Středoškolská odborná činnost 2006/2007

Obor 01 – matematika a matematická informatika

Dějiny kryptologie, softwarový projekt ENIGMA

Autor:
Petr Koupý
Gymnázium Blansko,
Seifertova 13,
678 01 Blansko, 4. ročník

Konzultant práce:
Mgr. David Kopal
(Gymnázium Blansko)

Blansko, 2007
Jihomoravský kraj

Prohlašuji tímto, že jsem soutěžní práci vypracoval samostatně pod vedením Mgr. Davida Kopala a uvedl v seznamu literatury veškerou použitou literaturu a další informační zdroje včetně internetu.

V Blansku dne 14.2.2007

_____

vlastnoruční podpis autora

Obsah

1. Úvod

„Touha odhalovat tajemství je hluboce zakořeněna v lidské přirozenosti. Dokonce i ten nejméně zvědavý člověk zpozorní, dostanou-li se mu do rukou jinak nedostupné informace. Občas se sice někomu poštěstí získat zaměstnání, jehož náplní je řešení záhad, většinou jsme však nuceni uspokojovat svou dychtivost luštěním různých hádanek sestavených jen tak pro zábavu. Málokdo se dostane v luštění záhad dále než ke křížovkám a detektivním příběhům, řešení tajuplných kódů je seriózní činností jen pro několik vyvolených."

John Chadwick
The Decipherment of Linear B
(Rozluštění lineárního písma B)

Dějiny kryptologie jsou od počátku nekončícím bojem mezi kryptografy a kryptoanalytiky. Snaha o utajení informace je jednou ze základních vlastností lidského vývoje. Plyne to z jednoduchého faktu – pokud má člověk lepší informace než ostatní, má mnohem větší šanci ve společnosti uspět.

Když kryptograf vymyslí fungující šifru, začnou kryptoanalytici pracovat na způsobu jejího prolomení. Čas ukázal, že k takovému prolomení dříve nebo později vždy dojde. V té chvíli přebírají pomyslný štafetový kolík zase kryptografové a celý proces začíná znovu.

Úspěšnost šifrování často rozhodovala válečné konflikty a stojí tak v pozadí zásadních historických mezníků. Toto neustálé soupeření mezi tvůrci a luštiteli šifer vedlo k celé řadě významných vědeckých objevů. Obě strany tohoto souboje byly nuceny ovládnout mnoho disciplín lidského vědění, od technologií přes matematiku až po lingvistiku, v dnešní době také např. teorii informace, kvantovou fyziku atd. Kryptologie výrazně přispěla třeba ke vzniku moderních počítačů. Zajímavé je, že se často stávalo, že úctyhodné intelektuální výkony kryptografů nebo kryptoanalytiků nebyly zveřejněny kvůli utajení. Za svého života nebyli tito anonymové nikdy ohodnoceni, uznání jim bylo vyjádřeno často až o několik desítek let později, když už nebylo potřeba staré informace tajit. Mnoho z nich se toho však již nedožilo. I dnes mezi námi možná chodí anonymní géniové, kteří prolomili „dokonalé" šifry 20. století.

Zvláště v současném informačním věku hraje kryptografie zásadní roli v životě každého z nás. Hovory mobilních telefonů jsou šifrované, stejně tak peněžní transakce nebo citlivé přenosy informací přes Internet. Lidé si pomocí kryptografických metod mohou šifrovat svá data nebo posílat e-maily. Vyvstává však nová otázka. Tajné služby a policejní složky odjakživa používají odposlech komunikace k usvědčení zločinců z jejich trestných činů. Z tohoto důvodu byly vždy používány slabé šifry, které jedinec většinou nebyl schopen rozluštit, ovšem vládním institucím s řádově vyššími finančními prostředky to nečinilo problém. Dnes však existují díky novým technologiím a výpočetní technice neprolomitelné metody zašifrování zprávy. Na jednu stranu je to dobře, protože člověk by měl mít přirozené právo na soukromí. Vedlejším efektem ale je, že i zločinci a teroristé mohou komunikovat naprosto bezpečně, bez strachu z odhalení. Ceníme si více soukromí nebo bezpečnosti? Existuje nějaký kompromis?

Celá práce je členěna do tří etap lidské historie. V každé této etapě je popsáno několik šifrovacích metod, které ve své době hrály nejdůležitější roli a ovlivnily další běh událostí nebo vývoj pozdějších šifer. Tyto hlavní pilíře kryptologie jsou však lemovány více či méně úspěšnými šiframi, které není v možnostech rozsahu této práce popsat. Dále je v práci začleněn softwarový projekt, jehož cílem bylo navrhnout a naprogramovat jednoduchý simulátor kryptosystému ENIGMA, který by umožňoval dávkové zašifrování velkého objemu textu.

2. Základní pojmy

Steganografie (steganography) Nauka o skrývání existence zprávy. Pojem vznikl spojením řeckých slov *steganos* (schovaný) a *graphein* (psát). Ve starověku se dřevěné tabulky zalívaly vrstvou vosku, do které se psalo – pokud se tedy vyryl text do dřeva a následně překryl voskem, byla tabulka považována za nepopsanou a mohla bezpečně putovat k příjemci. Dalším způsobem bylo napsat zprávu na vyholenou hlavu otroka. Až vlasy narostly, mohla být zpráva doručena. Do steganografie patří také známé psaní neviditelným inkoustem. V současnosti lze zprávu schovat např. do počítačových obrazových formátů .bmp nebo .jpg. Steganografie je zvláště účinná pokud se používá společně s kryptografií – tzn. schovaný text je zároveň šifrovaný.

Kryptologie (cryptology) Věda o utajení zpráv ve všech formách zahrnující kryptografii a kryptoanalýzu.

Kryptografie (cryptography) Nauka o skrývání obsahu zprávy. Pojem vznikl spojením řeckých slov *kryptos* (skrytý) a *graphein* (psát). Pojem je někdy obecně používán pro vědu o čemkoliv spojeném se šiframi a je alternativou k pojmu kryptologie.

Kryptoanalýza (crypto analysis) Věda o tom, jak bez znalosti klíče odvodit otevřený text ze šifrového textu.

Otevřený text (plaintext) Původní zpráva před zašifrováním. Je zvykem psát jej malými písmeny.

Šifrový text (cipher text) Zpráva po procesu šifrování. Je zvykem psát jej velkými písmeny.

Šifra (cipher) Jakýkoliv systém nebo algoritmus pro ukrytí smyslu zprávy tak, že je každé písmeno v původní zprávě nahrazeno jiným písmenem. Systém by měl mít zabudovanou flexibilitu, známou jako klíč.

Substituční šifra (substitution cipher) Každé písmeno zprávy je nahrazeno jiným znakem, ale ve zprávě si zachovává svoji pozici.

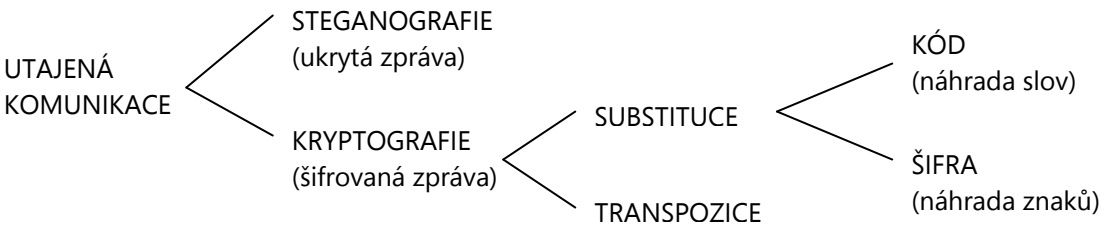
Transpoziční šifra (transposition cipher) Každé písmeno zprávy se přemístí ve zprávě na jiné místo, ale zachovává si svoji totožnost.

Kód (code) Systém pro ukrytí smyslu zprávy, který nahrazuje každé slovo nebo frázi jiným znakem nebo skupinou znaků. Seznam nahrazení je definován tzv. kódovou knihou. Systém nemá zabudovanou flexibilitu, protože existuje právě jeden klíč, jímž je kódová kniha.

Klíč (key) Element, který změní obecný šifrovací algoritmus ve specifický postup šifrování. Nepřítel může šifrovací algoritmus znát, ale nesmí znát klíč.

Symetrický klíč (symmetric key) Šifrovací i dešifrovací klíč je stejný. Používá se ve všech tradičních formách šifrování, to jest těch, které byly objeveny do 70. let 20. století.

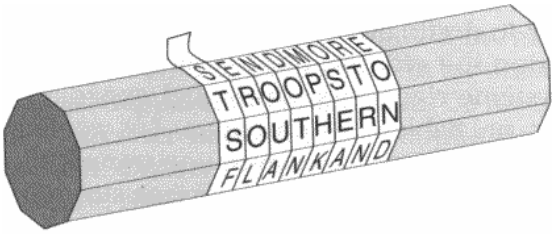
Asymetrický klíč (asymmetric key) Šifrovací a dešifrovací klíč je rozdílný. Každý jedinec má dva klíče – soukromý klíč a veřejný klíč. Tato metoda nevyžaduje přenos klíče mezi odesílatelem a příjemcem, čímž se značně zvyšuje bezpečnost. Příkladem kryptosystému s asymetrickým klíčem je RSA.



3. Starověk

V této kapitole je popsána nejpoužívanější starověká šifra, která se ve svých obměnách používala až do pozdního středověku, tzv. monoalfabetická substituční šifra. Jejímu používání předcházely některé transpoziční šifry, které byly teoreticky velmi bezpečné, ale zároveň časově velmi náročné při šifrování a dešifrování. Proto se používaly jednoduché systémy na zrychlení transpozice, jako třeba *scytale* - namotávání proužku se zprávou na úzký dřevěný válec, z něhož se následně přečetly jednotlivé řádky písmen (viz *Obrázek 1*). Následná kryptoanalýza však byla kvůli tomu natolik jednoduchá, že stačilo pouze vyzkoušet několik dřevěných válců s různým průměrem. Obecně řečeno bylo efektivní transpoziční šifry dosaženo až s příchodem informačních technologií.

Dále je v této kapitole popsáno rozluštění egyptských hieroglyfů a lineárního písma B. Starověká písma samozřejmě nemají nic společného s kryptografií. Záměrem starověkých písařů určitě nebylo schovat před námi informace. To je způsobeno tím, že jejich písmo je dávno zapomenuto. A tak přesto, že starověká písma nejsou skutečnou šifrou, jejich rozluštění si vyžaduje téměř stejný přístup jako kryptoanalýza libovolné šifry. Proto jsou zde zmíněny.



Obrázek 1: Scytale s namotanou zprávou.

3.1. Monoalfabetická substituční šifra

Jediná šifra, která se ve starověku rozsáhle uplatnila, byla monoalfabetická substituční šifra. Její první použití je popsáno Caesarem v Zápiscích o válce galské. Šlo pouze o nahrazení římských znaků řeckými. Caesar však používal také tzv. Caesarovu posunovou šifru, kde každé písmeno zprávy nahrazoval písmenem, které se v abecedě nacházelo o 3 místa dále. Tímto způsobem vznikají dvě abecedy – otevřená abeceda a šifrová abeceda. Pokud je napíšeme pod sebe, dostáváme tím klíč, protože vidíme, které písmeno šifrové abecedy odpovídá určitému písmenu v otevřené abecedě. Caesar používal posun o 3 místa, v principu však nic nebrání posunu o libovolný počet míst nebo dokonce libovolnému přeházení písmen v šifrové abecedě, čímž dostáváme řádově 400 kvadriliard možných šifrových abeced (klíčů). Pokud bychom vyzkoušeli každou vteřinu jeden klíč, trvala by nám kryptoanalýza miliardkrát déle než je dnes odhadovaná doba stáří vesmíru.

Otevřená abeceda	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Šifrová abeceda	J	L	P	A	W	I	Q	B	C	T	R	Z	Y	D	S	K	E	G	F	X	H	U	O	N	V	M
Otevřený text	e	t		t	u	,		b	r	u	t	e	?													
Šifrový text	W	X		X	H	,		L	G	H	X	W	?													

Tabulka 1: Příklad použití obecné substituce.

Po celý starověk byla tato šifra zárukou bezpečí. K jejímu prolomení došlo až v 10. stol. n. l. v islámských zemích. Pro srovnání – ve středověké Evropě došlo k tomuto objevu o 500 let později. Arabští kryptoanalytici se na základě dobré ekonomické situace a náboženství, které jim přikazovalo rozvíjet se ve všech oblastech lidského vědění, dostali na potřebnou úroveň vědomostí v matematice, statistice a lingvistice. Je známo, že v tehdejší státní správě se kromě citlivých textů šifrovaly dokonce i daňové záznamy.

Pro kryptoanalýzu monoalfabetické substituční šifry se využívá frekvenční analýza výskytu jednotlivých písmen v textu. Nejčastějším písmenem v anglicky psaném textu je písmeno **e** (12,7%), následuje **t** (9,1%), potom **a** (8,2%) atd. (viz *Tabulka 2*). Pro efektivní použití frekvenční analýzy je nutné mít dostatečně dlouhý šifrový text. Pokud je dlouhý pod 100 znaků, může dojít ke značným odchylkám ve výskytech písmen. Proto čím delší text je analyzován, tím větší je šance na úspěch. U frekvenční analýzy je také třeba znát jazyk, ve kterém je šifrový text napsán. Při luštění potom kryptoanalytikům ještě pomáhá lingvistika. Každý jazyk má své charakteristické znaky, např. jak často se určitá písmena vyskytují v sousedství jiných. Pro angličtinu je typický výskyt **h** před **e** (slova jako *the*, *then*, *they*), ale naopak velmi vzácný výskyt **h** po **e**. Navíc lze využít faktu, že se před podstatnými jmény píše určitý

člen. Pokud se v textu často opakuje samostatná trojice znaků, je velmi pravděpodobné, že se jedná o určitý člen *the*. Kombinací frekvenční analýzy a dobré znalosti vlastností daného jazyka lze snadno rozluštit i kratší nebo méně obvyklé texty.

Znak	a	b	c	d	e	f	g	h	i	j	k	l	m
Četnost [%]	8,2	1,5	2,8	4,3	12,7	2,2	2,0	6,1	7,0	0,2	0,8	4,0	2,4
Znak	n	o	p	q	r	s	t	u	v	w	x	y	z
Četnost [%]	6,7	7,5	1,9	0,1	6,0	6,3	9,1	2,8	1,0	2,4	0,2	2,0	0,1

Tabulka 2: Četnost znaků anglického textu. Vzorek pro vytvoření tabulky obsahoval 100 365 znaků.

Aby byla monoalfabetická substituční šifra odolnější vůči frekvenční analýze, lze použít tzv. *nuly* (klamače). Pokud bychom každé písmeno abecedy označily od 00 do 99, zbývá nám 74 nevyužitých čísel, které mohou být v textu náhodně rozházeny a kryptoanalytikovi tak ztíží rozluštění textu. Naproti tomu příjemce zprávy se dopředu domluví s odesílatelem jaké znaky má ignorovat (nuly jsou vlastně součástí klíče). Další možností je použití nespisovného jazyku nebo záměrných chyb v textu, což opět znemožňuje efektivní frekvenční analýzu. Posledním způsobem, jak substituci zdokonalit, je použití tzv. *nomenklátorů*, symbolů označujících celé slovo nebo skupiny slov. Přinášejí do šifry kódový prvek, který se opět musí stát součástí klíče.

