Kvantová kryptologie

Quantum cryptology

Libor Strnka

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Libor STRNKA**
Osobní číslo:	**A07569**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Kvantová kryptologie**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na téma základních pojmů kryptologie a historického vývoje odvětví.**
2. **Popište základní principy kvantového stavu a Heisenbergova principu neurčitosti.**
3. **Popište základní rozdíly principů klasické a kvantové kryptologie.**
4. **Vytvořte grafický výstup simulující kvantový přenos klíče (QKD).**
5. **Uveďte příklady reálného využití kvantové distribuce klíče.**
6. **Popište další možné využití principů kvantové fyziky v oblasti bezpečnosti.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **SINGH, Simon. Kniha kódů a šifer. Vlastimil Klíma; Michaela Tichá; Petr Koubský, Dita Eckhardtová. 1. Dotisk vyd. Praha : Dokořán, 2007. 382 s. Aliter; sv. 9. ISBN 80-86869-18-7.**
2. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. 1. vyd. Brno : Computer Press, 2004. 190 s. ISBN 80-251-0106-1.**
3. **HAWKING, Stephen. Ilustrovaná teorie všeho. Vít Mrázek; Martin Žofka. 1. vyd. Olomouc : Argo, 2004. 119 s. ISBN 80-7203-575-4**
4. **HAWKING, Stephen. Stručná historie času v obrazech. Štěpán Kovařík; Vladimír Karas. 1. Dotisk vyd. Praha : Argo, 2002. 256 s. ISBN 80-7203-422-7.**
5. **HAWKING, Stephen. Vesmír v kostce. Věra Amelová; Martin Žofka. 1. vyd. Praha : Argo, 2002. 216 s. ISBN 80-7203-421-9.**
6. **PIPER, Fred, MURPHY , Sean. Kryptogrefie : Průvodce pro každého. Pavel Mondschein. 1. vyd. Praha : Dokořán, 2006. 158 s. Průvodce pro každého . ISBN 80-7363-074-5.**
7. **HÁLA, Vojtěch. Kvantová kryptografie. Aldebaran bulletin [online]. 2005, č. 14 [cit. 2010-01-21]. Dostupný z WWW: . ISSN 1214-1674.**

Vedoucí bakalářské práce: **Ing. Roman Šenkeřík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato bakalářská práce je zaměřena na obecný popis principů kvantové kryptologie. Přináší historický přehled vývoje odvětví a jeho provázanost s technickým rozvojem lidské civilizace. Zabývá se současnými kryptologickými metodami, které hrají důležitou bezpečnostní roli v každodenní elektronické komunikaci či obchodování. Teoretická část je zaměřena na základní názvosloví, historický vývoj a obecné principy kvantové fyziky. Praktická část přináší konkrétní příklady využití principů kvantové fyziky v oblasti kryptologie i v oblasti bezpečnosti obecně. Nechybí ani srovnání míry bezpečnostních úrovní jednotlivých metod.

Klíčová slova:

Kryptologie, algoritmus, klíč, binární soustava, kvantová teorie, Heisenbergův princip neurčitosti, polarizace fotonu.

ABSTRACT

This work is aimed at a general description of the principles of quantum cryptology. It provides a historical overview of the development sector and its linkages with the technical development of human civilization. It deals with contemporary cryptological methods, which play an important role in the daily security of electronic communications and commerce. The theoretical part focuses on basic terminology, history and general principles of quantum physics. The practical part provides concrete examples of the principles of quantum physics in the field of cryptology in the field of security in general. There is also a comparison of the security levels of different methods.

Keywords:

Cryptology, algorithm, key, binary system, quantum theory, Heisenberg uncertainty principle, photon polarization.

"V Boha věříme, vše ostatní monitorujeme."

N. S. A.

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.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Přelom prvního a druhého tisíciletí našeho letopočtu bývá označován přechodem věku industriálního do věku informace. Tím se informace dostávají do popředí zájmu, tvoří základní stavební prvek společnosti ve všech jejich sférách a stávají se primárními nositeli hodnot. Tyto atributy vedly ke vzniku potřeby informace chránit před každým, vyjma jejich autora a příjemce.

Snaha utajit existenci zprávy, nebo alespoň utajit význam jejího obsahu, provázejí lidstvo prakticky od těch dob, kdy si člověk osvojil schopnost ukládat informace pomocí písma. Tato dovednost prošla za dobu své existence bohatým vývojem. Od zaznamenávání informací a poznatků pomocí primitivních maleb na stěny jeskyní, tedy obydlí původních obyvatel, přes písma realizována speciálními znaky (hieroglyfy – Egypt, klínové písmo – Asyřané, Babylóňané; některá se zachovala do dnešní doby např. Čína, Japonsko, Vietnam, Korea…), až po písmo, které v současnosti používá většina jazyků, tedy písmo alfabetické jinak řečeno hláskové. Metody záznamu informací takovým způsobem, aby byl jejich faktický obsah srozumitelný pouze tomu, komu jsou určeny, prošly neméně pestrým vývojem, jako umění písma samotné. Tento vývoj probíhal paralelně s technickým rozvojem lidské civilizace.

Práce se zaměřuje na pojem kryptologie v obecné rovině. Nejprve je popsán historický vývoj odvětví. Dále se věnuje rozmachu informačních technologií provázející přelom prvního a druhého tisíciletí našeho letopočtu ve vztahu ke kryptologii. Poté se zaobírá teoretickým popisem principů kvantové fyziky a jejich využití v kryptologii. Součástí je i popis praktického využití kvantových principů v reálném kryptografickém procesu. Závěrečná část poukazuje na očekávaný vývoj v oblasti.

První kapitola se věnuje vyčlenění základních pojmů souvisejících s problematikou kryptologie. Dále je zaměřena na chronologický popis historického vývoje odvětví v závislosti na rozvoji lidské civilizace a jejím technickém rozmachu. Popisuje vlastní důvody vzniku tohoto oboru a technické náležitosti jednotlivých evolučních stupňů kryptologie od dob samotného vzniku písemnictví až po věk, kdy si člověk zcela osvojil prostředky informačních technologií.

Druhá kapitola přináší obecný popis principů kvantové fyziky. Nastiňuje změnu paradigmatu při přechodu z Newtonovské fyziky na fyziku kvantovou. Přibližuje realizaci

principů kvantové fyziky, zejména pak Heisenbergovy relace neurčitosti, v oboru kryptologie.

Třetí kapitola slouží pro srovnání základních mechanismů klasické tzv. konvenční kryptologie a kvantové kryptologie. Je zde poukázáno na bezpečnostní úrovně porovnávaných metod, tím se stane snazším uvědomit si důležitost a rozsáhlost evolučního kroku, kterým bezesporu aplikace kvantových principů do oblasti kryptologie je.

Praktická část této práce obsahuje dílčí ukázky použití kvantové kryptografie. Popsány jsou základní principy jednotlivých protokolů a metod. Detailněji se zaměřuje na konkrétní protokol BB84, který se stal klasickým představitelem využití vlastností kvantové fyziky v oblasti zabezpečeného přenosu dat. Představen je i konkrétní komerční produkt, který funguje na principu kvantové distribuce klíče.

Ve č**tvrté kapitole** je graficky znázorněno schéma kvantového přenosu šifrovacího klíče (tzv. QKD). Toto lze považovat za hlavní stať celé práce, neboť právě na tomto příkladu bude názorně demonstrována bezpečnostní úroveň kvantové kryptologie. Popsány jsou zásadní aspekty protokolu BB84. Jeho odolnost vůči odposlechu včetně pravděpodobnosti odhalení nežádoucích subjektů na komunikační lince.

Závěrečná **pátá kapitola** je zaměřena na reálné využití kvantové kryptologie. Její technickou náročnost a možnosti nasazení této metody v praxi, dále se věnuje predikci vývoje problematiky. Poukazuje na další oblasti bezpečnosti, kde lze elementárních principů kvantové fyziky využívat. Je zde zmínka o projektu tzv. kvantového počítače. Část bude taky věnována popisu konkrétního komerčního produktu, který slouží ke kvantové distribuci klíče.

Závěr sumarizuje docílené poznatky. Cílem práce je přinést komplexní pohled na obor kryptologie. Popsat její historický vývoj, technickou a technologickou evoluci až po nejmodernější metody, které využívají poznatků moderní fyziky. Popis a grafická simulace konkrétního postupu při kvantové distribuci šifrovacího klíče usnadní představu o technických náležitostech nejmodernějších způsobů v oblasti kryptologie.

I. TEORETICKÁ ČÁST

1 VYMEZENÍ ZÁKLADNÍCH POJMŮ A HISTORICKÝ VÝVOJ

1.1 Vymezení základních pojmů

Kryptologie – vědecká disciplína zabývající se převodem informace (nejčastěji textu) do takové podoby, která je srozumitelná pouze se speciální znalostí a zpětným převodem takto upravené informace do podoby srozumitelné komukoliv

Kryptografie – vědní obor spadající pod oblast kryptologie, zabývá se výhradně převodem informací do podoby, která je srozumitelná jen s určitou znalostí; z řeckého *kryptós* (skrytý) a *gráphein* (psát); (tzv. *šifrování*)

Kryptoanalýza - v principu jde o antonymum kryptografie, tedy získávání původního textu z takového, který je převeden do podoby nečitelné bez speciální znalosti; z řeckého *kryptós* (skrytý) a *analýein* (uvolnit, rozvázat); (tzv. *dešifrování*)

Otevřený text – původní podoba informace, její obsah je srozumitelný každému, v literatuře se často užívá pojem *plain text,* s tímto pojmem souvisí i *otevřená abeceda*, což je sada znaků otevřeného textu

Šifrový text – informace převedené do podoby, která je srozumitelná pouze se speciální znalostí, s tímto pojmem souvisí i *šifrová abeceda*, neboli sada znaků zašifrovaného textu

Algoritmus – přesný návod nebo postup použité kryptografické metody

Klíč – detailní nebo upřesňující použití algoritmu

Steganografie – nauka o ukrytí samotné existence informace (nejčastěji zprávy v podobě textu), nedochází k žádné transformaci do podoby srozumitelné jen se speciální znalostí, objevením informace je k dispozici i její obsah bez nutnosti provést kryptoanalýzu; z řeckého *steganós* (schovaný) a *gráphein* (psát)

Alice, Bob, Eva – všeobecně přijaté označení účastníků komunikačního procesu, Alice a Bob symbolizují dvě komunikující strany, Eva zastupuje roli narušitele utajené komunikaci a snaží se o odposlech této komunikace

1.2 Historický vývoj kryptologie

1.2.1 Nejstarší zmínky

Potřeba utajit samotnou existenci zprávy (informaci) nebo její obsah provází lidstvo prakticky od samotného počátku písemnictví. Vědní disciplíny, které se touto činností zabývají, prodělaly za dobu své existence patřičné změny. Tyto transformace se děly převážně v paralele s technickým rozmachem lidské civilizace.

Důvody vzniku a rozvoje kryptologie byly převážně politického nebo vojenského charakteru. Kryptologie hrála a hraje důležitou roli v historii.

Nejstarší zmínky o používání utajené komunikace sahají až do roku 1900 př. n. l. do starého Egypta, kde se užívala **speciální sada hieroglyfů**, které byly srozumitelné jen úzké skupině předem obeznámených lidí, k nimž se měly informace dostat.

Za jeden z prvních konkrétních případů užití kryptologické metody lze považovat příběh řeckého vyhnance **Demarata**, který kolem roku 490 př. n. l. i přes své vyhnanství z Řecka do Persie cítil povinnost informovat domovinu o chystaném útoku perského krále **Xerexe**, který si chtěl podmanit vzpurnou Spartu a Atény. Zpráva upozorňující na tuto skutečnost byla zaznamenána na dřevěnou psací destičku, pod vrstvu vosku, která sloužila právě pro psaní textů. Tímto se destička jevila nepoužitá a bez jakéhokoliv náznaku podezření u stráží mohla být převezena z Persie až do Řecka. Tam byla zpráva odhalena a plánovanou expanzi Peršanů do Řecka se tímto podařilo odvrátit. Způsob popsaný v tomto příkladu spadá do oblasti **steganografie.**

Je tedy zjevné, že v počátcích kryptologie se užívalo převážně metod, které měly za účel ukrýt samotnou existenci zprávy. Způsobů realizace steganografie bylo nesčetně.

Užití steganografie znamenalo však poměrně nízkou bezpečnostní úroveň a časovou náročnost. Na řadu přišla **kryptografie**, tedy metoda utajení obsahu zprávy ne jejím fyzickým ukrytím, ale převedením zprávy do takové podoby, která byla srozumitelná jen se speciální znalostí, kterou disponoval pouze příjemce této zprávy a její adresát.

V mnoha případech docházelo ke kombinaci steganografie a kryptografie, čímž se bezpečnostní úroveň přenosu informace značně zvýšila. Příkladem může být užívání tzv.

mikroteček. Šlo o metodu, kdy byla zpráva zašifrována pomocí kryptografické metody a poté na fotografickém materiálu zmenšena do rozměru tečky v běžném textu. Takto upravena byla vlepena např. na dopisní papír na místo skutečné tečky ukončující nějaký úsek textu [1].

1.2.2 Transpozice a substituce

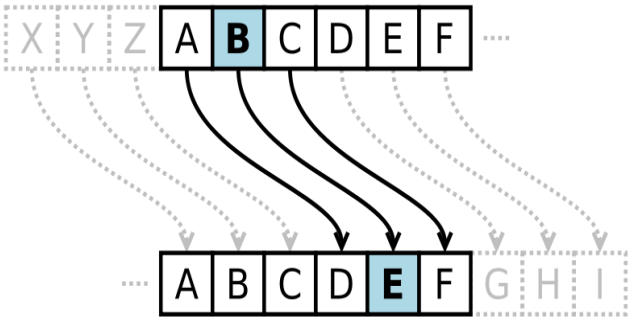
Jedním ze základních dělení kryptografie je dělení na **transpoziční** a **substituční** šifrování. První zmíněná metoda využívá k převodu textu zprávy do nesrozumitelné podoby posunu jednotlivých znaků otevřeného textu (tzv. otevřené abecedy) o předem dohodnutý počet znaků. V tomto případě je posun znaků otevřeného textu **algoritmem** a počet znaků, o který je posun realizován, je **klíčem** metody.

Zdárným příkladem použití transpoziční šifry je **Scytale ze Sparty.** Metoda spočívala v zapsání původní zprávy na proužek kůže, který byl omotán kolem tyče s předem dohodnutým průměrem. Tyč se stejným průměrem vlastnil jak odesilatel, tak příjemce zprávy. Po sepsání textu se proužek sejmul a nejčastěji omotán kolem pasu nositele (simulace koženého pásku – steganografie) byl doručen příjemci. Ten jej namotal na tyč se shodným průměrem a tím se pro něj zpráva stala čitelnou.

Obrázek 1 Scytale ze Sparty

Metoda transpozice se však postupem času stala z bezpečnostního hlediska naprosto nedostačující a tak přišla na řadu šifra substituční. Základem této metody je, jak již z názvu vyplývá substituce neboli náhrada. Každý znak otevřeného textu, byl nahrazen jiným znakem šifrového textu. Algoritmem je v tomto případě náhrada jednoho znaku otevřené abecedy za jiný znak šifrové abecedy. Klíčem je detailní postup, na jehož základě k nahrazení znaků dojde.

Nejznámějším příkladem substituční šifry je **Caesarova šifra**. Její princip spočíval ve vytvoření šifrové abecedy, která vznikla posunem otevřené abecedy o 3 znaky. Na obr. 2 představuje horní řádek znaky otevřené abecedy a spodní řádek představuje znaky šifrové abecedy. Jednotlivé šipky dokreslují náhradu (substituci) mezi oběma abecedami.



Obrázek 2 Caesarova šifra

(zdroj: www.cs.wikipedia.org)

Posun o tři písmena se po čase používání pochopitelně dostal do podvědomí těch, kteří chtěli nečitelný obsah zpráv rozluštit. Tím byla její bezpečnostní úroveň výrazně degradována.

Algoritmus substituční šifry však lze aplikovat i za použití jiného klíče, než jakým je posun právě o tři znaky. Začalo se tedy užívat **klíčových slov**[1] a **klíčových frází**[2]. Obvykle se volilo slovo či fráze takového rázu, aby bylo snadno zapamatovatelné jak pro odesilatele, tak pro příjemce. Pomocí těchto klíčů se bezpečnostní úroveň substituční šifry značně zvýšila. Použitím klasické Caesarovy šifry je možné zašifrovat otevřený text pouhými 25ti způsoby (to plyne z počtu znaků anglické abecedy, tedy 26, každý znak je tedy možno posunou právě o 25 znaků).

[1] Klíčové slovo je takové, které plní roli klíče upřesňující použití algoritmu substituční šifry

[2] Klíčová fráze je taková, která plní roli klíče upřesňující použití algoritmu substituční šifry

Pokud ovšem použije odesilatel obecnější substituční algoritmus, tedy nahradí-li každý znak otevřené abecedy znakem šifrové abecedy za užití klíčového slova nebo fráze, pak se počet možných způsobů šifrování zvýší na $4*10^{26}$ (tedy 400 kvandriliónů šifrových abeced!!). Jak je vidět v tabulce č. 1, horní řádek tvoří otevřená abeceda a spodní řádek abeceda šifrová. Ta vznikla za použití klíčového slova Julius Ceasar. Znaky šifrové abecedy v klíčovém slovu nebo frázi se neopakují a mezery se vypouští. Po vepsání klíčového slova nebo fráze do řádku určeného šifrové abecedě následuje zbytek otevřené abecedy v pořadí za posledním znakem klíčového slova nebo fáze a to již bez těch znaků, které byly použity v klíčovém slovu nebo frázi.

