Enigma

Zdroj: [6]

Druhy enigmy

Enigma, jak šel čas, procházela různými druhy vylepšení a to od jejího stvoření a civilního používání, až po mnohem složitější typy, používané během druhé světové války. Druhy enigmy se od sebe lišily použitím více rotorů, kterým se stávala enigma více bezpečnou. Dále druhem výstupu šifry z enigmy a v neposlední řadě čím dál více přidávanými mechanismy ke zhoršení možného rozluštění šifry, např. přidání rozvodné desky, která umožňovala prohození dvou kláves na klávesnici. [6]

3. Úvod do kryptografie

Slovo kryptografie pochází ze dvou řeckých slov kryptós (skryté) a gráphein (psát). Kryptografie je ale pouze jedna ze 3 velkých oblastí kryptologie, která je odvozena od řeckého logos (věda). Druhá velká oblast kryptologie je kryptoanalýza, která se nezabývá šifrováním jako kryptografie, ale právě rozluštěním, dešifrováním zašifrovaného textu. A poslední velká oblast zabývající se skrýváním informací se nazývá steganografie.

3.1. Základní pojmy

Kryptologie - věda zabývající se šifrováním, dešifrováním a skrýváním informací, zahrnuje v sobě všechny tři velké oblasti (kryptografii, kryptoanalýzu a steganografii).

Kryptografie - cílem této oblasti kryptologie je šifrování potřebných tajných informací a navrhování šifrovacích systémů, které dokážou zamezit rozluštění přenášené informace neoprávněnou osobou.

Kryptoanalýza - je oblast kryptologie, která zkoumá metody a luštění šifrovacích systémů. Jedná se o opak kryptografie a jejím hlavním cílem je rozluštit zašifrovaný text a získat z něj požadovanou přenášenou informaci.

Steganografie - je poslední z hlavních oblastí kryptologie a jejím cílem je zamezit zjištění neoprávněnou osobou, že daná zpráva vůbec existuje. Použití například neviditelných inkoustů atd. Použitím s kryptografií vytvoříme informaci ještě více chráněnou.

Otevřený text – původní informace, která je všeobecně srozumitelná, kterou chceme šifrovat, skrýt.

Šifrovaný text – je otevřený text zašifrovaný do podoby, která je srozumitelná jen oprávněné osobě.

Šifrování - cíl transformace je zašifrovat původní informaci do podoby, kdy potencionální útočník není schopen získat z posílané zprávy původní informaci a zároveň požadované osoby byli schopné přenášenou informaci získat. Výsledek šifrování je šifrovaný text.

Dešifrování – opak šifrování, kdy se snažíme díky známé metodě zašifrování získat z šifrovaných dat původní informaci, kterou přenášíme.

Klíč – jedná se o parametr šifrovacího algoritmu, bez kterého není možné původní informaci zašifrovat a naopak také získat z přenášené zprávy.

Šifrovací a dešifrovací algoritmus – šifrovacím algoritmem se rozumí přesný postup zašifrování, zapouzdření informace, kterou chceme chránit před cizími zraky. Dešifrovací algoritmus je přesný postup získání informace ze zašifrované zprávy.

Heslo – jeden z možných parametrů při autentizace, rozpoznání oprávněného uživatele. Heslo by nemělo být známé někomu jinému.

Symetrická šifra – je šifrovací technika, u které používáme na šifrování, ale i dešifrování zašifrované zprávy stejný klíč. Odesílatel i příjemce dané zprávy vlastní stejný tajný klíč, kterým je zpráva zašifrována a kterým může adresát zprávu dešifrovat.

Asymetrická šifra – je technika šifrování, u které odesílatel používá veřejný klíč pro zašifrování tajné informace a příjemce svůj soukromý klíč pro dešifrování zprávy.

Bloková šifra – jedná se o kryptografický algoritmus, který otevřený text šifruje po blocích různé délky bitů

Proudová (streamová) šifra – kryptografický algoritmus, při kterém jsou šifrovány jednotlivé bity postupně, bit po bitu.

Veřejný klíč – tento klíč používáme při zašifrování zprávy, je známý všem, ale nedokáže zprávu opět dešifrovat.

Soukromý klíč – je jen náš soukromý klíč vygenerovaný na našem počítači, veřejnosti utajený, používáme ho na dešifrování zprávy, která byla zašifrována klíčem veřejným. [7]

3.2. Základní kryptografické metody

Šifrování je přetváření otevřeného nechráněného textu do podoby tajného, jinými osobami nepřeložitelného řetězce znaků za pomocí různých kryptografických metod, ač historie kryptografie sahá velmi daleko do historie, velký rozvoj silných kryptografických algoritmů

nastává až s rozvojem matematiky. Mezi nejznámější algoritmy dneška patří například RSA, DES, SHA a další.

Základní kryptografické metody jsou:

- symetrické šifrování

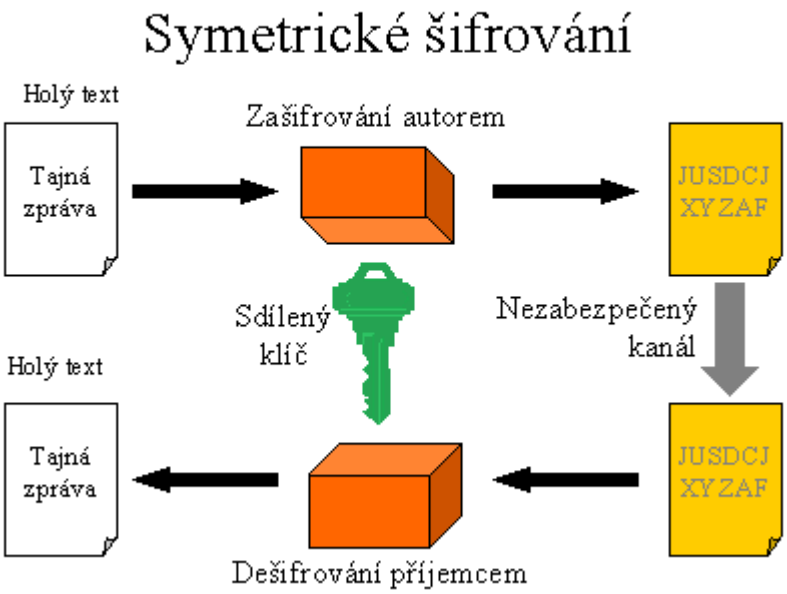
- asymetrické šifrování

- hashovací funkce

3.2.1. Symetrické šifrování

Symetrické šifrování je kryptografická metoda, která používá oproti ostatním metodám právě jeden stejný klíč pro zašifrování i dešifrování zprávy. Princip je velice jednoduchý a spočívá v tom, že odesílatel zašifruje otevřený text do zprávy pomocí stejného klíče, jako pak následně příjemce rozšifruje zprávu do otevřeného textu. První z nejznámějších algoritmů symetrického šifrování je DES (Data Encryption Standard), která byla používaná od roku 1976, ale bohužel tento algoritmus vydržel neprolomen pouze 17 let. Dodnes se ale používají navazující algoritmy a to 3-DES a IDEA.

Obrázek 3 - Symetrické šifrování



Zdroj: [21]

Výhody a nevýhody:

+ malá výpočetní náročnost

- šíření klíče (musíme dopravit příjemci nejen zašifrovanou zprávu, ale i klíč, kterým byla zpráva zašifrována)

Mezi nejzákladnější šifrovací metody symetrického šifrování se považuje metoda substitučního a transpozičního šifrování, které byly používány ve své základní podobě hlavně v historii a dnes se již považují za jednoduché a snadno prolomitelné.

3.2.1.1. Transpoziční šifrování

Tato metoda, stejně jako metoda substitučního šifrování, je sama o sobě velice jednoduchá a dá se předpokládat, že nebude těžké ji rozluštit. Principem tohoto šifrování je použitý otevřený text zašifrovat do podoby, kdy na zašifrování nepoužijeme jiný znak, ale pouze zpřeházíme za pomocí nějakého algoritmu pořadí znaků použitých v otevřeném textu tak, aby neoprávněné osobě nepředával text skrytou informaci. Tato metoda sama o sobě není

v dnešní době bezpečná a používaná byla především v historii. Čím kratší je otevřený text, který budeme šifrovat, tím bude šifra méně bezpečná, z důvodu použití méně znaků, z kterých méně kombinacemi můžeme poskládat správný původní šifrovaný text. Transpoziční šifrování je použito například v algoritmu dvojité transpozice, šifrovací kříže či Rail-Fence šifry. [9]

Výhody a nevýhody:

+ jednoduché šifrování

- snadno prolomitelné

- skoro nepoužitelné pro krátké zprávy

Principy základních transpozičních šifer

Sloupcová šifra

U sloupcové šifry zapisujeme text po řádcích o délce velikosti klíče a text k zašifrování čteme postupně po daných sloupcích podle klíče. Sloupcovou šifru dělíme na souměrnou a nesouměrnou. Souměrnou šifru doplníme náhodně zvolenými znaky, aby nezůstaly volná místa v mřížce, ale u nesouměrné šifry můžeme nechat volná místa, protože budeme číst nesouměrně ze sloupců.

Příklad

Zašifrujte otevřený text ZAHAJTE UTOKY pomocí sloupcové šifry souměrně a nesouměrně, obojí pomocí klíče „šifra“.

Řešení souměrné

Tabulka 1 - Sloupcová šifra - souměrná

Klíč	S	I	F	R	A
Váhy	5	3	2	4	1
Řádek 1	Z	A	H	A	J
Řádek 2	T	E	U	T	O
Řádek 3	K	Y	Q	S	A

Zdroj: vlastní úprava

Šifru rozdělíme na bloky, abychom předešli chybám, výsledný šifrovaný text pak je: JOA HUQ AEY ATS ZTK

Řešení nesouměrné

Tabulka 2 - Sloupcová šifra - nesouměrná

Klíč	S	I	F	R	A
Váhy	5	3	2	4	1
Řádek 1	Z	A	H	A	J
Řádek 2	T	E	U	T	O
Řádek 3	K	Y			

Zdroj: vlastní úprava

Výsledný šifrovaný text: JOH UAE YAT ZTK

Route šifra

U této šifry zapíšeme otevřený text do mřížky postupně po sloupcích a následně si určíme cestu zašifrování algoritmu, například čtení po řádcích nebo spirály z venkovního obvodu ke středu, u této šifry není stanoven přesně daný algoritmus, ale k zašifrování si vybereme jeden z možných algoritmů, jednu z možných cest přečtení textu.