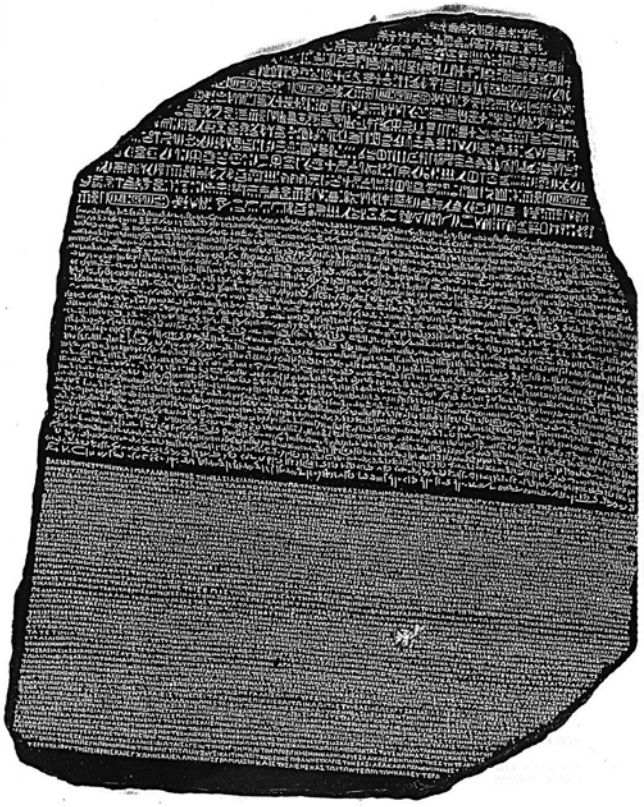
3.2. Egyptské hieroglyfy

Egyptské hieroglyfy (řecké slovo *hieroglyphia* znamená „posvátná plastika“) byly propracované symboly zdobící chrámové zdi asi od roku 3000 př. n. l. , avšak pro každodenní užití se souběžně s nimi vyvíjela zjednodušená forma nazývaná *hieratika*. Okolo roku 600 př. n. l. byla hieratika nahrazena ještě jednodušší *démotikou*. Všechny tři formy písma jsou fonetické, tzn. znak zastupuje určitý zvuk, stejně jako znaky moderních abeced. Ve 4. stol. n. l. však najednou egyptské písmo vymizelo. Příčinou bylo rozšiřující se křesťanství. Hieroglyfy byly časem zapomenuty.

V 17. stol. začaly první pokusy o zjištění jejich významu. Učenci si nechtěli připustit, že by tak stará civilizace mohla používat fonogramy, a tak byly hieroglyfy považovány za piktogramy. Vznikaly bláznivé výklady jednotlivých symbolů a z dnešního pohledu šlo spíše o lingvistickou alchymii než o seriózní výzkum.

Významný posun v luštění znamenal až nález Rosettské desky Napoleonovou armádou roku 1799 (viz *Obrázek 2*). Na desce je stejný text zapsán hieroglyfy, démotikou a řeckou alfabetou. Tímto byla získána obrovská nápověda. Vyvstaly však dva problémy. Jedním bylo značné poškození desky obzvláště v horní oblasti s hieroglyfy, což znamenalo že textu, který se nacházel zároveň ve všech třech oddílech, bylo poměrně málo. Druhým problémem byl neznámý egyptský jazyk, kterým se 800 let nemluvilo.

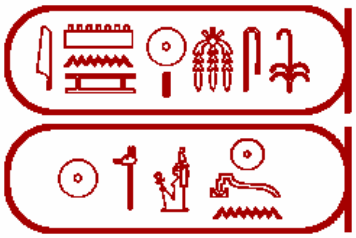
Prvním průkopníkem v luštění egyptského písma byl Angličan Thomas Young – fyzik, lingvista a také doktor. V hieroglyfické části Rosettské desky si všimnul krátkých zarámovaných skupin znaků,



Obrázek 2: Rosettská deska nalezená v Egyptě roku 1799.

tzv. *kartuší* (viz *Obrázek 3*). Stejné kartuše se v textu objevovaly i několikrát po sobě. Vzhledem k tomu, že v řecké části desky bylo několikrát zmíněno jméno Ptolemaios, Young se domníval, že kartuše by mohla vyjadřovat právě jméno panovníka, a tak se rozhodl přiřadit jednotlivým hieroglyfům jejich zvukové podoby. Tento postup zopakoval ještě na dalších kartuších z jiných nalezišť, ale potom svůj výzkum zastavil kvůli nátlaku přívrženců teorie, že hieroglyfy jsou piktogramy a fonetické použití hieroglyfů se používalo jen pro cizí řecká jména.

Jeho následovníkem se stal Jean-François Champollion, mladý francouzský lingvista. Pokračoval v Youngově výzkumu a přeložil několik dalších kartuší. Zlom však nastal až po nálezu reliéfů v chrámu Abú Simbel roku 1822. Jejich význam spočíval v tom, že byly dostatečně staré, aby neobsahovaly žádná řecká jména. Champollionovi se přeložením kartuše se jménem Ramsese podařilo dokázat, že hieroglyfy jsou skutečně fonogramy.

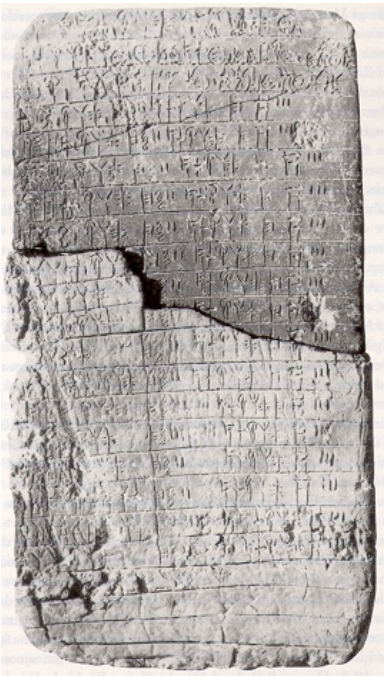


Obrázek 3: Kartuše s dvojím z mnoha verzí zápisu jména Ramsese.

Při překladu jednotlivých kartuší se zjistilo několik zajímavých věcí. Egyptští písaři často dbali na vizuální vzhled kartuše více než na text samotný, takže vynechávali samohlásky, některá písmena psali vedle sebe, jiná nad sebe. Některé slabiky nahrazovaly symboly (např. ve jméně Ramses, které bylo na kartuši zapsané jako *ra-meses*, byla celá slabika *ra* nahrazena symbolem slunce, a ne obvyklým znakem pro **r** a **a**). Často byly také nalézány odlišně vypadající kartuše, které však obsahovaly stejný text – každou psal jiný písař s jinými zvyklostmi.

I přes všechna tato úskalí se Champollionovy nakonec podařilo egyptské hieroglyfy rozluštit. Roku 1824, ve věku 34 let, zveřejnil všechny své objevy v knize *Précis du système hiéroglyphique*.

3.3. Lineární písmo B



Obrázek 4: Tabulka Lineárního písma B, datována kolem roku 1400 př. n. l.

V březnu roku 1900 sir Arthur Evans objevil ve vykopávkách v krétském Knossu dřevěnou truhlu plnou zachovalých hliněných tabulek s dosud neznámým písmem (viz *Obrázek 4*). Po bližším prozkoumání byly tabulky rozděleny do 3 skupin. První sada tabulek (2000-1650 př. n. l.) se skládala převážně z kreseb a jedná se pravděpodobně o piktogramy. Druhá sada (1750-1450 př. n. l.) byla popsána znaky s čistou linií, které byly následně pojmenovány lineární písmo A. Lineárním písmem A je psán známý Faistoský disk, na kterém jsou znaky psány do spirály. Toto písmo však stále čeká na své vyluštění, protože v současné době není dostatek nalezeného textu potřebného k jeho analýze. Poslední sada tabulek byla psána lineárním písmem B, kterého bylo nalezeno nejvíce a zároveň je nejmladší. Z tohoto důvodu byla největší šance na jeho rozluštění.

Brzy po nálezu bylo jasné, že se jedná o slabičné písmo – mělo 87 různých znaků (abecední písmo má 20-40 znaků, piktografické naproti tomu tisíce znaků). Tím však veškeré informace končily. Neexistoval žádný ekvivalent Rosettské desky, nic, co by archeologům dalo nějakou nápovědu. A navíc opět nebylo jasné, jakým jazykem je písmo psané. Přesto bylo písmo nakonec rozluštěno kombinací logiky a inspirace, které jsou mocným příkladem čisté kryptoanalýzy.

Z počátku se vytvořily dva tábory archeologů, které vedly spor o identitu jazyka pro písmo. Jedni tvrdili, že jazykem je řečtina, druzí oponovali, že je to minójština. 40 let nedošlo v luštění k žádnému pokroku. Nicméně v polovině 40. let se Alici Koberové, profesorce na americké Brooklyn College, podařilo udělat zásadní objev. Všimla si, že v textech se často objevují stejné skupiny znaků lišící se pouze zakončovacím znakem. Z toho usoudila, že se zřejmě jedná

o velmi ohebný jazyk, který koncovkou vyjadřuje rod, čas, pád a podobně. Pro zjednodušení přiřadila každému z 87 znaků dvojciferné číslo. Když si potom napsala skloňovaná slova pod sebe, přišla na další zajímavou věc. Předposlední slabika se v některých pádech lišila. Tento jev, nazývající se *přemosťující slabika*, je velmi charakteristický pro akkadštinu (viz *Tabulka 3*). Jde o to, že tyto předposlední slabiky mají společnou souhlásku, která je ještě součástí kmene, ale rozdílnou samohlásku, která je již součástí koncovky. Navíc pokud měla dvě rozdílná slova stejnou zakončovací slabiku, ale rozdílnou přemosťující slabiku, dalo se předpokládat že tyto přemosťující slabiky mají sice rozdílnou souhlásku, ale naopak společnou samohlásku. Na základě těchto myšlenek se již dala vytvořit tabulka vyjadřující určité vztahy mezi písmeny. Bohužel dále se Alice Koberová nedostala, protože v roce 1950 náhle zemřela.

	Slovo A	Slovo B	Akkadské slovo
První pád	25-67-**37**-57	70-52-**41**-57	sa-**da**-nu
Druhý pád	25-67-**37**-36	70-52-**41**-36	sa-**da**-ni
Třetí pád	25-67-**05**	70-52-**12**	sa-**du**

Tabulka 3: Dvě skloňovaná slova Lineárního písma B ve srovnání s akkadským slovem *sadanu*.

Plynule na ni navázal mladý anglický architekt Michael Ventris. Podle jejího schématu vytvořil komplexní tabulku vztahů jednotlivých znaků (viz *Tabulka 4*). Předpokladem pro další práci byl fakt, že pro slabičné písmo je charakteristické, že každá slabika se skládá vždy ze souhlásky a samohlásky. Pro anglická slova jako *minute* (minuta) to funguje. Problém však nastává třeba u slova *visible* (viditelný) a dále se stupňuje u slova *invisible* (neviditelný). Minójci by tedy museli tato slova zřejmě zapisovat jako *vi-si-bi-le* a *i-ni-vi-si-bi-le*. Tato úvaha znamenala pro Ventrise klíčový okamžik. Uvědomil si, že některá minojská slova musí začínat samostatnou samohláskou a navíc takových slov bude velmi málo. Proto začal hledat znak, který je na začátku slov jen velmi málo zastoupen. Našel znaky 08 a 61. Při tomto hledání však také narazil na 3 slova, která se v textu velmi často opakovala (08-73-30-12, 70-52-12 a 69-53-12). Shodou okolností jedno z nich obsahovalo na začátku velmi vzácný znak 08. Ventris použil svoji intuici a odhadl, že by to mohly být názvy důležitých měst. Jediné město, které odpovídalo schématu, byl Amnisos, důležitý přístav. Vyšlo mu tedy: 08-73-30-12=a-mi-ni-so=Amnisos. Když tyto 4 znaky doplnil do své tabulky, dostal kostru názvů zbylých dvou měst (70-52-12=?o-?o-so=? a 69-53-12=??-?i-so=?). Jediné vhodné názvy byly Knossos (70-52-12=ko-no-so) a Tulissos (69-53-12=tu-li-so). Z těchto tří slov již dostal tolik informací, že se z textů začala vynořovat slova velmi příbuzná řečtině. Postupně byla zaplněna celá tabulka vztahů a místo čísel měl Ventris jasné zvukové podoby slabik. Domněnka byla nakonec potvrzena – jazykem lineárního písma B byla vskutku velmi archaická řečtina.

	1	2	3	4	5
I					57
II	40		75		54
III	39				03
IV		36			
V		14			01
VI	37	05		69	
VII	41	12			31
VIII	30	52	24	55	06
IX	73	15			80
X		70	44		
XI	53				76
XII		02	27		
XIII					
XIV			13		
XV		32	78		

Tabulka 4: Ventrisova mřížka pro vztahy mezi jednotlivými znaky. Římské číslice značí souhlásky, arabské naproti tomu samohlásky. Tzn. všechny znaky z prvního sloupce mají společnou samohlásku atd.

4. Středověk

Prakticky po celý středověk se v Evropě používala monoalfabetická substituční šifra. Evropané byli přesvědčení o její neprolomitelnosti. Přestože v arabských zemích se již dávno používala frekvenční analýza, do Evropy tyto informace začaly přicházet až v průběhu 15. stol. Reakce se dostavila hned v 60. letech 15.stol. , kdy florentský umělec Leon Batist Alberti navrhl, že by se při šifrování mohlo používat více šifrových abeced zároveň. Svoji myšlenku však nijak nerealizoval, a tak musela Evropa na bezpečnější šifru čekat další století.

4.1. Vigenèrova šifra

Roku 1586 francouzský diplomat Blaise de Vigenère publikoval svoji práci *Traicté des chiffres*, ve které nejen ukázal slabiny monoalfabetické šifry a provedl její kryptoanalýzu, ale také popsal novou, polyalfabetickou šifru, údajně zcela odolnou vůči frekvenční analýze. Nová polyalfabetická šifra dostala jméno po svém vynálezci – Vigenèrova šifra, často se však lze setkat i s názvem *Le chiffre indéchiffrable*.

Vigenèrova šifra používá až 26 šifrových abeced, které jsou seřazeny pod sebou v tzv. *Vigenèrově čtverci*. Každá šifrová abeceda je vždy posunutá o jedno místo vůči té předchozí. Síla šifry spočívá v tom, že můžeme každé písmeno otevřeného textu šifrovat jinou šifrovou abecedou, čímž kryptoanalytikovi znemožníme použít klasickou frekvenční analýzu. Odesílatel se s příjemcem ale musí dopředu domluvit na pořadí použitých abeced. K tomu stačí dohodnout se na klíčovém slově. Mějme tedy otevřený text **invazezacnevecer** a klíčové slovo **UTOK**. Napřed si napíšeme otevřený text a nad něj několikrát po sobě klíčové slovo. Vezmeme první písmeno klíčového slova – to udává řádek ve čtverci, a tedy šifrovou abecedu (v našem případě abeceda začínající **u**). Dále si všimneme prvního písmene otevřeného textu – písmeno **i** udává sloupec čtverce. Na průsečíku těchto dvou souřadnic se nalézá písmeno **C**. Tímto způsobem se následně zašifruje celý text (viz *Tabulka 5* a *Tabulka 6*).

Klíčové slovo	U	T	O	K	U	T	O	K	U	T	O	K	U	T	O	K
Otevřený text	i	n	v	a	z	e	z	a	c	n	e	v	e	c	e	r
Šifrový text	C	G	J	K	T	X	N	K	W	G	S	F	Y	V	S	B

Tabulka 5: Příklad použití Vigenèrovy šifry. Využívají se 4 šifrové abecedy.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	**G**	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	**C**	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tabulka 6: Vigenèrův čtverec použitý pro zašifrování textu z *Tabulky 5*.

Téměř 300 let byla Le chiffre indéchiffrable opravdu považována za nerozluštitelnou. Roku 1854 však anglický mnohostranný učenec Charles Babbage po sázce se svým zubařem navrhl postup, jak provést kryptoanalýzu Vigenèrovy šifry. Jedinou slabinou šifry je opakování klíče. Čím je klíč kratší, tím méně abeced je použito. Ovšem velmi dlouhý klíč je zase nepraktický na přenášení, čímž se zvyšuje riziko jeho prozrazení. Proto lze předpokládat, že délka klíče se bude pohybovat mezi 5 a 20 znaky. Dochází tak k zajímavému jevu – u dlouhých textů je velmi pravděpodobné, že různé předložky, spojky, členy, případně jiná častá slova budou zašifrována stejnou částí klíče. Kvůli tomu bude v šifrovém textu docházet k opakujícím se skupinám znaků. Dalo by se namítnout, že je možné, aby dvě rozdílné sekvence písmen zašifrované jinou částí klíče daly náhodou stejný výsledek. Tento jev je však naopak velmi nepravděpodobný, takže se může zanedbat. Pokud tedy po prozkoumání textu kryptoanalytik nalezne několik skupin opakujících se řetězců, může změřit vzdálenost mezi nimi. Tímto dostane několik možných délek klíče, které jsou určeny děliteli nalezených vzdáleností. Většinou však pouze jedna z těchto délek souhlasí s dělitelností všech nalezených vzdáleností současně. Pokud je odhalena délka klíče, jsou známy i skupiny písmen, které jsou šifrovány stejnou šifrovou abecedou. U každé takové skupiny stačí provést frekvenční analýzu a celý problém se tím zjednodušuje na luštění monoalfabetické substituční šifry.