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

Tabulka 1 Jednoduchá substituční šifra

Otevřený text **kleopatra** by se zašifrováním pomocí uvedené tabulky 1 změnil na **vwszbjhfj.** Obecný substituční algoritmus se na dlouhá staletí stal dostatečně silným šifrovacím prostředkem. Výše popsaná substituční metoda za užití klíčového slova nebo fráze se řadí do skupiny tzv. **monoalfabetických substitučních šifer**[3]. Tato kryptografická technika byla vzhledem k technické vyspělosti lidstva v prvním tisíciletí n. l. naprosto dostačující. Užitím kryptoanalytické metody **brute force**[4] by luštitel k nalezení správného klíče a tím i otevřeného textu potřeboval dobu nesčetněkrát delší, než je odhadované stáří vesmíru [1].

1.2.3 Kryptoanalýza

Poslední čtvrtina prvního tisíciletí n. l. je považována za zlatý věk islámské civilizace. V té době se oblasti středního východu staly centrem obchodu a vzdělanosti. Tamější učenci se zaobírali detailním studiem pravosti obsahu náboženských textů, Koránu nevyjímaje. Při těchto činnostech si začali všímat určitých gramatických zákonitostí. Zjistili, že v dostatečně dlouhém textu je možno vysledovat různé pravidelnosti a výskyt

[3] Šifrování probíhá za užití jediné šifrové abecedy pro celý otevřený text

[4] Řešení hrubou silou, systematicky se zkouší každá myslitelná varianta, nevýhodou je časová náročnost

jednotlivých znaků se různí v závislosti na použitém jazyku. K těmto závěrům bylo možno dospět až za předpokladu dosažení určité úrovně vědomostí z oblasti statistiky, matematiky a lingvistiky.

To vše dalo vzniknout silnému kryptoanalytickému nástroji, který se nazývá **frekvenční analýza**[5]. Pomocí této metody bylo tedy možno obejít nereálnou analýzu prostřednictvím brute force a tím znatelně oslabit dosud neotřesitelnou bezpečnostní úroveň monoalfabetické substituční šifry. Proces frekvenční analýzy spočívá v porovnání percentuálních výskytů znaků otevřené abecedy konkrétního jazyka se znaky šifrového textu. Porovnáním obou hodnot je možné vyvodit, kterému znaku otevřené abecedy odpovídá konkrétní znak šifrového textu (viz tabulka 2) [1].

% VÝSKYT ZNAKŮ ANGLICKÉHO JAZYKA			
ZNAK	**%**	**ZNAK**	**%**
A	8,6	N	6,8
B	1,7	O	8,0
C	3,3	P	3,2
D	3,6	Q	0,0
E	10,5	R	4,9
F	0,2	S	6,3
G	0,2	T	5,1
H	2,2	U	4,0
I	7,5	V	4,3
J	2,2	W	0,0
K	3,6	X	0,1
L	4,2	Y	2,8
M	3,5	Z	3,2

Tabulka 2 Percentuální výskyt znaků anglického jazyka (zdroj: techpiece.wordpress.com)

[5] Metoda, která sleduje četnost výskytu znaků šifrového textu

1.2.4 Renesance odvětví v Evropě

Přelom 13. a 14. století n. l. znamená znovuoživení oboru kryptologie v Evropě. Centrem dění se stala Itálie, zejména pak Vatikán. Florentský polyhistor **Leon Battista Alberti** si zahrával s myšlenkou užít dvou šifrových abeced, čímž by se značně ztížila možnost úspěšného užití frekvenční analýzy.

Celou myšlenku dotáhl do finální podoby až francouzský diplomat **Blaise de Vigenére**. Ten přišel s návrhem použít hned 26 šifrových abeced. Tedy pro zašifrování každého ze znaků otevřené abecedy použít samostatnou šifrovou abecedu. Každá z 26ti šifrových abeced byla vůči předchozí posunuta právě o jeden znak (tabulka 3). Tento způsob se nazývá **polyalfabetická substituční 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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Tabulka 3 Vigenérův čtverec (zdroj: www.jifox.cz)

Pro názornost uvádím příklad zašifrování textu: JAN ANTONIN BATA pomocí klíčové fráze: SVEC ZE ZLINA.

OTEVŘENÝ TEXT	J	A	N	A	N	T	O	N	I	N	B	A	T	A
KLÍČOVÁ FRÁZE	S	V	E	C	Z	E	Z	L	I	N	A	S	V	E
ŠIFROVÝ TEXT	B	V	R	C	M	X	N	Y	Q	A	B	S	O	E

Tabulka 4 Schéma šifrování Vigenérovou šifrou

Postup je následující: První řádek tabulky tvoří otevřený text, druhý řádek tvoří klíčová fráze, pokud nemá shodný počet znaků s otevřeným textem, pak se klíčová fráze opakuje až po dosažení shodnosti počtu znaků.

První znak otevřeného textu, tedy písmeno J bude zašifrováno pomocí prvního znaku klíčové fráze, tedy písmene S. Ve Vigenérově čtverci (tabulka 3) je znak S roven 18. řádku. Je tedy nutno najít průsečík 18. řádku se sloupcem, který je označen tím znakem, jež chceme zašifrovat, tedy znakem J. Tabulka 3 jasně naznačuje, že tímto průsečíkem je znak B a to je první znak šifrového textu. Tímto způsobem se pokračuje znak po znaku otevřeného textu, až je celý zašifrovaný.

Tento příklad názorně demonstruje sílu polyalfabetické substituční šifry. Za pozornost stojí zejména znaky A a N z otevřeného textu. Za předpokladu užití monoalfabetické substituční šifry by právě tyto znaky byly velmi silným vodítkem pro aplikaci frekvenční analýzy. V případě Vigenérovy šifry jsou však všechna A i N zašifrována pomocí různých šifrových abeced a tím pádem se zašifrují pod různé znaky šifrového textu. Kryptoanalýza se tímto ocitla ve značné nevýhodě [1].

1.2.5 Le chiffre indechiffrable?!

Zavedením Vigenérovy šifry nastala pro luštitele šifer úmorná práce spojená s hledáním skulinky, kterou by mohli tuto metody prolomit. Podařilo se to britskému vynálezci jménem **Charles Babbage.** Ten si u šifrového textu povšimnul opakování určitých sekvencí, které mohlo vzniknout pouze tak, že shodné sekvence otevřeného textu byly zašifrovány stejnou části klíčového slova nebo fráze. Vypsal tedy všechny opakující se sekvence šifrového textu. Spočítal, v jakých intervalech se opakují a nalezením společného celočíselného dělitele těchto intervalů určil délku klíčového slova popř. fráze, šlo o tzv. **Kasiskiho test.**

Podle počtu znaků klíčového slova rozdělil šifrový text na stejný počet sekvencí, ty pak podrobil klasické frekvenční analýze, jež se provádí u monoalfabetické substituční šifry. Tímto postupem byl schopen určit posun konkrétní sekvence textu a tím i znak klíčového slova. Po získání všech znaků klíčového slova či fráze byla Vigenérova šifra, ač považována za neprolomitelnou, pokořena [1].

1.2.6 Průmyslová revoluce

V 18. století začal věk industrializace a tento trend se nevyhnul ani odvětví kryptologie. V této době rozvoje technických prostředků se monoalfabetická šifra stává nedostatečnou z hlediska bezpečnosti. Až nyní, téměř 200 let po svém vzniku, přichází na slovo Vigenérova šifra.

V roce 1854 přišel Samuel Morse se zcela novým způsobem komunikace prostřednictvím elektrického telegrafu. Tento vynálezce přišel i s novou abecedou, která byla určena právě pro komunikace prostřednictvím telegrafu. **Morseova abeceda** však není šifrovací metodou. Jedná se o způsob **kódování.** [6] Zde jsou znaky abecedy převedeny do sekvencí dlouhých a krátkých signálů, což je pro přenos za použití elektrického telegrafu praktičtější.

MORSEOVA ABECEDA							
A	.-	M	--	Y	-.--	6	-....
B	-...	N	-.	Z	--..	7	--...
C	-.-.	O	---	Ä	.-.-	8	---..
D	-..	P	.--.	Ö	---.	9	----.
E	.	Q	--.-	Ü	..--	.	.-.-.-
F	..-.	R	.-.	Ch	----	,	--..--
G	--.	S	...	0	-----	?	..--..
H	....	T	-	1	.----	!	..--.
I	..	U	..-	2	..---	:	---...
J	.---	V	...-	3	...--	"	.-..-.
K	-.-	W	.--	4	....-	´	.----.
L	.-..	X	-..-	5	.....	=	-...-

Tabulka 5 Morseova abeceda (zdroj: www.cs.wikipedia.org)

[6] Převod znaků určité skupiny do jiné, která je srozumitelná a zpracovatelná určitým zařízením. Zde není nutná žádná speciální znalost.

Playfairova šifra je typickým příkladem kryptologické metody v období průmyslové revoluce. Ta spočívá v rozdělení textu na **digrafy**[7]. Dále následuje vytvoření speciální tabulky o rozměrech 5x5 znaků (anglická abeceda jich má 26, ale znak J, tedy nejmíň častý znak anglické abecedy, se přidružuje ke znaku I). Tato tabulka začíná znaky klíčového slova, poté je doplněna o zbylé znaky abecedy s vynecháním těch, které byly použity pro klíčové slovo. Proces šifrování probíhá tak, že se nejprve určí jedno ze tří pravidel určené podle vzájemné polohy obou znaků digrafu v tabulce.

- pokud se znaky digrafu nachází ve stejném řádku, slouží pro šifrování znaky nacházející se vpravo od nich, nachází-li se znak v posledním sloupci tabulky, pak se užije znaku z prvního sloupce
- pokud se znaky digrafu nachází ve stejném sloupci, slouží pro šifrování znaky nacházející se pod každým z nich, nachází-li se znak v posledním řádku tabulky, pak se užije znaku z prvního řádku
- pokud neplatí ani jedna z výše uvedených možností, tak pro zašifrování prvního znaku digrafu poslouží ten znak, který leží v průsečíku řádku v němž se první znak digrafu nachází a sloupce v němž se nachází druhý znak digrafu, pro zašifrování druhého znaku digrafu se užije stejné metody, jako pro znak první (tabulka 6)

V příkladu naznačím zašifrování textu JAN ANTONIN BATA pomocí Playfairovy šifry a to za použití klíčového slova SVEC. Nejprve rozdělím otevřený text na digrafy:

IA-NA-NT-ON-IN-BA-TA

Poté je sestavena tabulka (tabulka 6), která bude obsahovat klíčové slovo SVEC:

[7] Digraf = dvojice písmen

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

Tabulka 6 Playfairova šifra

První digraf IA nemá společný sloupec ani řádek, proto je potřeba aplikovat třetí pravidlo. Řádek, na němž se nachází první znak digrafu otevřeného textu, tedy I má průsečík se sloupcem, v němž se nachází druhý znak digrafu, ve znaku N. Druhému znaku digrafu ten samý postup přisoudí znak S. Znamená to tedy, že digraf IA bude zašifrován do NS. Tímto způsobem se zašifrují i zbylé digrafy otevřeného textu.

Pro úplnost je naznačeno šifrování druhého digrafu otevřeného textu NA. Zde lze realizovat druhé pravidlo, tedy to o společném sloupci. Tento digraf bude mít po zašifrování podobu TH.

Výše uvedený příklad bude v zašifrované podobě vypadat následovně:

NS-TH-TZ-TI-KI-HS-ZH

Dešifrování zprávy spočívá v přesně opačném postupu, který je popsán výše. U této kryptologické metody je důležitá znalost klíčového slova na straně odesilatele i na straně příjemce.

Šifrovací metoda, která byla stvořena takříkajíc na míru přenosu informací pomocí Morseovy abecedy je **šifra ADFGVX**[8]**.** Jde o kombinaci substituční i transpoziční šifry. Postup určitým způsobem připomíná šifru Play-fair.

[8] Název této metody je tvořen znaky, které jsou pro přehlednost v Morseově abecedě hodně odlišné a eliminují tím možnost vzniku chyb při přenosu zprávy

1.2.7 Vrchol polyalfabetické substituční šifry

Jediná kryptografická metoda, o které bylo exaktně[9] dokázáno, že je nerozluštitelná a tím pádem maximálně bezpečná, je tzv. **jednorázová tabulková šifra** (angl. one-time pad cipher).

Podle Gilberta Vernama, který si tento způsob nechal v roce 1917 patentovat se někdy nazývá: **Vernamova šifra.**

Předpokladem maximální bezpečnostní úrovně jsou následující 3 kritéria:

- **klíč je stejně dlouhý jako otevřený text**
- **klíč je generován zcela náhodně**
- **klíč smí být použit pouze jednou**

Za dodržení výše uvedených podmínek spočívá bezpečnostní síla šifry v tom, že neexistuje jakákoliv matematická či logická spojitost mezi klíčem a otevřeným textem. Tím pádem neexistuje jakákoliv spojitost mezi otevřeným textem a šifrovým textem!

Například otevřený text o 21 znacích dává možnost vzniku $5*10^{29}$ stejně dlouhých klíčů a tím pádem i totožnému množství podob šifrového textu. Čistě teoretické použití brute force metody by v tomto případě nabídlo luštiteli všechny myslitelné zprávy o délce 21 znaků. Je tedy zřejmé, že pro získání faktického obsahu zprávy je tato překážka naprosto fatální. Pravost jednoho z mnoha získaných textů by mohla potvrdit jenom ta skutečnost, kdyby bylo užito klíče, který sám dává faktický smysl. To je však velmi nebezpečná forma stereotypu a při tvorbě klíče je nutno se takovému postupu vyhnout.

Samotné generování klíče je u one-time pad šifry technicky velmi náročné a pro tuto činnost je potřeba využít nejmodernějších prostředků, mezi které lze zařadit **Geigerův počítač**[10], který je schopen generovat naprosto náhodná čísla pomocí monitorování emise radioaktivity.

---

[9] C. E. Shannon podal exaktní důkaz v roce 1949

[10] Johannes Wilhel Geiger, německý fyzik, spolutvůrce Geiger-Müllerova počítače pro zjišťování množství radioaktivity

One-time pad šifra není ničím jiným, než klasickou Vigenérovou šifrou generovanou klíčem za výše uvedených podmínek [1].

1.2.8 Mechanizace kryptologie - Enigma

Za nejznámější kryptologické zařízení všech dob lze bez obav označit to, za jehož zrozením stál **Arthur Scherbius**. Tento německý vynálezce ve spolupráci se svým přítelem Richardem Ritterem sestrojil mechanizovanou a sofistikovanější variantu **Albertiho šifrovacího disku**[11], což přes nejrůznější modifikace vedlo ke konstrukci velmi důmyslného, mechatronického zařízení pro šifrování textu, které neslo pojmenování **Enigma**.

Princip Enigmy spočívá v tzv. **scramblerech.** Jde o pryžové kotouče, které jsou na plochých stranách opatřeny galvanickými kontakty, vnitřek kotouče ukrývá specifické uspořádání vodičů, které propojují vždy jeden vstup a jeden výstup (kontakt). Toto propojení je součástí výrobního tajemství scrambleru a hraje důležitou roli ve vztahu ke kryptologické funkčnosti celého zařízení.

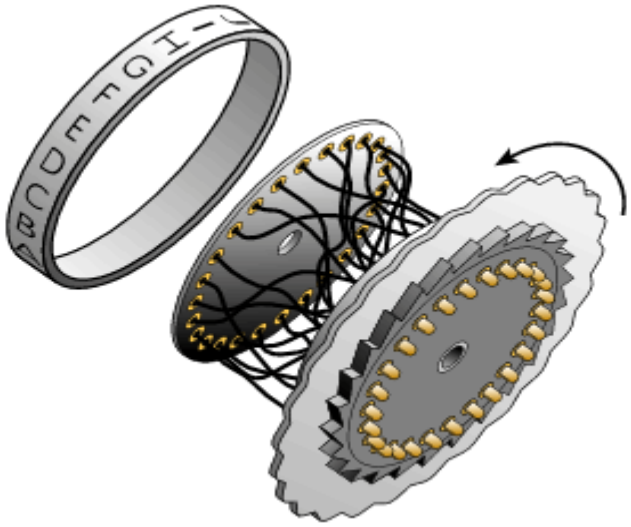
Vývoj zařízení byl poměrně rozmanitý až do jeho nasazení v armádě (1925). Vznikly různé modifikace, které se lišily svým určením (banky, průmyslové společnosti, armáda) na němž závisela i bezpečnostní úroveň každé varianty. Logicky se nejbezpečnější model používal právě v armádě. Ovšem i tento byl dále rozlišen pro konkrétní určení (např. varianta pro námořnictvo byla propracovanější než ta pro pozemní vojska).

Základem zařízení je **vstupní klávesnice**, která sloužila pro vkládání znaků otevřeného textu. Tyto znaky byly poté zašifrovány pomocí **scramblerů** a **propojovací desky**. Výsledný znak šifrové abecedy byl signalizován v horní části otevřeného víka zařízení. Enigma připomínala psací stroj. Od něj se lišila v zásadě tím, že po zmáčknutí klávesy nedojde k zachycení tohoto znaku skrze barevnou pásku na papír. Zadaný znak je převeden do šifrové podoby a následně signalizován obsluze na panelu.

---

[11] Prostředek pro transpoziční šifru, otevřená abeceda je na vnějším okraji, šifrová abeceda je na vnitřním. Klíčem této šifry je počáteční posun obou kruhů vůči sobě.

Nyní se zaměřím na samotné srdce Enigmy, scrambler. Jak bylo uvedeno výše, jde o pryžový kotouč, který ukrývá předem stanovené galvanické propojení vstupních a výstupních kontaktů, které jsou osazeny po obou stranách tohoto kotouče (obr. 3).



Obrázek 3 Scrambler

(zdroj: www.cryptomuseum.com)

Kontakty umístěné na stranách jednotlivých scramblerů sloužily k tomu, aby bylo možno uzavřít elektrický obvod.