Příklad

Zadání : Zašifrujte otevřený text ZAHAJTE UTOKY pomocí Route šifry směrem do středu, točící se doprava, začínající v pravém horním rohu.

Řešení:

Tabulka 3 - Route šifra

Z	A	E	O
A	J	U	K
H	T	T	Y

Zdroj: vlastní úprava

Výsledný šifrovaný text: OKY TTH AZA EUJ

Rail Fence šifra

Rail Fence šifra dostala jméno podle způsobu šifrování u této šifry. Základem této šifry je, rozložení otevřeného textu do předem určeného počtu kolejí, proto Rail Fence šifra. Principem této šifry je rozepsání otevřeného textu postupně po znacích na koleje od shora dolů až dojdeme na poslední kolej a tam zase nahoru. Výsledný šifrovaný text se přečte postupně z kolejí od první k poslední.

Příklad

Zadání: Zašifrujte otevřený text ZAHAJTE UTOKY pomocí 3 kolejí Rail Fence šifry

Řešení:

Tabulka 4 - Rail Fence šifra

Kolej 1	Z				J				T			
Kolej 2		A		A		T		U		O		Y
Kolej 3			H				E				K	

Zdroj: vlastní úprava

Výsledný šifrovací text: ZJT AAT UOY HEK

Dvojitá transpozice

Tato šifra je vylepšení sloupcové šifry, která nám šifruje oproti dvojité transpozici pouze jednou. Dvojitá transpozice nám zašifruje text stejně, jako u sloupcové šifry, ale zakódovaný text se šifruje ještě jednou za pomocí dalšího klíče, dá se použít i ten samý klíč jako k prvnímu šifrování. Dvojitá transpozice našla největší uplatnění během první světové války, kdy ji používala německá armáda.

Příklad

Zadání: Zašifrujte otevřený text ZAHAJTE UTOKY pomocí dvojité transpozice pomocí klíčů „šifra“ a „heslo“.

Tabulka 5 - Dvojitá transpozice – první část

Klíč 1	S	I	F	R	A
Váhy	5	3	2	4	1
Řádek 1	Z	A	H	A	J
Řádek 2	T	E	U	T	O
Řádek 3	K	Y			

Zdroj: vlastní úprava

Výsledný text po prvním šifrování zní: JOH UAE YAT ZTK

Tabulka 6 - Dvojitá transpozice - druhá část

Klíč 2	H	E	S	L	O
Váhy	2	1	5	3	4
Řádek 1	Z	A	H	A	J
Řádek 2	T	E	U	T	O
Řádek 3	K	Y			

Zdroj: vlastní úprava

Konečný výsledný text po zašifrování druhým klíčem: AEY ZTK ATJ OHU[9]

3.2.1.2. Substituční šifrování

Metoda substitučního šifrování je také, jako metoda transpoziční základem pro používané složitější šifry. Jedná se spíše o dělení šifer na základě použitého způsobu šifrování. Za substituční šifrování považujeme šifrování, kdy jak už samotný název daného šifrování naznačuje, budeme každý znak zprávy substitucí neboli nahrazováním měnit za jiný. Při následném dešifrování opět nahrazený znak vyměníme za původní podle určitého algoritmu. Substituční šifra je více bezpečná a to hlavně díky neomezení se na znaky uvedené v otevřeném textu, ale na znaky libovolné. Substituční šifrování stejně jako transpoziční nám zasahuje do velmi daleké historie, kde ale nebyly vyvinuty tak složité algoritmy jako jsou dnes používané a to hlavně díky málo vyvinutým matematickým vědám. Tzv. substituční šifrování nám, ale například ovlivňovalo i 2. světovou válku, kdy bylo implementováno do nejznámějšího kryptografického stroje, kterým byla enigma, která za pomocí klávesnice určovala znak, který chceme šifrovat a přes šifrovací mechanismus stroje se rozsvítila na pozadí určitého znaku na enigmě žárovka, která nám určila podobu zašifrovaného znaku. [8]

Výhody a nevýhody:

\+ možnost využití znaků, které neobsahuje otevřený text

\- v jednoduchých algoritmech má určitý znak ve zprávě pouze jednu určitou podobu

Druhy substitučních šifer:

- **Monoalfabetická substituční šifra** – otevřený text se zašifruje jen jednou pomocí jedné šifrovací abecedy, z toho vyplývá, že právě jednomu znaku odpovídá právě jeden znak z šifrovací abecedy.
- **Polyalfabetická substituční šifra** – každé písmeno se šifruje odlišnou šifrovací abecedou podle daného klíče.
- **Homofonní substituční šifra** – vybraná písmena z otevřeného textu (nejčastěji ty nejvíce používaná), se dají nahradit více než jedním znakem.
- **Bigramová substituční šifra –** určitý počet znaků z otevřeného textu se nahrazuje jinou skupinou znaků šifrovaného textu o stejném počtu. (Bigram = 2 znaky, trigram = 3 znaky, atd.)

- **Digrafická substituční šifra –** každý znak otevřeného textu je nahrazen 2 znaky zašifrovaného textu.

Principy základních substitučních šifer

Převrácená abeceda

Otevřený text se šifruje pomocí převrácení znaků u šifrované abecedy, pak písmeno A odpovídá u šifrované abecedy písmenu Z atd.

Příklad

Zadání: Zašifrujte otevřený text ZAHAJTE UTOKY pomocí substituční šifry převrácená abeceda.

Řešení:

Tabulka 7 - Převrácená abeceda

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Zdroj: vlastní úprava

Výsledný šifrovaný text: AZS ZQG VFG LPB

Caesarova šifra

Otevřený text se šifruje za pomocí posunuté šifrovací abecedy o x znaků. Za klíč k Césarově šifře můžeme považovat příslušný počet posunutí oproti klasické abecedě.

Příklad

Zadání: Zašifrujte otevřený text ZAHAJTE UTOKY pomocí Césarovi šifry o klíči A=E.

Řešení:

Pro naše zadání sestavíme šifrovací abecedu tak, že nám bude začínat písmenem E, které bude nahrazovat písmeno A.

Tabulka 8 - Caesarova šifra

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Zdroj: vlastní úprava

Výsledný šifrovaný text: DEL ENX IYX SOC

Posuvná substituční šifra s klíčem

Otevřený text se zašifruje pomocí vytvořené šifrovací abecedy, která bude začínat šifrovacím slovem, které nesmí obsahovat jeden znak vícekrát a dále bude pokračovat normální abecedou s vynechanými použitými znaky v klíči. Čím delší bude náš klíč, tím více proházená bude i šifrovací abeceda. [10]

Příklad

Zadání: Zašifrujte otevřený text ZAHAJTE UTOKY pomocí posuvné substituční šifry s klíčem „šifra“.

Řešení:

Sestavíme šifrovací abecedu tak, aby začínala naším šifrovacím klíčem „šifra“ a dále byla klasická abeceda s vynechanými znaky použitými v našem klíči.

Tabulka 9 - Posuvná substituční šifra s klíčem

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	I	F	R	A	B	C	D	E	G	H	J	K	L	M	N	O	P	Q	T	U	V	W	X	Y	Z

Zdroj: vlastní úprava

Výsledný šifrovaný text: ZSD SGT AUT MHY

Viegenerova substituční šifra

Viegenerova šifra patří do kategorie polyalfabetické substituční šifry a používá k zašifrování několika různých posunutí abecedy. Princip Viegenerovy šifry spočívá v tom, že nejvrchnější řádek Viegenerova čtverce obsahuje otevřený text a každé písmeno pak můžeme šifrovat kteroukoliv z 26 abeced. Pro zajištění větší bezpečnosti zašifrujeme každé písmeno pomocí jiné abecedy.

Obrázek 4 - Viegenerův čtverec

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Zdroj: [11]

Příklad:

Zadání: Pomocí Viegenerovy šifry zašifrujte otevřený text ZAHAJTE UTOKY, pomocí klíče „šifra“.

Řešení:

Tabulka 10 - Viegenerova šifra

S	I	F	R	A	S	I	F	R	A	S	I
Z	A	H	A	J	T	E	U	T	O	K	Y
R	I	M	R	J	L	M	Z	K	O	C	G

Zdroj: vlastní úprava

Výsledný šifrovaný text: RIM RJL MZK OCG [8]

3.2.1.3. Hybridní šifrování

Je metoda šifrování, při níž spojujeme více druhů šifrování do jednoho více bezpečného. Hybridní šifrování je založeno na principu zkombinování dvou šifrování za účelem získání bezpečnější šifry.

Výhody a nevýhody:

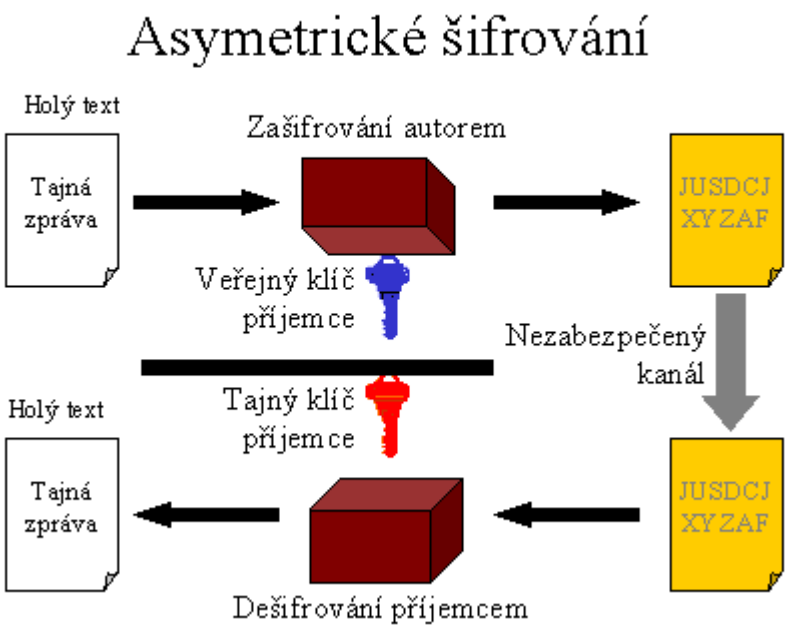
+ bezpečnější než jednotlivá šifrování transpoziční a substituční samostatně