Je až s podivem, že takový objev Babbage nikdy nepublikoval. Zřejmě mu v tom zabránila britská rozvědka kvůli tehdy probíhající Krymské válce. Roku 1863 však řešení publikoval jistý vysloužilý důstojník pruské armády jménem Friedrich Wilhelm Kasiski, který na ně přišel nezávisle na Babbagovi. Metoda kryptoanalýzy je tedy známá jako Kasiského test. Na Babbagovo prvenství historici přišli až ve 20. stol. při průzkumu jeho písemností.

4.2. Homofonní substituční šifra

Vigenèrova šifra se zpočátku příliš neujala, protože byla velmi náročná při šifrovacím a dešifrovacím procesu. Monoalfabetická substituce zase nedosahovala dostatečné bezpečnosti. Proto byl vytvořen kompromis nazývaný homofonní substituční šifra. Je to varianta klasické monoalfabetické substituce s tím rozdílem, že znaky mají podle své frekvence více zástupců pro šifrový text. Zástupci písmen jsou dvojciferná čísla, protože písmen je pro tento účel málo. Tak např. písmeno **a**, které má v angličtině přibližně 8% výskyt, bude mít 8 zástupců (dejme tomu 06, 15, 28, 33, 57, 64, 75, 89). Písmeno **q** se svým 0,1% výskytem ale dostane pouhého jednoho zástupce (třeba 44). Tímto způsobem je teoreticky zabráněno frekvenční analýze a šifra se velmi podobá polyalfabetické šifře. Je tu ale jeden zásadní rozdíl – v polyalfabetické šifře je možné, aby stejný zástupce v šifrovém textu představoval vždy jiný znak otevřeného textu. V homofonní šifře však zástupce 15 bude vždy znamenat písmeno **a**.

Přestože je homofonní substituční šifra oproti monoalfabetické výrazně bezpečnější, byla brzy také prolomena. Jak bylo již dříve zmíněno, každý jazyk má své specifické charakteristiky. Např. v angličtině po písmenu **q** vždy následuje jedině samohláska **u**. V kombinaci s nízkým výskytem obou písmen stačí v šifrovém textu najít tyto málo časté dvojice a vyzkoušet za ně dosadit právě zmíněná písmena. Jedná se vlastně o obrácenou frekvenční analýzu – luštitele zajímají znaky s nízkým výskytem a časté znaky jsou ignorovány. Kryptoanalýza je sice těžší, ale možná.

5. Novověk

Dalo by se říci, že 20. století bylo zlatým obdobím kryptologie. Začalo dvěma hroznými válkami, na jejichž pozadí došlo k několika naprosto zásadním kryptoanalytickým průlomům, bez nichž by možná dnešní svět nevypadal tak, jak jej známe. V 70. letech bylo objeveno asymetrické šifrování, které vyřešilo problém s přenosem klíčů a zároveň je s dnešní výpočetní technikou nerozluštitelné. Od 60. let se současně rozvíjela myšlenka kvantové kryptoanalýzy a kryptografie, jejichž rozluštění brání samotné fyzikální zákony našeho vesmíru.

5.1. Vernamova šifra

Je také známá jako *jednorázová tabulková šifra* (one-time pad) a funguje na stejném principu jako Vigenèrova šifra. Klíč zprávy ale musí být stejně dlouhý jako otevřený text. To s sebou nese několik problémů. Pokud má otevřený text tisíce znaků, musí i klíč být stejně rozsáhlý. Takový klíč je velmi obtížné distribuovat. Větším problémem je však vytvoření takového klíče. Nabízí se možnost použít nějaký známý text, dejme tomu ústavu Spojených států. To ale přináší riziko prolomení, protože každý jazyk obsahuje nějaká často používaná slova – v ústavě USA se např. velmi často vyskytuje pravidelný člen *the*. Takové pravidelnosti se samozřejmě při kryptoanalýze dá využít. Proto musí být klíč vytvořen naprosto náhodně. Dokonce i „náhodné" psaní na klávesnici není tak zcela náhodné – vzhledem k rozložení znaků a poloze rukou mají některé znaky vyšší frekvenci výskytu než jiné. Další možností je použít ke generování náhodných znaků počítače. Problémem ale je, že i generátory náhodných čísel se za náhodné považovat nedají – generují čísla podle určitého algoritmu, a proto jsou správně nazývány generátory pseudonáhodných čísel. Ač by se mohlo zdát, že kryptoanalýza je za takových podmínek přesto nemožná, s dnešní výpočetní technikou je realizovatelná. Pro opravdu náhodný proces musíme sáhnout do přírody – např. jaderný rozpad je kvůli své kvantové povaze skutečným generátorem náhodných čísel a je k tomuto účelu i používán. Posledním problémem je jednorázové použití klíče. Pokud by byl použit na více zpráv, kryptoanalytik by mohl srovnávat vztahy mezi oběma zprávami a hledat tak postupně znění klíče. Úspěch takového dešifrování je dokonce pravděpodobnější než v případě použití výše zmíněné ústavy USA.

Skutečná jednorázová tabulková šifra tedy musí splňovat 3 podmínky: klíč musí být stejně dlouhý jako otevřený text, musí být náhodně vytvořen a musí být použit nejvýše jednou. Pokud jsou tyto podmínky dodrženy, je matematicky dokázáno, že šifru nelze prolomit. Proto je považována za svatý grál kryptografie. Pro její neflexibilnost a nákladnost však nikdy nebyla použita v širokém měřítku.

5.2. ADFGVX

Při přenosu informací přes telegrafní spoje se většinou nebylo potřeba obávat zachycení zprávy nepřítelem. S vynálezem radiového přenosu se však situace změnila. Zprávy mohl zachytit kdokoliv, a tak muselo být použito dostatečné šifrování. Nové šifry, ač byly značně komplikované, byly pouze variacemi starých šifer. Příkladem je šifra ADFGVX, která se stala jednou z nejslavnějších šifer 1. světové války. Byla zavedena německou stranou hned na začátku války, aby byl zachován moment překvapení. Němci byli přesvědčeni, že ji nelze rozluštit. Šifra totiž kombinovala substituci a transpozici.

Napřed se náhodně vyplní mřížka 6x6 polí 26 písmeny abecedy a 10 čísly (viz *Tabulka 7*). Souřadnice sloupců a řádků jsou udány právě písmeny ADFGVX. Každé písmeno otevřeného textu je nahrazeno dvojící písmen z výše uvedené šestice. Tímto končí substituční část šifrování.

	A	**D**	**F**	**G**	**V**	**X**
A	4	r	a	i	0	n
D	c	7	h	6	x	v
F	q	l	2	e	u	3
G	8	g	k	t	z	d
V	p	9	o	1	y	j
X	f	s	b	m	w	5

Tabulka 7: ADFGVX mřížka.

Otevřený text	u	t	o	k	v	e	2	1	4	5
Substituční část	FV	GG	VF	GF	DX	FG	FF	VG	AA	XX

Tabulka 8: Substituční část ADFGVX šifry.

Pro transpoziční část šifrování je nutné vymyslet klíčové slovo, které se napíše do prvního řádku nové tabulky. Substituční část šifry se potom napíše pod něj. Následně se jednotlivé sloupce uspořádají podle abecedy vzhledem ke klíčovému slovu. Výsledná šifra vznikne po přečtení jednotlivých sloupců po sobě (viz *Tabulka 9*).

N	E	M	O
F	V	G	G
V	F	G	F
D	X	F	G
F	F	V	G
A	A	X	X

»

E	M	N	O
V	G	F	G
F	G	V	F
X	F	D	G
F	V	F	G
A	X	A	X

Tabulka 9: Transpoziční část ADFGVX šifry.

Šifrový text: VFXFAGGFVXFVDFAGFGGX

Šifrový text vzniká kombinací substituce a transpozice; příjemce a odesilatel musí sdílet substituční tabulku a transpoziční klíčové slovo. Zvolená šestice písmen ADFVGX je použita kvůli rozdílnosti jednotlivých znaků v Morseově kódu, což snižuje pravděpodobnost chyb v přenosu.

Začátkem června 1918, 2 měsíce po začátku války, bylo německé dělostřelectvo připraveno zahájit finální úder na Paříž. V té době však již francouzský kryptoanalytik Georges Painvin stihl odhalit tajemství zašifrovaných německých textů. Pařížská obrana mohla být posílena právě na místech, kam se měl německý úder směřovat. Další velkou ranou německé kryptografii bylo dešifrování tzv. Zimmermannova telegramu britskou rozvědkou. Telegram byl diplomatickou depeší určenou politickým představitelům Mexika. Obsahoval návrh společného jednání proti Spojeným státům, které dosud nebyly ve válce, ale jejich vstup do ní se v budoucnu jevil jako nevyhnutelný. Právě dešifrovaný text této depeše přesvědčil amerického prezidenta k okamžitému vstupu USA do války, čímž skončila i šance na německé vítězství. Němci si však své porážky na kryptografickém poli nebyli vědomi až do roku 1924, kdy Anglie již nepovažovala za důležité informace utajovat.

Šifra ADFVGX nebyla jedinou šifrou 1. světové války. Se všemi ostatními ale měla společné to, že používala staré principy, a proto byla velmi rychle prolomena. Kromě klasického šifrování také vznikl nový podobor kryptologie, tzv. analýza provozu. V době, kdy se zrovna luštila nová šifra a nebylo možné zprávy číst, se alespoň zjišťovala poloha vysílače zprávy. Vysílače byly často umístěny na lodích, ponorkách nebo na velitelských stanovištích. Z prostého sledování pohybu těchto objektů se často dal odhadnout záměr nepřítele.

5.3. Enigma

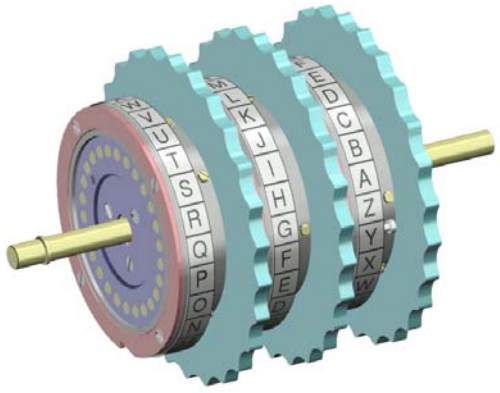
Obrázek 5: Armádní verze Enigmy se 3 scramblery.

Kryptoanalýza měla v 1. světové válce jasně navrch. Řešení krize nabídl však hned po válce německý vynálezce Arthur Sherbius. Jeho zařízení, nazývané Enigma, pracovalo na bázi polyalfabetické šifry v kombinaci s monoalfabetickou. Nešlo tak o žádný nový způsob šifrování. Síla Enigmy spočívala v něčem jiném – v mechanizaci šifrovacího procesu, což jej umožnilo natolik zkomplikovat, že byl teoreticky neprolomitelný.

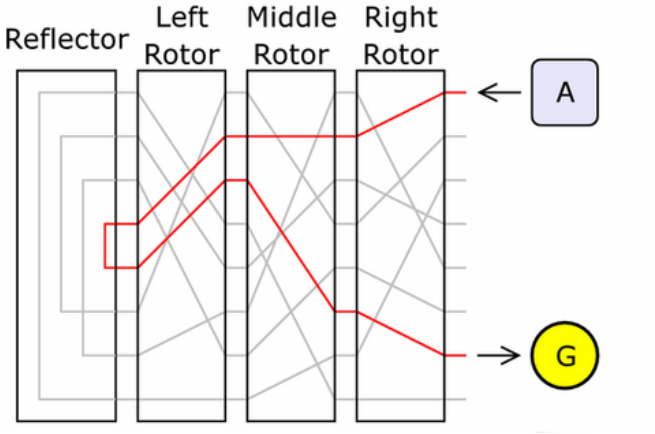
První verze Enigmy měla 3 otočné válce s 26 písmeny abecedy, tzv. *scramblery* (viz *Obrázek 6*). Scramblery byly vlastně mechanickou verzí Vigenèrova čtverce, protože střídaly jednotlivé šifrovací abecedy. Každý válec měl v sobě elektrické cesty, které elektrický impuls po otočení posílaly vždy jinudy, a tedy na jinou cestu v dalším scrambleru (tzn. pokud 2x po sobě zapíšeme písmeno **a**, vždy bude zašifrováno jinak). Abeceda na scrambleru byla vůči elektrickým cestám uvnitř fixovaná, v pozdějších verzích Enigmy se dala vůči cestám posunovat, což zvýšilo celkový počet možností nastavení (tento mechanismus se nazýval *prstenec*).

Pokud došlo ke kompletnímu otočení jednoho scrambleru, vedlejší se posunul o jedno písmeno atd. Každý válec šlo na počátku šifrování nastavit do jedné z 26 poloh. To dává dohromady 26x26x26=17576 možností (ve skutečné Enigmě to ale bylo kvůli mechanické konstrukci převodů pouze 26x25x26=16900). Válce se navíc mezi sebou daly uspořádat 6 různými způsoby.

Za všemi třemi scramblery byl ještě jeden prvek nazývaný *reflektor*, který zde byl z ryze praktických účelů konstrukce – nijak nezvyšoval počet možností nastavení. Jeho úkolem bylo, aby se Enigma dala používat jak při šifrování, tak i při dešifrování. Sekundárním efektem ale bylo, že žádné písmeno otevřeného textu nemohlo zastupovat sebe sama v šifrovém textu. To se na první pohled zdá být správné, ovšem snižuje to počet uvažovaných možností při kryptoanalýze.

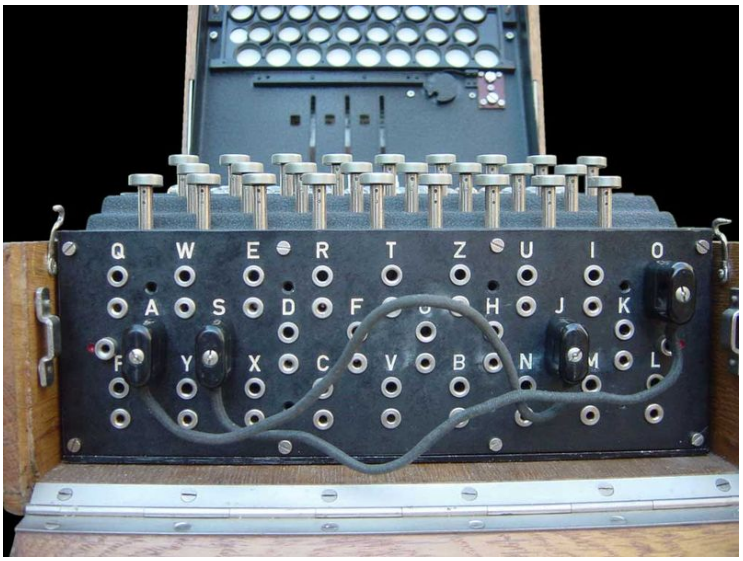


Obrázek 6: Tři navzájem zpřevodované scramblery .



Obrázek 7: Průřez scramblery a reflektorem. Uspořádání elektrických cest se při každém otočení mění.

Obrázek 8: Ve spodní části je klávesnice. Nad ní se nachází výstupní signální deska. Úplně nahoře je potom nastavení scramblerů.



Obrázek 9: Propojovací deska pod klávesnicí umožňovala sadou 6 kabelů zaměnit identitu až 6 párů písmen.

Vstupním prvkem Enigmy byla *klávesnice*, výstupním prvkem *signální deska* (viz *Obrázek 8*). Klávesnice byla propojena přes tzv. *propojovací desku* (viz *Obrázek 9*), která byla schopná zaměnit až 6 párů písmen šesticí kabelů. Nula až šest kabelů je takto možné zapojit 105578918576 způsoby.