Šifrování probíhalo obdobně, jako psaní na běžném psacím stroji. Obsluha zadala znak otevřeného textu a elektrický proud, který probíhal skrze složité zapojení scramblerů, generoval znak šifrového textu.

Proces dešifrování probíhal analogicky, tzn. příjemce nejprve obdržel zašifrovanou zprávu. Jednotlivé znaky této zprávy vkládal pomocí vstupní klávesnice, načež mu signalizační panel zobrazoval znaky původního, otevřeného textu.

Bezpečnostní úroveň každého šifrovacího zařízení tvoří mnoho aspektů, nejdůležitějším je však počet možných kombinací, které je zařízení schopno generovat

Než začala obsluha Enigmy se samotným šifrováním, bylo nutno provést nastavení přístroje. To se dělo na základě údajů **kódové knihy**. Distribuce knihy kódů pro každý den zvlášť by sebou nesla řadu logistických problémů, delší interval by naopak znamenal vyšší bezpečnostní riziko pro tento veledůležitý prvek celého systému.

Kniha kódů stanovovala detailní nastavení pro každý den, jež se týkalo třech bodů:

- pořadí scramblerů v přístroji (123, 132, 213, 231, 312, 32) = **6**
- počáteční natočení scramblerů (26x26x26) = 26^3 = **17 576**
- nastavení propojovací desky (viz níže)
- celkem **105 456**

Uvedená čísla značí počet možných počátečních nastavení Enigmy. V případě pořadí jednotlivých scramblerů je k dispozici 6 možností, co se natočení scramblerů týče, pak je možno toto provést na 17576 způsobů, pokud se obě čísla vynásobí, je počet možných nastavení roven **105 456**.

Rozšiřujícím prvkem se stala **propojovací deska.**, Ta propojovala galvanické vedení jednotlivých kláves vstupní klávesnice mezi sebou. Pokud například na propojovací desce došlo k propojení znaku A a B, pak po stisknutí klávesy A má elektrický obvod takovou podobu, která by vznikla stisknutím klávesy B, to samé platí naopak. Jednodušeji řečeno, propojovací deska prohodila jednu klávesu za druhou. Celkem bylo možno propojit 6 párů znaků vstupní klávesnice. Toto propojení bylo součástí **knihy kódů.** Propojovací deska tedy přispěla k celkovému počtu možných nastavení číslem **100 391 791 500.**

Uvedený počet možných nastavení Enigmy vzrostl použitím propojovací desky z původních **105 456** na **10 000 000 000 000 000** tedy **$1{,}0 * 10^{16}$** (t. j. 1 peta kombinace = biliarda = milion miliard). Pro kryptoanalytiky, kteří by chtěli rozluštit zprávy šifrované pomocí Enigmy, nastal skutečný problém.

Němci samotní vycházeli z předpokladu, že nepřítel má přístroj k dispozici. To jednoznačně potvrzovalo, že **bezpečnostní úroveň nespočívá v utajení přístroje, ale v utajení jeho počátečního nastavení.**

Díky špionážním praktikám neloajálního němce Hanse-Thila Schmidta, se tajné dokumenty týkající se technických detailů Enigmy dostaly do rukou francouzské zpravodajské službě a následně do Polska, do Biuro Szyfrow. Mimo jiné obsahovaly tyto dokumenty i detailní popis kódových knih (logicky však neobsahovaly obsah těchto knih, který byl každé 4 týdny jiný). Dále z nich bylo možné částečně vyvodit vnitřní zapojení scramblerů.

Nejvýznamnější postavou v boji s Enigmou se stal **Marian Rejewski**. Ten využil svých matematických dovedností a na základě určitých kryptografických stereotypů ze strany obsluhy Eingmy dokázal sestrojit zařízení, tzv. **Bomby**, které pomáhali polským kryptoanalytikům číst tajnou komunikaci Němců.

Rejewski dokázal využít opakování klíčů, které byly na začátku každé vysílané zprávy. Podařilo se mu oddělit problém počtu možných nastavení propojovací desky a scramblerů, což snížilo počet celkových možných konfigurací přístroje o několik řádů.

V roce 1938 však došlo ke zvýšení bezpečnostní úrovně Enigmy a přibyly další 2 scramblery. Současně se používaly stále jenom 3, ale počet možných uspořádání scramblerů vzrostl z 6 na 60. Do této situace bylo nutno používat 6 paralelně zapojených bomb pro generování způsobu nastavení. Zvýšením počtu možných uspořádání scramblerů na desetinásobek bylo z technických a finančních důvodů vyloučeno sestavit takový stroj, který by byl i přes tento nárůst schopen nadále pracovat. Situace se pro polské kryptoanalytiky zhoršila navíc tím, že počet kabelů na propojovací desce vzrostl z 6 na 10. Počet možných klíčů tímto vzrostl ze současných $1{,}0*10^{16}$ na $1{,}59*10^{20}$.

Těsně před začátkem druhé světové války předali Poláci svoje znalosti Britům. Ti navázali na práci polské kryptoanalytické elity. Nejznámějším pokračovatelem Rejewskeho práce se stal **Alan Turing**. Ten vedl svůj boj s již vylepšenou Enigmou obdobným způsobem, jenom využil jiné kryptografické slabiny, která se netýkala opakování klíče na začátku zprávy, ale opakování určitých slov v závislosti na čase, kdy byla zpráva vysílána. Například ráno zprávy začínaly nejčastěji informacemi o počasí. To ho vedlo k sestrojení mechanismu podobného Bombám.

Boj s Enigmou se zapsal do dějin kryptologie i tím, že centrem pozornosti kryptoanalytiků se nestal samotný princip zařízení (algoritmus), ale nedokonalosti a neúplnosti, ke kterým docházelo při samotném používání zařízení. Zmíněné příklady jasně deklarují lidský faktor, co by nejslabší článek. Podobný způsob boje se šifrou se uplatňuje i v současnosti, tedy v 21. století [1].

1.2.9 Problém distribuce klíče (symetrická, asymetrická kryptologie)

Autorem zařízení, které lze označit za první programovatelný počítač, je anglický matematik s německým původem **Max Newman**. Ten navázal na myšlenky Alana Turinga

a sestrojil zařízení, jehož jádro tvořilo 1500 elektronek. Ty byly o poznání rychlejší, než elektro-mechanická relé, která tvořila základ Turingových **Bomb**. Newmanův počítač nesl název **Colossus**.

Používání počítačů, co by prostředků kryptologie, se sebou neslo tři výhody oproti klasickým metodám:

- počítač nebyl limitován konstrukčními vlastnostmi
- rychlost výpočtů
- práce s binárními čísly

Tyto přednosti umožňovaly velmi rychlé rozšíření počítačů, jako prostředků pro tvorbu dokonalejších šifer a zároveň útoků na ně. Bylo možno sestrojit takový počítač, který simuloval práci Enigmy s padesáti scramblery, z nichž každý měnil svoji polohu podle požadavku autora. To by byl v případě mechanického sestrojení takové modifikace Enigmy velmi obtížně řešitelný problém.

Ve výčtu výhod počítačové formy kryptologie stojí zmínka o práci s binárními čísly. To znamená, že znaky otevřeného textu jsou nejprve převedeny do dvojkové (binární) soustavy na základě různých protokolů, nejčastěji jde o kódování pomocí **ASCII**[12]**.**

Principy šifrování zůstávají nezměněny. Převod do dvojkové (binární) soustavy je velmi vhodný. Znaky vyjádřené kombinacemi dvou hodnot 0 a 1 jsou přijatelnější pro zařízení, které své elektronické obvody mění dle potřeby na:

- sepnuto = proud prochází = (1)
- nesepnuto = proud neprochází = (0)

Pro názornost uvedu příklad šifrování otevřeného textu BATA pomocí triviální transpozice, ovšem realizované v binární soustavě. Tabulka 7 obsahuje zápis otevřeného textu (OT) a převod do šifrového textu (ŠT). Výsledné znaky závisí na použitém kódování!

[12] Norma, která určuje každému znaku unikátní číselnou hodnotu. Původně 127 (7bit) znaků, pro jazyky, které používají znaky s diakritikou došlo k rozšíření na 255 (8bit) znakovou verzi. Pro potřeby konkrétních jazykových mutaci je použito kódování, které vrchním 128 znakům přiřadí znaky požadované příslušným jazykem.

Algoritmem takové šifry je výměna pozic jednotlivých bitů otevřeného textu. Klíčem je výměna dvou sousedících bitů. Tímto je možné provádět transpozici uvnitř samotného písmene, navíc je možné prohodit bity dvou sousedících znaků OT.

OT	B	A	T	A
OT binární zápis	01000010	01000001	01010100	01000001
Transpozice (prohození) dvou sousedících znaků 1-2, 3-4, 5-6				
ŠT binární zápis	10000001	10000010	10101000	10000010
ŠT dekadický zápis	129	130	168	130
ŠT ASCII znak	ü	é	Ę	é

Tabulka 7 Ukázka binární transpozice otevřeného textu BATA

Lze použít i počítačovou modifikaci substitučních šifer. Otevřený text převedený do binární soustavy a klíčové slovo nebo fráze taktéž převedené do dvojkové soustavy se sečtou prostřednictvím **exkluzivní disjunkce**[13]**.**

XOR ⊕	VSTUP	
	X	Y
0	0	0
1	0	1
1	1	0
0	1	1

Tabulka 8 Pravdivostní tabulka XOR

(exkluzivní disjunkce)

[13] Logická operace jejíž hodnota je pravda (1) tehdy, kdy se vstupní hodnoty shodují (0+0 nebo 1+1). V opačných případech je její hodnota nepravda (0).

Z počátku bylo použití výpočetní techniky k účelům kryptologie umožněno pouze tomu, kdo je vlastnil, tedy armáda nebo státní aparát.

Na přelomu 40. a 50. let spatřil světlo světa **tranzistor**[14]**.** V této době došlo k prvním komerčním nasazením počítačů. Počátkem padesátých let vyvinula firma IBM svůj první počítač a v té době byl vyvinut i první programovací jazyk. V roce 1959 byl vyroben první **integrovaný obvod**[15].

V roce 1973 Americký standardizační úřad vyzval o návrhy šifrovacího systému, který bude přijat za standard. V úvahu připadal systém **Lucifer**. Jeho autorem je německý emigrant pracující později pro IBM, **Horst Feistl**. Jeho původní verze, která pracovala s bloky otevřeného textu o délce 128 bitů, nebyla přijata na popud **NSA**[16] z důvodu vysoké bezpečnostní úrovně celého systému. NSA se zasadila o snížení množství použitelných klíčů pro tento systém, který byl stanoven na 56. V roce 1976 byla tedy oficiálně přijata 56-bitová verze kryptologického systému Lucifer a pojmenována **DES.**[17] Na konci 90. let byla bezpečnostní úroveň tohoto systému značně oslabena a proto jej, coby kryptologický standard v USA, nahradil systém **AES**[18]**.**

Systém DES byl tedy řešením bezpečnostní úrovně kryptologického systému založeného na výpočetní technice. Šlo a kombinaci substituční a transpoziční šifry, která byla realizována na blocích 56 bitů (ve skutečnosti jich bylo 64, ale 8 z nich bylo paritních).

---

[14] Polovodičová součástka, základ integrovaných obvodů, procesorů, pamětí. Slabá změna proudu či napětí na vstupu je schopna vyvolat velkou změnu na výstupu.

[15] Spojení více miniaturních součástek do jednoho celku. Takový celek tvoří elektrický obvod, který vykonává složitější funkce.

[16] National Security Agency – vládní kryptologická organizace spadající do kompetence Ministerstva obrany USA, primárním úkolem je sběr a analýza zahraniční komunikace, dále ochrana informačních systémů uvnitř vlády USA.

[17] Data encryption standard

[18] Advanced encryption system (od r. 1997 symetrická šifra Rijndael o délce 128, 192 nebo 256 bitů)

Do popředí zájmu se však dostal problém, který nebyl v oblasti kryptologie ničím novým, ale provázel ji jako stín prakticky od jejího počátku.

Distribuce klíčů, problém, který s komerčním rozmachem prostředků výpočetní techniky a tím i rozmachu kryptologických systémů nabíral na intenzitě. Šlo zejména o logistické řešení distribuce klíčů. Obě komunikující strany kryptologického systému musely sdílet totožný klíč, bez něhož by nebylo možné zašifrovanou zprávu dešifrovat. V polovině 70. let byl vyvinut šifrovací systém, který problém distribuce klíčů vyřešil. Tento počin je považován za jeden z nejvýznamnějších průlomů v historii kryptologie [1] [6].

Whitfield Diffie a **Martin Hellman** se pustili do řešení problému distribuce klíčů. Uvědomovali si tu skutečnost, že celá věc připomíná problém **Hlava XXII.**[19] Aby dvě komunikující strany (Alice a Bob) mohly sdílet tajemství v podobě zašifrované zprávy, aniž by ji odposlouchávající osoba (Eva) byla schopna přečíst, musí dříve sdílet tajemství v podobě klíče. Aby mohli tajně sdílet klíč, musí před ním tajně sdílet další klíč. Takto celý problém pokračuje do nekonečna.

Diffie, Hellman a Ralph Merkle, který se přidal později, zaměřili svoji pozornost na **jednocestné funkce[20].** Příklad jednocestné funkce z běžného života lze nalézt prakticky kdekoliv. Smíchání dvou barev v jedné nádobě lze označit za jednocestnou funkci. Samotné smíchání není žádný problém, rozdělit však barvu na dvě původní složky je velmi obtížné.

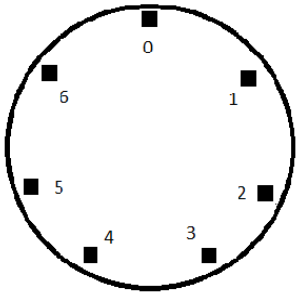
Modulární aritmetika je oblastí matematiky, která je bohatá na výskyt jednocestných funkcí. Tato aritmetika pracuje s konečnou množinou čísel, která je uspořádána do kruhu, proto se někdy označuje jako **hodinová aritmetika**. Na níže uvedeném obrázku 4 je možno si názorně představit výpočet: 2 + 3 = 5 (mod 7) a 2 + 6 = 1 (mod 7). Pokaždé je

---

[19] Zlidovělé označení absurdní situace, do nekonečna se opakujícího problému. Podle románu Josepha Hellera – Catch XXII z II. světové války.

[20] Jednocestná funkce je taková, u které lze ze vstupů snadno určit výsledek. Avšak z výsledku určit vstupy (inverzní funkce) je velmi složité. Počet možných výsledků je veliký a každý z nich je nutno ověřit. To je náročné na prostředky výpočetní techniky.

výchozím bodem na ciferníku číslo 2 a k němu je ve směru hodinových ručiček přičten potřebný počet.



Obrázek 4 Modulo 7

Modulární aritmetika je součástí našeho každodenního života, aniž bychom o tom hlouběji přemýšleli. Pokud v 11 hodin dopoledne víme, že se ze zaměstnání dostaneme nejdříve za šest hodin, neuvažujeme tak, že domů půjdeme v 17 hodin, ale v 5. To v řeči modulární aritmetiky znamená $11 + 6 = 5 \ (mod12)$.

Běžná aritmetika má tu vlastnost, že pokud neznáme výsledek určité funkce, můžeme se k tomu pravému dopracovat. Vezmeme-li v úvahu následující příklad:

$$6^x = 216$$

Úkolem je vypočítat neznámou x. Pokud budeme předpokládat, že $x = 4$, pak je snadné porovnat výraz 6^4 s výrazem na pravé straně. 1296 se v žádném případě nerovná 216. Je tedy zjevné, že odhadovaná hodnota x byla příliš vysoká. Proto přichází na řadu vyzkoušet to samé s menším číslem, tentokráte to bude číslo 3. Hodnota 6^3 se skutečně rovná 216. V klasické aritmetice tedy existuje možnost hledat správnou hodnotu z předchozích, nepřesných odhadů.

V modulární aritmetice je tomu jinak. Opět je úkolem najít hodnotu x tentokrát ve výrazu $3^x \ (mod\ 7) = 1$. Pokud dosadím za x číslo 5, pak bude hodnota výrazu vlevo rovna číslu 5. To je příliš, hledám takové x, které přidělí výrazu vpravo hodnotu 1. V předchozím odstavci logika klasické matematiky velela v takovém případě snížit hodnotu testované hodnoty. To by ovšem v tomto případu vedlo k další chybě, protože hledaná hodnota neznámé x je 6. Toto je jasný důkaz odlišnosti modulární aritmetiky od té klasické. Invertovat funkce v modulární aritmetice je daleko složitější proces, který klade značné

nároky na prostředky výpočetní techniky a hlavně neposkytuje možnost odvodit správný výsledek od neúspěšných pokusů!

Hellman si tuto vlastnost modulární aritmetiky plně uvědomoval a v roce 1976 přišel s jednocestnou funkcí:

$$Y^x \pmod P$$

Tato formule, jak ukáže následující diagram, se stala převratným okamžikem v historii kryptologie. Alice a Bob prostřednictvím nezabezpečené linky sdílí taková data, která Evě nijak nepomohou odhalit jejich utajenou komunikaci, jinak řečeno z těchto informací není Eva schopna identifikovat klíč, který Alice s Bobem mohou použít např. pro DES šifru.

