Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Elektronické průkazy totožnosti

Tomáš Mandys

Bakalářská práce

2009

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Katedra informačních technologií
Akademický rok: 2008/2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Tomáš MANDYS**

Studijní program: **B2646 Informační technologie**

Studijní obor: **Informační technologie**

Název tématu: **Elektronické průkazy totožnosti**

Zásady pro vypracování:

Cílem práce bude popis a charakteristika vybraných druhů elektronických průkazů totožnosti, jejich výhod, nevýhod a použité technologie. Teoretická část: V teoretické části bakalářské práce budou představeny a zhodnoceny druhy elektronických průkazů totožnosti: pas, občanský průkaz a el. podpis. Budou popsány technologie a algoritmy, které se používají pro zabezpečení těchto průkazů. Zároveň budou popsány výhody a nevýhody těchto průkazů s ohledem na ochranu dat a soukromých údajů. Implementační část: Bude obsahovat rozbor výhod a nevýhod vybraného algoritmu, na základě tohoto rozboru bude realizován pokus o vylepšení tohoto algoritmu. V případě více chyb, vytvoření vlastního algoritmu, který by tyto chyby neobsahoval.

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

Porubský, Š. a Grošek, O.: Šifrovanie. Algoritmy, Metódy, Prax. Grada, Praha 1992. Gruska: Kódování, kryptografie a kryptografické protokoly Zákon o ochraně osobních údajů (101/2000 Sb.)

Vedoucí bakalářské práce: **Ing. Zdeněk Šilar**
Katedra informačních technologií

Datum zadání bakalářské práce: **15. ledna 2009**

Termín odevzdání bakalářské práce: **15. května 2009**

Univerzita Pardubice Česká republika

L.S.

doc. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan
vedoucí katedry

V Pardubicích dne 31. března 2009

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury. Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č.121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 26. 8. 2009

Tomáš Mandys

ANOTACE

Práce by měla sloužit jako základní text pro zájemce o podrobnější informace o novinkách v oblasti přenosu osobních dat a průkazů totožnosti. Zájemce by po přečtení práce měl být schopen pochopit základní pojmy z problematiky kryptografie.

KLÍČOVÁ SLOVA

elektronické osobní údaje, cestovní pas, občanský průkaz, kryptografie

TITLE

This work will have to serve as basic text for persons interested in more detailed informations about news in transfering personal informations and indentifications. Applicant will be able to understand basic notions of cryptology problematic after reading this work.

KEYWORDS

Electronical personal informations, passport, identity card, cryptology

Obsah

Seznam obrázků

Slovník pojmů

Kryptografie - nauka o metodách utajování smyslu zpráv převodem do podoby čitelné pouze se speciální znalostí. Slovo kryptografie pochází z řečtiny – kryptós znamená skrytý a gráphein je psát.

Steganografie - věda zabývající se utajením komunikace prostřednictvím ukrytí zprávy. Slovo vzniklo spojením řeckých slov steganós – schovaný a gráphein

Kryptoanalýza – věda o metodách získávání obsahu šifrovaných informací bez přístupu k tajným informacím, jedná se o opak kryptografie. Slovo pochází z řeckých slov kryptós a analýein - uvolnit

Kryptologie – věda zahrnující všechny tři předchozí nauky

Asymetrické šifry – kryptografické algoritmy používané od sedmdesátých let dvacátého století , které používají jiný klíč pro šifrování a jiný klíč pro dešifrování.

Symetrické šifry – kryptografické algoritmy, které používají pro šifrování a dešifrování stejný klíč

Veřejný klíč – veřejná část dvojice klíčů v asymetrické kryptografii (public key), veřejný klíč bývá široce dostupný a může být používán k šifrování zpráv a verifikaci digitálních podpisů.

Soukromý klíč – utajovaná část dvojice klíčů v asymetrické kryptografii (private key), soukromý klíč je výhradním vlastnictvím jedné entity a není nikomu jinému sdělován, je používán k dešifrování zpráv zašifrovaných veřejným klíčem a k vytváření digitálních podpisů (které lze verifikovat veřejným klíčem)

OCR - neboli optické rozpoznávání znaků je metoda, která pomocí scanneru umožňuje digitalizaci tištěných textů, s nimiž pak lze pracovat jako s normálním počítačovým textem.