Celkově měla Enigma 16900 x 6 x 105578918576 klíčů, což je přes 10 biliard. Je třeba zmínit, že pozdější Enigmy byly kromě prstence ještě vybaveny sadou dalších několika scramblerů a kabelů, takže operátor měl větší výběr. Tato pozdější opatření vedla k dalšímu násobení již tak velkého počtu klíčů.

Z toho lze vyvodit, že Enigma je ve své podstatě složena z dvojice jednoduchých mechanismů. První tvoří sada scramblerů, což je klasická polyalfabetická šifra, která s sebou však nese poměrně malý

počet klíčů. Naproti tomu propojovací deska odpovídá primitivní monoalfabetické šifře, ovšem do celého souboru přináší velmi velký počet klíčů. Kombinací těchto dvou mechanismů vzniká velmi silný kryptosystém.

Klíč šifrované zprávy je tvořen pořadím scramblerů (např. 3-1-2), jejich počáteční orientací (např. W-E-G) a nastavením propojovací desky (např.: A>L, P>S, D>V, K>J, O>Z, C>G). Tyto klíče byly distribuovány každý měsíc v tzv. kódové knize. Každý klíč byl stanoven na jeden den. Aby nebylo každý den šifrováno obrovské množství textu pouze jedním klíčem, zavedli Němci pravidlo, že denním klíčem bude šifrováno pouze prvních 6 znaků zprávy, které budou obsahovat 2x po sobě libovolnou počáteční orientaci scramblerů pro dešifrování zbytku zprávy. Opakování bylo pojistkou proti překlepu nebo radiové interferenci.

Sherbius s Enigmou slavil již od počátku úspěch. Poptávka po přístroji byla kromě soukromého sektoru a bankovnictví také v armádě. Pro každou část trhu byla sestrojena speciální verze Enigmy, která se lišila počtem a vnitřní strukturou scramblerů. Scherbiův vynález ve své době poskytl Německu nejdokonalejší šifrovací systém na světě.

Země Dohody se po válce destabilizovaného Německa nebály, a tak ani Francouzi ani Angličané nepodnikali kroky proti nové šifře. Jediná země, jejíž kryptoanalytici začali Enigmu luštit, bylo Polsko. Oddělení Biuro Szyfrow se ale bez dokumentace k armádní Enigmě nemohlo dozvědět správné vnitřní zapojení scramblerů. Problému pomohl neloajální zaměstnanec německého šifrovacího úřadu, Hans-Thio Schmidt, který za peníze poskytl francouzským agentům kompletní dokumentaci armádní Enigmy, na jejímž základě byla v Polsku vytvořena její replika. Na jejím prolomení začal pracovat mladý matematik Marian Rejewski.

Využil výše zmíněného opakování trojpísmenné orientace scramblerů na začátku zprávy. Přestože neznal denní klíč, mohl tvrdit, že mezi 1. a 4. písmenem zachycených zpráv je určitý vztah. Pokud za den zachytil dostatečný počet zpráv, byl schopen sestavit celou tabulku těchto vztahů. Dále Rejewského zaujalo, že jednotlivé návaznosti písmen v tabulce tvoří uzavřené smyčky.

	1.	2.	3.	4.	5.	6.
První zpráva	L	O	K	R	G	M
Druhá zpráva	M	V	T	X	Z	E
Třetí zpráva	J	K	T	M	P	E

Tabulka 10: Trojice zachycených zpráv.

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

Tabulka 11: Z dostatečného množství zpráv lze vytvořit tabulku vztahů.

A	>	F	>	W	>	A													3 spojení
B	>	Q	>	Z	>	K	>	V	>	E	>	L	>	R	>	I	>	B	9 spojení
C	>	H	>	G	>	O	>	Y	>	D	>	P	>	C					7 spojení
J	>	M	>	X	>	S	>	T	>	N	>	U	>	J					7 spojení

Tabulka 12: Nalezené smyčky a počty spojení mezi nimi.

Nalezení smyček a počtu spojení bylo zlomovým krokem, protože Rejewski brzy zjistil, že je jedinečné pro každé nastavení scramblerů a navíc nebylo závislé na propojovací desce – písmena v cyklech by sice byla jiná, ale na počet spojení by to nemělo vliv. Problém se z řádů biliard zredukoval na něco přes 100000 možných kombinací scramblerů. Rejewski strávil celý jeden rok vytvářením katalogu, v němž jednotlivé kombinace spojení odpovídaly dennímu klíči. Potom již stačilo nahlédnout do katalogu, nastavit podle kombinace počtu spojení odpovídající klíč a následně zprávu dešifrovat. Vlivem neznámého zapojení propojovací desky se samozřejmě vyskytly chyby, které bylo již jednoduché v kontextu odhalit a opravit. Přestože Němci po určité době změnili způsob vysílání zpráv a katalog přestal fungovat, Rejewski se nenechal odradit. Sestavil mechanickou verzi katalogu, přístroj, který postupně zkoušel všechny možné kombinace a zastavil se na té, která odpovídala dennímu klíči.

Přístroji se začalo říkat *bomba* (kvůli tikotu, který při práci vydával). Vzhledem k 6 možným kombinacím scramblerů muselo každý den pracovat paralelně 6 bomb.

Až do konce 30. let mělo Polsko jako jediný stát Evropy naprostou kontrolu nad německou komunikací. Roku 1938 však došlo k neočekávanému zvratu. Německo v přípravách na bleskovou válku zvýšilo bezpečnost Enigmy přidáním dalších 2 scramblerů a 4 propojovacích kabelů. Tím se zvýšil počet možných kombinací scramblerů ze 6 na 60 a počet zaměněných písmen z 12 na 20. Polsko v této situaci nebylo schopné vytvořit 60 paralelních bomb. Se svým tajemstvím se svěřilo 2 měsíce před válkou Anglii a Francii. Angličané po začátku války převzali po Polácích štafetový kolík.

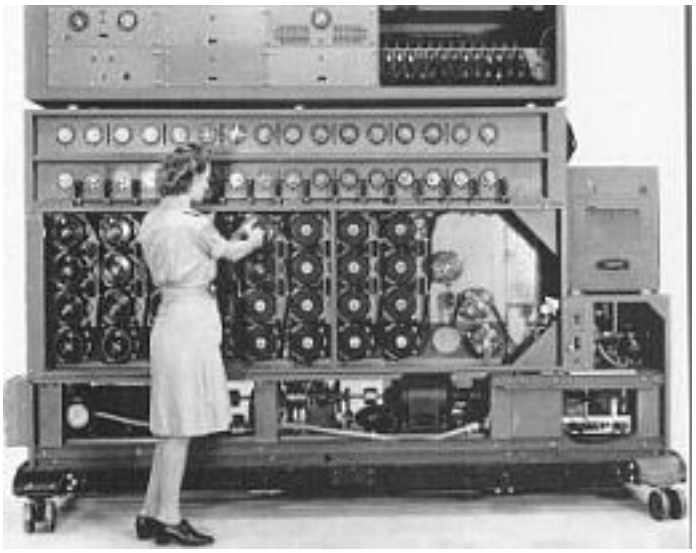
V hrabství Buckinghamshire, v Bletchley Parku, byla založena nová centrála britské kryptoanalýzy s dostatečným počtem pracovníků, aby bylo možné zvládnout očekávaný nápor informací. S pomocí Rejewského metody byli brzy schopni dešifrovat dokonce i námořní Enigmu se 4 scramblery (k tomuto účelu však museli přepadnout meteorologickou loď a ukrást jednu námořní Enigmu, aby znali její vnitřní zapojení). Britští kryptoanalytici se setkávali s velmi nedbale volenými klíči – někteří němečtí operátoři volili sekvence po sobě jdoucích písmen na klávesnici, jiní např. používali neustále dokola iniciály svých dívek apod. Navíc bylo zakázáno na propojovací desce spojovat vedle sebe ležící písmena, což opět o něco snížilo počet možností. Tak to fungovalo až do roku 1940, kdy Němci přestali na začátku opakovat klíč, což bylo stěžejním pilířem Rejewského metody.

Tento krok naštěstí dostatečně dlouho dopředu předpokládal Alan Turing, jeden z nejlepších matematiků Bletchley Parku. U zachycených zpráv si všiml, že např. předpověď počasí je posílána vždy ve stejnou hodinu a má vždy stejnou strukturu. Proto bylo možné s velkou pravděpodobností odhadnout pozici německého slova *wetter* (počasí). Tím pádem by stačilo pouze vyzkoušet jednotlivé orientace scramblerů, až by se objevilo požadované slovo. Při využití tohoto předpokladu však do hry znovu vstupuje propojovací deska a s ní i obrovský počet možností. Turing byl nucen vymyslet, jak ji opět eliminovat. Vydal se podobnou cestou jako Rejewski a začal hledat smyčky (viz *Tabulka 13*).

Odhadovaný otevřený text	w	e	t	t	e	r
Známý šifrový text	E	T	J	W	P	X

Tabulka 13: Uzavřená smyčka w > e > t > w.

Každou část této smyčky nechal řešit jednomu přístroji Enigma. V případě příkladu z tabulky 13 by byly scramblery druhého přístroje posunuty o jednu pozici a scramblery třetího přístroje o tři pozice. Tímto ovšem zatím nijak neklesl počet klíčů potřebných k vyzkoušení. Zásadním krokem bylo propojení těchto tří přístrojů tak, aby si navzájem předávaly své výstupy. Zde totiž došlo k zajímavému jevu – ať už byla propojovací deska zapojena jakkoliv, pokud se zapojily dvě po sobě, navzájem se vyrušily. Problém se tedy opět značně zredukoval a stačilo prověřit řádově menší počet kombinací. Turing nakonec sestrojil mnohem složitější variantu Rejewského bomby.



Obrázek 10: Turingova bomba.

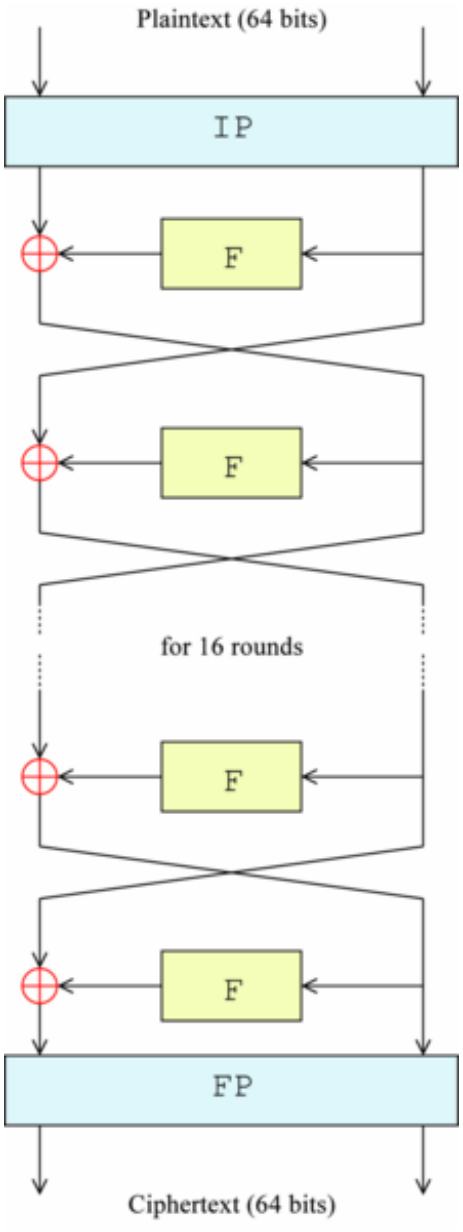
Ke konci války německé velení zavedlo novou, řádově komplikovanější mechanickou šifru Lorenz SZ40. I tuto se Turingovi podařilo prolomit – pomocí přístroje Colossus sestaveného z 1500 elektronek. Po celou válku byly německé depeše dešifrovány a vojenská strategie spojenců tak byla přímou reakcí na získané informace. Je třeba si uvědomit, že prolomení tak složitých šifer by nebylo možné, kdyby před válkou nebyla získána dokumentace od Schmidta, kdyby Němci neopakovali klíč, kdyby nedodržovali úplně stejnou strukturu meteorologických hlášení, kdyby nevolili ledabyle klíče a nakonec kdyby

si nebyli tak jistí neprolomitelností Enigmy. Druhá světová válka byla jasným vítězstvím kryptoanalytiků, bez nichž by možná dopadla úplně jinak (dá se setkat s tvrzením, že prolomení Enigmy válku znatelně zkrátilo a ušetřilo životy).

Bletchley park a úspěchy lidí, kteří v něm pracovali, byly dlouho střeženým tajemstvím a veřejnost se je dozvěděla až v průběhu 70. let. Alanu Turingovi byla po válce kvůli jeho homosexualitě soudně nařízena hormonální léčba, po které měl zdravotní a osobní problémy. Roku 1954, ve věku 42 let, jeden ze skutečných géniů kryptoanalýzy spáchal sebevraždu.

5.3. DES, AES

Informační věk s sebou přinesl i elektronické šifrování. Stále se jedná o klasické symetrické šifry, jejichž výhodou je, že výpočetní silou počítačů může být jejich složitost a komplikovanost dovedena až do extrémů. Každý znak je reprezentovaný 8 bitovým binárním číslem v ASCII (American Standard Code for Information Intercharge). Z toho plyne další výhoda – šifrování vlastně probíhá uvnitř jednotlivých písmen, protože substituci nebo transpozici podléhají jednotlivá binární čísla.



Obrázek 11: Feistelovo schéma DES.

Začátkem 70. let byl v laboratořích IBM Horstem Feistelem navržen kryptosystém Lucifer, který byl roku 1977 přijat jako americký šifrovací standart DES (Data Encryption Standard). Obrovská síla šifry se však nelíbila americké bezpečnostní agentuře NSA (National Security Agency), a proto do designu šifry před přijetím standartu značně zasahovala, aby byla svou výpočetní silou schopna šifru prolomit vyzkoušením všech klíčů (tzv. útok brutální silou – *brute force attack*). NSA proto snížila délku klíče na pouhých 56 bitů. DES byl díky tomu bezpečný pouze do konce 90. let, kdy výpočetní síla osobních počítačů stoupla natolik, že organizované skupiny kryptoanalytiků byly schopny spojením svých počítačů šifru rozluštit během jednoho roku (tzv. distribuované výpočty – *distributed computing*). Navíc byl také za 250 000 USD postaven stroj DES cracker, skládající se z 1536 čipů, který si s DES poradí během 56 hodin.

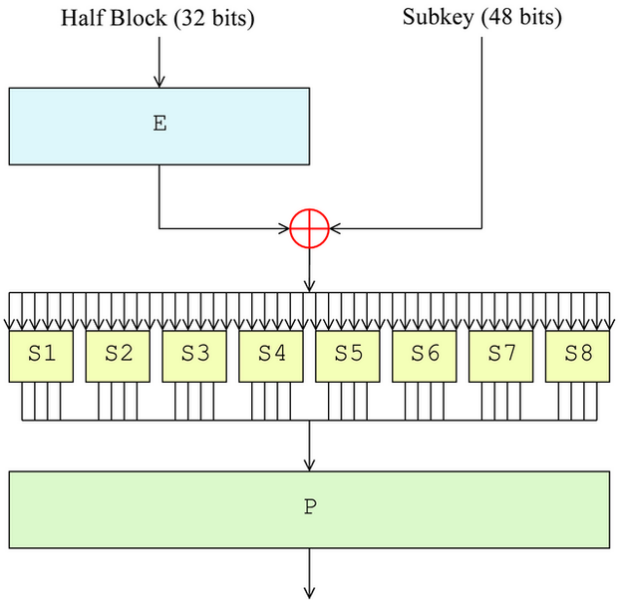
Základní princip DES vysvětluje Feistelovo schéma (viz *Obrázek 11*). Otevřený text v ASCII kódu je rozdělen na bloky po 64 bitech. Po inicializační permutaci (IP), která však nemá žádný kryptografický význam a je zde pouze kvůli lepší hardwarové implementaci, se blok rozdělí na dva menší, 32 bitové bloky. Pravý blok projde Feistelovou funkcí (F) a následně je pomocí logické funkce XOR (viz *Tabulka 14*) sečten s levým blokem. V další fázi šifrování si bloky vymění roli – původní pravý blok přechází do role levého bloku a výstup první fáze do role pravého bloku. Po proběhnutí 16 kol tohoto míchání dojde k finální permutaci (FP), která je opakem inicializační permutace. Výsledkem celého procesu je 64 bitový blok šifrového textu.