3.2.2. Asymetrické šifrování

Asymterické šifrování se odlišuje od symetrického právě v existenci více než jednoho klíče a to rozdílného k zašifrování a následném dešifrování zprávy. Tato metoda využívá dva druhy klíčů a to klíč veřejný, který používáme pro zašifrování daného textu a soukromý klíč, který je generován až u vlastníka a je známý jen jemu. Veřejný klíč je všeobecně známým všem, ale k rozluštění zprávy u správného příjemce dojde až v moment použití správného soukromého klíče, který správně doplní dvojici veřejný a soukromý klíč. Jeden z nejznámějších asymetrických algoritmů je RSA (River-Shamir-Adelman) algoritmus. Který je založen na vygenerování vysokého prvočísla jako veřejného klíče, kde dál za pomocí různých složitých

matematických operací získáme další vysoké prvočíslo a to je již zmíněný soukromý klíč. Bezpečnost tohoto algoritmu spočívá ve velmi náročném rozkladu vysokých čísel a to jak v požadavcích hardwarového vybavení, tak i v časové náročnosti. Mimo RSA v této kategorii známe například DH (Diffie-Hellman) algoritmus. [8]

Obrázek 5 - Asymetrické šifrování



Zdroj: [21]

Výhody a nevýhody:

+ menší hrozba získání klíče (každá strana má svůj jedinečný klíč)

+ lehké ověření identity u partnera se soukromým klíčem

- velká výpočetní náročnost

3.2.3. Hashovací funkce

Hashovací funkce je jednocestná kryptografická metoda, která ze vstupního řetězce znaků vygeneruje hash, nebo-li otisk o předem dané délce bitů. O této metodě se mluví jako o jednocestné, protože nejsme schopný z výstupního hashe dostat původní řetězec znaků. Toto

je výhoda při dostání se hashe k neoprávněné osobě, která nedokáže z hashe získat vstupní data. Dále je u této funkce matematicky nemožné, aby u dvou různých vstupních řetězců znaků byl otisk nebo-li hash stejný a to i v případě, kdy řetězec bude odlišný jen v jednom znaku. Výhodou této metody je, že v případě použití hashovací funkce vícekrát po sobě na stejný vstupní řetězec, bude výsledek otisku pořád stejný. Použití hashovací funkce v praxi vidíme například u SHA (Standard Hash Algorithm) algoritmu. U názvu tohoto algoritmu se můžeme ještě setkat s číslem za pomlčkou u zkratky SHA. Například SHA-256, tento název nám udává, že algoritmus SHA nám bude generovat hashe o délce 256 bitů. [8]

Výhody a nevýhody:

+ právě jeden řetězec má právě jeden možný hash

- je nemožné získat z hashe původní řetězec znaků

4. Moderní kryptografické systémy používané v ICT

Moderní metody, které používáme v ICT (Information and Communication Technologies), zcela vycházejí ze základních kryptografických metod, které jsme si popsali v předchozí kapitole. Musíme brát v úvahu, že základní metody byly používané ještě před nástupem výpočetních strojů a ve většině případů musel stačit kryptogramům jen papír a pero, v dávné historii ani to a přesto dokázali používat takové kryptografické metody, které spolehlivě chránily jejich tajné informace. Ovšem s nástupem moderní éry a příchodem výpočetní techniky se staly tyto metody zastaralé a snadno rozluštitelné. Proto musely přijít na řadu takové kryptografické systémy, které odolají hrozbám dnešní doby a poskytnou nám bezpečnou komunikaci i s našimi nejcennějšími informacemi.

Všechny zde popisované systémy vycházejí ze dvou základních metod a to metoda symetrického šifrování a metoda, která řeší nedostatky symetrického šifrování a to metoda asymetrického šifrování. Hlavním představitelem metody symetrického šifrování je DES (Data Encryption Systém), který už byl prolomen a jeho nástupci jako je například IDEA či Triple DES. Naopak typickým představitelem asymetrický metody šifrování je systém RSA.

4.1. Systémy vycházející z metody symetrického šifrování

4.1.1. DES

DES (Data Encryption Systém) byl ve vývoji od roku 1960, kdy na něm začala pracovat společnost IBM, pro tehdy komerční využití chránění systému plateb a tenkrát ještě pod jménem Lucifer. Díky neustálému zlepšování se stal tento systém jedním z kandidátů na standart šifrování dat, kterým se později i stal v roce 1977 a byl pojmenován Data Encryption Standart. Tento systém byl původně používán jako vládní šifrovací systém, ale později se rozšířil i do komerční sféry a stal se nejpoužívanějším kryptografickým systémem té doby. Už od zrození tohoto standardu mnozí poukazovali na nedostatky tohoto systému a to zejména na příliš krátký 56 bitový klíč. Proto se systém DES stal terčem mnoha útoků a zkoušení, které odkryly většinu hlavních záporných vlastností systému. Ukázalo se, že hlavní nevýhodou u

tohoto systému zůstává od počátku mnohými poukazovaný krátký 56 bitový klíč. Díky této nevýhodě se podařilo v roce 1998 sestrojit stroj pojmenovaný DES-Cracker, který dokázal za použití hrubé síly (zkoušením všech možných kombinací) šifru rozluštit. Díky možnosti napadení původního systému DES, byl vyvinut nástupce Triple DES, který byl místo DES přijat za standard. V roce 2002 vznikl standard nové generace AES (Advanced Encryption Standard). Také se můžeme setkat se zkratkou DEA (Data Encryption Algorithm), nejedná se o nic jiného než o systém DES, ale pojmenován DEA v normě ANSII z roku 1980. [12]

4.1.1.1. Popis DES

Systém DES označujeme za symetrický, blokový systém, protože k zašifrování a rozšifrování používáme jen jeden klíč. A blokový, protože nešifruje postupně jednotlivé znaky, ale šifruje otevřený text po blokách o délce 64 bitů. Systém používá dvě ze základních kryptografických technik a to difůzi a konfůzi.

Difůze – tuto techniku si můžeme popsat jako potřebu závislosti šifrovaného textu na každém bitu otevřeného textu, ale i každého bitu klíče.

Konfůze – tato technika se stará, aby jev popsaný v technice difůze, byl co nejvíce komplikovaný

Otevřený text, který máme na vstupu systému DES je rozdělen do bloků o velikosti 64 bitů a následně je šifrován a výstupem z algoritmu jsou opět bloky po 64 bitech, ale již šifrovaného textu. Systém DES používá k zašifrování 16 rund a při každé rundě se aplikuje šifrovaní, celkem 16 krát.

Z důvodu dnes již nedostatečné ochrany informací při použití kryptografického systému DES, se rozhodly firmy navázat na tento kryptografický systém a vytvořily další varianty DES.

4.1.1.2. Varianty DES

Triple DES

Varianta Triple DES, které se také říká násobný DES, z důvodu použití více klíčů, které prodlužují velikost klíče, který byl u systému DES hlavním nedostatkem. Metoda Triple DES

používá systém DES jako stavební prvek nového systému a aplikuje na něj šifrování s třemi různými klíči, tímto procesem se odstraňuje hlavní nedostatek základní metody DES. Při použití třech různých klíčů získáváme klíč o velikosti 168 bitů (3x56 bitů), při použití dvou různých klíčů 112 bitů (2x56 bitů). Při použití 3 stejných klíčů, ale zůstává délka klíče pořád nedostatečná 56 bitů. Triple DES je dnes oficiálním platným standardem nahrazující systém DES.

RDES

Varianta RDES se liší od DES pouze v závislosti na klíči výměny levé a pravé poloviny v poslední rundě, které je u systému DES měněno automaticky. Měnění polovin je součásti šifrování kryptografického systému DES. Systém RDES nevylepšuje systém DES, co se týče bezpečnosti, a proto se tato varianta téměř nepoužívá.

DESX

Varianta DESX byla vyvinuta společností RSA Data Security a používá ke zlepšení samostatného systému DES navíc tzv. whitenning (bílení), které se nám snaží přidáním dalšího 64 bitového klíče k původnímu 56 bitovému prodloužit nedostatečný klíč z 56 bitů na 120 bitů.

DES s nezávislými klíči

Tento systém vylepšuje stávající systém DES, který používá 16 klíčů v každé rundě šifrovacího procesu odvozených z jednoho klíče. Tento fakt právě odstraňuje systém DES s nezávislými klíči, který používá pro šifrování každý rundy jiný klíč, nezávislý na hlavním klíči.

GDES

GDES, kterému se také říká zobecnění DES, který si ukládá za cíl zrychlení klasického systému DES použitím zpracování různě dlouhých bloků oproti klasickému DES, kde se zpracovávají bloky po 64 bitech.

CRYPT (3)

Tato varianta systému DES je používána u unixových systémů. [12]

4.1.2. IDEA

IDEA (International Data Encryption Algorithm), tento systém nebo také algoritmus je také blokový se symetrickým šifrováním. Tento systém vznikl v roce 1990 a byl vyvinut firmou Ascom-Tech, kterou byl později i patentován, na základě jednoho z projektů. Algoritmus IDEA je volně dostupný v kompletním šifrovacím balíku PGP, kde je brán za hlavní šifrovací systém, který tento algoritmus zahrnuje. Tento algoritmus není volně šiřitelný z důvodu existence patentu tohoto systému. Rychlost oproti systému DES je přibližně jednou tak velká a zároveň s mnohem vyšší bezpečnosti u systému IDEA.

Princip IDEA

Princip u tohoto systému je podobný jako u systému DES, jedná se také o blokový systém, který rozděluje otevřený text do bloků o velikosti 64 bitů. Liší se, ale už ve velikosti klíče, kdy u DESu byl 56 bitový a dnes již nedostačující. Velikost klíče u systému IDEA se rovná 128 bitů, které už jsou průměrné a prozatím dostačující. Šifrování probíhá již ale už jen v 8 rundách. Nejdříve se klíč rozdělí na 52 podklíčů, pomocí kterých se pak v jednotlivých rundách šifruje otevřený text. V každém kole se provádí složité šifrování, které napomáhá k vyšší bezpečnosti systému IDEA, toto šifrování se ve všech kolech periodicky opakuje, ale i přesto systém IDEA nebyl doposud prolomen (ani hrubou silou = zkoušením všech možných možností) a považuje se stále za jeden z nejbezpečnějších symetrický kryptografický systémů. [13]

4.1.3. AES

Při prolomení standardu DES v roce 1997, bylo více než jasné, že je potřeba pro ochranu politických, ale i vojenských informací začít používat nový standard a tento problém se stal nutností, kdy bylo potřeba co nejrychleji najít dobré řešení. Americký institut standardizací a technologií NIST (National Institute of Standards and Technology), který standardizoval i právě prolomený systém DES, proto vyhlásil veřejné výběrové řízení na přijetí nové šifry, která bude nejlépe splňovat podmínky NIST. Záměrem bylo vyvinout novou flexibilní šifru, která se dá použít jak pro vládní účely, tak pro komerční využití, ale i soukromé účely. Mezi podmínky jež NIST uvedl, bylo například:

- Standard má zvládat pracovat s 8,32 a 64 bitovými procesory.
- 128 bitová bloková šifra.
- Má podporovat délky klíčů 128, 196 a 256 bitů.