1 Úvod

Již několik posledních let se mluví o převodu některých průkazů totožnosti a osobních údajů do elektronické formy. Cestovní pas si již v dnešní době dokáží mnozí představit jako malý čip, který je součástí papírové verze. Pas i občanský průkaz již mnoho let obsahují strojově čitelné oblasti, pro zjednodušení a zrychlení identifikace osob. Někteří již jistě plánují zařízení datové schránky na komunikaci s úřady a své dokumenty podepisují elektronickým podpisem.

Přes všechny tyto možnosti ještě stále existuje mnoho lidí, kteří žádnou tuto elektronickou eventualitu nepoužívají, avšak zaručeně o nich už něco slyšeli. Pokud takový člověk má snahu sehnat si detailnější informace, naráží mnohdy na velké množství odborných článků, které jsou bez předchozích znalostí nepochopitelné, popřípadě na ještě větší množství matoucích článků rádoby odborníků. Nikde jsem ovšem nenašel takovou publikaci, která by čitateli vysvětlila jaké výhody a nevýhody má svěření jeho osobních údajů něčemu tak exaktnímu a pro mnohé stále nepochopitelnému jako je čip nebo trocha paměti na serveru. Zároveň však je nutné poznamenat, že jak se ještě občas objeví oznámení o novinkách ohledně datových schránek, nových pasech či občanských průkazech, tak jsem skoro nikdy nenarazil na informování, jak že je tato novinka kryptograficky chráněna. Jak jsou vůbec naše data v moderním elektronickém přenosu chráněna? Také na tyto otázky by měla moje práce odpovědět.

V první části práce se budu snažit čitatele přesvědčit o tom, že ačkoliv možná o kryptografii a šifrování dat nikdy neslyšel, přesto je tato věda již přes tři tisíce let stará. Podávám zde velice zhuštěný a na důležité události zestručněný vývoj kryptografických metod. U nejzajímavějších nebo nejdůležitějších metod se snažím pomocí návodu nebo vysvětlujícího obrázku čitatele seznámit s vnitřním fungováním dané šifry nebo systému. V další kapitole se snažím dokázat, že kryptografie je součástí našeho nedávno uplynulého i současného života. Následující kapitola se věnuje jmenovaným novinkám, použité technologii jejich výroby i kryptografickým metodám, které chrání data svěřovaná těmto novinkám. Zároveň se zde pokouším ukázat hlavní výhody i nevýhody plynoucí z těchto novinek a také předestřít možnosti, jak se některé z těchto novinek mohou dále vyvíjet. Poslední kapitola se zaobírá šifrou RSA. Na této šifře se snažím čitateli ukázat, jak se taková šifra vytváří, jaký byl a je její vývoj a také jaké případné slabiny byly objeveny a jak tyto slabiny odstranit.

2 Historie kryptografie

Pojem kryptologie jste možná ještě nikdy neslyšeli, přestože je tato věda stará již několik tisíc let. Po celou dobu měla mezi lidmi nádech lehkého tajemna, ani v oficiálním třídění matematických věd nebyla kryptologie dlouho uváděna.

„Kryptologie se dělí na kryptografii a kryptoanalýzu a někdy se uvádí že obsahuje také steganografii. Kryptografie se zabývá matematickými metodami se vztahem k takovým aspektům informační bezpečnosti jako je důvěrnost, integrita dat, autentizace entit a původu dat. Ve starším chápání to byla především disciplína, která se zabývala převedením informace do podoby, v níž je obsah této informace skryt“ [1].