$Y^x \pmod P$	
ALICE	**BOB**
Alice se s Bobem dohodne na hodnotách Y a P tak, aby Y < P Y = 4, P = 7	
Alice si stanoví člo 6 a uchová jej v tajnosti. Toto číslo nazve **A**	Bob si stanoví číslo 8 a uchová jej v tajnosti. Toto číslo nazve **B**
Alice vloží číslo A do funkce $Y^A \pmod P$ $4^A \pmod 7$ $4^6 \pmod 7 = 4096 \pmod 7 = 1$	Bob vloží číslo B do funkce $Y^B \pmod P$ $4^B \pmod 7$ $4^8 \pmod 7 = 65536 \pmod 7 = 2$
Výsledek označí Alice znakem **α** a pošle jej Bobovi	Výsledek označí Bob znakem **β** a pošle jej Alici
Pokud Eva po celou dobu odposlouchala znamená to, že zná hodnoty Y = 4, P = 7, α = 1, β = 2 Tato čísla NEJSOU KLÍČ !! Proto z jejich znalosti nemůže Eva nikterak těžit	
Alice použije **β** do následujícího vztahu: $\beta^A \pmod 7$ $= 2^6 \pmod 7 = 64 \pmod 7 = \mathbf{1}$	Bob použije α do následujícího vztahu: $\alpha^B \pmod 7 =$ $1^8 \pmod 7 = 1 \pmod 7 = \mathbf{1}$
KLÍČ = 1	

Tabulka 9 Distribuce klíče Diffie-Hellman-Merkle

Výsledek dlouholeté práce byl na světě. Schéma (tabulka 9) obsahuje malá čísla pro zjednodušení, ve skutečnosti by všechny výpočty probíhaly s neporovnatelně většími čísly.

V roce 1977 Diffie, Hellman a Merkle podali žádost o patent. Tímto bylo zničeno jedno z největších dogmat kryptologie. Alice a Bob už nemuseli sdílet žádné tajemství proto, aby byli schopni sdílet klíč. Přes obrovský krok dopředu, který tento systém pro kryptologii znamenal, nelze jej označit za dokonalý.

Whitfield Diffie chtěl metodu rozšířit. Doposud popsané metody se souhrnně nazývají **symetrické šifrování.** Jde o takový způsob, který k šifrování i dešifrování používá totožný klíč. Ať už se jednalo o jednoduché substituční šifry, Play-fair, Enigmu i Diffie-Hellman-Merkle metodu distribuci klíče, všechny spadají do oblasti symetrické kryptologie. V každém z případů je nutné, aby odesilatel i příjemce disponovali totožným klíčem. S tím je, jak již bylo několikrát zmíněno, spojena celá řada problémů, zejména pak logistických.

Diffie přišel s myšlenkou formulovat **asymetrickou šifru.** Alice by disponovala dvojicí klíčů, z nichž jeden by byl **klíč veřejný.** Tento by byl k dispozici každému, kdo by chtěl Alici poslat zašifrovanou zprávu. Druhým klíčem by byl **klíč soukromý,** který by Alice držela v naprosté tajnosti. Použitím soukromého klíče by šifrový text pořízený za pomoci veřejného klíče Alice mohl být převeden zpět na text otevřený. Veřejný klíč by sloužil pouze k zašifrování, proces opačný, tedy dešifrování by za jeho pomoci nebyl možný.

To naznačuje, že asymetrická šifra zcela eliminuje problémy té symetrické. Odpadá problém možného zcizení klíče, který musí odesilatel i příjemce sdílet. Pokud by použili metodu distribuce klíče D-H-M, odpadá obava z odposlechu klíče, ale nezbaví se podmínky synchronní komunikace. Zjednodušeně nemusí v reálném čase sdílet žádné hodnoty, které obě strany použijí ke generování klíče. Asynchronní šifrování zaručuje, že veřejný klíč si může odesilatel vyhledat na místech tomu určených kdykoliv bez nutnosti synchronizace s příjemcem. To například vyhovuje základnímu principu asynchronní e-mailové komunikace [1].

Diffie, Hellman a Merkle svoji myšlenku o asymetrické šifře do zdárného konce nepřivedli. Nepodařilo se jim jako prvním nalézt vhodnou matematickou funkci, která by principy asymetrické kryptologie mohla uvést do funkčního stavu.

Nalezení takové matematické funkce se podařilo jiné trojici kryptografů. **Ronald Rivest**, **Adi Shamir** a **Leonard Adleman**. Ti přišli s myšlenkou rozkladu velmi velkého čísla na **prvočíselný součin**[21] neboli **faktorizaci.**

Tato matematická funkce je jednocestná, protože vynásobit mezi sebou dvě velká prvočísla není problém. Avšak získat prvočíselný součin z dostatečně velkého čísla je poměrně závažná výpočetní úloha.

Za dostatečně veliké prvočísla se uvažují taková, která mají minimálně 10^{308} řádů.

Podle počátečních písmen příjmení autorů, nese první asymetrická šifra označení **RSA.** Tato šifrovací metoda staví svoji bezpečnostní úroveň na absenci matematického algoritmu, který by faktorizaci usnadnil.

V roce 1977 byl udělen patent na šifru RSA. Je nutné podotknout, že prakticky stejný objev učinila trojice britských vědců z vládní organizace **Government Communication Headquartes** v **Cheltenhamu**, tedy z instituce, která vznikla z fragmentů již známého Bletchley parku. **James Ellis**, **Clifford Cocks** a **Malcolm Williamson** přišli na totožný systém, který spatřil světlo světa díky Rivestovi, Shamirovi a Adlemanovi a to v době, kdy ještě nebyl popsán systém přenosu klíče Diffie-Hellman-Merkle. Jelikož byla GSHQ vládní institucí a její aktivity podléhaly přísnému utajení, mohla být zpráva o práci britských tvůrců asymetrického algoritmu zveřejněna až na konci 90. let 20. století.

Následující postup má za úkol naznačit princip fungování algoritmu RSA. Jde o velmi zjednodušený zápis, který je uskutečněn za použití nápadně malých čísel pro lepší představu o funkčnosti celého systému. Ve skutečnosti se pracuje s čísly, která jsou neporovnatelně větší.

[21] Prvočíslo je takové přirozené číslo, které beze zbytku dělitelné číslem 1 a sebou samým (např. 5, 7, 11,..)

RSA

Alice zvolí dvě (v reálné situaci velmi vysoká) prvočísla **p** a **q.**

$p = 17, q = 11$

Tato čísla uchová v tajnosti.

Vynásobením obou prvočísel p a q získá Alice číslo **N**.

$N = p * q = 17 * 11 = 187$

Alice zvolí další číslo **e** a to tak, aby **e** a **(p - 1) * (q - 1)** neměli společného dělitele (e = 7).

Alice zveřejní čísla N a e, ta jsou **Veřejným klíčem.**

Bob chce poslat Alici zprávu, která obsahuje jediný znak **X.**

Tato zpráva je označena znakem **M** a je převedena (nejčastěji pomoci ASCII) do číselné (dekadické) podoby: **M = X = 88**

Bob zašifruje zprávu **M** do šifrové podoby **C** pomocí vztahu:

$$\mathbf{C = M^e \pmod N}$$

$$C = 88^7 \pmod{187}$$

$$\boldsymbol{C = 11}$$

Alice za pomocí svých utajených hodnot p a q vypočítá hodnotu **d.**

$$e * d \equiv 1 \pmod{(p - 1) * (q - 1)}$$

Tento výpočet se děje za použití rozšířeného Euklidova algoritmu.

$$7 * d \equiv 1 \pmod{16 * 10}$$

$$7 * d \equiv 1 \pmod{160}$$

$$\mathbf{d = 23}$$

Hodnota **d** je **soukromý klíč** (označován jako soukromý exponent) Alice.

Alice dešifruje zprávu C následujícím výpočtem:

$$M = C^d \pmod N$$

$$M = 11^{23} \pmod{187}$$

$$\underline{\mathbf{M = 88 = X}}$$

Převodem dekadické hodnoty 88 prostřednictvím ASCII získá Alice znak **X**, který jí poslal Bob za přispění asymetrické šifry RSA.

Tento chronologický postup jasně ukazuje, v čem spočívá hlavní síla asymetrické šifry. Alice a Bob v tomto případě nesdílí žádné tajemství, které je klíčové k úspěšnému a bezpečnému přenosu zprávy. Místo toho využívají principů modulární aritmetiky, která svou jednocestnou charakteristikou nedovolí Evě ze znalostí hodnot **C**, **N** a **e** vypočítat hodnotu **M** [1].

1.2.10 Informační věk

Závěr dvacátého století je obdobím postindustriálním v němž jsou nositeli hodnot informace. Důkazem toho budiž rozmach elektronické komunikace nebo elektronického obchodování, které jsou pro přelom tisíciletí zcela charakteristickým. Potřeba nakládat s takovým množstvím informací způsobem, který zaručí jejich bezpečný přenos na místo určení a to tak, aby byl vyloučen zásah nežádoucích subjektů, vedla k rozšíření kryptologie do rozrůstající se sítě navzájem propojených osobních počítačů (internet) a tedy i k obyčejným lidem. Zatímco byla po dvě tisíciletí kryptologie věda určená zejména vojenským a vládním kruhům, pak konec prvního milénia přináší vstup tohoto odvětví do života každého subjektu široké veřejnosti, který ke své komunikaci užívá elektronická média.

Existence algoritmů, jakým byl i zmíněný RSA, zabezpečovala pro kryptografii dostatečně vysokou bezpečnostní úroveň. Tento fakt sebou nesl i jedno negativum. Stejným způsobem mohli tuto dostatečně bezpečnou šifru užít i ti lidé, jejichž úmysly realizované za pomocí elektronické komunikace mohly vykazovat prvky protiprávního jednání.

Toto je poměrně zásadní problém. I tato mince má své dvě strany a bylo proto zapotřebí hledat kompromis, který jednak zaručoval soukromým subjektům dostatečný pocit bezpečí v elektronické komunikaci či obchodu a na druhou stranu umožňoval státním orgánům,

zejména pak policii, určitou formu kontroly, která mohla vést k odhalení trestné činnosti již v okamžicích jejího plánování.

Hledáním takové rovnováhy se zabýval i americký odborník v oblasti IT **Phil Zimmerman**. Ten je autorem projektu **PGP**[22]**.** Zimmermannovi bylo jasné, že užití asymetrické šifry (RSA) pro běžnou elektronickou komunikaci vyžaduje značné technické a časové nároky. Proto uvažoval o systému, který by skloubil **rychlost symetrické šifry a bezpečnostní úroveň šifry asymetrické.**

PGP tak funguje tím způsobem, že Bob zašifruje zprávu určenou Alici symetrickou šifrou **IDEA**[23], což znamená nižší časovou a technickou náročnost. Šifra IDEA vyžaduje totožný klíč pro šifrování i dešifrování, jelikož jde o symetrickou šifru. Takový klíč je tedy nutné distribuovat bezpečnou cestou k Alici. Pro tento úkon použije Bob šifru RSA, což je asymetrická šifra. Bob tedy vyhledá veřejný klíč Alice a tím zašifruje klíč k šifře DES, kterou je zašifrován samotný obsah zprávy. Tato kombinace symetrické a asymetrické šifry přináší technické i časové úspory.

Zimmermanovi však zbývalo vyřešit ještě jeden problém, který byl s bezpečností elektronické komunikace spojen. Byla jím **autentizace.**[24] Pokud Bob aplikoval uvedený postup kombinující symetrickou a asymetrickou šifru, pak existovala téměř stoprocentní jistota, že obsah zprávy si mohla přečíst jen a pouze Alice. Na druhou stranu však nebylo možné zaručit, že autorem takové zprávy je právě Bob. Tomu nahrával fakt, že kdokoliv, v našem případě Eva, se mohl vydávat za Boba. Eva tím pádem z dostupných zdrojů použila veřejný klíč Alice, tím zašifrovala klíč k šifře IDEA, kterou byla zašifrována zpráva, pod níž se podepsala, co by Bob. Toto je poměrně zásadní problém, ale i ten našel své řešení.

Digitální podpis je kryptografický řetězec, jehož hodnota se odvíjí od samotného obsahu zprávy, tak od jejího odesilatele**.** Tento prvek zajišťuje jednak **integritu dat**[25] a

---

[22] Software sloužící k šifrování a podepisování elektronických dokumentů, jeho základem je algoritmus RSA.

[23] Symetrická šifra podobná DES.

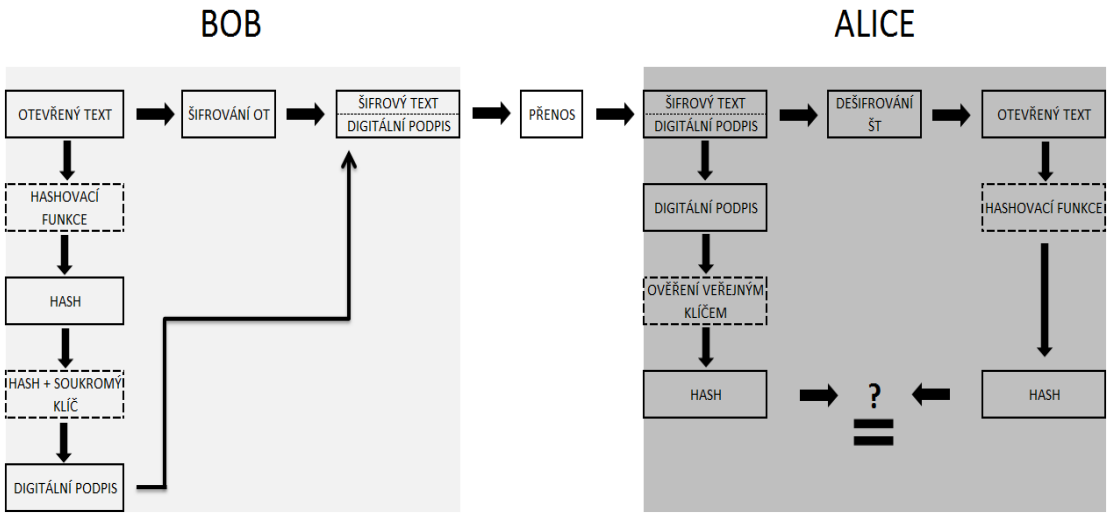
[24] Proces, který má za úkol ověřit identitu subjektu. Ekvivalent konvenčního podpisu.

[25] Ujištění, že přístup a editaci dat mohou provádět pouze osoby s patřičným oprávněním

jejich původ. Proces digitálního podpisu funguje tak, že odesilatel Bob vytvoří z části zprávy, kterou posílá Alici tzv. **hash**[26]**.** Tento otisk zašifruje svým **soukromým klíčem** (jde tedy o odlišný postup, než při samotném šifrování klíče zprávy, protože při něm by Bob k zašifrování užil veřejný klíč Alice) a přiloží jej k zašifrované zprávě. Alice obdrží zašifrovanou zprávu spolu s podpisem. Zprávu dešifruje tak, že pomocí svého soukromého klíče dešifruje nejprve klíč k IDEA šifře, kterou je zašifrován samotný obsah zprávy.

Aby se skutečně ujistila, že zpráva pochází od Boba, pak z dešifrované zprávy vytvoří totožnou hashovaní funkcí otisk dešifrované zprávy, jak to učinil Bob. Navíc použije Bobův veřejný klíč k odemknutí jeho podpisu. Tímto má Alice vedle sebe dva hashe, které jednoduše porovná. Pokud se shodují, pak si může být jista tím, že zprávu skutečně poslal Bob.

U digitálního podpisu se použití veřejného a soukromého klíče otočí oproti samotnému šifrování. Hash může za pomoci soukromého klíče vytvořit pouze jeho majitel (drží-li jej dostatečně v tajnosti). Ověřit tento hash však může každý, kdo zná veřejný klíč spárovaný se soukromým klíčem majitele. Na obrázku 5 je celý postup převeden do přehledného schématu [6].



Obrázek 5 Schéma digitálního podpisu

[26] Výstup hashovaní funkce, která velký objem dat převede na relativně malý výstup (někdy označován, jako digitální otisk zprávy)

2 ZÁKLADNÍ PRINCIPY KVANTOVÉ TEORIE

2.1 Vznik kvantové teorie

Pokud je cílem této kapitoly popsat důvody vzniku kvantové teorie, její základní vlastnosti a odlišnosti od předchozích náhledů na fyziku, pak je nutno vrátit se do roku 400 př. n. l., do doby v níž žil řecký filozof Démokritos. Ten uvažoval nad tím, zda je možno hmotu dělit do nekonečna. Jeho zájem se upřel na fakt, zda existuje nějaká mezní velikost, která již nemůžou být dále rozdělena na dvě menší části. Základní stavební prvek, který si představoval, jako velmi malé zrnko písku, pojmenoval **atom**[27]**.**

Snaha spatřit základní stavební prvek motivovala v osmnáctém století švýcarského matematika Daniela Bernoulliho. Ten si byl vědom toho faktu, že pokud nemůžeme přímo pozorovat každý jednotlivý atom, pak to bude možno provést nepřímo na větším množství. Ke svým experimentům se proto uchýlil na práci s plynem. Využil jeho vlastností, zejména pak ve stlačeném stavu.

Na Bernoulliho práci navázal anglický vědec Robert Boyle, ten v roce 1660 potvrdil domněnky a představy o atomech, jako miniaturních zrníčcích, které v prostoru poletují ve složitých drahách.

Konečný důkaz, který definitivně potvrdil hypotézy všech výše uvedených vědců, přinesl roku 1827 Robert Brown. Svým pozorováním zrnek pylu vznášejících se ve vodě připravil teoretický základ pro práci Alberta Einsteina, který v roce 1905 záhadný pohyb zrnek pylu ve vodě vysvětlil. Dokázal, že tento pohyb je způsoben neustálým bombardováním zrnek pylu jednotlivými molekulami vody. Einstein dokonce vypracoval matematický důkaz, který pomohl předpovědět pohyb zrnek a jeho závislost na velikosti molekuly vody.

Francouzský fyzik Jean Baptis Perrin využil Einsteinovy práce a určil velikost molekuly vody na 10^{-8} metru.

[27] Z řeckého a-tomos, což v překladu znamená nedělitelný.

V roce 1980 byl za pomocí **řádkovacího tunelového mikroskopu (STM[28])** poprvé v historii lidstva skutečně spatřen atom. Je však nutné podotknout, že STM je neoptické zařízení, které vytváří obraz na základě údajů z miniaturní sondy. Tato sonda tvoří hrot mikroskopu a na základě měření elektrických jevů sestavuje jakési obrazy jednotlivých atomů.