A	B	A **xor** B
0	0	0
0	1	1
1	0	1
1	1	0

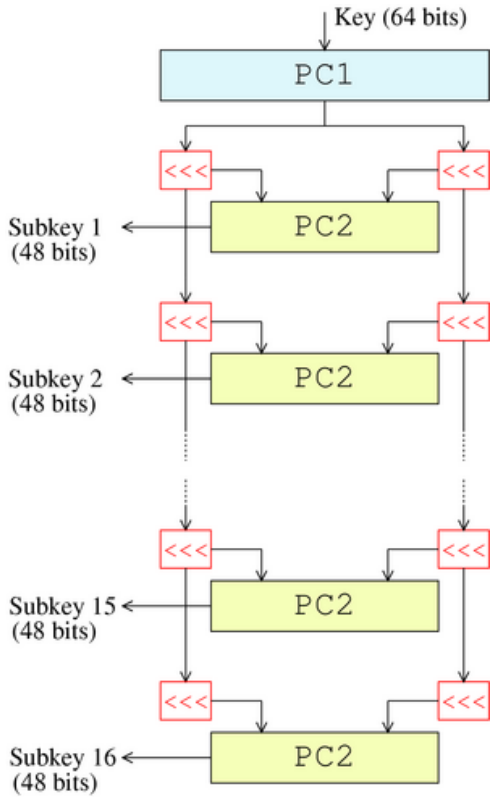
Tabulka 14: Logická funkce XOR, neboli eXclusive OR. Rozdíl oproti klasické funkci OR nastává, když jsou na vstupu dvě logické 1. XOR odpovídá ve výrokové logice negaci ekvivalence.

Samotná Feistelova funkce je rozdělena na 4 části (viz *Obrázek 12*):

1. *Expanze (Expansion)*
   Vstupní 32 bitový blok je pomocí duplikace některých bitů zvětšen na 48 bitů.
2. *Smíchání s klíčem (Key mixing)*
   48 bitový blok je pomocí funkce XOR sečten se 48 bitovým subklíčem, odvozeným z hlavního 64 bitového klíče (viz dále).
3. *Substituce (Substitution)*
   48 bitový blok je rozdělen na 8 částí po 6 bitech. Každá šestice je substituována 4 bity podle schématu nazývaného S-box (viz dále).
4. *Permutace (Permutation)*
   32 bitový blok je promíchán na základě pevného schématu nazývaného P-box (*Permutation box*).



Obrázek 12: Feistelova funkce.



Obrázek 13: Odvození subklíčů.

Odvození jednotlivých subklíčů probíhá následujícím způsobem (viz *Obrázek 13*). Z hlavního 64 bitového klíče je permutačním výběrem (PC1 – *permutation choice 1*) vytvořen 56 bitový klíč použitý pro vlastní šifrování. Zbylých 8 bitů slouží ke kontrole parity, kvůli možné chybě při přenosu dat. 56 bitů je následně rozděleno do dvou 28 bitových bloků. Každý z těchto bloků je o jeden nebo dva bity posunut doleva (v angličtině je použito slovo rotace). Následně se z každého 28 bitového bloku vytvoří dalším permutačním výběrem (PC2 – *permutation choice 2*) dvojice 24 bitových bloků, jejichž spojením vznikne subklíč. Tímto způsobem je vytvořeno 16 subklíčů, každý pro jedno kolo šifrování. Celý proces vytváření subklíčů se dá invertovat kvůli dešifrování, což je velmi důležité pro jednoduchou hardwarovou implementaci DES.

Substituční schéma (S-box – *Substitution box*) je stěžejní částí celého DES šifrování (příklad viz *Tabulka 15*). Přináší do kryptosystému nelineární prvek, bez kterého by byl snadno prolomitelný. Substituční schémata byla navržena a vygenerována podle speciálních algoritmů tak, aby byly vynechány jednoduše uhodnutelné varianty. Bohužel právě zde zasáhla NSA, když při schvalování návrhu všechna schémata změnila podle vlastních algoritmů.

	0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
00	0010	1100	0100	0001	0111	1100	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1100	0011	**1001**	1000	0110
10	0100	0010	0001	1011	1100	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1100	0100	0101	0011

Tabulka 15: Šestice vstupních bitů se rozdělí na vnější dvojici a vnitřní čtveřici – např. **0**1101**1** se rozdělí na **01** a 1101. Tyto dvě čísla pak určují souřadnice výstupní čtveřice bitů ve schématu – v tomto případě **1001**.

Po neúspěchu DES byla na přelomu tisíciletí vyhlášena volná soutěž o návrh nového symetrického kryptosystému. Vyhrál kryptosystém Rijndael (podle tvůrců – Vincent Rijmen a Joan Daemen), který byl roku 2002 přijat jako AES (Advanced Encryption Standard). Zpočátku byla délka klíče 128, 192 a 256 bitů. V současnosti se používá AES až s 512 bitovým klíčem. AES sice podlehl nově objeveným metodám jako diferenciální nebo lineární kryptoanalýza – je však třeba zmínit, že vždy šlo pouze o teoretické útoky, které počítaly s malým počtem kol a rozsáhlým šifrovým textem, z čehož plyne že kryptoanalýza AES je v praxi zatím nedosažitelná.

Mechanismus AES vychází z velmi složité matematiky, kterou zde není možné do podrobna popsat. Základní princip se ale velmi podobá DES. Na základě délky klíče je vytvořen odpovídající blok binárních čísel, která jsou následně rozdělena na čtverce 4x4. Tyto čtverce jsou dále promíchány jako u DES s využitím Rijndael funkce (počet kol záleží na délce klíče). Rijndael funkce se dá rozdělit do 4 hlavních částí (viz *Obrázek 14-17*):

1. *AddRoundKey*

   Podobně jako u DES je pole 4x4 bitů sečteno pomocí funkce XOR se subklíčem odvozeným z hlavního klíče.

2. *SubBytes*

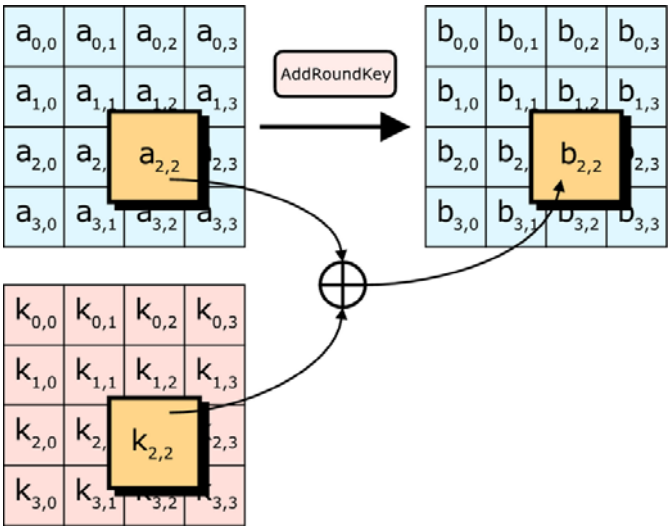
   Každý bit z čtvercového pole je nahrazen záznamem v substitučním schématu (S-box). Právě nový nelineární algoritmus při vytváření substitučního schématu tvoří zásadní rozdíl v bezpečnosti oproti DES.

3. *ShiftRows*

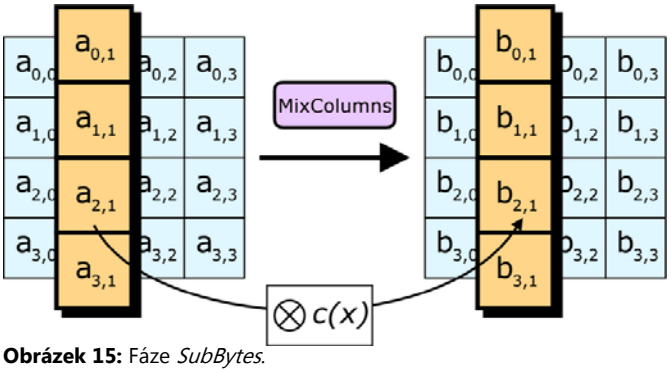
   Jedná se o promíchání jednotlivých bitů v poli. První řádek je zachován, ve druhém dochází k přeskočení o jedno místo, ve třetím o dvě místa a ve čtvrtém o tři místa.

4. *MixColumns*

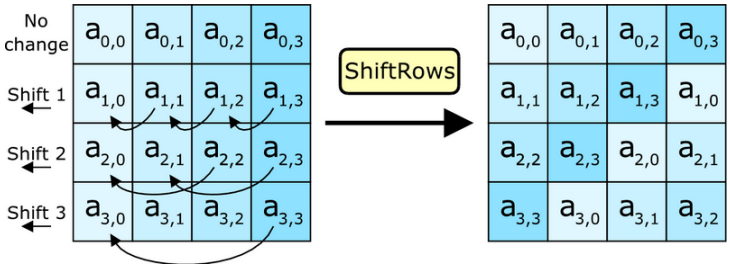
   Každý sloupec o 4 bitech je nahrazen novým sloupcem. Proces je tvořen lineární funkcí, ve které každý ze 4 vstupních bitů ovlivňuje všechny výstupní bity.



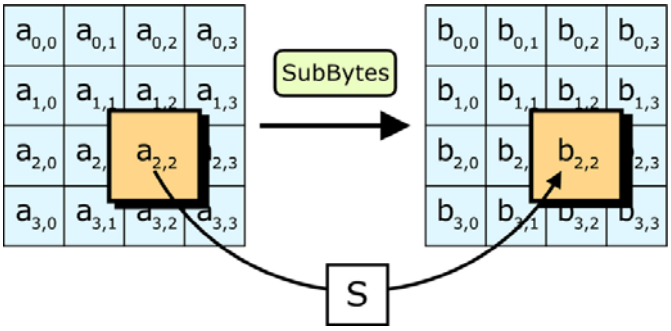
Obrázek 14: Fáze *AddRoundKey*.



Obrázek 15: Fáze *SubBytes*.



Obrázek 16: Fáze *ShiftRows*.



Obrázek 17: Fáze *MixColumns*.

5.4. DHM, RSA, PGP

Po celá staletí se kryptografie setkávala s jedním závažným problémem, kterým je distribuce klíčů. Příjemce a odesílatel zprávy si vždy před zahájením komunikace museli klíč předat. Tento fakt byl po celou historii považován za kryptografické dogma. Zároveň je to nejslabší článek sebelepší šifry, jelikož předání klíče lze odposlechnout. Distribuce klíčů byla pro vládní instituce vždy finančně velmi náročná a navíc činila i logistický problém – např. za 2. světové války se kvůli měsíčním kódovým knihám musely ponorky a lodě pravidelně vracet do svých přístavů. S příchodem informačního věku a obrovskému navýšení objemu přenosu informací se však tento problém stal nadále neudržitelný. Navíc finanční prostředky vydané vládou na zabezpečení své komunikace by pro libovolnou soukromou firmu znamenaly jistý bankrot.

Roku 1976 došlo k vyřešení problému distribuce klíčů. Je známo jako schéma DHM podle svých tvůrců – Whitfield Diffie, Martin Hellman, Ralph Merkle. Schéma se dá připodobnit k velmi jednoduchému myšlenkovému pokusu s bednou, ve které je zpráva, a visacím zámkem. Odesílatel do bedny vloží zprávu a zamkne ji svým zámkem. Následně ji odešle příjemci, který na ni přidá svůj vlastní zámek a odešle ji zpátky původnímu majiteli. Ten pouze odstraní svůj vlastní zámek a naposled odešle bednu k příjemci zprávy, pro kterého již není problém bednu otevřít. Je patrné, že k předání klíče nedochází. Pro matematickou realizaci tohoto myšlenkového experimentu byla potřeba jednosměrná funkce (příkladem z reálného světa je třeba smíchání dvou barev – proces je nevratný, jednosměrný). Všichni tři tvůrci věděli, že vhodné jednosměrné funkce by se mohly nacházet v modulární aritmetice - např. u funkce $3^x \pmod 7 = 1$ je velmi těžké zjistit hodnotu x. Po dvou letech plných usilovné práce a neúspěchů se roku 1976 dostavil výsledek, na který přišel Martin Hellman. Schéma DHM lze využít např. při distribuci klíče pro symetrické šifry jako DES nebo AES a značně tak zvýšit jejich bezpečnost.

Schéma je popsáno v následující tabulce. V popisování kryptologických mechanismů je zvykem nazývat odesílatele a příjemce jako Alici a Boba a možného nepřítele, který se snaží zprávu zachytit a rozluštit, jako Evu.

	Alice	Bob
Funkce	Pro jednosměrnou funkci $\mathbf{Y^x \pmod P}$ se telefonicky dohodnou na hodnotách **Y=7** a **P=11**. Eva může poslouchat.	
Krok 1	Zvolí číslo **A=3** a uchová je v tajnosti.	Zvolí číslo **B=6** a uchová je v tajnosti.
Krok 2	Vypočítá jednosměrnou funkci $\mathbf{Y^A \pmod P = 7^3 \pmod{11} = 2}$.	Vypočítá jednosměrnou funkci $\mathbf{Y^B \pmod P = 7^6 \pmod{11} = 4}$.
Krok 3	Číslo **α=2** zatelefonuje Bobovi. Eva může poslouchat.	Číslo **ß =4** zatelefonuje Alici. Eva může poslouchat.
Výměna	Sdělovaná čísla zatím nejsou klíčem, takže přestože je Eva zachytí nebude díky jednosměrnosti funkce schopna vytvořit klíč (protože nezná číslo A a B).	
Krok 4	Vypočítá jednosměrnou funkci $\mathbf{ß^A \pmod P = 4^3 \pmod{11} = 9}$.	Vypočítá jednosměrnou funkci $\mathbf{\alpha^B \pmod P = 2^6 \pmod{11} = 9}$.
Klíč	Oba dospěli ke stejnému číslu **9**, které činí klíč. Eva, která poslouchala všechny hovory, jej není schopná vytvořit.	

Tabulka 16: Příklad použití DHM schématu při výměně klíče.

Přestože schéma DHM byla pozoruhodná myšlenka, nebyl to kompletní kryptosystém, ale pouze způsob výměny klíče. Navíc se stále jednalo o symetrické šifrování, kdy šifrovací i dešifrovací klíč jsou identické. Opravdový zlom v dějinách kryptografie nastal roku 1977, kdy došlo ke zrození kryptografie s asymetrickým klíčem. Revoluční kryptosystém se podle svých tvůrců nazývá RSA (Ronald Rivest, Adi Shamir, Leonard Adleman). Princip spočívá v tom, že každý jedinec má dva klíče – veřejný a soukromý. Oba klíče jsou ve spojení jednosměrnou matematickou funkcí při vynásobení dvou prvočísel. Součin, který vzniká, je velmi náročné zpátky rozdělit na své prvočíselné činitele. Tento proces, známý jako faktorizace, je po celou historii ve snaze matematiků nějakým způsobem zkrátit, protože zatím všechna nalezená řešení mají exponenciální náročnost výpočtu. Zde tedy vzniklý součin reprezentuje veřejný klíč a dva prvočíselní činitelé tvoří soukromý klíč. Pokud chce Alice odeslat Bobovi zprávu, stačí

aby si třeba na Internetu našla jeho veřejný klíč, pomocí něhož zprávu zašifruje. Po šifrování je však i sama Alice neschopná zprávu dešifrovat – jediný člověk na světě, který je toho schopen, je Bob se svým soukromým klíčem. Celé šifrování RSA stojí na nemožnosti rychle faktorizovat velké číslo. Pokud někdy v budoucnu budeme schopni rychle faktorizovat, celá bezpečnost RSA se zhroutí. Například v roce 1994 bylo k rozložení 129 ciferného čísla zapotřebí 8 měsíců práce na více než 1000 počítačích. V praxi se dnes používá součin v řádu 10^{308} a více, což je současnou výpočetní technikou naprosto nedosažitelné. V následující tabulce je ukázán kryptosystém RSA na jednoduchém příkladu s velmi nízkými čísly.