Hlavním úkolem kryptografie bylo dokázat, aby i zpráva zachycená nepovolanou osobou, byla pro tuto osobu nečitelná. Tím se velice liší od steganografie, jejím úkolem je skrýt samotnou existenci zprávy tak, aby ji nikdo, krom povolané osoby, nebyl schopen najít. Pokud tuto zprávu najde, je již běžně čitelná. Zatímco hlavními nástroji kryptografie byly a jsou šifry, steganografie si vystačí s neviditelnými inkousty a podobnými taktikami. Během staletí se kryptologie vyvíjela k větší složitosti tak, jak se vyvíjela samotná lidská civilizace a mnohokrát také ovlivnila běh dějin. Zejména utajení nebo vyzrazení strategických vojenských informací mělo zásadní vliv na výsledky válek. Také prozrazení politických intrik, přípravy atentátů nebo třeba jen prozrazení milenců, to vše může úzce záviset na bezpečném přenosu informací a na schopnostech protivníka zprávu zachytit a rozluštit.

2.1 Starověk

Již devatenáct století před naším letopočtem se začala psát historie kryptografie. Přibližně z této doby se dochovaly zmínky o tom, že někteří z egyptských písařů používali ve svých zápiscích nestandardní hyeroglify, aby tak znemožnili jejich čtení cizím osobám.

První skutečně důležité vědomosti byly šifrovány nejspíše kolem roku 1500 před naším letopočtem. Přibližně z té doby pocházejí nalezené hliněné tabulky z Mezopotámie, které šifrovaně popisují způsob glazování výrobků v hrnčířské dílně.

Někdy kolem roku 550 př. n. l. začali hebrejští písaři používat substituční šifru s názvem atbash, pracující na principu obrácení abecedy. Tato šifra je první skutečně dochovanou šifrou v lidské historii. Mimo jiné jsou jí napsány části Starého zákona.

A	B	G	D	H	V	Z	Ch	T	Y	K	L	M	N	S	O	P	Tz	Q	R	Sh	Th
Th	Sh	R	Q	Tz	P	O	S	N	M	L	K	Y	T	Ch	Z	V	H	D	G	B	A

Obrázek č.1 - šifra Atbash [3]

Jedna z nejdůležitějších zpráv pro existenci západní civilizace byla také předána utajeně. Jednalo se o zprávu, která pomohla Řekům v boji proti perské armádě. Jeden z řeckých velitelů náhodou zjistit termín, kdy král Xerxes vytáhne se svou armádou proti Řekům. Rozhodl se o tom své krajany informovat tak, že seškrábal vosk ze dvou dřevěných psacích destiček a přímo na dřevo zprávu napsal. Tyto destičky poté opět zalil voskem, aby při běžné kontrole vypadaly jako nepoužité. Zpráva se dostala na místo určení, byla přečtena a mimo jiné i díky tomu byla Xerxova armáda poražena.

Nejspíš první psanou zmínkou o podivné formě steganografie pochází ze zápisků Hérodota, který ve svých Dějinách popsal jiný způsob dopravování informací u Řeků. Tento způsob spočíval v tom, že se otrokovi oholila hlava, zpráva se napsala otrokovi na hlavu a posléze se čekalo než otrokovi znovu narostou vlasy. Tento způsob byl prokazatelně použit při koordinaci povstání proti Peršanům v pátém století před naším letopočtem.

Řekové se však nespokojili jenom se skrýváním zpráv. Jedni z nejlepších válečníků, Sparťané, v pátém století před naším letopočtem vynalezli zařízení zvané „skytale“. Princip tohoto zařízení byl velmi jednoduchý. Na dřevěnou tyč určité šířky byl pod jistým úhlem namotán papyrový proužek, na který se kolmo psalo. Po odmotání proužku se dala zpráva opět přečíst pouze tehdy, pokud měl příjemce tyč se stejným průměrem.