Dalším, neméně důležitým objevem v oblasti atomů byla jejich odlišnost, kterou objevil francouzský šlechtic Antoine Lavoisier. Ten určil 23 základních dále nedělitelných prvků. Tento seznam v dnešní době čítá 92 prvků.

Za neméně důležitý objev lze označit práci francouzského chemika Henriho Becquerela, který v roce 1896 objevil radioaktivitu.

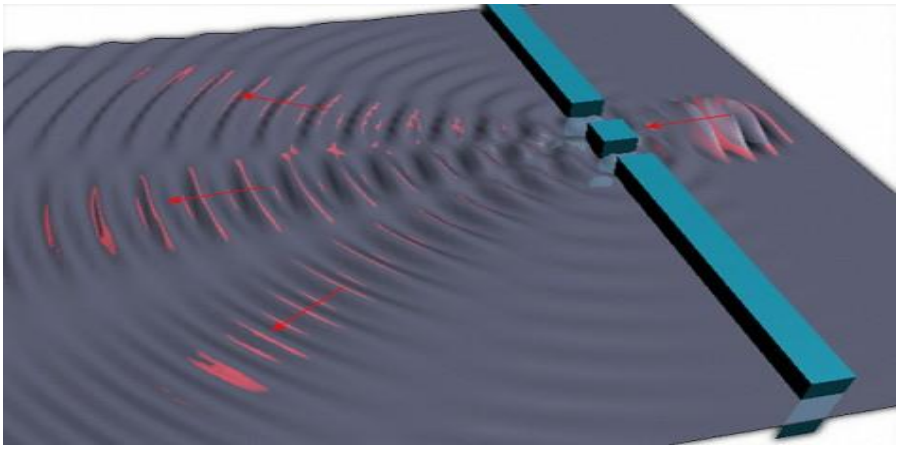
Novozélanďan Ernest Ruherford využil přítomnosti tzv. **alfa částice**, která vzniká při radioaktivním rozpadu částic. Pomocí těchto alfa částic zkoumal vlastnosti jiných atomů. Tuto metodu aplikovali v roce 1909 Němec Hans Geiger a novozélandský fyzik Ernest Marsde. Jejich experiment spočíval v ostřelování extrémně tenké zlaté fólie alfa částicemi. Očekávali, že alfa částice bez problémů projdou skrze fólii a svůj let ukončí na stínítku, kde zanechají stopu. Alfa částice však nečekaně skrze fólii neprošly a odrazily se zpět. V té době již svět věděl o první subatomární částici, kterou byl elektron. Nyní bylo jasné, že dosavadní představa o stavbě atomu není přesná.

To, co odrazilo alfa částice zpět, bylo jádro atomu. Tvoří 99,99 celkové hmoty každého atomu a je neporovnatelně menší ve vztahu k celkové velikosti atomu. To znamená, že hmotu, která je všude okolo a včetně nás, tvoří převážně prázdnota. Tento poznatek byl v kolizi s Maxwellovou teorií elektromagnetismu, která každému nabitému tělesu, jež mění svoji rychlost a směr, připisuje vyzařování elektromagnetické vlny neboli světla. To by ovšem znamenalo, že elektrony, které kolem jádra obíhají, jako Měsíc kolem Země, postupně ztratí svoji energii a ve spirálovité dráze se zhroutí do jádra. Tento scénář se však nenaplňuje a je tedy zjevné, že Ruherfordův model atomu má jistou mezeru. Tu zaplňuje kvantová teorie [4].

[28] Z anglického Scanning Tunelling Microscope, v roce 1981 jej sestrojili Gerd Binning a Heinrich Rohrer

2.2 Vlnově-částicová povaha světla

Thomas Young, anglický lékař stál za zrodem chápání světla, jakožto vlny. Se svým štěrbinovým experimentem jasně prokázal, že světlo skutečně vykazuje vlastnosti vlny. Výsledky jeho pokusů značně připomínaly chování vln na hladině rybníka (obr. 6). Štěrbinový experiment poukázal na zajímavou vlastnost světelného vlnění, na tzv. **interferenci**[29].

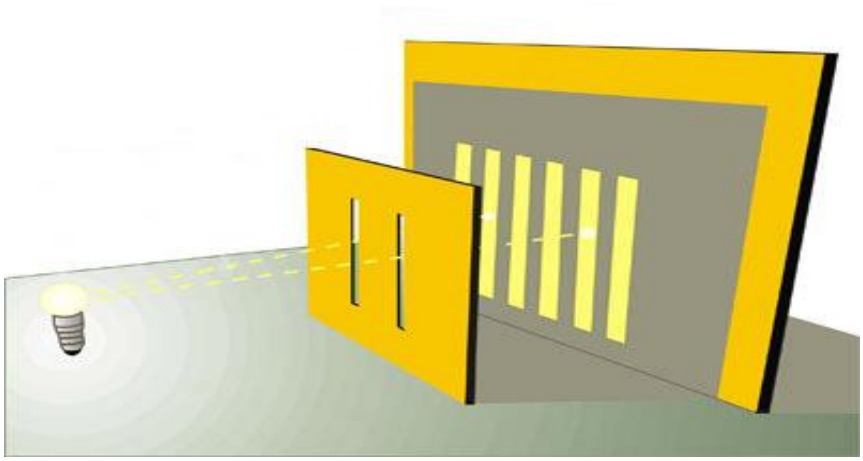


Obrázek 6 Ukázka interference vln na hladině kapaliny

(zdroj: www.superstruny.aspweb.cz)

Youngův experiment probíhal tak, že na stínítko s dvojicí vertikálních štěrbin dopadalo světlo (obr. 7). Na druhém stínítku, umístěném za tím se štěrbinami, vznikly tzv. interferenční obrazy, což byl nezvratný důkaz vlnové povahy světla.

[29] Proces vzájemného ovlivňování se vln v různých bodech jejich průběhu. Např. vrchol a údolí vlny se navzájem ruší, zatímco interference dvou vrcholů přináší zesílení.



Obrázek 7 Youngův štěrbinový experiment

(zdroj: www.gnosis9.net)

Představa světla, co by vlny byla přijímána do okamžiku objevu **fotoelektrického jevu**[30], jehož autorem je Albert Einstein. Vedle tzv. **Comptonova rozptylu**[31] jde o jasný důkaz, že v těchto případech vykazuje světlo charakteristiku částice a ne vln!

Vlnově-částicová povaha světla neboli vlnově-korpuskulární charakteristika znamenala naprostý převrat ve fyzice. Do roku 1900 byla fyzika praktickým nástrojem pro předpovídání. Na základě vstupních informací bylo možno předpovědět jevy, které nastanou s brilantní přesností. Toto pravidlo však ve světě částic nefunguje.

V reálném světě lze předpovědět věci, které se na první pohled jeví nepředvídatelnými. Například to, kde skončí kulička rulety lze určit s naprostou přesností. Potíž je pouze v tom, že množství vstupních informací, které k takovému výpočtu potřebujeme, je neskutečně velké. Ve světě částic je **přítomnost zcela náhodných jevů** naprostou samozřejmostí. Tento poznatek přiměl Einsteina ke slavnému výroku: *„Bůh nahraje s vesmírem v kostky!“* Tento výrok kontroval britský matematik a astrofyzik Stephen

[30] Fyzikální jev, při němž dochází k uvolňování elektronů z látky v důsledku absorpce elektromagnetického vlnění

[31] Fyzikální jev, při kterém dochází ke změně vlnové délky elektromagnetické záření v důsledku srážky tohoto záření s atomy pevné látky

Hawking: *,,Nejen že Bůh hraje s vesmírem v kostky, navíc vrhá kostky tam, kde je nemůžeme vidět!‘‘*

Klasická Newtonovská fyzika o pohybu a gravitaci je schopna předpovědět zítřejší polohu planety s naprostou přesností. To samé **nelze** implementovat na úrovni atomů, tam lze určit pouze **pravděpodobnou** dráhu letu částice. **Kvantová fyzika je založena na neurčitosti.**

Zmíněnou pravděpodobností chování částice se zabýval rakouský fyzik Erwin Schrödinger. Ten sestavil rovnici tzv. **pravděpodobnostní vlny**. Šlo o matematické vyjádření pravděpodobnosti výskytu částice v prostoru na základě průběhu imaginární vlny. V místě, kde měla imaginární pravděpodobnostní vlna dvojnásobnou výšku, byla pravděpodobnost výskytu částice čtyřnásobná (to bylo dáno nutností vztáhnout pravděpodobnost výskytu částice k druhé mocnině velikosti pravděpodobnostní vlny v tomtéž bodě).

Schrödingerova rovnice poskytuje možnost alespoň **předpovídat pravděpodobnost,** s jakou lze danou částici nalézt v prostoru a čase, obecněji jde o předvídání pravděpodobnosti chování částic. To je jistá míra kompenzace domněnky, že svět na částicové úrovni je řízen naprosto nepředvídatelnými pravidly a připomíná spíše chaos [4].

Pravděpodobnostní vlny, za jejichž popisem stál Schrödinger, přisuzují částicím, jak se mají chovat. Jde o určitou spojnici mezi vlnovým charakterem částic a vlněním všeho druhu.

Skutečnost, že mohou částice vykazovat chování, které je vlastní vlnám vede k jevu, který se nazývá **kvantové tunelování.** Tento jev popisuje vlastnosti a chování částic, které by při porovnání s objekty lidského měřítka budilo přinejmenším údiv. Kvantové tunelování umožňuje částicím procházet bariérou, která je vyšší než energie samotné částice. To je možno díky vlnovému chování částic a tedy tím, že se nechovají, jako lokalizovaný objekt.

Pro představu: Světlo v určitém mezním úhlu nemůže opustit skleněný hranol a odráží se zpátky do něj. Pokud ovšem k tomuto hranolu přiložíme další, a to velmi blízko, pak světlo jakoby přeskočí do tohoto druhého hranolu. Je to umožněno tím, že na pomezí prvního hranolu se fotony přeci jenom dostanou do určité (třebaže jenom minimální) vzdálenosti z něj. Toto jednoznačně potvrzuje vlnovou povahu částic a to, že nejsou

lokalizované. Za předpokladu, že ona minimální vzdálenost, o kterou foton opustí první hranol, je větší než mezera mezi oběma hranoly, ocitne se foton uvnitř druhého hranolu. Tím pádem překonal bariéru, která byla větší než jeho energie. V měřítku lidského světa by to znamenalo něco v tom smyslu, že vezmete svoje osobní auto do náručí a přehodíte jím dvacetipodlažní dům [4].

Kvantové tunelování je představováno i jevem, který už byl v této práci zmíněn. Únik alfa částic z radioaktivních látek by za předpokladu fungování klasické fyziky na úrovni atomů nebyl myslitelný. Je to dáno tím, že alfa částice nemají takovou energii, aby byly schopny uniknout z atomového jádra. Přesto se tak děje a to za přispění vlnové povahy těchto částic [4].

2.3 Heisenbergův princip neurčitosti

V kapitole 2.2 padla zmínka o vlnově-částicové povaze světla. To mimo jiné znamená, že částice (např. částice světla – foton) vykazují známky chování, které je vlastní vlnám. Jednou z charakteristik vln je to, že mohou existovat jejich kombinace neboli **superpozice.** Pokud se tato vlastnost aplikuje na částice, pak to znamená, že se částice může v totožném okamžiku nacházet na různých místech. Navíc může v tomtéž okamžiku provádět řadu odlišných procesů.

Důkazem superpozice částice je Youngův štěrbinový experiment, který je proveden s toutéž dvojicí stínítek, na které svítil zdroj světla. Tentokrát však za použití tak slabého zdroje, který na první stínítko vyšle jediný foton. Přesto se na druhém stínítku objeví charakteristické pruhy (interferenční obrazce), které vznikly interferencí světelného vlnění. Taková skutečnost nahrává domněnce, že každý jednotlivý foton projde oběma štěrbinami a interferuje sám se sebou. Foton je v superpozici dvou stavů. Jedním tímto stavem je pravděpodobnostní vlna, která fotonu ukládá cestu pravou štěrbinou, druhým je pravděpodobnostní vlna, která mu určuje projít levou štěrbinou.

Ve skutečnosti však nelze docílit pozorování toho, že se částice skutečně nachází na dvou místech najednou. Lze pozorovat pouze **důsledek** této superpozice.

Velmi důležitým pojmem v oblasti kvantové teorie je **dekoherence. Fakt, že okolní svět je informován o superpozici nějaké částice, vede ke zničení této superpozice!** Jinými slovy řečeno, pokud např. foton odražený od částice, která se momentálně nachází

v superpozici, dorazí k nějakému detekčnímu zařízení, z něhož byl vyslán, superpozice tím okamžikem zaniká a **superponovaná částice se stává lokalizovanou [4].**

Hlavním důvodem proč v reálném světě nelze pozorovat superpozice je ten, že pomocí fotonů dochází k permanentní informovanosti o částicích, které tvoří okolní hmotu. Tím pádem jsou neustále měřeny a viděny, co by lokalizované.

Svět částic však přináší ještě jedno omezení v měření. **Heisenbergův princip neurčitosti** přináší tu skutečnost, že dvě, jednoznačně spojené veličiny elementárních částic (zejména poloha a rychlost) nelze měřit s naprostou přesností. Platí, oč přesněji je změřena rychlost takové částice, tím nepřesnější bude její poloha a naopak. Takové omezení svým způsobem zachovává možnost existence interference částic a tím pádem i elementárních principů kvantové teorie.

Heisenbergův princip neurčitosti je tou oblastí kvantové teorie, které se využívá v oblasti **kvantové kryptologie,** ta bude popsána v následujících kapitolách.

3 KVANTOVÁ KRYPTOLOGIE

3.1 Základ kvantové kryptologie

Kvantová kryptologie, zejména pak kryptografie je zatím posledním článkem evolučního řetězce tohoto odvětví. Jedná se o naprosto přelomový počin v historii disciplíny.

V kapitole 2.2 padla zmínka o odlišnosti fyzikálních principů světa kolem nás a toho na atomární úrovni. Těchto odlišností využívá i kvantová kryptologie, zejména pak její podobor zabývající se převodem otevřeného textu do šifrového, tedy kryptografie.

Cílem této části je popsat základní princip a odlišnost kvantové kryptografie. Přesněji řečeno, následující text se věnuje distribuci klíče za přispění zákonitostí kvantové fyziky. Tento způsob se označuje **QKD**[32]**.**

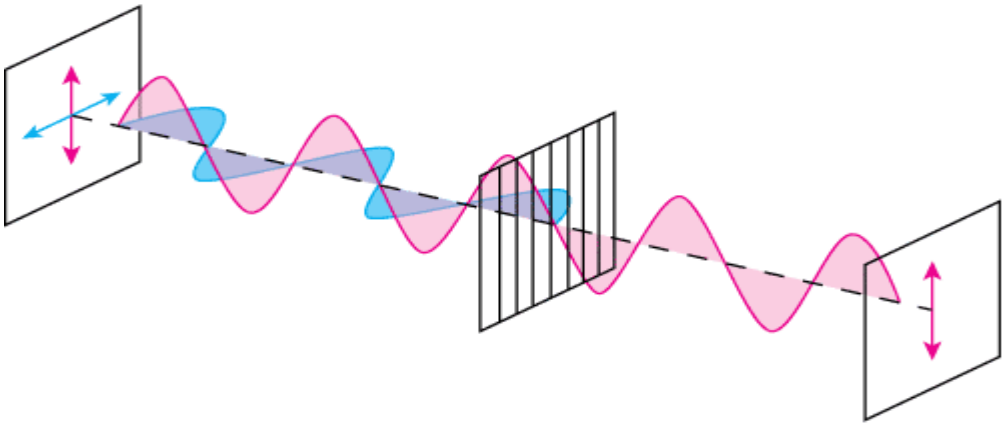
Jedním z hlavních rysů a odlišností kvantové fyziky od té tradiční je přítomnost zcela náhodných jevů, které nelze předvídat na základě sebevětšího množství vstupních informací. Dalším prvkem, který kvantové distribuci klíče přiděluje roli převratné technologie, je Heisenbergův princip neurčitosti. Jak je zmíněno v kapitole 2.3, znemožňuje tento princip přesné měření jedné z jednoznačně spojených veličin bez toho, aniž by došlo k ovlivnění té druhé. Dále je poukázáno, že tento fakt je pro výjimečnost systému QKD zcela zásadní.

Bezpečnostní úroveň kvantové distribuce klíče QKD je založena na faktu, že jakýkoliv pokus Evy naslouchat tajné komunikaci mezi Alicí a Bobe bude odhalen a to právě díky tomu poznatku, že Eva bude odposlech realizovat prostřednictvím měření. Jak již zaznělo, měření určité veličiny má za následek změnu. Tato změna indikuje přítomnost odposlechu na komunikačním kanále [1].

[32] Quantum key distribution = kvantová distribuce klíče

3.2 Kvantová distribuce klíče

Za zrodem prvního protokolu, který je postaven na kvantové distribuci klíče stál **Charles Bennett** a **Gilles Brassard**. Ti navázali na myšlenku **Stephena Wiesnera**, který v 60. letech jako první začal uvažovat o spojení fyziky fotonů a bezpečnosti. Weisnera zajímala zejména **polarizace**[33] fotonu.