Do soutěže se přihlásilo celkem 15 kandidátů z celého světa, do druhého kola se jich dostalo pouze 5.

- Rijndael
- RC6
- Twofish
- MARS
- Serpent

4.1.3.1. Základní šifry, které byly použity pro vznik standardu AES

Rijndael

Rijndael, který se nakonec umístil na prvním místě a stal se vítězem, je dodnes považován za nejlepší šifru mezi blokovými algoritmy vůbec. Dosud je napadán ohledně nízké bezpečnosti a zpochybňován na mnoha místech, ale faktem zůstává, že ještě nikdy nebyl dokázán průnik do tohoto algoritmu. Algoritmus Rijndael je založen na matematickém návrhu, který byl také jednou z mnoha pochybností u odvrácených stran tohoto algoritmu. Algoritmus samotný využívá pro šifrování různého počtu rund, v závislosti na délce klíče. Pro délku klíče 128,196 a 256 bitů bylo stanoveno 10,12 nebo 14 rund. Rijndael splňoval všechny kritéria, které NIST pro nový AES požadoval, ač mezi ostatními algoritmy byli i bezpečnější, než je Rijndael, byl vybrán NIST jako přiměřeně bezpečný na případný možný útok. Oproti konkurenci, Rijndael velmi vyčníval, v porovnání rychlostí zpracování, kde byl zhruba 2x rychlejší než konkurence. [14]

RC6

Tato šifra vyvinuta firmou RSA Laboratories, je založena na vysoké flexibilitě a podle velikosti šifrovaných bloků či klíče se také mění název, respektive přesné parametry se udávají za název šifry RC6. RC6 není ale úplně nový algoritmus, protože jádrem RC6 jsou dvě paralelně propojené předchůdci této verze, tedy RC5. Toto propojení bylo potřeba zrealizovat z důvodu nároků na požadavky nového AES, které vydala instituce NIST. RC5 lze také charakterizovat za velmi bezpečný systém, který i díky paralelnímu propojení dvou předchozích verzí je velice jednoduchý. Výhodou u tohoto algoritmu jsou menší nároky na ROM a RAM paměť, oproti ostatní konkurenci, a ačkoliv nebyl vybrán institucí NIST jako AES, je to stále jeden z nejlepších symetrických blokových systémů.

Blowfish, Twofish

Blowfish je předchůdce systému twofish, který se dostal do nejlepších 5 systémů, které splňovaly požadavky při výběrovém řízení nového standardu AES. Blowfish vznikl po prolomení šifry DES, jako reakce na potřebu nového systému. Tento systém je podobný systému DES, používá taky vstupní a výstupní 64 bitové bloky, jediný rozdíl je u Blowfish použití klíče rozdílné délky, který nám zvyšuje bezpečnost.

Twofish je nástupce systému Blowfish a jeden z nejlepších šifrovacích systémů současnosti. Pracuje se 128 bitovými bloky a umožňuje použití klíče až 256 bitů, při šifrování používá 16 rund. Je to jeden z nejrychlejších šifrovacích systémů, ale stále je mnohem pomalejší než Rijndael. Výhodou je již zmíněná rychlost a to, že systém je volný.

Mars

Šifrovací systém Mars má volitelnou délku klíče 128-448 bitů. Šifrování a dešifrování se provádí stejně jenom s obráceným pořadím rund. Důvodem vysoké bezpečnosti je použití dvou druhů rund, kterým se ale systém stává velice složitý.

Serpent

Serpent je nejbezpečnějším šifrovacím algoritmem ze všech 5 finalistů a to zejména díky použití 32 rund, což je několika násobek nejmenšího ještě bezpečného počtu rund. Tento fakt je odůvodněn použitím systému i v delší budoucnosti, kdy už nebude bezpečné ani použití teď bezpečného počtu rund a má samozřejmě za následek velice bezpečný systém, ale na úkor

snížení výkonu šifry. Délka klíče je také volitelná, avšak nejvíce 256 bitů. Systém je, jak i autoři sami o něm říkají velice bezpečný, ale je také velice jednoduchý. [14]

4.2. Systémy vycházející z metody asymetrického šifrování

4.2.1. RSA

Systém RSA je pojmenovaný po svých třech autorech a to Rona Rivesta, Adi Sharmira a Len Adlemana, kteří jako první po vzniku myšlenky asymetrické kryptografie, přišli v roce 1977 se svým asymetrickým kryptografickým systémem. Tento algoritmus byl patentován až po 6 letech po jeho objevení, v roce 1983 a to firmou RSA security, kterou mezitím stačili založit právě tři autoři systému RSA. Nyní nejvíce rozšířená šifra RSA se stává čím dál více napadaná ohledně bezpečnosti, protože šifra je založená na matematicky velmi složitém principu, rozkladu velkých prvočísel, avšak ne nerozluštitelná, ale za velmi dlouhou dobu, která se odvíjí od použité technologie k prolomení šifry. Ale i při použití dnešní technologie se stává šifra bezpečnou při použití dostatečně dlouhého klíče, přelom může nastat kdykoliv, kdy nějaký matematický vědec přijde s jednodušší metodou rozkladu dvou prvočísel a nebo příchodem ještě výkonnějších technologií. Velkou hrozbou je možný příchod kvantových počítačů. Právě této matematické techniky je používáno v systému RSA a potažmo v celé oblasti asymetrického šifrování, kde používáme dvojici klíčů veřejného a soukromého. Veřejný klíč používáme výhradně k zašifrování zprávy a je veřejně dostupný oproti soukromému klíči, který se udržuje v tajnosti a slouží k dešifrování zprávy. Oba klíče musí být dostatečně silné, aby nebylo možné z jednoho z nich získat ten druhý a naopak ani s použitím těch nejmodernějších výpočetních prostředků.

Velkou nevýhodou asymetrického šifrovacího systému RSA je velká náročnost šifrování, z které vyplývá velmi pomalá rychlost při šifrování velkých objemů dat. Z tohoto důvodu se asymetrická metoda šifrování používá většinou jen k šifrování pomocných prostředků a ne přímo k šifrování celé zprávy. Toto se většinou používá se spojením s nějakým symetrickým šifrovacím systémem, kde je složité právě jeden šifrovací klíč přenést od odesílatele k příjemci. Celý princip spočívá v zašifrování celé požadované informace pomocí symetrického šifrování a následně na klíč, který byl použit k zašifrování u symetrického šifrování, je použit systém asymetrického šifrování, který nám zašifruje už jen klíč, který není

tak objemný jako celá zpráva a proto se na to hodí použít asymetrický systém šifrování. Dále se používá asymetrický systém při tvorbě elektronického podpisu. Ale přirozeně s použitím asymetrického šifrování se již v dnešní době setkáváme téměř všude, například při použití mobilního telefonu či platebního bankomatu atd. [15]

4.2.1.1. Průběh komunikace asymetrického šifrovacího systému RSA

Vysvětlení průběhu komunikace si vysvětlíme pomocí reálných objektů, kterými budou v našem příkladu Alice – odesílatel, Martin – příjemce a Eva která se snaží získat tajnou informaci.

1) Alice a Martin mají každý svůj generátor klíčů, který jim vygeneruje každému veřejný a soukromý klíč. Oba dva veřejné klíče jsou známé Alici, Martinovi i Evě.

2) Alice před odesláním zašifruje informaci pomocí svého soukromého klíče. To ale není dostačující, protože by ji mohl rozšifrovat kdokoliv, kdo zná veřejně dostupný veřejný klíč Alice. Proto musí Alice zprávu zašifrovat ještě jednou a to za pomoci veřejného klíče Martina.

3) Martin dostane zašifrovanou zprávu od Alice, kterou rozšifruje jen svým soukromým klíčem, tímto je zaručeno, že danou zprávu může rozšifrovat pouze on. A dále musí rozšifrovat ještě jednou a to za pomoci veřejného klíče Alice, po kterém již získá zašifrovanou informaci.

4) Eva, která se snaží získat tajnou informaci má znalost obou veřejných klíčů i přenášené zprávy, ale z této kombinace není schopná získat přenášené informace.

Nejvíce nebezpečným článkem možného průniku do systému RSA je volba krátkých klíčů. Použití velmi krátkých klíčů při šifrování si snižujeme zásadně bezpečnost používaného asymetrického systému RSA.

4.2.2. El Gamal

Ačkoliv asymetrický kryptografický systém El Gamal, byl vyvinut déle než již prvně uvedený systém RSA, není tak masivně používán a do popředí se dostává spíše až dnes, kdy se začíná rozebírat teorie bezpečnosti rozkladu vysokých čísel na prvočísla, která je právě používána u systému RSA. Autor, podle kterého byl systém i pojmenován, založil tento systém na úplně jiném schématu, než je použit u systému RSA. U tohoto systému autor nejde cestou rozkladu vysokých čísel na prvočísla, ale je založen na složitosti výpočtu diskrétního algoritmu. Hlavní nevýhodou proč se tento systém nepoužívá v tak širokém měřítku jako metoda RSA, je velkým objemem zašifrované zprávy oproti textu který chceme přenést. Objem u takovéto zašifrované zprávy se může navýšit až jednou tolik než objem otevřeného textu. [16]

4.2.3. DSA

DSA algoritmus, jinak taky Digital Signature Algorithm, je volně přeložen jako algoritmus digitálního podpisu, který byl navržen v NIST (Národní Institut Standardů a Technologií) v roce 1991, jako jeden z článku standardu DSS (Digital Signature Standard), který byl přijat v roce 1993. Algoritmus DSA byl patentován a jeho tvorba byla přiznána D.W. Krawitzovi, dnes již bývalému pracovníkovi Národní bezpečností agentury Spojených států amerických. Algoritmus samotný je založen na El Gamalovu algoritmu, který vychází ze složitosti výpočtu diskrétního algoritmu. [17]

5. Aplikace kryptografie

Používání kryptografie se od jejího vzniku pořád rozvíjí, v dávných dobách byla využívána zejména pro tajné taktické operace, ať už za období spartských vojsk, či za vedení velkého vojevůdce Julia Ceasera. Během období světových válek a s rozvojem matematiky a techniky, se oblast kryptografie dočkala velkých skoků směrem výše, co se týče rozvoje, ale i bezpečnosti. Ovšem největšího rozvoje se kryptografie dočkala až s příchodem prvních počítačů, které byly schopné nám velice ušetřit práci se složitými výpočty. Dnešní kryptografie je velmi obsáhlá oblast, která se stále snaží zajistit bezpečné soukromí, ale nyní nejen ve vysoké politice a u tajných vojenských operací, ale probojovala se již i do komerčního, ale i soukromého použití. V dnešní době konkurenčního boje a rozvoje komerčních taktických řešení na úrovni strategického rozhodování, je kryptografie nezbytnou nutností k udržení firemní strategie firmy.