Obrázek č.2 – skytale [2]

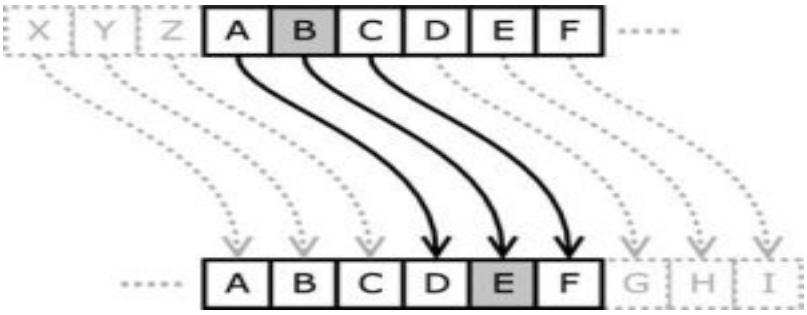
Přibližně ve stejné době vynalezl řecký spisovatel Polybius systém signalizace, který byl později převzat jako další základní kryptografická metoda. Seřadil písmena do

čtverce, kde očísloval řady i sloupce. Každé písmeno tak bylo reprezentováno dvěma čísli, číslem řady a číslem sloupce.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Obrázek č.3 - Polybiuv čtverec [13]

Další zaznamenaná novinka v šifrování se objevila až za vlády Julia Caesara. Touto novinkou byla lehká substituční šifra s normální abecedou, kdy se jednotlivá písmena v zašifrované zprávě dešifrovala pouze posunem o nějakou určenou hodnotu. Bylo to velmi primitivní a jednoduché na rozluštění, avšak tou dobou bylo jen málo lidí gramotných, navíc díky přepisu z Latiny do Řečtiny ani lidé se základním vzděláním nebyli schopni tuto jednoduchou šifru rozluštit.



Obrázek č.4 - Caesarova šifra [13]

Situace se změnila ve staré Indii. Tady již lidé byli vedeni ke gramotnosti, proto i ve známé učebnici erotiky Kámasútře je v části „Smyslná žena“ uvedeno na 44. a 45. místě z celkového počtu 64 dovedností, které by měla umět žena, která chce dosáhnout úspěchu
u mužů, ovládat: „Osvojte si tajná písma a šifry nebo si vynalezněte vlastní“. Některé tehdy běžně používané šifry se dostaly do poznámek této knihy. Přesné datum tohoto svazku není známo, ale odhaduje se někdy mezi prvním až čtvrtým stoletím našeho letopočtu.

V roce 776 byla v arabských zemích sepsána první kniha pojednávající čistě jenom o kryptografii. Bohužel pár let po svém napsání byla ztracena a od té doby již nikdy

nenalezena. Toto však není jediná její rarita. Další zvláštností je, že je v ní poprvé popsán kryptografický systém, který později použila německá armáda při sestrojení šifrovacího stroje Enigma. Princip systému je založen na znalosti správně odhadnuté části otevřeného textu na začátku zprávy, touto částí textu byla zbytková část šifrována.

2.2 Novověk

Rok 1379 se stal v kryptografické historii slavný tím, že v tomto roce byla vytvořena nejdéle sloužící šifra. Jednalo se o první šifru sestávající se z kombinace substituční abecedy a primitivního kódu. Tento typ kódu se používal ve své základní myšlence některými diplomaty ještě následujících 450 let, i když už byly mezitím vynalezeny daleko silnější a elegantnější šifry.

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

nebo

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

Obrázek č.5 - Záměnová šifra [2]

Prvními evropskými knihami, které prokazatelně obsahují šifrované pasáže jsou knihy sepsané Geoffreyem Chaucerem okolo roku 1392. Tento spisovatel psal jak některé pasáže, tak i většinu svých poznámek pod čarou šifrovanou formou. Jednalo se o jednoduchou substituci s abecedou skládající se ze znaků, číslic a symbolů.

První encyklopedií, která obsahovala pojem kryptologie je encyklopedie z roku 1412. Obsahuje informace o některých používaných substitučních a transpozičních šifrách. Poprvé se zde objevuje myšlenka rozdílné substituce pro každý znak otevřeného textu. Mimo to se také poprvé objevuje téma kryptoanalýzy. Uvádí se zde tabulka výskytu jednotlivých písmen nebo seznam dvojic písmen, které se v jednom slově nemohou vyskytovat.

S vynálezem knihtisku se pojí další milník. V roce 1518 bylo poprvé vydána tištěná kniha o kryptografii. Obsahovala sice povětšinou již jinde napsané metody a šifry, ale i některé doposud neuveřejněné náměty. Jejím hlavním přínosem bylo to, že uváděla přesné citace z dřívějších knih a i díky většímu množství výtisků se hodně dlouho uchovaly informace o již dávno ztracených tiscích.