1	Alice zvolí dvě prvočísla **p=17** a **q=11**, která uchová v tajnosti.
2	Alice vynásobí **p·q=N=17 · 11=187**.
3	Alice si dále zvolí číslo **e=7**. (čísla **e** a **(p-1) · (q-1)** nesmí mít společného dělitele)
4	Alice uveřejní svůj veřejný klíč, tvořený číslem **N** a **e** např. na Internetu.
5	Bob chce odeslat písmeno **X**, které převede do ASCII kódu. **X=1011000**, což v desítkové soustavě odpovídá číslu **88**. Získává tedy číslo **M=88**.
6	Bob nalezne veřejný klíč Alice a společně s číslem **M** jej dosadí do šifrovacího vzorce: $\mathbf{C=M^e(mod\ N)}$ $\mathbf{C=88^7(mod\ 187)=[88^4(mod\ 187)\cdot 88^2(mod\ 187)\cdot 88^1(mod\ 187)](mod\ 187)}$ $\mathbf{C=[132\cdot 77\cdot 88](mod\ 187)}$ $\mathbf{C=894432(mod187)=11}$
7	Bob pošle šifrový text **C=11** Alici. Pokud Eva text zachytí, není jej schopná dešifrovat, protože nezná soukromý klíč Alice.
8	Alice vytvoří svůj soukromý klíč **d** podle následujícího vzorce: $\mathbf{e\cdot d=1(mod\ (p-1)\cdot (q-1))}$ $\mathbf{7\cdot d=1(mod\ 16\cdot 10)}$ $\mathbf{7\cdot d=1(mod\ 160)}$ $\mathbf{d=23}$ (při výpočtu je nutné použít tzv. rozšířený Euklidův algoritmus)
9	Alice šifrový text **C** vloží do dešifrovacího vzorce: $\mathbf{M=C^d(mod\ 187)}$ $\mathbf{M=11^{23}(mod\ 187)=[11^{16}(mod\ 187)\cdot 11^4(mod\ 187)\cdot 11^2(mod\ 187)\cdot 11^1(mod\ 187)](mod\ 187)}$ $\mathbf{M=[154\cdot 55\cdot 121\cdot 11](mod\ 187)}$ $\mathbf{M=11273570(mod\ 187)=88}$
10	Alice převede číslo **88** do binární soustavy (**1011000**) a následně vyhledá odpovídající znak v ASCII kódu (**X**).

Tabulka 17: Jednoduchý příklad použití RSA.

Základní princip RSA je jednoduchý, jeho implementace v praxi s sebou ale nese několik problémů. V prvé řadě jsou potřeba velmi velká prvočísla pro získání dostatečně velkého součinu. U takto vysokých čísel je však exaktní otestování prvočíselnosti časově velmi náročné, takže se používá probabilistické testování prvočíselnosti na základě Fermatovy-Eulerovy věty (=Malá Fermatova věta), kdy stačí dosáhnout pravděpodobnosti $p=1-10^{-20}$. Pokud se ale náhodou testuje tzv. Carmichaelovo číslo, test je mylně vyhodnotí jako prvočíslo. Přestože je dokázáno, že Carmichaelových čísel je nekonečně mnoho, jsou naštěstí poměrně řídce zastoupena na číselné ose – pouze 16 čísel v řádu 10^5. Dále při odvození soukromého klíče je nutné použít složitější matematiku s využitím rozšířeného Euklidova algoritmu. I přes všechny problémy při softwarové nebo hardwarové implementaci činí RSA jeden z nejdokonalejších šifrovacích nástrojů, kterým lidstvo v současné době disponuje.

Pokud se RSA použije obráceně, tedy šifruje se soukromým klíčem a dešifruje se veřejným, vzniká ověření totožnosti známé jako elektronický podpis. Pokud odesílatel zašifruje zprávu svým soukromým klíčem a příjemce ji úspěšně dešifruje odesílatelovým veřejným klíčem, může si být příjemce jistý totožností odesílatele, protože nikdo jiný nemá odesílatelův soukromý klíč. Kombinací obou metod vzniká prakticky neprůstřelné šifrování. Napřed zprávu zašifrujeme soukromým elektronickým podpisem a následně veřejným klíčem příjemce. Ten zprávu přijme, dešifruje svým soukromým klíčem a vzniklý text znovu dešifruje našim veřejným elektronickým podpisem. Tím je zároveň zaručena jak totožnost, tak i bezpečnost.

Princip DHM a RSA byl však objeven již o 4 roky dříve v britském Government Communication Headquaters (GCHQ). V roce 1973 zde tuto myšlenku rozvedli dva vědci – James Ellis a Clifford Cocks.

Jejich objev nicméně skončil kvůli nařízení britské vlády pouze jako přísně tajný dokument v archivech GCHQ. Svět musel další 4 roky počkat, než bude princip nezávisle vynalezen akademickými vědci v Americe.

První veřejně použitelnou softwarovou implementaci RSA naprogramoval počítačový vědec Phil Zimmerman. Zveřejnění jeho výtvoru ale bránily hned dvě věci. Jednak nedostal povolení používat patentovaný systém RSA od společnosti RSA Data Security Inc. a dále použití RSA veřejností by znamenalo znemožnění odposlechu americkým bezpečnostním složkám, což bylo v rozporu s tehdejším zákonem. Nakonec se Zimmerman odvážil k riskantnímu činu, kdy roku 1991 uveřejnil kopii svého programu PGP (Pretty Good Privacy = Docela Dobré Soukromí) na tehdejším Usenetu (předchůdce world wide webu). Hned roku 1993 byl obviněn FBI z nelegálního vývozu zbraní z Ameriky (kryptosystémy byly v zákoně klasifikovány jako zbraň). Program se však po světě bleskově rozšířil, a proto po 3 letech soudního sporu bylo v roce 1996 obvinění staženo – federální úřady pochopily, že svůj boj prohrály. Roku 2002 Zimmerman založil svoji vlastní společnost PGP Corporation (www.pgp.com), která pravidelně software aktualizuje a vylepšuje. Z původně freewarového programu je dnes bohužel komerční produkt. Dřívější freewarové nebo alternativní verze programu lze stáhnout na adrese http://www.pgpi.com/.

5.5. Hashovací funkce

Přestože hashovací funkce nejsou přímo kryptosystémem použitelným k šifrování zpráv, zastupují důležitou úlohu v současné kryptografii. Jsou uplatňovány při vytváření elektronických podpisů, při rozeznávání hlasu a při kontrole integrity dat (při kopírování, stahování, kompresi, dekompresi atd.). Obecně jde o funkci, která z řetězce o libovolném počtu znaků vytvoří řetězec o pevném počtu znaků (viz *Tabulka 18*). Takový řetězec by měl být naprosto unikátní, ovšem již z definice hashe plyne, že musí existovat tzv. kolize – případy, kdy dvojice rozdílných vstupních řetězců dává stejný hash. Dobrá hashovací funkce se tedy musí vyznačovat tím, že pravděpodobnost kolize je velmi malá a umělý výpočet kolize je velmi složitý.

Vstupní řetězec	MD5 hash
Vim, ze nic nevim. Socrates	`08A99C0447038FC53B310875D65C3975`
Buh nehraje v kostky. Albert Einstein	`917F4A3113B43458D861053229FB370F`
velky pes	`AD4233AD43F6481EEFAE12DCBBEDD308`
velky les	`9C3620409BEE6A6871FBF249CD42CDC2`

Tabulka 18: Příklady MD5 hashe. Velikost výstupní hodnoty je 32 znaků.

Obecně fungují hashovací funkce na následujícím principu – vstupní řetězec je rozdělen na několik stejně velkých částí, které jsou následně jednotlivě zpracovány a každá z nich ovlivňuje výsledný řetězec. Hashovacích funkcí je navrženo poměrně velké množství, ovšem nejrozšířenější a nejznámější jsou MD (Message Digest), navržená Ronaldem Rivestem, a SHA (Secure Hash Algorithm), navržená NSA. Jejich verze, velikost řetězců a odolnost vůči kolizím je popsána v následující tabulce.

Funkce	Velikost výstupu	Počet znaků	Kolize
MD4	128 bit	32	Ano
MD5	128 bit	32	Ano
SHA-0	160 bit	32	Ano
SHA-1	160 bit	32	Ano
SHA-2	256/512 bit	32	Ne

Tabulka 19: Přehled nejpoužívanějších hashovacích funkcí.

Z tabulky je vidět, že bezpečnost hash funkcí je postupně prolamována. Např. MD5 byla prolomena v průběhu let 2005 a 2006 českým kryptologem Vlastimilem Klímou, který navrhl algoritmus, jak na obyčejném osobním počítači spočítat kolizi během několika sekund. SHA-2 se dosud zdá být bezpečná, ovšem její prolomení je zřejmě pouze otázkou času.

5.6. Kvantová kryptografie a kryptoanalýza

Ačkoliv fakta plynoucí z kvantové fyziky zní člověku na první pohled kontroverzně, je kvantový popis přírody to nejlepší, co dnešní věda má. Již celé jedno století z kvantových vlastností přírody lidská společnost těží – jaderné reakce, křemíkové procesory, laserové technologie atd. Kvantová fyzika zasáhla všechny vědecké oblasti a výjimkou nebyla ani informatika a kryptologie.

Již v 19. stol. přišel Thomas Young (podílel se na rozluštění egyptských hieroglyfů) na to, že svazky fotonů se při průchodu dvěma štěrbinami chovají podobně jako vlny na moři – za deskou se štěrbinami se vytvoří interferenční obrazec. Světlo má tedy vlnovou povahu. Překvapení však přišlo ve 20. stol., kdy technologie pokročila natolik, že vědci mohli stejný experiment provést postupným střílením vždy jen jednoho fotonu, který nechal na stínítku jasně rozlišitelný zásah. Po dostatečném počtu takto vystřelených fotonů vznikl z jednotlivých zásahových bodů opět interferenční obrazec. To však zdánlivě není možné, protože osamocený foton by neměl s čím interferovat. Výsledek pokusu lze vysvětlit mnoha způsoby. Foton je ve stavu superpozice, což znamená, že foton se jednoduše nachází v obou štěrbinách zároveň a interferuje sám se sebou. Nejznámějším vysvětlením je teorie mnoha světů, kdy se předpokládá, že realita se před průchodem fotonu štěrbinou rozděluje na dvě reality, které spolu posléze interferují. Tato a další teorie vždy vedou ke stejnému výsledku, který říká, že dokud není kvantový systém změřen, nachází se v superpozici všech možných stavů. Tento jev postihuje např. také spin, nebo-li rotaci, částice. Při pozorování bude spin vždy buď doprava nebo doleva, ovšem pokud se částice nachází v superpozici, rotuje na obě strany současně.

Právě kvantové vlastnosti spinu je využito v modelu tzv. kvantového počítače. Celý koncept rozvinul v roce 1984 David Deutsch. Normální počítač operuje s bity, které mohou nabývat hodnot 1 nebo 0. Oproti tomu kvantový počítač obsahuje qubity (quantum bit), které mohou nabývat hodnot 1 a 0 zároveň. Opravdový výkon kvantového počítače tedy plyne z toho, že několik qubitů je schopných reprezentovat všechna možná čísla, která se z nich dají vytvořit, současně. Při kvantovém počítání je masově využit paralelismus. Pokud např. potřebujeme zjistit číslo, v jehož druhé a třetí mocnině se nachází všech devět číslic desítkové soustavy, normální počítač bude muset začít postupně prověřovat čísla od 1 dále. Nakonec se zastaví na čísle 69, které mimochodem jako jediné splňuje počáteční podmínku. Pokud každé číslo bude testovat 1 sekundu, celá operace bude trvat 69 sekund. Naproti tomu kvantový počítač umocní a otestuje všechna čísla společně a celý výpočet bude trvat pouze 1 vteřinu. Zde je vidět, že výkonnost kvantového počítače je závislá na počtu qubitů, ze kterých je tvořen – např. se 3 qubity je schopen provádět 2^3=8 operací současně. V současnosti se odhaduje, že ve vesmíru je přibližně 10^{120} částic, takže by se teoreticky dalo říci, že na simulaci takového souboru částic by stačil kvantový počítač s pouhými 398 qubity (2^{398} velmi přibližně odpovídá 10^{120}).

Protože qubity musí být tvořeny kvantovým objektem, nabízí se právě aplikace částic a jejich spinů. V blízké minulosti bylo uskutečněno několik experimentů s qubity umístěnými v optických chladičích, kde nebyly „proměřovány" okolními částicemi, a tak mohly být laserovým pulsem uvedeny do superpozice, která po svém kolapsu při měření vyzářila požadovanou informaci. Kvantové počítače jsou tedy možné nejen teoreticky, ale i prakticky (i když zatím s velmi nízkým počtem qubitů). Situace by se dala přirovnat k prvním pokusům s klasickými počítači, jako Colossus nebo Eniac.

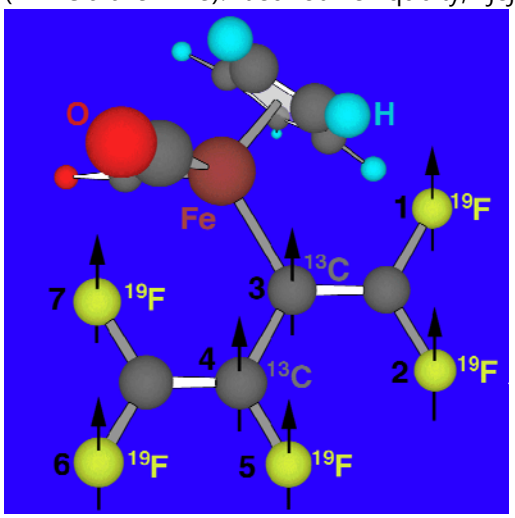
V kryptoanalýze je aplikace kvantového počítání poměrně zřejmá. Matematické problémy jako faktorizace nebo útoky brutální silou by s paralelismem kvantových počítačů rázem vymizely. Bezpečnost šifer jako RSA nebo AES by byla zlomena.

Kvantové počítání však zpočátku trpělo jedním nedostatkem – nebyl vymyšlen žádný software, žádný algoritmus využívající kvantových vlastností. Až roku 1994 Peter Shor z AT&T Bell Laboratories v New Jersey uspěl v definování užitečného programu pro kvantový počítač, tzv. Shorův faktorizační algoritmus. Shorův algoritmus (viz *Tabulka 20*) je sice určený pro budoucí kvantové počítače, ovšem už při jeho použití v konvenčním počítači je dosaženo rychlejšího počítání faktorizace než s klasickým zkoušením dělitelů, dokud nevyjde dělení beze zbytku. Hned roku 1996 Lov Grover, zaměstnanec stejného institutu, přišel s dalším algoritmem, tentokrát řešícím prozkoušení všech možností zároveň, což by prolomilo šifry na principu DES a AES.

1	Zvolíme číslo, které chceme faktorizovat – např. **15**.
2	Dále zvolíme libovolné číslo, které je menší než **15** – např. **7**.
3	Nyní postupně umocňujeme **7** a zjišťujeme zbytky po dělení **15**, dokud si nejsme jistí opakováním určité číselné vlny: $\mathbf{7^1=7(mod\ 15)}$ $\mathbf{7^2=4(mod\ 15)}$ $\mathbf{7^3=13(mod\ 15)}$ $\mathbf{7^4=1(mod\ 15)}$ $\mathbf{7^5=7(mod\ 15)}$ $\mathbf{7^6=4(mod\ 15)}$ $\mathbf{7^7=13(mod\ 15)}$ atd.
4	Ze zbytků po dělení vytvoříme číselnou vlnu **7,4,13,1** a zjistíme u ní periodu, která je rovna **4**.
5	Periodu vydělíme dvěma (**4/2=2**) a výsledek použijeme jako exponent pro dříve zvolené číslo **7**, takže $\mathbf{7^2=49}$. Pokud je perioda lichá, je nutné začít znovu a ve druhém kroku zvolit jiné číslo.
6	Nyní vezmeme dvě sousední čísla od čísla **49**, což jsou **48** a **50**, a postupně nalezneme jejich největší společné dělitele s číslem **15**. Vyjde nám **NSD(48,15)=3** a **NSD(50,15)=5**.
7	Výsledkem tedy je **5** a **3**, což jsou skutečně faktory čísla **15**.