Někdy se musíme zamyslet nad správnosti použití kryptografie v daném případě, při použití kryptografie tam, kde není potřeba, nebo aplikování špatného druhu kryptografie, může mít za následek nefunkční, nebo také naopak záporný efekt použití kryptografie. Příkladem může být vymyšlený příklad, kdy máme školní databázi s jednotlivými třídami, předměty, žáky a jednotlivé známky žáků z předmětů. Když vezmeme v potaz, že si chceme ušetřit práci a zašifrujeme pouze jednotlivé známky žáků z jednotlivých předmětů, aby nebylo možné zjistit, co má daný žák za známky. Ale nesprávnost použití daného způsobu šifrování spočívá v tom, že v prvním případě nabourání se do databáze může neautorizovaná osoba dělat změny v databázi, přeskočíme li fakt, že se vůbec do databáze dostane. Další z chyb aplikování kryptografie na databázi je možnost osoby, která může zasahovat do databáze a vidí u sebe zašifrované známky v podobě nějaké kombinace znaků, není těžké si zjistit, který spolužák má dobré známky a přepsat si místo svojí kombinace šifrovaného textu spolužáka, čímž docílí stejně dobrých známek jako spolužák. A takových případů najdeme více, proto by se užití kryptografie na určitých místech mělo vždy pořádně zvážit.[8]

Doposud jsme se stále zabývali tím, že kryptografie slouží jen k zajištění utajení informace, což není jediný cíl kryptografie, ale jeden z možných cílů. Dá se říci, že kryptografie má jeden z hlavních cílů zajištění utajení informace, s přihlédnutím na ICT hlavně utajení přenášené informace, ale to není jediné možné použití kryptografie.

Využívání dnešní kryptografie:

- utajení informací
- bezpečný přenos informací
- zajištění důvěrnosti dat
- autentizace a ověřování integrity
- digitální podpis

5.1. Používané kryptografické aplikace používané v ICT

Používaných aplikací, které v sobě skrývají nějaký prvek kryptologie nebo aplikace přímo zabývající se jakýmkoliv oborem kryptologie, je velká řada. S vývojem výpočetní techniky se aplikování kryptologie do oblasti informačních technologií čím dál více implementuje a to do všech odvětví tohoto rozsáhlého oboru. Pro představu jak se dá kryptografie v ICT použít, jsem vybral na vysvětlení pár protokolů SSH a SSL a dále bych se rád zmínil o v dnešní době hodně probírané tématice, které se říká digitální podpis.

5.1.1. Protokol SSH

Základním důvodem, proč se protokol SSH používá, je chráněné (šifrované) spojení mezi klientem a vzdáleným serverem, většinou přes veřejné nechráněné prostředí, a proto je vhodné použít tento protokol a zajistit si tak bezpečnost přenášených informací. Plno lidí si v dnešní době stále neuvědomuje, že používáním nezabezpečených protokolů jako je ftp, telnet, pop3, http a dalších, ulehčuje práci získání informací z odposlechu neoprávněným osobám. Náhradou zmíněných protokolů jsou aplikace používající protokol SSH. SSH protokol je založen na připojení klient server, kde na serveru (sshd) je inicializován SSH protokol, který je zpracováván na klientské stanici a pomocných podpůrných programů. Protokol SSH se nyní dělí na dvě verze SSH1 a SSH2, z nichž verze 1 je zastaralá a nedoporučuje se již používat. Servery by měli být, ale zpátky kompatibilní, aby se zabránilo potížím mezi přechodem jednotlivých verzí. [18]

5.1.1.1. SSH1

Protokol SSH verze 1 je zastaralý a v současné době málo bezpečný protokol, který pracuje oproti SSH verzi 2 na úplně jiném funkčním principu. Nedostatečná bezpečnost protokolu spočívá například v nešifrovaní celé hlavičky jednotlivých paketů. Díky tomuto nedostatku u protokolu SSH verze 1 se hrozbou stává možnost odposlechu z důvodu odklonění spojení.

5.1.1.2. SSH2

Důvodem, proč je protokol SSH2 tak úspěšný, je dobře navržená struktura celého protokolu, která se skládá ze 3 spolu vzájemně komunikujících vrstev tohoto protokolu a to transportní, ověřovací a vrstvy spojení.

Transportní vrstva

Tato vrstva se nám stará o prvotní výměnu klíčů a autentizaci, ale má za úkol hlídat také integritu přenášených dat a hlídat obnovování klíčů po jedné hodině nebo po přenesení 1GB dat. Výsledkem výměny klíčů je hodnota K-společný klíč a H-hash. Používaný algoritmus pro výměnu klíčů je Diffie-Hellman asymetrický kryptografický algoritmus.

Ověřovací vrstva

Ověřovací vrstva se nám stará o authentizaci klientů, kteří se i starají o samostatnou authentizaci, kterou v případě SSH neřídí server, ten jen odpovídá na autorizační požadavky.

Základní metody serveru u protokolu SSH2 pracující na ověřovací vrstvě

- Password – ověření správnosti hesla, které je zasíláno v textové podobě, ale bezpečně po již zašifrovaném spojení.
- Public key – kontrola správnosti se znalostí veřejného klíče. Toto je jediná metoda, kterou musí každý server SSH podporovat. Ostatní metody jsou již doplňkové. Klient odesílá veřejný klíč společně s názvem algoritmu, v kterém byl vygenerován. Server zkontroluje autentifikaci uživatele, pomocí zaslaných údajů a v případě shody odpoví zasláním těchto údajů zpět.
- None – tato metoda se používá bez autentifikace, a proto se používá například jen pro zjištění možných používaných metod serverem.

Vrstva spojení

Všechny spojení realizovány protokolem SSH2 jsou uskutečňovány v kanálech, které jsou skládány do jednotlivého spojení nad transportní vrstvou. Tato vrstva se nám stará o navázání a správu spojení o správnosti použití kanálů, v závislosti na kanálových požadavcích. Každý kanál SSH spojení, funguje oboustranně a SSH spojení může obsahovat více kanálů. Na této vrstvě klient žádá server o přiřazení komunikačního portu.

Sestavení spojení:

1. Klient pošle serveru žádost na sestavení spojení a použití dané verze protokolu SSH
2. Server odpoví posláním veřejného klíče klientovi
3. Klient pomocí něj zašifruje svůj klíč a pošle zpět na server
4. Teď mají klient i server stejný šifrovací klíč k šifrování komunikace

5.1.1.3. SSH služby

SSH službami rozumíme aplikace, které jsou založeny již na zmíněném šifrovacím protokolu SSH, který využívají k šifrovanému spojení u své aplikace. [18]

SFTP – klasický protokol ftp, přenáší veškerá data po síti v nezašifrované podobě. To neznamená nic jiného, než, že v případě odposlechu, takového nezašifrovaného spojení, může útočník snadno zjistit, například přihlašovací údaje k ftp. K zabránění takových případů můžeme použít FTP protokol založený na chráněném kanálovém spojení SSH, který se jmenuje SFTP (SSH File Transfer Protokol), někdy také označován jako Secure File Transfer Protokol. Protokol SFTP používáme pro bezpečný přenos souborů za pomoci počítačové sítě. SFTP protokol se nám nestará o samotnou authentizaci a bezpečný přenos dat, o tyto vlastnosti se nám stará samotný SSH protokol, který je implementován. S pojmem SFTP se můžeme setkat také u názvu programu, který nám popisovaný přenos souborů aplikuje.

X11 forwarding – tato služba se nám stará o vzdálenou bezpečnou komunikaci připojení vzdáleného PC pomocí grafického prostředí.

Port forwarding – tzv. tunelování portů je metoda, při níž vytváříme tunel spojení za pomocí šifrovaných kanálu SSH z jednoho konce spojení na druhý. U tohoto tunelování můžeme přesměrovávat místní porty nebo i vzdálené porty.

Remote control – podobný jako X11 forwarding, ale ke vzdálené správě používá jen textové rozhraní.

5.1.2. Protokol SSL

Protokol SSL (Secure Socket Layer) je protokol vymyšlený firmou Netscape a pracuje mezi Transportní a Aplikační vrstvou TCP/IP modelu. Tento protokol se stará o sestavení zašifrovaného spojení a komunikaci, ale nestará se již, který z aplikačních protokolů využíváme k takovému spojení. Je na první pohled velmi podobný protokolu SSH a napomáhá tomu také fakt, že oba dva tyto protokoly se starají o přenos dat mezi dvěma uzly za pomocí vytvoření šifrovacího tunelu a mnoho dalších vlastností. Oba dva tyto protokoly jsou velice univerzální a díky tomu teoreticky snadno zaměnitelné. Proto je také tak těžké najít rozdíly mezi těmito dvěma protokoly, ale jeden velký rozdíl mezi nimi tady je, a to v možném způsobu užití autorizace. U protokolu SSL je autorizace možná, ale ne povinná a tak je možný anonymní přenos oproti SSH protokolu, kdy je autorizace povinná. Rozdíl je také ve způsobu autorizace. [19]

Samotný SSL protokol se dále dělí na dvě části:

Record Protokol

Handshake Protokol

Kdy část pojmenovaná Record Protokol se stará o šifrování a přenos aplikačních dat a část Handshake Protokol se stará o navázání, správu spojení a authentifikaci.