Roku 1553 zavedl Giovan Batista Belaso myšlenku použití hesla jako šifrovacího klíče pro opakované polyalfabetické šifry. Tento standart se dnes označuje jako Vigenèrova šifra.

otevřený text	S	T	A	S	T	N	E	A	V	E	S	E	L	E
klíč	H	E	S	L	O	H	E	S	L	O	H	E	S	L
šifrový text	A	Y	T	E	I	V	J	T	H	T	A	J	E	Q

Obrázek č.6 - Vigenérova šifra [2]

Přibližně asi ve stejném roce uveřejnil Giovanni Battista Porta svou práci o šifrách, kde mimo jiné uvádí tzv. spřežkovou šifru. Je to na tehdejší dobu revoluční myšlenka nešifrovat každé písmeno ale rovnou dvojici písmen. Tím se zvětšil počet možných šifrovaných objektů a tím se ztížila i možnost prolomení šifry. Také zde poprvé rozdělil šifry na substituční, transpoziční a substituční symbolové, tj. s použitím cizí abecedy. Doporučuje také použití synonym a gramatických chyb pro ztížení kryptoanalýzy.

V roce 1585 napsal Blaise de Vigenére knihu o šifrách, kde jsou popisovány první klíčové šifrovací a dešifrovací systémy, ve kterých závisí nová zašifrovaná písmena na písmenech minulých. Mnoho jeho nápadu zůstalo zapomenuto a jejich idea byla opět oživena až v 19. století. Některé z Vigenérových principů se používají dodnes. Podobným způsobem dnes pracuje třeba velice využívaná šifra DES v některých svých módech.

Šestnácté století se také proslavilo prvními luštiteli. Asi nejznámějším z nich byl Francois Viete, který se proslavil luštěním šifrovaných depeší španělského krále a předáváním těchto depeší francouzskému panovníkovi. Mnoho let trvalo, než Španělé pochopili, jak se jejich tajné depeše dostávají do Francie. Nebyli však ochotni uvěřit, že je možné jejich šifru rozluštit a proto Vieta obvinili ze spolku s ďáblem.

Další význačnou událostí lze označit až vynález Thomase Jeffersona z roku 1790. Jefferson spolu s matematikem Robertem Pattersonem vymyslel kotoučovou šifru. Ta byla po dlouhé době znovu objevena a předělána do několika forem. Jednu z nich používaly i americké námořní jednotky za druhé světové války.

2.3 Devatenácté a polovina dvacátého století

Devatenácté století mnoho rozvoji kryptografie nepřálo. Většina šifer používaných v té době byla většinou pouze analogickými k již dávno vynalezeným. Dokonce se mnohdy jednalo o méně složité šifry než byly původní. Obrovský rozmach kryptografie zažila ve

století dvacátém a to zejména díky druhé světové a studené válce Ačkoliv i první světová válka byla obdobím důležitosti skrytí tajných rozkazů, povětšinou se používaly pouze kódy a šifry vynalezené v dobách již dávno minulých. Známý úryvek z Haškova Švejka, kdy jsou nadřízení informováni o nové šifře, která je však již dávno vynalezená, bohužel nebyla pouhým vtipem, ale přesnou výpovědí, jak to v tehdejších armádách vypadalo.

Teprve druhá světová válka však znamenala obrovský rozmach šifer a kódovacích systémů. Z nejznámějších je možno uvést například šifrovací stroj Enigma, kód Navajo nebo japonskou šifru zvanou Purpurový kód, na kterou Japonci celou válku spoléhali a Američané ji již před válkou prolomili.