Tabulka 20: Příklad použití Shorova faktorizačního algoritmu.

K prvnímu praktickému použití Shorova algoritmu došlo roku 2001 ve výzkumných laboratořích IBM. Jako kvantový počítač byla použita molekula, jejíž 7 atomů bylo využito jako qubity (viz *Obrázek 18*). Jednotlivé qubity, jejich spiny a energetické hladiny jejich elektronů byly programovány pomocí radiofrekvenčních pulsů, což umožnilo vytvořit základní logická hradla. Výstupní informace byly detekovány pomocí nukleární magnetické rezonance, kdy se Fourierovou transformací měřila perioda vyzářené vlny. Molekula tedy umocnila zvolené číslo zároveň na všechny potřebné exponenty a vyzářila informaci o periodě. Po změření periody se již zbytek výpočtu (tedy krok 5, 6, 7 v Shorově algoritmu) počítal na klasickém konvenčním počítači. Úspěšně se podařilo faktorizovat číslo 15 na jeho faktory 5 a 3.



Obrázek 18: Současný nejvýkonnější kvantový počítač na světě. Formální chemický název molekuly $C_{11}H_5F_5O_2Fe$ je: dikarbonylcyklopentadienyl(perfluorobutadien-2-yl)železo = pentafluorobutadienyl cyklopentadienyldikarbonyl-železo komplex

Jak je vidět, kvantová kryptoanalýza by s využitím kvantového počítače byla schopná rozlomit jakoukoliv dnešní šifru. Naštěstí souběžně s myšlenkou kvantové kryptoanalýzy byl rozvíjen i koncept kvantové kryptografie – v roce 1984 Charlesem Bennettem. Kvantová kryptografie je svou povahou nerozluštitelná, protože tomu brání fyzikální zákony. Nabízí se kombinace kvantové kryptografie s Vernamovou šifrou, kdy se pomocí kvantové kryptografie vytvoří a přenese k příjemci jednorázová tabulka (klíč), která se potom aplikuje na běžnou symetrickou Vernamovu šifru.

Bezpečný přenos jednorázové tabulky spočívá ve kvantových vlastnostech fotonu. Při vyslání fotonu můžeme určit jeho polarizaci – tzn. rovinu, ve které kmitá. Pro účely kvantové kryptografie stačí 4 typy polarizace – jejich označení je **– | / ** (tedy horizontála, vertikála, stoupající diagonála, klesající diagonála). Příjemce bude mít dva polarizační filtry – jeden ve tvaru **+** a druhý ve tvaru **x**. Pokud se na horizontální nebo vertikální fotony použije **+** filtr, projdou beze změny své polarizace. Pokud se ale použije **x** filtr, fotony budou nuceny s 50% pravděpodobností zkolabovat do jednoho z diagonálních stavů (protože diagonální filtr je vlastně o 45 stupňů otočený oproti horizontálně-vertikálnímu filtru). Tento jev umožňuje Alici a Bobovi posílat bezpečně klíč, aniž by jej Eva mohla číst. Navíc Alice a Bob mohou bez problémů zjistit, zda Eva naslouchá. Dejme tomu, že Alice chce Bobovi poslat zprávu o 1000 binárních číslech za použití Vernamovy šifry. Musí tedy vytvořit stejně dlouhý klíč. Celý postup posílání klíče je názorně popsán v následující tabulce.

1	Alice pošle Bobovi dostatečný počet (více než dvojnásobek potřebné délky klíče) různě polarizovaných fotonů – při posílání volí naprosto náhodně ze čtveřice možných polarizací.
2	Bob při přijímání volí náhodně ze dvojice svých polarizačních filtrů. Statisticky vzato se trefí asi v 50% do správně zvoleného filtru, tak aby si foton zachoval svoji polarizaci.
3	Bob zavolá Alici nezabezpečenou telefonní linkou a řekne jí, kdy používal jaký filtr. Alice mu odpovídá, zda volil správně nebo ne. Fotony se špatně zvoleným filtrem oba vyřadí ze svého seznamu. Pokud Eva poslouchá, ví jaké byly použity filtry, ale nezná polarizace fotonů, které filtry procházely.
4	Alice a Bob by měli postupovat tak, aby v této chvíli měli něco přes 1000 fotonů – např. 1075. To jim umožní vybrat naprosto náhodně 75 fotonů z celého souboru a zatelefonovat si opět nezabezpečenou telefonní linkou jejich celé polarizace. Pokud Eva poslouchala, a tedy proměřovala fotony polarizačními filtry, musela se přibližně v 50% zmýlit, čímž změnila polarizace takových fotonů. Bob je potom sice mohl zachytit správným filtrem a po prvním telefonátu s Alicí je zařadit do seznamu správných, ovšem při druhém telefonátu se naleznou nesrovnalosti – Alice třeba vyslala horizontální foton, ale Bob přijal vertikální. To je jasným důkazem toho, že Eva poslouchala. Po otestování všech 75 náhodných fotonů je pravděpodobnost toho, že by se Eva ve všech náhodou trefila, rovna asi jedna ku milionu. V případě, že Alice a Bob Evu odhalí, je nutné celý klíč smazat a celý proces začít znovu.
5	Pokud test proběhne úspěšně, stačí již každé polarizaci přiřadit logickou hodnotu 1 nebo 0. Dejme tomu že **– /** budou 1 a **| ** budou 0. Výsledný řetězec 1000 binárních čísel se použije jako jednorázový klíč pro Vernamovu šifru.

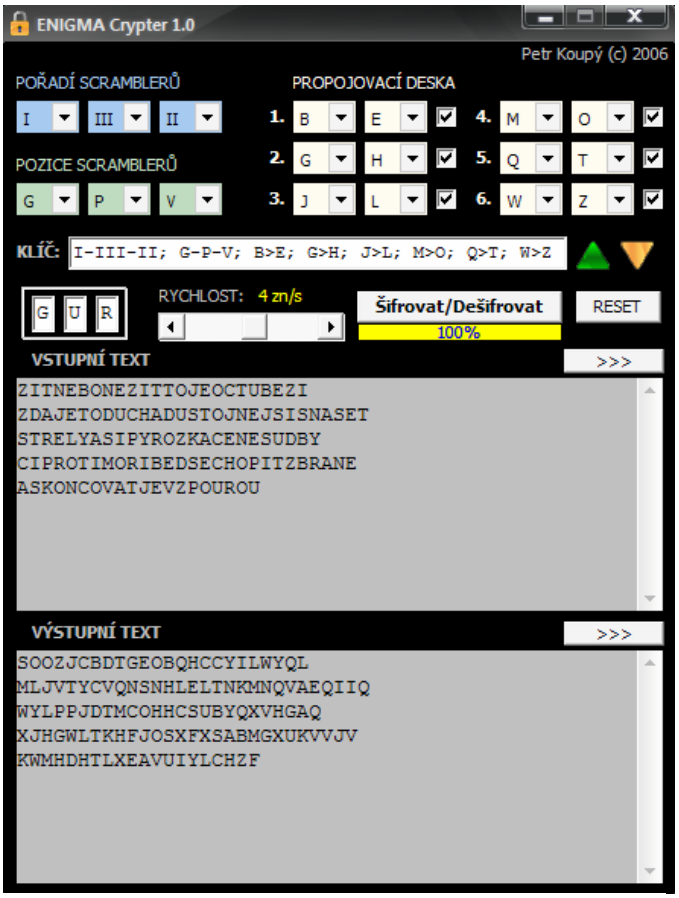
Tabulka 21: Příklad použití kvantové kryptografie.

Z uvedeného je patrné, že kvantová kryptografie s využitím informačních technologií pro automatizaci a zrychlení celého procesu řeší současně problém distribuce klíče a všechny nepraktické vlastnosti Vernamovy šifry. Vzniká dokonalý kryptosystém, konečné řešení kryptografie, které je odolné i vůči kvantové kryptoanalýze.

Již roku 1988 Charles Bennett realizoval kvantový přenos klíče na vzdálenost 30cm. V roce 1995 výzkumníci ženevské univerzity implementovali kvantovou kryptografii do optického vlákna spojujícího města Ženeva a Nyon, vzdálená 23 km. V květnu 2002 se švýcarské firmě ID Quantique podařilo spojení na vzdálenost 60 km. V červnu 2003 společnost Toshiba Research Europe vylepšila vzdálenost na 100 km. 9. března 2004 firma ID Quantique a americká společnost Magiq prohlásily, že mají k dispozici kvantovou technologii, která umožňuje přenos zpráv pomocí kvantové kryptografie na vzdálenost 120 km a mohou ji poskytnout komerčnímu sektoru.

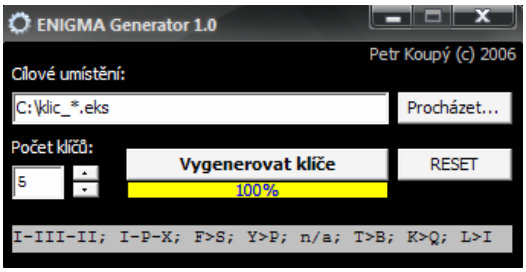
6. Softwarový projekt ENIGMA

Cílem softwarového projektu bylo naprogramovat šifrovací nástroj, který by umožnil převádět text do šifry ENIGMA. Na Internetu lze nalézt několik podobných programů, ale prakticky žádný z nich neumožňuje pohodlné převádění velkého množství textu. Jejich uživatelské rozhraní se většinou snaží být věrnou kopií německého přístroje pro šifrování Enigmy a celkově tyto programy slouží spíše pro demonstraci. Uživatel je tak nucen zadávat jednotlivá písmena na virtuální klávesnici připomínající psací stroj, čímž je převod většího množství textu prakticky znemožněn.



Obrázek 19: ENIGMA Crypter při šifrování úryvku z Hamleta.

Vývoj tohoto programu se proto ubíral jiným směrem. Hlavní prioritou bylo navrhnout jednoduché uživatelské rozhraní, umožnit efektivní distribuci klíčů a hlavně v co největší míře přizpůsobit program pro zpracování velkého množství textu. Výsledkem je program **ENIGMA Crypter** (viz *Obrázek 19*). Kromě klasického psaní je implementováno i vkládání textu ze schránky a z textových souborů. Protože šifra ENIGMA pracuje pouze z 26 základními písmeny abecedy, program obsahuje vstupní filtry, které odstraňují veškerou interpunkci a mezery mezi slovy. Kvůli zachování logické struktury textu jsou čísla a několik často používaných znaků filtrem překládána na česká slova (např. znak „1" je nahrazen řetězcem „JEDNA"), zbytek znaků je zcela vypuštěn. Zašifrovaný text lze opět buď uložit do souboru anebo kopírovat do schránky.



Obrázek 20: ENIGMA Generator při vytváření klíčů.

Aby byla šifra ENIGMA bezpečná, je nutné každou zprávu šifrovat novým klíčem. V případě, že by měl klíč pokaždé vytvářet uživatel, zde vzniká určité bezpečnostní riziko, protože člověk není schopen vytvořit velký počet klíčů s dostatečnou mírou náhodnosti. Z tohoto důvodu je k hlavnímu programu přiložen program **ENIGMA Generator** (viz *Obrázek 20*). Jde o generátor klíčů, který je určen k vytvoření stovek náhodných klíčů za několik sekund.

Na následujících stranách je stručný návod k programům a některé dodatečné informace vztahující se ke zdrojovému kódu atd. Kompletní zdrojové kódy v Delphi a oba programy zkompilované pro Windows se nachází na datovém nosiči spolu s elektronickou verzí práce.

6.1 ENIGMA CRYPTER VERZE 1.0

1. ÚVOD
2. TECHNICKÉ DETAILY
3. NÁVOD K POUŽITÍ
4. OSTATNÍ DOPORUČENÍ
5. COPYRIGHT

1. ÚVOD

Program slouží k dávkovému šifrování a dešifrování textu pomocí šifry ENIGMA používané během druhé světové války. Konkrétně se jedná o základní verzi ENIGMY se třemi scramblery, kterou na začátku války používaly jednotky *Wehrmacht* a *Luftwaffe*. Program používá stejný vnitřní mechanismus, takže je s prvotní verzí ENIGMY kompatibilní (dokáže dešifrovat německé válečné zprávy z počátku války). Kompatibilita není zajištěna pro pozdější verze ENIGMY, které měly více scramblerů a jiné vnitřní zapojení, a pro námořní verzi ENIGMY, kterou používaly jednotky *Kriegsmarine*.

2. TECHNICKÉ DETAILY

Systémové požadavky:	Windows™ 98, ME, 2000, XP, Vista
Scrambler I:	EKMFLGDQVZNTOWYHXUSPAIBRCJ
Scrambler II:	AJDKSIRUXBLHWTMCQGZNPYFVOE
Scrambler III:	BDFHJLCPRTXVZNYEIWGAKMUSQO
Reflektor B (široký):	YRUHQSLDPXNGOKMIEBFZCWVJAT
Otáčecí pozice I:	Q (pokud scrambler I přechází z Q na R, vedlejší scrambler se otočí o 1 pozici)
Otáčecí pozice II:	E (pokud scrambler II přechází z E na F, vedlejší scrambler se otočí o 1 pozici)
Otáčecí pozice III:	V (pokud scrambler III přechází z V na W, vedlejší scrambler se otočí o 1 pozici)
Propojovací deska:	6 kabelů (propojení až 6 párů písmen)
Počet kombinací klíče:	10705702343606400

Poznámka: Při otáčení scramblerů se navíc uplatňuje jev (tzv. *doublestep*), kdy dojde k otočení scramblerů i když nejsou ve svých obvyklých otáčecích pozicích. Pokud se otočením pravého scrambleru dostal prostřední scrambler do své otáčecí pozice, dojde v příštím kroku k otočení všech tří scramblerů o jedno místo.

3. NÁVOD K POUŽITÍ

NASTAVENÍ KLÍČE

Klíč sestává ze tří oddílů. Prvním oddílem je pořadí scramblerů, což určuje v jakém pořadí se scramblery budou otáčet. Druhým oddílem je počáteční pozice každého scrambleru v abecedě. Třetím oddílem je propojení 0 až 6 párů písmen v abecedě na propojovací desce. Musí být nastaven vždy celý pár, jinak je klíč neúplný. Klíč lze uložit do souboru pro pozdější použití nebo za účelem distribuce klíče příjemci. Uživatel může klíč nastavovat buď manuálně nebo načíst klíč vygenerovaný programem **ENIGMA Generator 1.0**.

NASTAVENÍ RYCHLOSTI

Program je defaultně nastaven na nejvyšší možnou rychlost limitovanou pouze výkonem procesoru. Při této rychlosti je deaktivováno okénko pozic jednotlivých scramblerů, protože snižuje výkon algoritmu. Pro demonstrační účely lze snížit rychlost šifrování na 2 až 100 znaků za sekundu (rychlosti jsou přibližné). Při snížené rychlosti je aktivováno okénko s pozicemi scramblerů. Rychlost lze nastavovat i v průběhu (de)šifrovacího procesu.

VSTUPNÍ A VÝSTUPNÍ TEXT

Vstupní text lze psát přímo do příslušného okna v programu, vkládat ze schránky nebo vkládat ze souboru. Šifra ENIGMA umožňuje zpracovat pouze 26 velkých znaků abecedy. Z tohoto důvodu program neregistruje velikost písmen, diakritiku, neabecední znaky, čísla a mezery. Pro zachování základní logické struktury textu vkládaného ze schránky nebo ze souboru jsou čísla a znaky +-*/%@ převedeny na česká slova. Ostatní znaky jsou ignorovány. Výstupní text je možné kopírovat do schránky nebo ukládat do souboru.

RESET

Činnost programu lze kdykoliv přerušit stisknutím tlačítka RESET, čímž dojde k uvedení programu do jeho počátečního stavu po spuštění.

4. OSTATNÍ DOPORUČENÍ

DISTRIBUCE KLÍČE

Pro zajištění maximální bezpečnosti by se měl pro každou zprávu používat nový klíč. Pro zajištění vysoké bezpečnosti stačí používat každý den nový klíč. Klíč by neměl být distribuován zároveň se zprávou stejným informačním kanálem. Např. pokud je zpráva posílána přes Internet, měl by být klíč předán buď osobně na datovém nosiči nebo sdělen telefonem.