Sestavení SSL spojení

SSL spojení je založeno na principu asymetrické šifry, kdy pro zašifrování a rozšifrování používáme dvojici rozdílných klíčů. Veřejný klíč a soukromý klíč. Soukromým klíčem se dá rozšifrovat zpráva, která byla zašifrována klíčem veřejným.

1) Klient pošle požadavek na spojení serveru SSL, požadavek také obsahuje informace o verzi SSL a nastavení šifrování.

2) Server odpoví na klientský požadavek posláním daného certifikátu serveru

3) Podle certifikátu, který klient obdržel od serveru, si klient může ověřit správnost serveru. Certifikát dále obsahuje veřejný klíč serveru.

4) Na základě obdržení veřejného klíče klient vygeneruje základ šifrovacího klíče, kterým se následně bude kódovat komunikace. Informace již zašifruje veřejným klíčem serveru a pošle mu ho.

5) Po přijetí zprávy ji server rozšifruje pomocí svého soukromého klíče. Z tohoto vygenerují klient a server hlavní šifrovací klíč společné komunikace.

6) A server si ještě potvrdí, že od této chvíle budou spolu navzájem komunikovat v šifrovaném přenosu.

7) Je vytvořeno šifrovací spojení mezi klientem a serverem za pomocí nově vygenerovaného šifrovacího klíče.

Existuje také možnost, kdy se nemusí tento postup opakovat pořád od začátku, takový případ může nastat v případě, kdy v nedávné době došlo k šifrovanému spojení. V tomto případě je

postup mnohem jednodušší a klient zasílá serveru zároveň s požadavkem na navázání spojení také ID předchozího spojení. V případě, kdy server žádost přijme, nemusí se opakovat celý postup navázání spojení, ale naváže se na předchozí přístup. [18]

Ověření serveru klientem

Pro zjištění důvěryhodnosti serveru je zapotřebí si zjistit hned několik věcí spojených s daným certifikátem serveru. Při neshodě jednoho z uvedených bodů, je spojení klienta se serverem hned ukončeno.

U serverového certifikátu můžeme ověřovat zda:

- je certifikát stále aktuální, nevypršela platnost certifikátu
- certifikát je podepsán správnou certifikační autoritou, kterou je například v ČR www.ica.cz
- zda souhlasí podpis CA –certifikační autority s podpisem na certifikátu
- certifikát je opravdu pro danou doménu vhodným certifikátem

Ověření klienta serverem

U SSL je ale možné požadovat také autorizaci od serveru po klientovi, který se prokazuje při průběhu navázání spojení. Dále ověřování funguje podobně jako u serverového. U ověřování klienta se na serveru můžou brát v potaz ještě další věci, například zda klient není zapsán v nějaké databázi a podobně.

6. Dnešní vývoj kryptografie

Dnešní kryptologie a všechny její odvětví se vyvíjí mimořádně rychle, je to spojeno s růstem dnešních technologií a výpočetních výkonů, které nám dávají mnohem větší příležitosti pro vývin kryptologie. Další důvod exponenciálního růstu kryptografie je neustále se zvyšující potřeba začlenění kryptografie do nových a nových aplikací. Dnešní kryptografii nalezneme například u sestavení mobilních hovorů, nebo při navštívení nějakých z velkého množství internetových stránek a mohl bych uvést mnoho dalších příkladů. Důvodem velkého zájmu je dnešní doba, v které si nedokážeme představit již život bez dnešních technologií a neustále se nám zvyšují nároky a požadavky na používané technologie. Zvyšující se nároky na technologie, ale většinou plynou ze stále se rozvíjejícího konkurenčního boje, ale i politických a státních organizací, které potřebují pro svoje tajné informace vždy maximální stupeň zabezpečení. Ale s rostoucím vývinem dnešních technologií přicházejí i hrozby pro kryptografii, kterým musí kryptografie čelit a proto se neustále vyvíjet. Dnešní kryptografické metody si dokážou poradit s nárůstem výpočetního výkonu díky zvyšování délky šifrovacích klíčů, ale největší hrozba pro dnešní standardy používané v kryptografii je určitě možný příchod kvantových počítačů, které by si dokázaly poradit například s rozluštěním dnes nejvíce používané asymetrické šifry RSA, ale i dalších asymetrických šifer. S touto hrozbou by se měla vypořádat poměrně nová technologie Kvantová kryptografie, která nyní čelí jako novinka nejrůznějším diskuzím, ale zatím všechny diskuze o nebezpečnosti, byly nakonec vyvráceny nebo bylo dokázáno, že chyba byla na straně lidí, kteří daný systém sestavovali. Kvantová kryptografie se řadí k Vernamově šifře jako jedna z nejbezpečnějších kryptografických metod vůbec. Právě proto v této kapitole o dnešních trendech v kryptografii si více rozebereme tuto poměrně novou šifru, kterou lze zakoupit již i ke komerčnímu použití, ale zatím za poměrně dost veliké peníze, cca. 70000 amerických dolarů. Další z témat, o kterém bych se chtěl v této kapitole více zmínit, je digitální podpis, který se začíná dostávat do podvědomí už nejen počítačově gramotných lidí, ale široké veřejnosti, která se snaží začínat používat elektronický podpis.

6.1. Kvantová kryptografie

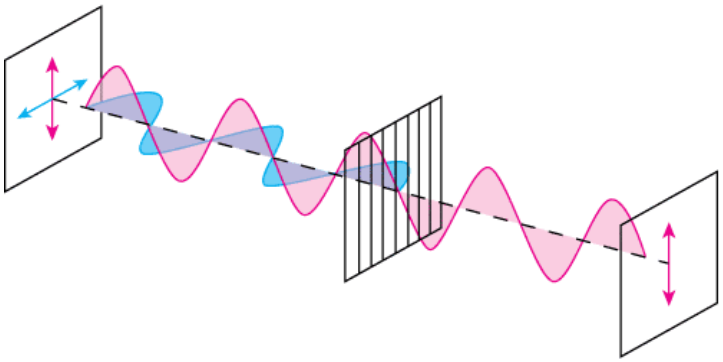
V poslední době se do popředí začíná dostávat pojem kvantových počítačů, ale také kvantové kryptografie. Celý základ kvantové metody, se datuje již od dob Alberta Einsteina, který

přišel v roce 1905 s teorií, která se týká kvantů světla. Tato teorie pojednává o tom, že při emisi nebo absorpci světla se energie světla předává po částech – kvantech. Více si řekneme o kvantové kryptografii, která je jednou z nejbezpečnějších typů kryptografie vůbec, i přesto, že tato metoda nedokáže zabránit odposlechu, který se hned identifikuje a může přestat s vysíláním. V novinách či na internetu se občas objeví nějaký článek o prolomení této kryptografie, zatím není žádný prokázán a vždy se ukázalo, že se jedná jen o lidskou chybu spojenou s realizací kvantové kryptografie. Symetrické technologie, jsou jako takové velmi bezpečné, ale velké riziko u nich nastává s dopravou šifrovacího klíče od odesílatele k příjemci, tento fakt se snažila vyřešit svým příchodem asymetrické šifrování. Dnes nejvíce používané asymetrická šifrovací metoda RSA, je založena na principu dvou klíčů veřejného pro zašifrování a soukromého pro dešifrování, asymetrický systém je založen na principu ne snadno dosažitelného rozkladu dvou prvočísel při použití dostatečně dlouhého klíče, kdy je sice možné rozluštit tuto šifru, ale za velmi dlouhou dobu s použitím dnešní technologie. Velkou hrozbou se stává vysoký pokrok v oblasti výpočetních technologií a možný příchod kvantových počítačů. Kvantové šifrování se dostává do podvědomí lidí, zejména s prvním kryptografickým protokolem, který byl založen na kvantové mechanice v roce 1984 a pojmenován BB84. [20]

6.1.1. Princip kvantové kryptografie

Při vysvětlení principu, musíme až do úplných základů kvantové fyziky, kdy si představíme foton, který představuje již na začátku této kapitoly zmiňované kvantum světla, objevené A. Einsteinem. Tedy základní jednotkou světla je foton. A kvantová kryptografie je založena právě na stavu těchto fotonů. Stavu fotonu se rozumí jeho polarizace. Polarizované světlo se stává ze světelného zdroje, za který dáme skleněný hranol nebo polarizační destičku jak je ukázáno na obrázku.

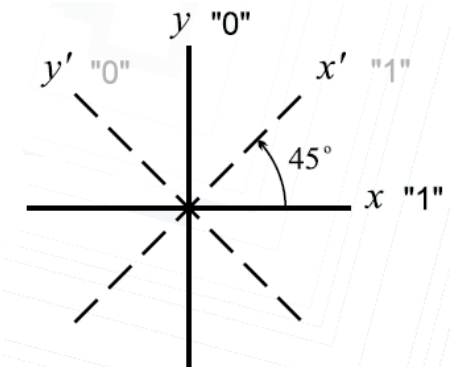
Obrázek 6 - Polarizace fotonů



Zdroj: [20]

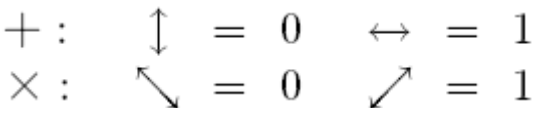
Základním principem kvantové kryptografie tedy jsou, jak vidíme na obrázku dvě navzájem kolmé lineární polarizace a dvě polarizační báze otočené o 45°, jejímž výsledkem jsou kódovací stavy obrázek.