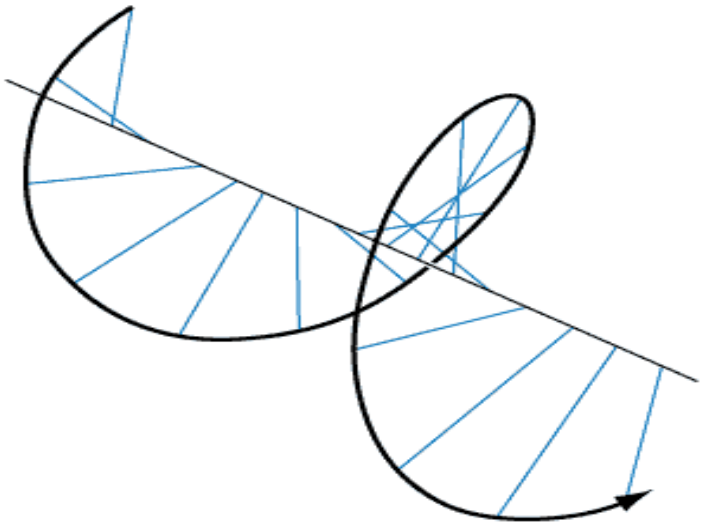


Obrázek 8 Polarizace světla (zdroj: www.fotoroman.cz)

Foton pohybující se volným prostorem osciluje v různých směrech, které jsou kolmé k ose pohybu. Užitím polarizačního filtru (obr. 8) lze dosáhnout toho, že za polarizačním filtrem ve své cestě pokračují jenom ty fotony, které mají shodnou orientaci oscilace, jakou má polarizační filtr. Navíc, některé fotony jsou schopny filtrem prostoupit, i když nemají shodnou rovinu oscilace. Tohoto poznatku využívá právě QKD.

Ve skutečnosti fotony oscilují v celém rozsahu 360° (obr. 9).

[33] Pojem polarizace v tomto kontextu znamená úhel oscilace fotonu kolem osy směru svého šíření



Obrázek 9 Skutečný rozsah polarizace fotonu

(zdroj: www.fotoroman.cz)

Pro názornost jsou použity pouze 4 základní směry polarizace fotonu. Tyto 4 směry jsou rozděleny do dvou bází (+ a **x**). Rozdělení polarizací fotonů hraje důležitou roli v konkrétní ukázce kvantové distribuce klíče. Následující schéma (obr. 10) znázorňuje tyto 4 základní polarizace ve dvou bázích při pohledu v ose šíření fotonu.

Obrázek 10 Základní polarizace fotonu

Wiesner použil tyto 4 základní polarizace pro svůj projekt **kvantových peněz.** Cílem jeho snažení bylo vytvořit takový bezpečnostní prvek na bankovkách, který by nebylo možné překonat jakýmkoliv napodobením.

Uvažoval tak, že by každá bankovka obsahovala 20 světelných pastí. V každé z pastí by se nacházel foton, který by byl polarizován jedním ze 4 způsobů. Orientaci polarizace každého konkrétního fotonu by znal pouze omezený počet lidí a tyto polarizace by byly

uvedený v přísně utajovaném dokumentu, který by obsahoval sériové číslo bankovky a 20 polarizací, jež byly pro tuto konkrétní bankovku použity.

Proces ověření pravosti takové bankovky by mohl vypadat následovně: Foton uvolněný ze světelné pasti by prošel skrze připravený **polarizační filtr**[34]. Jelikož ověřovatel pravosti (banka) zná polarizaci každého konkrétního fotonu, pak použije polarizační filtr orientovaný shodně s polarizací fotonu. Na obrázku 8 je takový polarizační filtr znázorněn. Tento filtr propustí pouze světlo, které je orientováno svisle a zároveň odfiltruje to s vodorovnou oscilací.

Světlo, které osciluje v bázi **x** je na tom trochu jinak. Zde přichází na řadu jedna z vlastností kvantové fyziky. Fotony orientované v bázi **x** buď projdou filtrem, který je orientován svisle a změní svoji polarizaci z úhlopříčné na svislou, nebo vůbec neprojdou. Potíž je však v tom, že nelze žádným způsobem určit, kdy a které fotony skutečně projdou a které nikoliv. V tomto okamžiku se fotony z báze **x** ocitají v tzv**. kvantovém dilematu.**

Z pohledu případného padělatele by situace vypadala následovně: Jeho úkolem by bylo nejprve provést přesný falzifikát samotné bankovky s určitým sériovým číslem. Je mu známo, že k tomuto číslu se váže 20 fotonů s přesně danými polarizacemi. Musí tedy do světelných pastí umístit fotony a nastavit jejich polarizaci podle té bankovky, kterou právě falšuje. Nezbývá mu, než otevřít první světelnou past originální bankovky a zvolit jeden ze 4 polarizačních filtrů. Pokud například zvolí polarizační filtr svislý a foton jím projde, pak si může být stoprocentně jist pouze tím, že foton v této pasti nebyl polarizován vodorovně. Takový foton by totiž svisle orientovaným filtrem určitě neprošel. Nemůže však se stoprocentní jistotou určit, zda jde o foton polarizovaný svisle, nebo zda jde o jednu z polarizací báze **x.** Jak již bylo zmíněno, úhlopříčné polarizace mají padesátiprocentní pravděpodobnost, že projdou svislým filtrem a změní tím svoji polarizaci a padesátiprocentní pravděpodobnost, že filtrem neprojdou.

Přímé měření polarizace fotonu je nemyslitelné vzhledem k přítomnosti Heisenbergova principu neurčitosti. Ten by v tomto případě způsobil tu skutečnost, že přesné měření

[34] Optický prvek, který propustí pouze tu část světla, která je polarizovaná do shodného směru

polarizace by vedla k její změně! Původní polarizace by se tím pádem změnila a padělatel by pak neměl možnost určit její orientaci.

To padělateli prakticky neumožňuje vytvořit dokonalou napodobeninu takové bankovky, protože je nanejvýš pravděpodobné, že v některé ze světelných pastí zvolí špatnou polarizace fotonu.

Tento projekt pochopitelně není možné realizovat. Prve chybí technický prostředek, který by byl schopen foton se známou polarizací umístit do takové světelné pasti. Náklady na takovou bankovku by mnohonásobně převýšily její nominální hodnotu.

Wiesner však tímto vybudoval velmi slušný základ pro práci pánů Bennetta a Brassarda, kteří podobný princip uplatnili ve svém projektu [1].

II. PRAKTICKÁ ČÁST

4 PRAKTICKÉ PŘÍKLADY VYUŽITÍ QKD

4.1 Úvod do praktické části

Následující část je hlavním prvkem celé bakalářské práce. Zde jsou výše popsané rozdíly kvantové fyziky demonstrovány na konkrétních příkladech použití. Protokol BB84, jehož základní funkcionalita je graficky znázorněna, se stal nejpoužívanějším představitelem kvantové kryptografie v nejrůznějších publikacích a článcích věnovaných tomuto tématu. Na popis tohoto protokolu volně navazují grafická schémata, která mají za úkol povzbudit představu o precizní účinnosti tohoto systému detekovat případný odposlech komunikační linky.

Praktická část práce se věnuje i další možnosti využití kvantové fyziky při distribuci šifrovacího klíče.

Nechybí srovnání kvantové kryptografie s konvenční kryptografií. Důraz je kladen na rozdíl v bezpečnostní úrovni jednotlivých systémů. Zařazen je i průřez konkrétními produkty kvantové kryptografie, které jsou v dnešní době dostupné na trhu.

Samotný závěr nastiňuje odhadovaný vývoj odvětví.

4.2 BB84

BB84 je název protokolu QKD, který je spojením počátečních písmen příjmení svých autorů (Bennett, Brassard) a roku vzniku.

Hlavním posláním je distribuce klíče mezi Alicí a Bobem za užití principů kvantové fyziky. Podobně, jako v případě Wiesnerových kvantových peněz i zde hrají hlavní roli polarizace fotonů.

Klíč, coby předmět distribuce, je převeden do binární podoby. To je velmi praktické, protože počet možných orientací v každé ze dvou bází je 2, jak je znázorněno na obr. 10. Každá orientace v bázi má přidělenou binární hodnotu 0 a 1.

Alice v tomto případě vysílá emisi fotonů s různými polarizacemi, které představují logické 0 a 1. Přitom je nutné, aby **nepředvídatelným způsobem** střídala báze **x** a **+.** Eva čelí podobnému problému jako padělatel kvantové bankovky. Pomocí dvojice detekčních zařízení na polarizaci fotonu (**x** detektor a **+** detektor) musí změřit každý přicházející foton.

Problém je v tom, že **x** detektor bude špatně měřit ty fotony, které pochází z **+** báze. Může se jí sice podařit změřit **x** detektorem původní foton ↕, který zastupuje logickou 1 tak, že jej právě **x** detektor vyhodnotí jako ↗↙ což je taky logická hodnota 1. Může se však stát, že jej vyhodnotí jako ↖↘ a to je vážný problém. Tím je dáno, že Eva nemůže s jistotou detekovat celé znění zprávy, protože netuší, jaké báze a polarizace Alice volila. Uvažovat na nějakém rozdělení fotonu a změřit jej podle obou bází je zbytečné, foton nelze žádným způsobem klonovat. Nedovoluje to Heisenbergův princip neurčitosti.

V této situaci je však nyní i Bob. Ten taky netuší, jaké báze Alice použila pro konkrétní fotony, a proto bude polovina fotonů, které si poznamená, označených rozdílnou polarizací, než kterou Alice použila.

Bennett a Brassard vyřešili tento problém rozfázování celé distribuce klíče do následujících etap [1]:

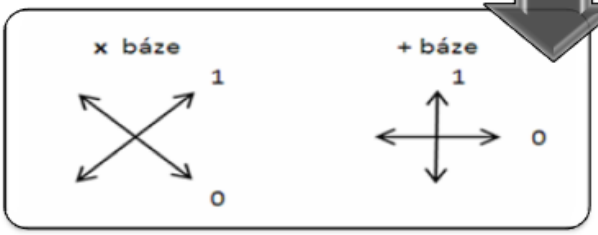
- Alice vysílá emisi polarizovaných fotonů dle náhodně vybraných bází **x** a **+**
- Bob fotony přijímá náhodně voleným **x** detektorem a **+** detektorem a zapisuje si hodnoty polarizací ke každému jednotlivému měření včetně zvoleného detektoru (báze)
- Alice po nezabezpečené lince sdělí Bobovi, která polarizační schémata (báze) použila pro jednotlivé fotony, zmínka o konkrétních polarizacích (a tím i zmínka o binárních hodnotách jednotlivých fotonů) však nepadne!
- Pokud Eva nenaslouchala komunikaci, pak sdílí Alice a Bob shodnou sérii polarizací a tím i shodnou sérii bitů
- Aby si byli Alice i Bob jisti, že Eva není přítomna na lince a neodposlouchává ji, pak obětují sérii fotonů a jejich hodnoty si po veřejné lince sdělí, tyto fotony již nadále neberou v potaz
- pokud se série binárních hodnot těchto fotonů shodují, pak je jisté, že Eva linku neodposlouchávala
- dojde-li k rozporu binárních hodnot, je nanejvýš pravděpodobné, že Eva tajně naslouchala a celá komunikaci tím pádem musí začít znovu, na jiné lince

4.3 Grafické znázornění chronologie protokolu BB84

Alice vygeneruje sérii zcela náhodných čísel a převede je do binární soustavy

1000010 1000001 1010100 1000001

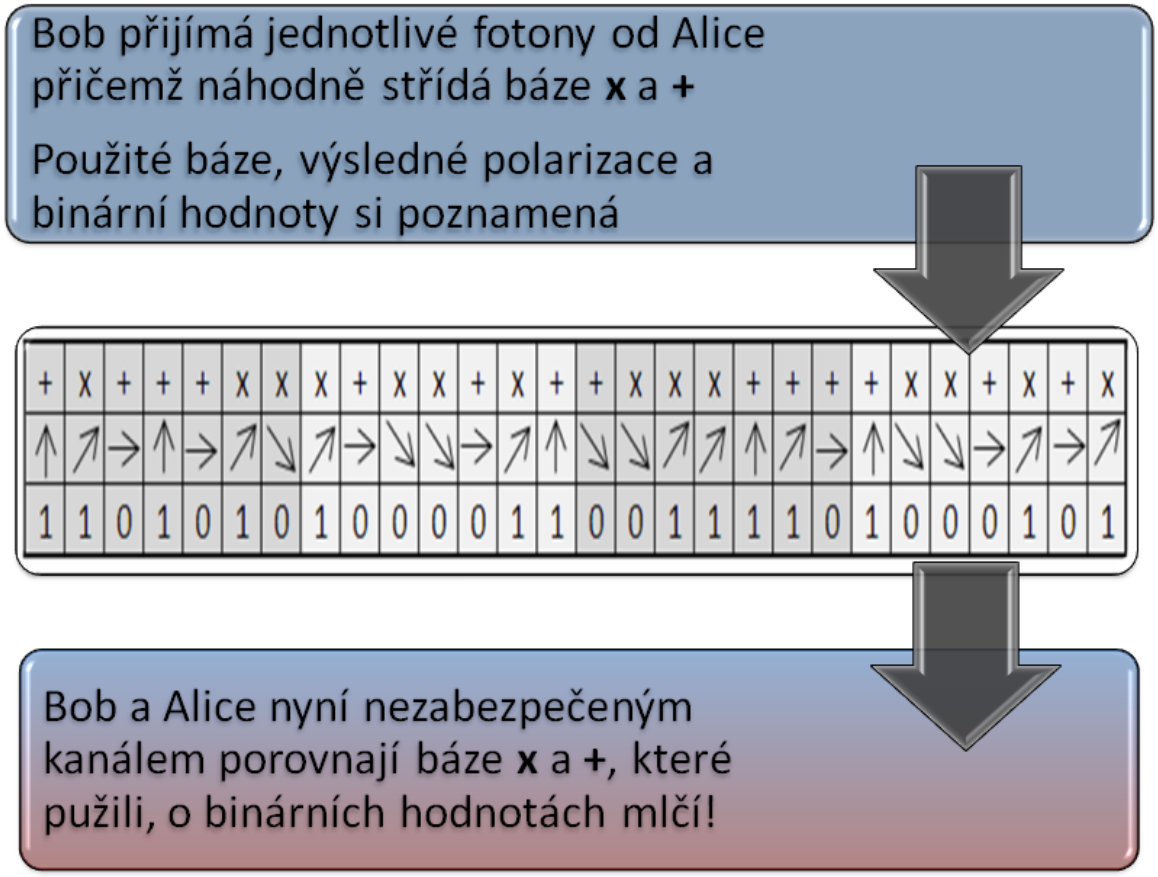
Pro každý bit zvolí náhodně jednu z bází **x** nebo **+**

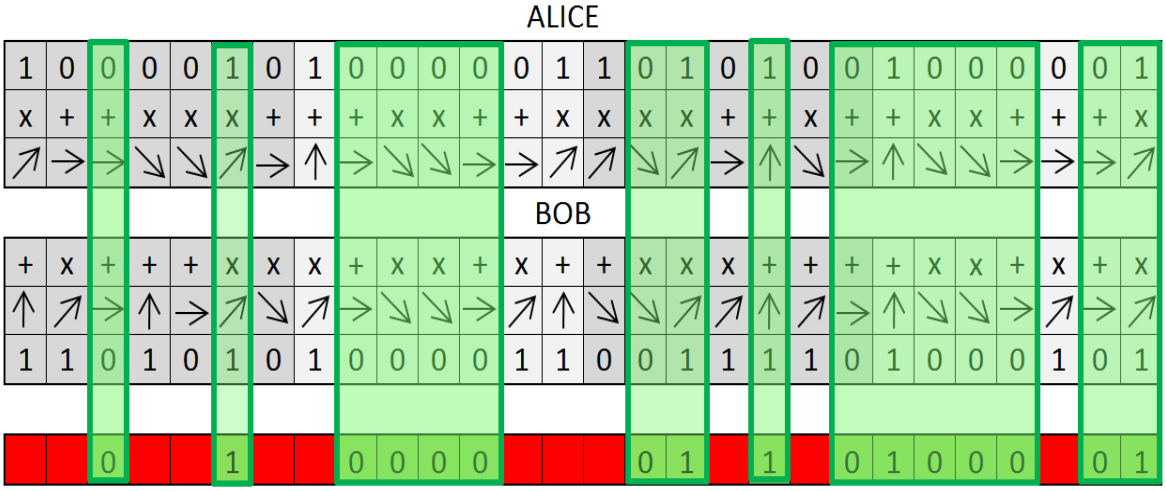


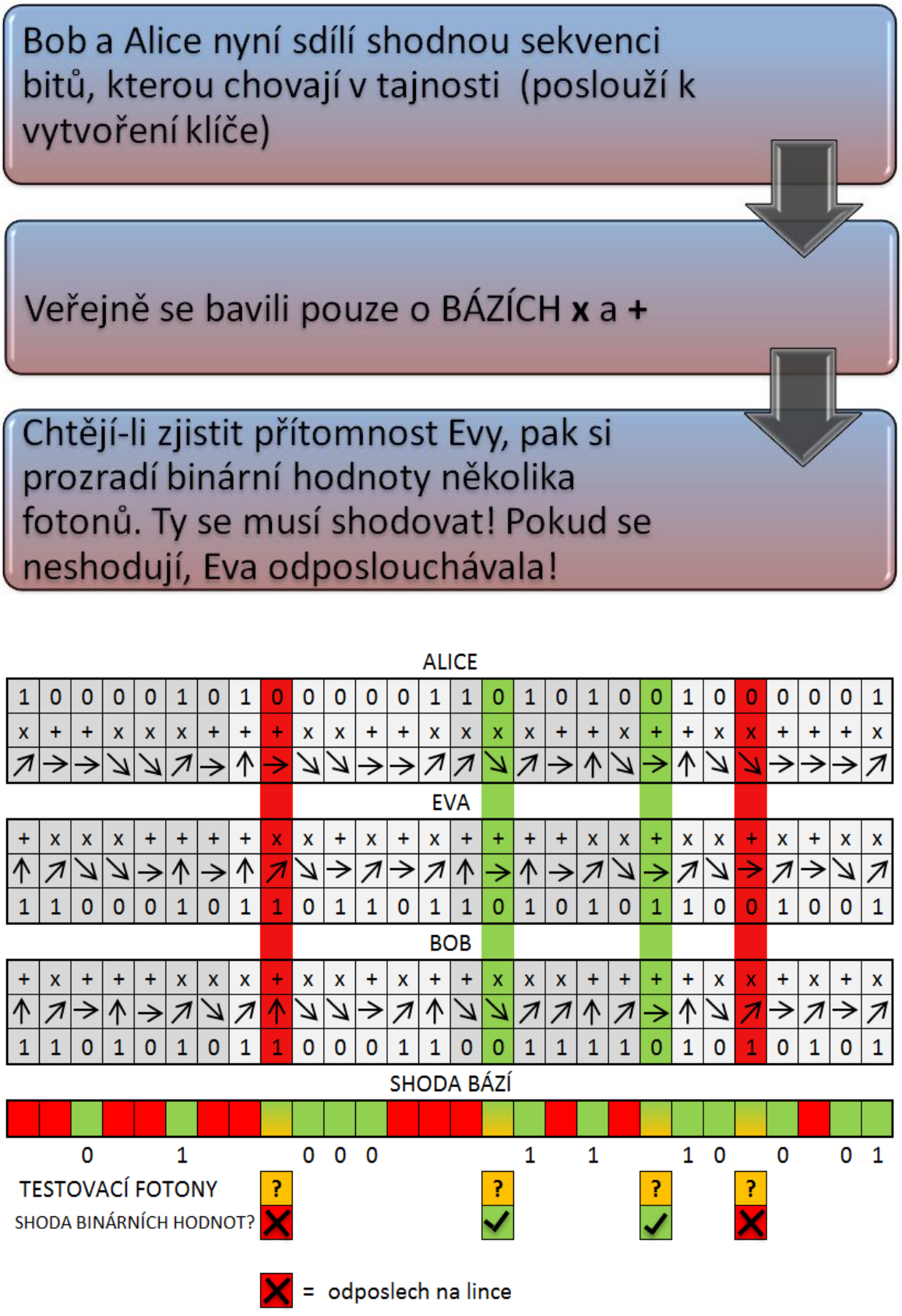
Jednotlivé polarizace fotonů (↑→↗↘) jsou určeny dle binární hodnoty a použité báze **x** nebo **+**