ZÁKLADNÍ INTERPUNKCE

Operátoři ENIGMY používali pro zpřehlednění textu následující způsob šifrování:

X = tečka
Y = čárka
UD = otazník
XX = středník
YY = pomlčka
KK****KK = závorky

PSANÍ TEXTU

Kvůli zachování základního formátování textu na řádky je doporučeno nezačínat a nezakončovat text snadno odhalitelnou frází. Opakování stejných slov po sobě také vede ke snížení bezpečnosti.

5. COPYRIGHT

ENIGMA Crypter 1.0

Copyright (C) 2006 Petr Koupý (madchicken@seznam.cz)

Tento program je volný software; můžete jej šířit a modifikovat podle ustanovení Obecné veřejné licence GNU, vydávané Free Software Foundation; a to buď verze 2 této licence anebo (podle vašeho uvážení) kterékoli pozdější verze.

Tento program je rozšiřován v naději, že bude užitečný, avšak BEZ JAKÉKOLI ZÁRUKY; neposkytují se ani odvozené záruky PRODEJNOSTI anebo VHODNOSTI PRO URČITÝ ÚČEL. Další podrobnosti hledejte v Obecné veřejné licenci GNU (http://www.gnu.org/licenses/gpl.html).

6.2 ENIGMA GENERATOR VERZE 1.0

1. ÚVOD
2. TECHNICKÉ DETAILY
3. NÁVOD K POUŽITÍ
4. OSTATNÍ DOPORUČENÍ
5. COPYRIGHT

1. ÚVOD

Program slouží k dávkovému vytváření klíčů pro šifru ENIGMA. Souborový formát klíče je kompatibilní s programem **ENIGMA Crypter 1.0**.

2. TECHNICKÉ DETAILY

Systémové požadavky:	Windows™ 98, ME, 2000, XP, Vista
Počet kombinací klíče:	10705702343606400
Přípona klíče:	*.eks (enigma keys)
Velikost klíče:	45 bajtů

3. NÁVOD K POUŽITÍ

UMÍSTĚNÍ KLÍČŮ

Nejprve je nutné nastavit cestu k místu, kam se mají klíče vygenerovat. Defaultní jméno klíče „klic_cislo“ lze libovolně přenastavit.

POČET KLÍČŮ

Lze nastavit 1 až 999 klíčů.

Upozornění: Není doporučeno generovat velký počet klíčů na Plochu a do kořenových adresářů diskových jednotek.

RESET

Činnost programu lze kdykoliv přerušit stisknutím tlačítka RESET, čímž dojde k uvedení programu do jeho počátečního stavu po spuštění.

4. OSTATNÍ DOPORUČENÍ

POUŽITÍ

Program byl navržen pro vygenerování měsíční nebo roční kódové knihy, kterou si osobně předá odesílatel s příjemcem na datovém nosiči (např. disketa). Pokud je např. na disketu vygenerováno 31 klíčů, číslo každého klíče odpovídá dnu v měsíci. Odesílatel i příjemce tedy daný den používají klíč s tímto číslem. Kvůli zajištění bezpečnosti je silně doporučeno používat každý den nový klíč.

5. COPYRIGHT

ENIGMA Generator 1.0

Copyright (C) 2006 Petr Koupý (madchicken@seznam.cz)

Tento program je volný software; můžete jej šířit a modifikovat podle ustanovení Obecné veřejné licence GNU, vydávané Free Software Foundation; a to buď verze 2 této licence anebo (podle vašeho uvážení) kterékoli pozdější verze.

Tento program je rozšiřován v naději, že bude užitečný, avšak BEZ JAKÉKOLI ZÁRUKY; neposkytují se ani odvozené záruky PRODEJNOSTI anebo VHODNOSTI PRO URČITÝ ÚČEL. Další podrobnosti hledejte v Obecné veřejné licenci GNU (http://www.gnu.org/licenses/gpl.html).

6.3. Dodatečné informace

ENIGMA Crypter 1.0

Kompilátor:	Borland® Delphi® for Microsoft® Windows™ Version 10.0.2166.28377 Update 1
Zdrojový kód:	1899 řádků
Velikost:	852 992 bajtů
MD5:	d5238f168be4507e5fb70a07311c29ed
SHA1:	e7da3086519acd839d0132a69d011ac521478050
RIPEMD160:	cb8752ba5573bf3e8516a862de576ea7612ffe25
CRC32:	7354f896

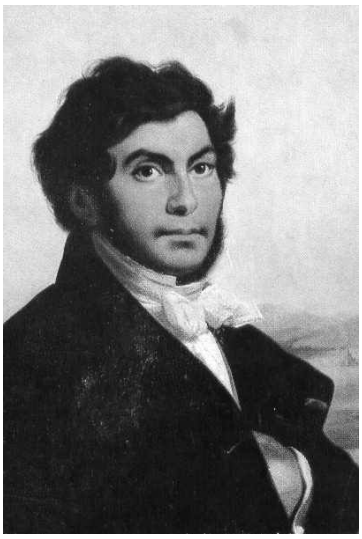
ENIGMA Generator 1.0

Kompilátor:	Borland® Delphi® for Microsoft® Windows™ Version 10.0.2166.28377 Update 1
Zdrojový kód:	384 řádků
Velikost:	476 672 bajtů
MD5:	28c8b0982e37881c9885ed967d6fa931
SHA1:	801ebfc3930309229b477dc3bc4cb2be2e9de8a0
RIPEMD160:	72682e387746a58e72c0a9ee58feb6d7de5e29a7
CRC32:	b93a8cfe

7. Osobnosti kryptologie


Gaius Julius Caesar (100-44)


Thomas Young (1773-1829)

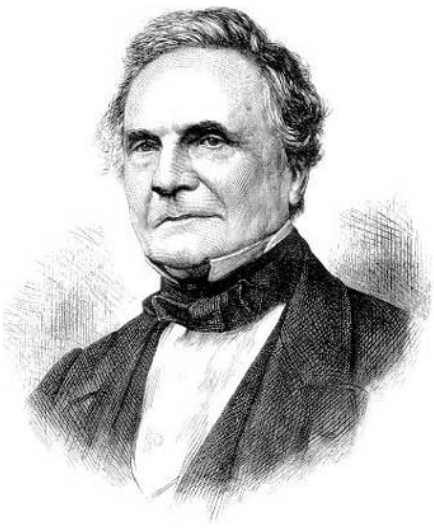

Jean François Champollion (1790-1832)


Arthur John Evans (1851-1941)

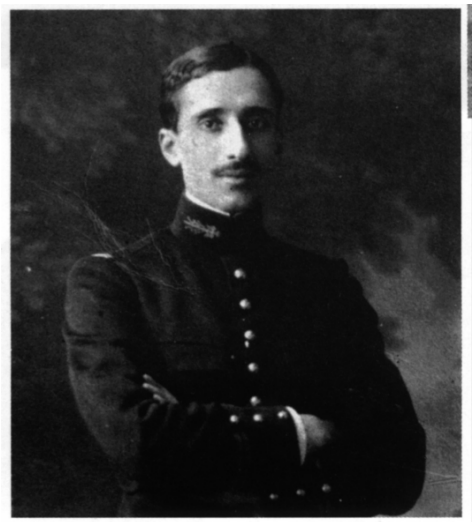

Alice Kober (1906-1950)


Michael George Ventris (1922-1956)


Blaise de Vigenère (1523-1596)


Charles Babbage (1791-1871)


Gilbert Sandford Vernam (1890-1960)



Georges Painvin (1886-1980)

Marian Rejewski (1905-1980)

Alan Mathison Turing (1912-1954)

Horst Feistel (1915-1990)

Vincent Rijmen (*1970)

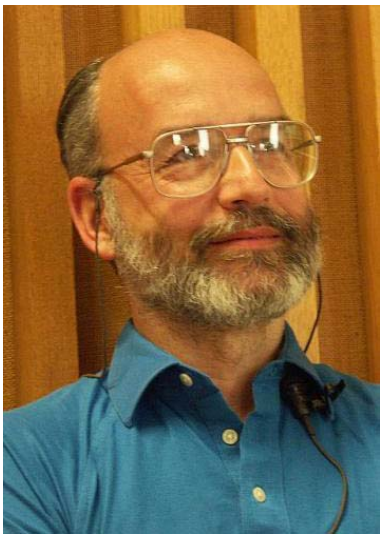
Joan Daemen (*1965)

Whitfield Diffie (*1944)

Martin Edward Hellman (*1945)

Ralph Merkle (*1952)


Ronald Linn Rivest (*1947)


Adi Shamir (*1952)


Leonard Max Adleman (*1945)


James Ellis (1924-1997)


Clifford Christopher Cocks (*1951)


Philip Zimmerman (*1954)


David Deutsch (*1953)


Peter Shor (*1959)


Charles Bennett (*1943)

8. Závěr

Zatímco tvůrci kódů a šifer vždy usilovali o nejlepší způsob utajení informací, luštitelé se snažili o pravý opak. Při souboji byly obě skupiny nuceny nasazovat technologie a poznatky z mnoha oborů. Kryptologie se stala jedním z impulsů technického rozvoje.

V historii bylo lidstvo několikrát svědkem toho, že i sebelepší šifra, kterou všichni považovali za neprolomitelnou, byla nakonec překonána. Někdy to plynulo z její samotné nedokonalosti, jindy z chyby lidského faktoru. Ať tak či onak, jednou měla převahu kryptografie, podruhé kryptoanalýza. V současnosti společnost spoléhá na šifry jako AES a RSA. Kryptoanalýza je u nich znemožněna astronomickou výpočetní náročností. Kryptoanalytici si ale našli jinou cestu – tzv. postranní kanály (*side channels*). Informace potřebné k rozluštění čerpají např. z chybových hlášení počítačových programů, z času, po který šifrovací stroj pracuje, nebo z elektromagnetického záření, které vydává. Ač to zní neuvěřitelně, v průběhu let 2005 a 2006 bylo uskutečněno několik takových pokusů.

Zbývá naděje, že se lidstvo v budoucnu bude moci spolehnout na kvantové metody kryptologie. Kvantová kryptoanalýza má hotové algoritmy a výzkum kvantových počítačů pokračuje mílovými kroky. První pokusy s kvantovými počítači musely probíhat za velmi nízkých teplot a ve velmi čistém prostředí. Dnes se však již začíná uvažovat o realizaci qubitů pomocí uhlíkových nanotrubiček za normální pokojové teploty. Dalším kandidátem na reprezentaci qubitů jsou tzv. kvantové tečky – elektrony nahuštěné v potenciálové jámě vytvořené polovodiči se chovají jako elektrony v obalu atomu (zaujímají energetické hladiny). I přesto je prakticky použitelný kvantový počítač prozatím hudbou budoucnosti. Můžeme si tím ale být úplně jistí? Za autora postupu dešifrování Vigenérovy šifry byl po více než sto let považován Kasiski, nikoliv Babbage. O dešifrování přístrojů Enigma a Lorenz se svět dozvěděl až s odstupem mnoha desítek let. Za první programovatelný počítač byl po léta považován ENIAC, nikoliv Colossus. Systémy DHM a RSA byly ve skutečnosti vyvinuty v GCHQ čtyři roky před tím, než se jimi pánové Diffie, Hellman, Merkle, Rivest, Shamir a Adleman vůbec začali zaobírat. Je tedy docela možné, že bezpečnostní agentury jako NSA již kvantové počítání dávno plně ovládly a běžně je používají. Nemá však smysl o tom spekulovat – až se kvantové počítání dostane na dostatečnou úroveň v akademické oblasti, možná se všichni dozvíme pravdu.

Oproti tomu kvantová kryptografie je již realitou a potřebná technologie je připravená k vypuštění na trh. Také se začíná rozvíjet kryptografie založená na eliptických křivkách, o kterých se soudí, že by mohly být velmi dobrou perspektivou pro nové kryptografické postupy. Zůstává však otázka zmíněná v úvodu: Jak se k takovým technologiím a metodám postavit? Jak je používat, aby obohatily informační věk a zároveň nechránily zločince?

9. Seznam použité literatury

Singh, S.: *Kniha kódů a šifer (The Code Book)*,
Praha: Argo, Dokořán, 2003. ISBN 80-7203-499-5 (Argo), ISBN 80-386569-18-7 (Dokořán).

Johnson, G.: *Zkratka napříč časem (A Shortcut Through Time)*,
Praha: Argo, Dokořán, 2004. ISBN 80-7203-609-2 (Argo), ISBN 80-86569-83-7 (Dokořán).

Hey, T.; Walter, P.: *Nový kvantový vesmír (The New Quantum Universe)*,
Praha: Argo, Dokořán, 2005. ISBN 80-7203-699-8 (Argo), ISBN 80-7363-000-1 (Dokořán).

Písek, S.: *Začínáme programovat v Delphi*,
Praha: Grada, 2000. ISBN 80-247-9008-4 (Grada).

Svoboda, L; Voneš, P; Konšal, T; Mareš, M.: *1001 tipů a triků pro Delphi*,
Praha: Computer Press, 2001. ISBN 80-7226-529-6 (Computer Press).

Wikipedia: *Kryptologie,*
Dostupné z URL: http://cs.wikipedia.org/wiki/Kryptologie/

Wikipedia: *Egyptian Hieroglyph,*
Dostupné z URL: http://en.wikipedia.org/wiki/Egyptian_hieroglyph/

Wikipedia: *Linear B,*
Dostupné z URL: http://en.wikipedia.org/wiki/Linear_B/

Wikipedia: *Enigma Machine,*
Dostupné z URL: http://en.wikipedia.org/wiki/Enigma_machine/

Wikipedia: *Bombe,*
Dostupné z URL: http://en.wikipedia.org/wiki/Bombe/

Wikipedia: *Hash Function,*
Dostupné z URL: http://en.wikipedia.org/wiki/Hash_function/

Wikipedia: *Message Diggest,*
Dostupné z URL: http://en.wikipedia.org/wiki/Message_digest/

Wikipedia: *MD5,*
Dostupné z URL: http://en.wikipedia.org/wiki/MD5/

Wikipedia: *SHA Hash Function,*
Dostupné z URL: http://en.wikipedia.org/wiki/SHA_hash_functions/

Wikipedia: *Advanced Encryption Standard,*
Dostupné z URL: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard/

Wikipedia: *Data Encryption Standard,*
Dostupné z URL: http://en.wikipedia.org/wiki/Data_Encryption_Standard/

Wikipedia: *RSA,*
Dostupné z URL: http http://en.wikipedia.org/wiki/RSA/

Wikipedia: *Side Channel Attack,*
Dostupné z URL: http://en.wikipedia.org/wiki/Side_channel_attack/

Wikipedia: *Steganography,*
Dostupné z URL: http://en.wikipedia.org/wiki/Steganography/

Klíma, V.: *MD5 collisions,*
Dostupné z URL: http://cryptography.hyperlink.cz/MD5_collisions.html

PGP International: *Pretty Good Privacy software,*
Dostupné z URL: http://www.pgpi.org/

Pell, O.: *Cryptology,*
Dostupné z URL: http://www.ridex.co.uk/cryptology/index.html

Bitto, O.: *Historie kryptologie,*
Dostupné z URL: http://www.fi.muni.cz/usr/jkucera/pv109/2003/xbitto.htm

Kupča, V.: *Teorie a perspektiva kvantových počítačů,*
Dostupné z URL: http://cml.fsv.cvut.cz/~kupca/qc/

IBM Corporation: *STM Galerry,*
Dostupné z URL: http://www.almaden.ibm.com/vis/stm/gallery.html

IBM Corporation: *IBM's Test-Tube Quantum Computer Makes History,*
Dostupné z URL: http://domino.research.ibm.com/comm/pr.nsf/pages/news.20011219_quantum.html

Quantum Information Processing: *Introductory Tutorials,*
Dostupné z URL: http://www.quantiki.org/wiki/index.php/Category:Introductory_Tutorials/

Klíma, V.: *Eliptické křivky,*
Dostupné z URL: http crypto-world.info/klima/2002/chip-2002-09-134-136.pdf

Crypto-World: *Archiv časopisu,*
Dostupné z URL: http://crypto-world.info/index2.php