Obrázek 7 - Kolmé lineární polarizace a dvě polarizační báze otočené o 45°



Zdroj: [20]

Obrázek 8 - Kódovací stavy

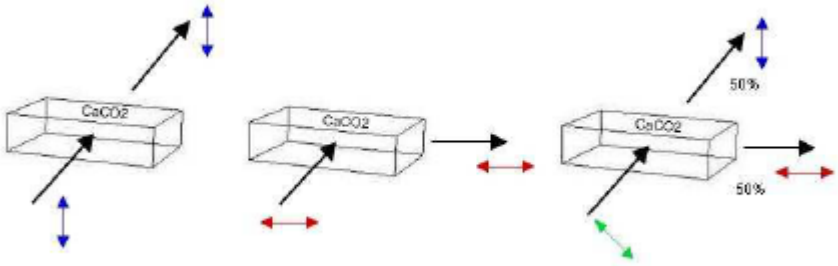


Zdroj: [20]

Nyní jsme si rozebrali, jakým způsobem s použitím světla můžeme šifrovat, ale na straně příjemce při dešifrování se setkáváme s opačným mechanizmem a to s rozebráním světla na

jednotlivé, přenášené polarizace. K tomuto účelu nám v praxi slouží optický hranol (krystal), který nám dokáže horizontálně polarizované světlo propustit a vertikálně polarizované světlo odklonit. V případě, kdy nám dopadnou na krystal diagonálně polarizovaný fotony, se nám světlo rozkládá na dvě půlky, z nichž jedna projde krystalem a druhá se odkloní. Zde popisované zjišťování polarizace nám názorně zobrazuje obrázek.

Obrázek 9- Průchod fotonů krystalem



Zdroj: [20]

Při kontrole odposlechu se využívá Heisenbergerovu principu, který nám říká, že v případě měření vlastností u jednotlivých částic není možné měření aplikovat, bez ovlivnění daných částic. V našem případě to znamená změnu nesené zprávy mezi příjemcem a odesílatelem, kdy v případě pasivního odposlechu, který se provádí přes ohyb optického vlákna, se nám mění výkon přijímaných fotonů. Proti tomuto typu odposlechu se můžeme bránit použitím optického vlákna, které je odolné proti ohybům. V druhém případě a to aktivním odposlechu, útočník zavede do cesty svoje zařízení, které bude přijímat a znova odesílat jednotlivé fotony, které nám nesou jako hodnotu jednotlivé bity. Ale z důvodu útočníkovy neznalosti polarizační báze způsobí na straně příjemce zprávy chyby, které vedou k detekování odposlechu. V případě, kdy útočník zjistí polarizační bázi, se stává neviditelným, z tohoto důvodu je potřeba časté měnění polarizačních bází.

Kvantová kryptografie má ale i svoje nevýhody, ke kterým patří například autorizace, kterou kvantová kryptografie vůbec neřeší a útočník při přerušení kanálu se může vydávat za odesílatele nebo příjemce. Proto není vhodné a většinou se používá kvantová kryptografie se spojením jiného symetrického systému, který řeší autorizace například AES, takovému spojení dvou kryptografických systému říkáme systém hybridní. Ale problém autorizace není jediná nevýhoda tohoto systémů, dále sem patří potřeba přímého optického spojení mezi

uživatelem A a B, bez použití zesilovačů, takovéto spojení velmi zkracuje celkovou možnou přenosovou vzdálenost, která začala při vývinu a prvním zkoušení tohoto systému na 30 cm a nyní může takovéto spojení dosahovat vzdálenost až několika desítek kilometrů. Nejtěžší na celém kryptografickém systému, je dobře navrhnout a sestrojit systém, který dokáže správně vysílat a přijímat jednotlivé fotony, které nesou informaci o jednotlivých bitech na patřičnou vzdálenost. Od tohoto důvodu velké náročnosti se odvíjí i vysoká cena těchto systémů.

Protokol BB84 – Protokol, který jak už jsem uvedl na začátku tohoto tématu, je první protokol svého druhu využívající kvantové mechaniky a pojmenován po autorech, kterými jsou Charles Bennett a Gilles Brassard a roku kdy byl vytvořen tedy 1984. Tento protokol je založený na zde vysvětleném principu kvantové kryptografie, tedy na principu polarizačních bází u přenášených fotonů. V příkladu komunikace pomocí tohoto protokolu uvedu pro odesílatele písmeno A, příjemce B a možného útočníka si můžeme představit pod písmenem C.

Příklad komunikace s použitím kvantové kryptografie a protokolu BB84

1. **A** generuje fotony z možných 4 rovin a odesílá je **B**
2. **B** provádí přijímání (měření) příchozích fotonů a náhodně střídá báze
3. **B** posílá **A** svoje použité báze, které následně **A** potvrdí
4. **B** získal přenášenou zprávu, v případě chyb je přítomen útočník **C**
5. **B** posílá náhodně vybrané bity pro kontrolu
6. **A** potvrdí přijaté bity, v případě odposlouchávajícího útočníka **C** dochází k chybám

Protokol E91 – Tento protokol je založený také na kvantové mechanice, fungující ale na odlišném principu použití fotonů. U protokolu E91 se setkáváme s metodou propletených fotonů, nebo-li korelujícího stavu dvojice částic. V praxi to znamená, že dvojice jsou na sobě závislé. A při například aplikování měření na jednu z těchto částic se změní stav druhé částice, která je v korelujícím vztahu s první částicí. Princip této metody spočívá v generování dvojice fotonů, kdy spin prvního z fotonů, je orientován nahoru a druhý dolu. Jeden z těchto fotonů je nechán na přijímací straně, druhý je poslán příjemci. Tímto způsobem

přijme příjemce celý klíč, ale obrácený oproti klíči odesílatele. Znamená to tedy, že příjemce je schopný si získat z poslaných bitů správný klíč. Pro kontrolu se klíč odešle na protější stranu, kde je zkontrolována správnost. V případě odposlechu klíče nejsou shodné, protože jak už jsem uvedl v předchozí kapitole díky Heisenbergerovu principu by se změnily spiny u jednotlivých fotonů a při kontrole dojde k detekci odposlechu. [20]

6.2. Elektronický podpis

Nástup nových technologií nám přináší i mnoho nových možností do oblasti mezilidské komunikace a právě jedna ze zde mnoha zmiňovaných možností je elektronický podpis. S elektronickým podpisem se můžeme setkat také pod názvem digitální podpis, nejedná se ale o nic jiného, ale spíše o to kde je používán. S názvem elektronický podpis se můžeme setkat zejména v Evropě oproti tomu pojem digitální podpis je prosazován hlavně v USA, problém s pojmenováním tohoto podpisu pak nastává spíše v právní sféře.

Pod pojmem elektronický (digitální) podpis, se neskrývá jen nahrazení klasického dnes používaného ručního podpisu pro ověřování dokumentů, ale i další možnosti, které se skrývají pod tímto názvem jako je na příklad šifrování přenášeného podepsané dokumentu, skrz veřejnou síť, ale i možnost šifrování pro vlastní potřebu za pomoci vytvořeného soukromého klíče a také integrita přenášené zprávy.

Pojem elektronický podpis se objevil poprvé v roce 1976 v knize Nové směry v Kryptografii, jejími autory jsou Whitfield Diffie a Martin Hellman, tenkrát pod pojmem digitální podpis. Základní myšlenkou elektronického podpisu byla záměna klasického ručního podpisu, s dodržením podmínky jednoznačného potvrzení identity v prostředí digitálního světa a také nemožnost zfalšování takového podpisu.

Požadované vlastnosti elektronického podpisu:

- identifikace odesílatele
- zaručení integrity
- nemožnost zneužití

Můžeme se také setkat s pojmy obyčejný elektronický podpis nebo zaručený elektronický podpis. Tyto dva pojmy bychom již zaměňovat neměli, jedná se o dvě různé věci. Zaručený elektronický podpis je to samé co si zde popisujeme a je to další slovní ekvivalent k digitálnímu či elektronickému podpisu. V případě mluvení o obyčejném elektronickém podpisu, máme na mysli podpis náš ruční, ale převedený do datové podoby (skenování).

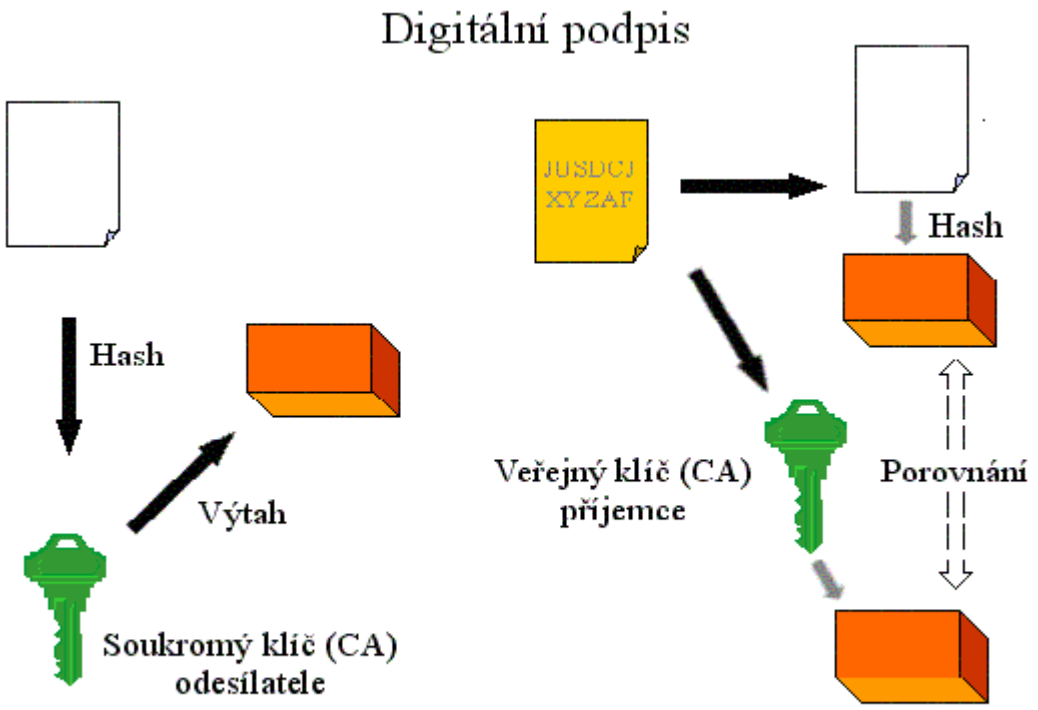
6.2.1. Princip elektronického podpisu

Princip elektronického podpisu spočívá v podepsání daného elektronického dokumentu soukromým klíčem odesílatele, s možností příjemce si za pomoci našeho veřejného klíče zjistit, zda se jedná o pravého odesílatele. Z důvodu velmi složitého a časově náročného podepisování celého dokumentu soukromým klíčem odesílatele se nejdříve vytvoří pomocí jednocestné hashovací funkce tzv. hash neboli otisk a ten potom následně podepíše

Využití hashovací funkce při komunikaci:

1. Odesílatel provede hash dokumentu pomocí svého soukromého klíče pro elektronický podpis.
2. Odesílatel přiloží hash k posílanému dokument a celý zašifruje pomocí veřejného klíče příjemce.
3. Příjemce obdrží zprávu, kterou rozšifruje pomocí svého soukromého klíče a provede hash dokumentu za pomocí veřejného klíče odesílatele a hashe porovná.
4. V případě shody obou otisků má příjemce záruku pravosti dokumentu, v případě neshody se celá akce musí opakovat znova.