1000010							1000001							1010100							1000001						
1	0	0	0	0	1	0	1	0	0	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0	0	0	1
x	+	+	x	x	x	+	+	+	x	x	+	+	x	x	x	x	+	+	x	+	+	x	x	+	+	+	x
↗	→	→	↘	↘	↗	→	↑	→	↘	↘	→	→	↗	↗	↘	↗	→	↑	↘	→	↑	↘	↘	→	→	→	↗

Emisi polarizovaných fotonů odešle Bobovi


Bob přijímá jednotlivé fotony od Alice
přičemž náhodně střídá báze x a +
Použité báze, výsledné polarizace a
binární hodnoty si poznamená
Bob a Alice nyní nezabezpečeným
kanálem porovnají báze x a +, které
pužili, o binárních hodnotách mlčí!


ALICE
BOB

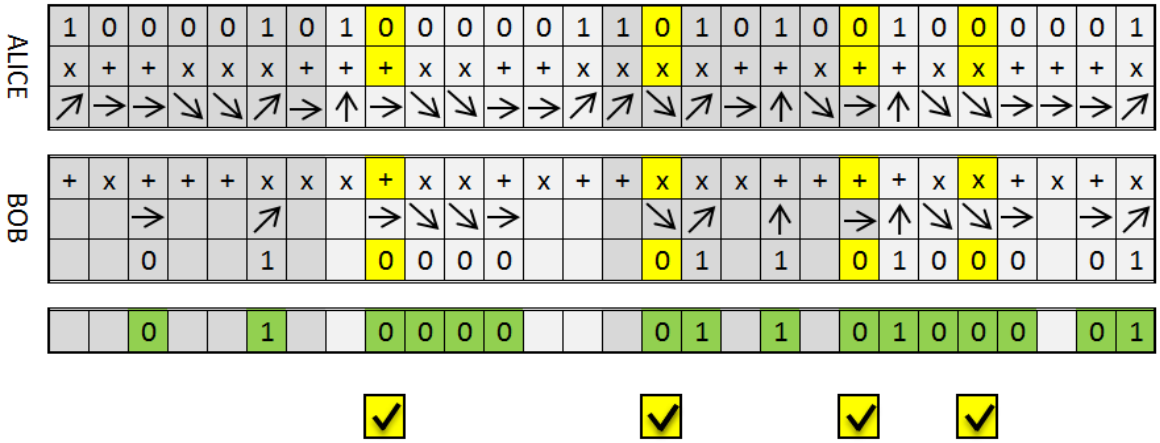


Obrázek 11 Grafické schéma protokolu BB84

4.4 Detekce přítomnosti odposlechu na lince

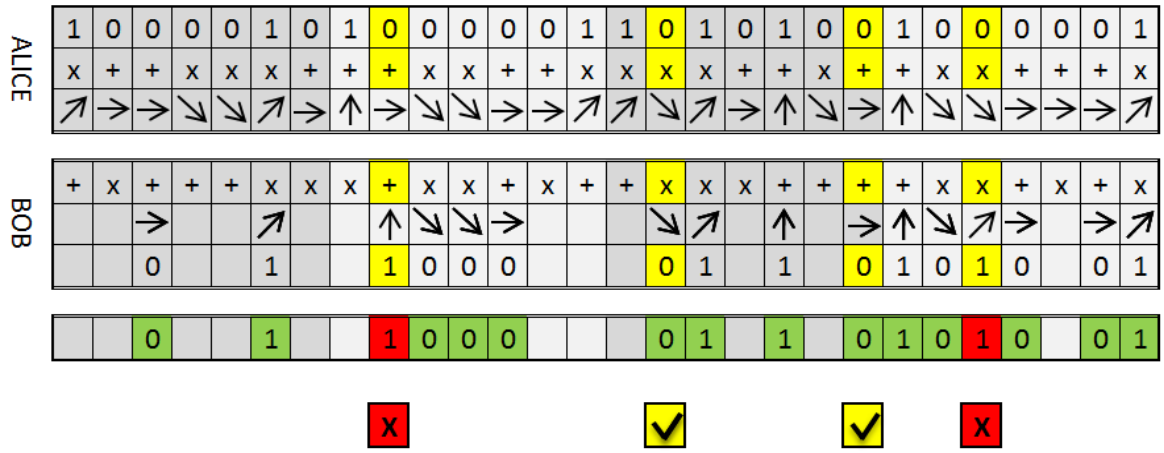
Následující dvě schémata názorněji demonstrují princip detekce přítomnosti odposlechu na lince protokolu BB84.

První schéma (obr. 12) obsahuje výměnu čtyř testovacích fotonů (žluté zvýraznění). Použité báze a binární hodnoty těchto fotonů se shodují. Alice s Bobem si mohou být jisti, že Eva tuto komunikaci nerušila.



Obrázek 12 Úspěšný přenos - detekce odposlechu negativní

Následující schéma (obr. 13) naopak simuluje tu situaci, kdy Eva narušila komunikaci mezi Alicí a Bobem. Jak již bylo uvedeno, Eva svým odposlechem změní polarizace některých fotonů. Důkazem detekce tedy bude ta skutečnost, že polarizace fotonů u nichž Alice i Bob volili shodnou polarizační bázi bude nestejná a tím i výsledná binární hodnota.



Obrázek 13 Neúspěšný přenos – detekce odposlechu pozitivní

Proces obětování sekvence již vyměněných bitů má za úkol detekovat případný odposlech. Vzhledem ke skutečnosti, že **Eva nemá technickou možnost nezměnit** odposlechnuté fotony, její odhalení je u dostatečně velké sekvence velmi pravděpodobné. Fotony, které posloužily k indikování odposlechu jsou nadále vyloučeny z procesu distribuce klíče. Ve skutečnosti je počet obětovaných fotonů minimální ve srovnání s celkovým počtem přenášených fotonů v dané relaci.

4.5 Pravděpodobnost odhalení odposlechu

V uvedeném příkladu je celý postup pro přehlednost demonstrován na řadě 28 bitů. Ve skutečnosti se pracuje s řádem kilo bitů (1000 a více). Tato skutečnost je dána tím, že při větším počtu bitů stoupá pravděpodobnost odhalení odposlechu, jelikož je možné použít více testovacích fotonů.

Pravděpodobnost, že Eva zvolí špatnou bázi, je 50%. Pravděpodobnost, že ve špatné bázi zvolí špatnou polarizaci fotonu je rovněž 50%. Součin těchto dílčích pravděpodobností je roven hodnotě 25%. Pokud tedy Eva nepřetržitě odposlouchává konkrétní relaci, pak způsobuje 25% chyb. Pokud Alice a Bob obětují *n* bitů, co by testovací fotony, pak je pravděpodobnost, že Eva nebude odhalena:

$$P = (1-0,25)^n = 0,75^n$$

Naopak pravděpodobnost, že Eva bude odhalena je:

$$P' = 1-0,75^n$$

Pokud si Alice a Bob vymění 100 testovacích fotonů, pak bude pravděpodobnost neodhalení Evy $P = 0,3*10^{-10}$ % a pravděpodobnost odhalení Evy P‘ = 99,99% [7].

Důležitým prvkem kryptografie obecně je **autentizace**[35]. Tento problém se nevyhýbá ani kvantové kryptografii. Eva totiž může použít takový postup, kdy de facto rozdělí komunikační kanál mezi Alicí a Bobem. Při komunikaci s Alicí se bude tvářit jako Bob, naopak k Bobovi se bude tvářit jako Alice. To je poměrně závažný problém. Kvantová kryptografie, respektive kvantová distribuce klíče řeší tuto záležitost následovně:

[35] Proces ověření identity dvou komunikujících stran

- Alice s Bobem na začátku komunikace zvolí konvenční způsob autentizace
- v průběhu procesu QKD použijí část zaručeně tajného klíče, který vzešel z kvantové distribuce, k příští autentizaci
- jinými slovy, nafouknou informaci plynoucí z QKD pro samotnou distribuci klíče a navíc pro autentizaci, kterou použijí při další relaci
- distribuce klíče pomocí kvantového protokolu slouží k samotnému přenosu klíče a část této zaručeně tajné komunikace slouží pro příští proces autentizace

4.6 EPR protokol

Je dalším kryptologickým prostředkem, který využívá principů kvantové fyziky. Tento systém je založen na tzv. **spinu**[36] **částic**.

Název protokolu je odvozen od **EPR paradoxu** (Einstein, Podolski, Rosen). Jde o přímý důsledek kvantové teorie. Pokud dojde ke změně některé z vlastností prvku společného systému, pak se tato změna projeví i na dalším prvku téhož systému. Platí i za předpokladu, že prvky totožného systému jsou od sebe libovolně vzdáleny.

Této zajímavé vlastnosti využil Arthur Eckert a v roce 1991 vytvořil protokol pro kvantovou distribuci klíče **E91**. Základem metody je kvantová propletenost dvojice částic. U takového páru částic nemá význam hovořit o jednotlivých složkách samostatně, ale o systému, jakožto celku. Jelikož jakákoliv změna na jedné složce vede k okamžitému ovlivnění složky druhé.

Ústředním prvkem protokolu a zároveň nositelem informace je **qubit.**[37] Přesněji je to právě spin qubitů, který hraje klíčovou roli. Dva qubity z jednoho systému mají celkový spin rovnající se nule. Lze si představit tak, že jeden qubit má spin po směru hodinových ručiček a druhý spin proti směru (přirovnání k běžně známé rotaci).

---

[36] vnitřní vlastnost elementární částice, která má blízký vztah k běžnému chápání točivosti, rotace objektu, ale není s ním zcela totožná [5]

[37] kvantové bity (angl. quantum bit = qubit)

Zákon o zachování úhlové hybnosti ukládá, že celkový nulový spin tohoto systému musí zůstat nezměněný, dokud pár existuje [5]. Zvláštností propletenosti částic (v případě kvantové kryptografie jde o fotony) je to, že se oba qubity mohou nacházet ve stavu superpozice. Tato skutečnost je podmíněna izolovaností systému. V okamžiku, kdy dojde k dekoherenci jedné ze složek systému a dosud superponovaná částice se stane lokalizovanou (dojde k měření na částici), druhá složka systému se stane taky lokalizovanou a to v přesně opačném spinu, než je ten, ve kterém je lokalizovaná první. Nezáleží na vzdálenosti, která obě složky systému dělí!

Realizace samotného kvantového přenosu probíhá odlišně od protokolu BB84. V případě EPR protokolu nejde o distribuci částic směrem od Alice k Bobovi. Zde vystupuje třetí strana, která generuje dvojice qubitů. Ty mají superponované spiny. Pokud má tedy první qubit spin rovný hodnotě 1, pak druhý bude roven 0.

Každá z komunikujících stran, Alice a Bob, získá jednu z dvojice fotonů. Tyto fotony dohromady tvoří systém, pro nějž je charakteristický nulový spin. Do okamžiku měření se obě částice nacházejí v superponovaném stavu. Jakmile Alice změří spin fotonu, pak jej lokalizuje. Pokud se měřený spin rovná hodnotě 1, pak foton, který má Bob musí mít spin roven hodnotě 0.

Alice měří přidělené qubity pomocí zcela náhodně vybraných bází. Stejně jak tomu bylo u protokolu BB84. Obě komunikující strany po ukončení relace posoudí použité báze a budou nadále vycházet jenom z těch, jejichž báze volili shodně. Stejně jako u BB84 půjde o 50% případů.

Změří-li Alice spin s hodnotou 1, pak je díky popletenosti částic jisté, že pro foton z téhož systému musí Bob změřit spin s hodnotou 0 a naopak.

Tento protokol poskytuje ochranu proti Evině odposlechu následujícím způsobem. Jestliže Alice a Bob disponujíc sekvencí fotonů měřenou shodnými bázemi, pak princip propletenosti zaručuje, že každý z nich naměří opačnou hodnotu spinu. To si ověří již uvedeným obětováním několika přenesených qubitů. Pokud byla Eva přítomna a relaci odposlouchávala, pak by došlo k narušení propletenosti a výsledky by neodpovídaly předpokládaným hodnotám. Tato skutečnost slouží, jako detekce odposlechu [1].

5 BEZPEČNOSTNÍ ÚROVEŇ A VYUŽITÍ

5.1 Srovnání QKD s asymetrickou šifrou

Pod pojmem konvenční šifrování je v této spojitosti uvažováno o asymetrickém šifrování typu RSA. Porovnáním kvantové distribuce klíče a jejího evolučního předchůdce, tedy asymetrické šifře, je cílem nastínit, v čem se QKD stala skutečně převratným bodem historie tohoto odvětví.

Koncept asymetrické kryptografie, který vznikl koncem 70. let 20. století, je vyústěním snahy najít určitý matematický model. Tento měl svou povahou splňovat vysoké nároky na prostředky výpočetní techniky při realizaci výpočtů tohoto modelu. Rozklad velkých čísel na prvočíselný součin je ideálním řešením.

Asymetrická šifra byla tedy koncipována a dodnes stojí na tom předpokladu, že **zatím nebyl vyvinut** takový technický prostředek, který by výrazně zkrátil čas potřebný k řešení matematické úlohy.

V případě algoritmu RSA je důležité poznamenat, že zvyšujícím se počtem vstupních dat při útoku na tuto šifru (délka klíče) **exponenciálně** roste počet elementárních operací, které je nutné vykonat. Tento poznatek ponechává algoritmu RSA určitou jistotu, že v dohledné době nebude možný útok vykonaný prostřednictvím konvenčních prostředků výpočetní techniky.

Kvantová distribuce klíče zakládá svoji bezpečnostní úroveň na samotných **principech a zákonitostech kvantové fyziky.** Je tedy nemožné vůbec uvažovat o takovém technickém prostředku, který by tyto zákony pomohl obejít a tím ohrozit bezpečnost QKD [6].

Nyní se kryptoanalýza dostává do poměrně složité situace. Historie je důkazem toho, že každý algoritmus, ač považován za sebebezpečnější, nakonec neodolal útokům kryptoanalytiků. V některých případech byl pokořen samotný algoritmus (např. Vigenérova šifra). V jiných bylo využito bezpečnostních mezer, které vznikaly slabou kryptografickou disciplínou, zaváděním určitých stereotypů a obecně nedokonalostí lidského faktoru (Enigma). V případě QKD se kryptoanalytici musí soustředit jen a pouze na bezpečnostní slabiny, které přímo nesouvisí se samotným algoritmem, protože ten je v tomto případě jištěn samotnými zákonitostmi kvantové fyziky.

5.2 Reálné využití QKD

V době vzniku protokolu BB84, tedy v 80. letech 20. století se QKD realizoval v laboratorních podmínkách na velmi malé vzdálenosti (řády desítek cm) za velmi malých přenosových rychlostí (jednotky bitů za sekundu). To bylo pro reálné nasazení systému naprosto nedostačující.

Hlavním nedostatkem byla absence technických řešení, která umožňovala pracovat s jednotlivými fotony na přijatelné vzdálenosti a s přijatelným datovým tokem. Vývojem optických vláken a modernějších detektorů fotonů se však tento problém začal odbourávat.

Počátkem 21. století začaly soukromé společnosti, které se orientují na vývoj zařízení sloužících pro kvantovou distribuci klíče, prodávat zařízení schopná přenášet fotony na vzdálenosti desítek kilometrů. Taková čísla jsou již uspokojivá.

Společnosti, které se vývojem QKD zabývají, již začaly implementovat své komerční systémy kvantové distribuce klíče i do veřejných optických sítí. Ostré nasazení kvantové kryptografie v armádě a to, že je v současnosti plně využívána, lze z největší pravděpodobností předpokládat.