Obrázek 10 - Vytvoření elektronického podpisu



Zdroj: [22]

Certifikační autorita – jedná se o nezávislý subjekt, který nám garantuje totožnost majitele soukromého a veřejného klíče. Většinou se jedná o organizaci, u nás například I. certifikační autorita PVT, která získala akreditaci na možnost poskytování certifikačních služeb podle zákona o elektronickém podpisu. Certifikační autorita má za úkol registrace žádostí o certifikace, ověření identity, vydávání a zneplatnění certifikátů.

Digitální certifikát - jedná se o certifikát v digitální podobě, který nám dohromady oficiálně svazuje subjekt s veřejným klíčem subjektu. V certifikátu jsou dále uvedeny identifikační údaje subjektu, sériové číslo certifikátu, doba platnosti, a identifikace certifikační autority, která certifikát vydala. Certifikát je také podepsán soukromým klíčem certifikační autority.

Celý proces používání elektronického podpisu:

1. Odesílatel a příjemce si musí obstarat aplikaci k vytváření a ověřování elektronického podpisu.

2. Odesílatel si vygeneruje za pomoci obstarané aplikace svůj soukromý a veřejný klíč.

3. Veřejný klíč si nechá zaregistrovat u certifikační autority, která si ověří totožnost subjektu a vystaví mu certifikát.

4. Odesílatel za pomoci svého soukromého klíče může podepisovat elektronické dokumenty a příjemce takto podepsaného dokumentu si díky vystavenému certifikátu a veřejného klíče příjemce může ověřit pravost původu.

Z právního hlediska je elektronický podpis blíže formulován hlavně v zákoně o elektronickém podpisu 227/2000 sb.. Elektronický podpis souvisí s ochranou osobních dat, a proto musíme brát v úvahu také další právní předpisy, jako je občanský zákoník, zákon o ochraně osobních údajů a zákon o ochraně spotřebitele. [22]

7. Závěr

Kryptografie je velké a stále se rozvíjející téma, které jsem nemohl a ani mým cílem nebylo v této práci popsat celé. Mým cílem bylo přiblížit toto téma ne jenom lidem, které se v oboru ICT pohybují. V práci jsem shrnul vývin tématu od úplných začátků až do dnešní doby a také směr jakým se tato oblast může dále vyvíjet. Snažil jsem se o vysvětlení základních principů oblasti kryptografie a její dělení podle různých hledisek, poukázání na nedostatky a nesprávnost aplikování principů v některých případech. Dále jsem s přihlédnutím na obor ICT více popsal vybrané používané standardy, protokoly a algoritmy, které používá dnešní kryptografie.

Velkou hrozbu pro kryptografii, jak ji známe dnes nebo alespoň její určité části, vidím již v blízké budoucnosti, kdy je možný příchod kvantových počítačů. Tento příchod by způsobil revoluci v kryptografii a používané šifry. Příchod by měl za následek snadněji dešifrovatelné šifry a to zejména asymetrické šifry, které jsou založeny na velmi složitých matematických výpočtech. S vývojem kvantových počítačů, ale také úzce souvisí vývoj kvantové kryptografie, která je jedna z nejnovějších a nejbezpečnějších kryptografických metod a neustále se vyvíjí.

S kryptologií a všemi oblastmi, kterými se zabývá, se dnes setkáváme téměř na každém kroku, aniž bychom o tom kolikrát věděli. Je to způsobeno dnešním neustále se rychle vyvíjejícím komerčním světem, v kterém je potřeba ochrany osobních či firemních informací nutností. Tento obor, který se rozvíjel již od dávné minulosti, kdy bylo potřeba kryptografie pro zašifrování válečných zpráv, zažil hlavní rozvoj s příchodem techniky a pokročilé matematiky během minulého století. Kryptografie dneška je prvotně zacílena právě na obor ICT, který v dnešní době využíváme pro vzdálenou komunikaci nejvíce a který se stal jedním z hlavních trendů této doby.

8. Literatura

[1] KÁJÍNEK, Milan. Velká epocha: Tajemství šifer - po stopách kryptografie a steganografie I. [on-line]. 2008. [cit. 2011-11-16]. Dostupný z WWW: <http://www.velkaepocha.sk/200806195364/Tajemstvi-sifer-po-stopach-kryptografie-a-steganografie-I.html>.

[2] KÁJÍNEK, Milan. Velká epocha: Tajemství šifer - po stopách kryptografie a steganografie II. [online]. 2008. [cit. 2011-11-16]. Dostupný z WWW: <http://www.velkaepocha.sk/200806265405/Tajemstvi-sifer-po-stopach-kryptografie-a-steganografie-II.html>.

[3] KÁJÍNEK, Milan. Velká epocha: Tajemství šifer - po stopách kryptografie a steganografie III. [on-line]. 2008. [cit. 2011-11-16]. Dostupný z WWW: <http://www.velkaepocha.sk/200807045462/Tajemstvi-Sifer-Po-stopach-Kryptografie-a-Steganografie-III.html>.

[4] KÁJÍNEK, Milan. Velká epocha: Tajemství šifer - po stopách kryptografie a steganografie IV. [on-line]. 2008. [cit. 2011-11-16]. Dostupný z WWW: <http://www.velkaepocha.sk/200807115516/Tajemstvi-sifer-Po-stopach-kryptografie-a-steganografie-IV.html>.

[5] HURAJ, Ladislav. Stručná histórie šifrovania: Dôležité medzníky v histórii kryptografie. [online]. 2003. [cit. 2011-11-16]. Dostupný z WWW: <http://www.fpv.umb.sk/~huraj/historia/historia.html>.

[6] KUČERA, Jan. Enigma. [online]. 2007. [cit. 2011-11-20]. Dostupný z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2007/xpulkrab.htm>.

[7] PINKAVA, Jaroslav. Základy kryptografie I: Kryptografie dneška. [online]. 1998. [cit. 2011-11-20]. Dostupný z WWW: <http://www.crypto-world.info/pinkava/uvod/bulletin1.pdf>.

[8] PIPER, Fred; MURPHY, Sean. Kryptografie. 1. vyd. v českém jazyce. Překlad Pavel Mondschein. Praha: Dokořán, 2006, 157 s. ISBN 80-736-3074-5.

[9] ČERNEK, Rastislav. Klasická kryptografia a jej slabiny: Transpozičné šifry. [online]. 2011. [cit. 2011-12-03]. Dostupný z WWW: <http://kris.uniza.sk/franekova/KB/KB/ref/S3_R2_A.pdf>.

[10] PŘICHYSTAL, Jan. Monoalfabetické substituění šifry. [online]. 2010. [cit. 2011-12-03]. Dostupný z WWW: <https://akela.mendelu.cz/~jprich/predn/substituce.pdf>.

[11] ZLÁMAL, Martin. Kryptologie: Viegenerova šifra. [online]. [cit. 2011-12-04]. Dostupný z WWW: < http://www.zeminem.cz/kryptografie/kryptologie/vigenerova-sifra/>.

[12] BAJEROVÁ, Jana; DITTRICHOVÁ, Lucie; TURBÁKOVÁ, Lucie. KRYPTOLOGIE - UNIVERZITA HRADEC KRÁLOVÉ: Data Encryption System. [online]. [cit. 2011-12-14]. Dostupný z WWW: <http://kryptologie.uhk.cz/5.htm>.

[13] JANECKÝ, Michal. KRYPTOLOGIE - UNIVERZITA HRADEC KRÁLOVÉ: IDEA. [online]. [cit. 2011-12-14]. Dostupný z WWW: <http://kryptologie.uhk.cz/idea_cz.htm>.

[14] KRYPTOLOGIE – UNIVERZITA HRADEC KRÁLOVÉ: AES. [online].

[cit. 2011-12-16]. Dostupný z WWW: <http://kryptologie.uhk.cz/7.htm>.

[15] FRÁŇA, Jan; MIKULECKÝ, Petr; SKALSKÝ Michal. KRYPTOLOGIE - UNIVERZITA HRADEC KRÁLOVÉ: RSA - Popis. [online]. [cit. 2011-12-17]. Dostupný z WWW: <http://kryptologie.uhk.cz/62.htm>.

[16] KLÍMA, Vlastimil; ROSA, Tomáš. Kryptologie pro praxi – schémata ElGamal. [online]. 2004. [cit. 2011-12-21]. Dostupný z WWW: <http://crypto.hyperlink.cz/files/ST_2004_06_16_16.pdf>.

[17] PINKAVA, Jaroslav. Moderní kryptografické algoritmy pro elektronický podpis. [online]. 2000. [cit. 2011-12-28]. Dostupný z WWW: <http://crypto-world.info/pinkava/konference/cack.pdf>.

[18] SSL, SSH. [online]. [cit. 2011-12-29]. Dostupný z WWW: <http://roger.jikos.cz/ssl-ssh.html>.

[19] SSL – Certifikáty: SSL Protokol. [online]. [cit. 2011-12-30]. Dostupný z WWW: <https://www.ssl-certifikaty.cz/o-certifikatech/ssl-protokol/>.

[20] REICHERT, Pavel; ABILOV, Albert; ŠIFTA, Radim. Komunikační technologie: Kvantová kryptografie v optickém přenosovém systému. [online]. [cit. 2012-01-05]. Dostupný z WWW: <http://elektrorevue.cz/cz/download/kvantova-kryptografie-v-optickem-prenosovem-systemu/>.

[21] ŠUMOVÁ, Věra. Elektronický podpis. [online]. [cit. 2012-01-07]. Dostupný z WWW: <http://sandbox.cz/~varvara/El_podpis/index.html>.

[22] BERÁNEK, Marek; LÍPA, Tomáš; PODZIMEK, Ondřej. KRYPTOLOGIE - UNIVERZITA HRADEC KRÁLOVÉ: Elektronický podpis. [online]. [cit. 2012-01-09]. Dostupný z WWW: <http://kryptologie.uhk.cz/54.htm>.

9. Seznam obrázků

10.Seznam tabulek