Kvantová distribuce klíče, jak už její název napovídá, neslouží k samotnému šifrování otevřeného textu. Je to **prostředek, který je určen pro naprosto tajné sdílení klíče** mezi komunikujícími stranami. Samotný proces zašifrování otevřeného textu je realizován např. užitím one-time pad šifry. Je to podobná situace, jako u hybridního šifrování, kde asymetrická (bezpečnější) šifra slouží k vytvoření klíče, který je použit pro zašifrování OT pomocí symetrické šifry.

(PUŽMANOVÁ, Rita. Kvantová kryptografie pro bezpečnou distribuci klíčů. *Lupa.cz - server o českém internetu* [online]. 13.5.2004, 1, [cit. 2010-05-06]. Dostupný z WWW: <http://www.lupa.cz/clanky/kvantova-kryptografie-pro-bezpecnou-distribuci-klicu/>. ISSN 1213-0702.)

5.2.1 Konkrétní produkt v oblasti QKD

Americká společnost MagiQ je jedna z prvních, která přišla s konceptem komerčního nasazení systému kvantové distribuce klíče. Tato společnost se zabývá vývojem optických vláken, hi-speed elektronikou a v neposlední řadě zařízení pro aplikaci kvantové kryptografie.

Její technologické a komerční úspěchy deklaruje ta skutečnost, že do obchodních záběrů společnosti patří vládní organizace, jakými jsou NASA, U. S. ARMY a U. S. NAVY.

Vlajkový produkt společnosti v oblasti kvantové kryptografie je **MagiQ QPN™ Security gateway 8505.** Toto řešení v sobě kombinuje bezpečnostní prvky klasické **VPN**[38] a bezpečnostní přednosti kvantové distribuce klíče.

Systém navíc kombinuje nejsilnější konvenční principy výměny klíče spolu s těmi kvantovými. Zařízení je navíc umístěno v šasi, které je navrženo v proti-sabotážním provedení (tamper-evident chassis).

MagiQ QPN™ Security gateway 8505 disponuje plnohodnotnou optickou vrstvou pro QKD s vlastním vysílačem a přijímačem. Nejlepšími optoelektronickými součástkami. Funkcí pro obnovu klíče s frekvencí 100 změn za 1 sekundu. Plnohodnotným generátorem náhodných čísel. Prostřednictvím tohoto zařízení je možno realizovat přenos dat na vzdálenost až 100 km. Je plně kompatibilní s protokoly BB84, AES (256 bit), 3DES.

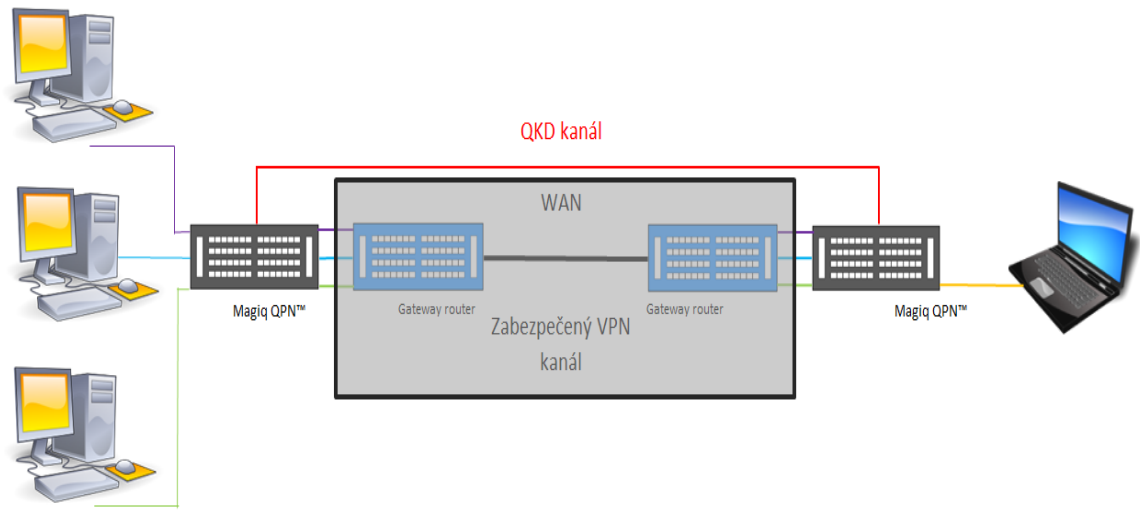
Produkt disponuje řadou standardních rozhraní (např. 16x RJ 45 konektor), nastavitelným 10/100 ethernetem apod. Samozřejmostí je, že splňuje celou řadu certifikačních standardů a to i mimo USA. Lze jej integrovat do systému **PKI**[39]**.** MagiQ QPN™ Security gateway 8505 Console je softwarové uživatelské rozhraní, které usnadňuje obsluhu celého systému, navíc napomáhá dokonalé kontrole nad procesem distribuce klíče včetně detailního nastavení.

Lze jej provozovat prostřednictvím veřejných optických sítí, což značně usnadňuje jeho nasazení a odpadá finanční i logistická náročnost aplikace tohoto systému.

---

[38] Virtuální privátní síť, spojení dvou stanic je realizováno prostřednictvím otevřené veřejné sítě (internet). To s sebou nese bezpečnostní rizika, proto je zabezpečení VPN ošetřeno autentizací komunikujících stran a šifrováním veškerého datového toku.

[39] Public Key Infrastructure – správa a distribuce veřejných klíčů v asymetrické kryptografii, ověřování elektronických podpisů bez nutnosti individuální kontroly



Obrázek 14 MagiQ QPN™ Security gateway 8505 (zdroj: www.magiqtech.com)

Schéma přenosu dat prostřednictvím Magiq QPN™ Security gateway 8505 (obr. 14) jasně deklaruje rozdělení komunikačních cest na samotný přenos dat skrze zabezpečenou VPN a kvantovou distribuci klíče prostřednictvím běžného optického vodiče.

Systém zaručuje dokonalou bezpečnost právě tím, že odděluje problém distribuce klíče a samotný přenos informací. Pokud přesto dojde k detekci odposlechu na QKD relaci, pak je tato skutečnost indikována. Tento fakt zvyšuje samotnou bezpečnostní úroveň. Data se začnou přenášet až v tom okamžiku, kdy je detekce odposlechu na kvantovém kanále negativní.

(*Magiqtech.com* [online]. 2007 [cit. 2010-05-02]. Magiqtech. Dostupné z WWW: <http://www.magiqtech.com/MagiQ/Products_files/8505_Data_Sheet.pdf>.)

5.3 Předpokládaný vývoj QKD

Konec první dekády 21. století se nese ve znamení postupného a velmi volného rozvoje QKD do soukromé sféry. Předmětem spekulací může být nasazení tohoto systému ve vládních a vojenských kruzích nejmocnějších zemí světa. Zaručené informace o nasazení QKD v těchto oblastech pochopitelně k dispozici nejsou, jelikož se jedná o citlivé sféry z hlediska vnitřní bezpečnosti.

Masivní rozšíření kvantové kryptografie do širšího soukromého sektoru však zatím očekávat nelze. Důležité je uvědomit si, že tento systém je stále ve fázi vývoje. Náklady na jeho pořízení a začlenění do dílčích informačních systémů mnohonásobně převyšují náklady, které souvisí s chráněným zájmem. Dalším důležitým faktorem je technická a provozní náročnost systému.

Výše uvedený příklad systému Magiq QPN™ Security gateway 8505 je určen pro komerční použití, ale je třeba brát v úvahu jeho cenu. Ta se pohybuje v řádech desítek tisíc amerických dolarů. Je tedy nepravděpodobné, že se systém kvantové distribuce klíče bude ubírat podobnou cestou, jako tomu bylo u systému PGP.

Navíc stále ještě existují takové kryptografické metody, které lze považovat za bezpečné. Hybridní šifrování (asymetrické + symetrické) je dostatečně bezpečným prostředkem pro nasazení ve firmách i pro soukromé účely. Otázkou však zůstává, na jak dlouho. Je zřejmé, že do okamžiku nalezení vhodného technického prostředku, který by prolomil bezpečnostní úroveň asymetrické šifry, nebude potřeba nahrazovat stávající kryptografické systémy natolik akutní, aby mohlo dojít k masivnímu nasazování QKD v podnikových informačních systémech [1].

5.4 Další využití kvantové teorie v oblasti bezpečnosti

Myšlenka **kvantového počítače** a obecně využití kvantové fyziky k výpočetním operacím je převážně dílem anglického vědce **Davida Deutsche.** Ten v osmdesátých letech dvacátého století přišel s konceptem výpočetního zařízení založeného na principech kvantové teorie. Konvenční prostředky výpočetní techniky se opírají o zákony klasické fyziky a tím pádem jsou jejich výpočetní kapacity poměrně omezeny. Kvantový počítač by byl postaven na bázi atomární úrovně a tím pádem by se opíral o zákonitosti kvantové fyziky, které nabízejí mnohem větší možnosti, co se výpočetních kapacit týká.

Základní jednotkou klasického počítače je tranzistor. Veškeré operace se realizují prostřednictvím binární soustavy. To je velmi praktické vzhledem k existenci dvou různých stabilních stavů tranzistoru. Vypnuto – Zapnuto.

Kvantové počítání využívá jednu ze základních kvantových vlastností částic. Na rozdíl od konvenčních obvodů, které se mohou v jednom okamžiku nacházet jenom v jednom

logickém stavu 0 nebo 1, může kvantový počítač díky charakteristice **qubitů** pracovat s hodnotou 0 i s hodnotou 1 zároveň.

Jednou ze základních charakteristik částic v kvantovém světě je to, že se může nacházet ve dvou stavech nebo místech najednou. Je to dáno vlnovou charakteristikou, kterou každá částice nese (superpozice).

Pokud je nějaká základní matematická úloha (např. faktorizace menšího čísla) řešena prostřednictvím konvenčního počítače, pak jsou jednotlivé úkony zařazeny do fronty. Provede se první úkon, porovná se s očekávaným výsledkem (předepsaným kritériem). Jestliže se výsledek neshoduje s očekávanou hodnotou, přichází na řadu další pokus. Proces pokračuje až do okamžiku, kdy výsledek odpovídá očekávané hodnotě a tím je úloha vyřešena.

Při výpočetně náročnějších úkonech je toto schéma dost svazující a je to právě tento důvod, proč doposud nebyla prolomena šifra RSA s dostatečně dlouhým klíčem.

Kvantový počítač by však mohl znamenat skutečný průlom. Je možné např. využít **spinu částic,** kdy pravotočivý spin by představoval logickou 0 a levotočivý logickou 1. Soustava sedmi částic s různými spiny by mohla představovat celkem 127 číslic v dekadické soustavě.

V pojetí klasické výpočetní techniky by jedna kombinace spinů znamenala jednu číselnou hodnotu. Pro testování rovnosti této hodnoty s předpokládaným výstupem by bylo potřeba vkládat a testovat jednu kombinaci sedmi spinů po druhé. To je ovšem časově náročné a problém konvenčního počítání to neřeší. Zcela jiná situace je za přítomnosti superpozic těchto částic. Pokud bude všech 7 částic dokonalé izolovaných od svého okolí a nedojde tím k dekoherenci, pak budou tyto částice v superpozicích a budou tedy představovat všech 128 možných kombinací najednou!

Je nutné však brát v úvahu tu skutečnost, že udržení částice v superpozici je možné pouze do té doby, než dojde k jakékoliv interakci s takovou částicí. To by mohlo znamenat skutečný problém, pokud by například kvantový počítač vyslal požadavek na výsledek směrem ke qubitům, v tom okamžiku by superpozice zanikla a výpočet by nebyl úspěšný. Z tohoto důvodu jsou kvantové počítače omezeny na určitý typ operací. Pokud však lze nějaký problém interpretovat do takové podoby, která bude povaze kvantového počítače

vyhovovat, pak bude jeho řešení vyžadovat minimální zlomek času oproti konvenčním počítačům.

Dalším úskalím je vytvoření vhodného programu pro takový počítač. Tímto se zabýval **Peter Shor** a **Lov Grover**. Tito dva vědci stojí za zrodem prvních programů, které by mohly být vhodnými kandidáty pro práci s kvantovými počítači. Navíc program Petera **Shora je vhodný právě pro faktorizace obrovských čísel, což je vlastnost, která se náramně hodí pro boj s RSA.**

V roce 2001 byl v laboratořích IBM proveden experiment s kvantovým počítačem. Tento pracoval se 7 qubity a faktorizoval číslo 15 na prvočíselný součin.

(KULHÁNEK, Petr. Kvantové počítače. *Aldebaran Bulletin* [online]. 2003, 21, [cit. 2010-05-06]. Dostupný z WWW: <http://www.aldebaran.cz/bulletin/2003_21_qua.html>.)

V roce 1977 byla uspořádána čtenářská soutěž o nalezení prvočíselných součinitelů čísla o délce 129 cifer. Faktorizace takového čísla zabrala stovkám počítačů téměř 8 měsíců. Pokud by byla myšlenka kvantového počítače realizována, pak by číslo milionkrát větší mohlo být faktorizováno za zlomek takového času! Je tedy zjevné, že koncept kvantového počítače je v hledáčku nejedné vládní organizace. Ten, kdo bude disponovat takovým zařízením, získá nástroj, kterým bude schopen prolomit dnes neotřesitelnou bezpečnost algoritmu RSA a tím se dostat k informacím nevídané hodnoty [1].

ZÁVĚR

Práce přinesla přehled názvosloví, které je spojeno s oblastí kryptologie. Byly zmíněny nejvýznamnější historické milníky tohoto odvětví a případy, které vstoupily do podvědomí široké veřejnosti.

Bylo poukázáno na rozmach metod užívaných v oboru kryptologie. Zejména propracovanost jednotlivých algoritmů, jejich bezpečnostní úroveň a vazby na technický rozvoj lidské civilizace. Popsána byla důležitost kryptologie v historii lidstva i její vliv na průběh největšího ozbrojeného konfliktu v dějinách.

Hlavní část práce se věnovala srovnání konvenčních způsobů kryptologie a zcela odlišné, kvantové kryptologie. Zaměřila se na obecnou charakteristiku kvantové fyziky, její základní principy a rozdíly, které ji odlišují od klasické fyziky. Uveden byl detailní příklad užití asymetrické šifry, tedy takové, která v dnešní době zatím splňuje bezpečnostní požadavky. Byl popsán příklad kvantové distribuce klíče, čili metody, která využívá principů kvantové fyziky. Tato byla porovnána s asymetrickou šifrou. Na základě těchto srovnání je tedy možné představit si, jakým evolučním krokem kvantová kryptografie bezesporu je.

Zmíněn byl taky konkrétní komerční systém, který ke své činnosti využívá vlastností kvantové kryptologie. Konkrétně jde o zařízení sloužící ke kvantové distribuci klíče. Tento produkt je uvolněn pro celosvětový trh, což znamená, že kvantová kryptologie se již stala součástí života nejširší veřejnosti.

Závěr práce se věnoval dalšímu užití principů kvantové fyziky v oblasti bezpečnosti. Zmínka padla o kvantovém počítači a jeho možném budoucím nasazení v boji s výpočetně náročným bojem s šifrou RSA.

ZÁVĚR V ANGLIČTINĚ

Work has led to an overview of terminology that is associated with the field of cryptology. Were mentioned the most important historical milestones of the industry and those that entered the public consciousness.

It pointed to the expansion of the methods used in the field of cryptology. Particular strength of the various algorithms, their level of safety and links to the technical development of human civilization. Described the importance of cryptology in the history of mankind and its greatest impact on the course of armed conflict in history.

The main part was devoted to a comparison of conventional methods and cryptology entirely different, quantum cryptology. Focused on general characteristics of quantum physics, its basic principles and the differences that distinguish it from classical physics. Given a detailed example of the use of asymmetric ciphers, ie, those who today still meets the safety requirements. He described an example of quantum key distribution, ie a method which uses principles of quantum physics. This was compared with an asymmetric cipher. Based on these comparisons it is possible to imagine how an evolutionary step in quantum cryptography is without a doubt.

Variety was also a particular commercial system, which utilizes its business properties of quantum cryptography. Specifically, the device used for quantum key distribution. This product is released for a worldwide market, which means that quantum cryptography has become part of life for the general public.

Conclusion of work devoted to the further use of the principles of quantum physics in the security field. Mention fell on a quantum computer and its possible future use in fighting with computationally intensive fight with RSA encryption.

SEZNAM POUŽITÉ LITERATURY

[1] SINGH, Simon. *Kniha kódů a šifer.* Vlastimil Klíma; Michaela Tichá; Petr Koubský, Dita Eckhardtová. 1. Dotisk vyd. Praha : Dokořán, 2007. 382 s. Aliter; sv. 9. ISBN 80-86869-18-7.

[2] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. 1. vyd. Brno : Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

[3] HAWKING, Stephen. *Ilustrovaná teorie všeho.* Vít Mrázek; Martin Žofka. 1. vyd. Olomouc : Argo, 2004. 119 s. ISBN 80-7203-575-4.

[4] HAWKING, Stephen. *Stručná historie času v obrazech.* Štěpán Kovařík; Vladimír Karas. 1. Dotisk vyd. Praha : Argo, 2002. 256 s. ISBN 80-7203-422-7.

[5] HAWKING, Stephen. *Vesmír v kostce.* Věra Amelová; Martin Žofka. 1. vyd. Praha : Argo, 2002. 216 s. ISBN 80-7203-421-9

[6] PIPER, Fred, MURPHY , Sean. *Kryptografie : Průvodce pro každého.* Pavel Mondschein. 1. vyd. Praha : Dokořán, 2006. 158 s. Průvodce pro každého . ISBN 80-7363-074-5.

[7] HÁLA, Vojtěch. Kvantová kryptografie. Aldebaran bulletin [online]. 2005, č. 14 [cit. 2010-01-21]. Dostupný z WWW: <http://www.aldebaran.cz/bulletin/2005_14_kry.php >. ISSN 1214-1674

SEZNAM OBRÁZKŮ

SEZNAM TABULEK