Německo za 2. světové války používalo k utajování zpráv zejména mechanický stroj Enigma, který prováděl poměrně složité operace se vstupním textem, ale zároveň se dal poměrně snadno ovládat. Původní nápad při výrobě Enigmy byl mezipodniková komunikace. Teprve po šesti letech běžné výroby se velitelství Třetí Říše dalo přesvědčit o nutnosti nákupu tohoto přístroje. Po zakoupení byla Enigma prozkoumána předními německými odborníky a byly navrženy některé změny, které by bylo třeba provést, aby se dala používat pro vojenské účely. Problém nastal při dodávce prvních kusů nové verze Enigmy. Nešťastnou náhodou se jeden prototyp dostal do rukou polských odborníků, kteří ji zkoumali více než čtrnáct dnů, než se na chybu přišlo. Svoje poznatky po vypuknutí války nabídli svých kolegům z Velké Británie. Mimo jiné i díky této práci Poláků se spojencům podařilo prolomit kód Enigma a napomoci tak k výhře ve válce. Enigma měla původně 3 kolečka, která se otáčela, podobě jako mechanické počítadlo a každé mělo jinak propojené vstupní a výstupní kontakty, tím se měnil průběh proudu a i výsledné písmeno zašifrovaného textu. Později začalo ponorkové námořnictvo používat čtyřrotorové Enigmy.

Obrázek č.7 – šifrovací stroj Enigma [4]

Ještě před zapojením USA do války se američtí specialisté zabývali možností vytvoření šifry, která by byla pro nepřítele neprolomitelná. Z první světové války měli vcelku slušné zkušenosti se šifrou založenou na jazyku indiánských kmenů Choctaw a Cherokee. Přemýšleli tedy, jestli by nebylo vhodné vybrat některý z dalších indiánských nářečí. Tohoto faktu si byl vědom i Adolf Hitler. Ten ještě před začátkem války vyslal do Ameriky třicet svých nejlepších antropologů, aby zkoumali místní domorodá nářečí. I přes veškerou snahu se jim to však nepodařilo, mimo jiné i kvůli existenci velkého množství těchto dialektů. I tak se však Američané německými antropology nechali vystrašit natolik, že zamítli nasazení většího množství indiánských vojáků při invazi do Normandie.

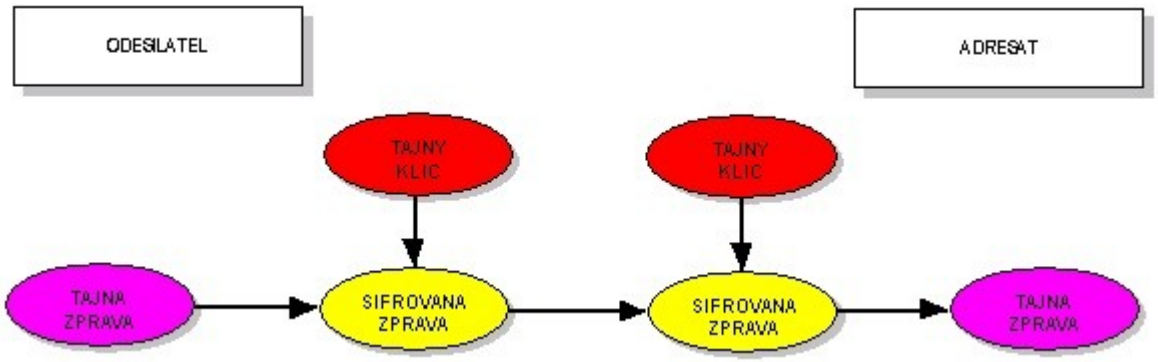
Kód Navajo byl založen na jazyku indiánského kmene specifického tím, že v podstatě neexistovala jeho psaná verze. Zároveň také existovaly velké rozdíly ve vyslovování jednotlivých samohlásek. Tyto aspekty zapříčinily, že tato šifra jako jedna z mála nebyla za celou svou dobu používání nikdy rozluštěna a prolomena. V roce 1968 byl odtajněn projekt kód Navajo běžným civilistům a teprve až v roce 2000 byla odtajněna jména tehdejších šifrantů a byla jim povětšinou in memoriam udělena zlatá medaile amerického kongresu. S ohledem na tuto událost byl natočen film Windtalkers, který sice skutečnosti nevykreslil zrovna nejpřesněji, alespoň však podpořil zájem o šifranty z druhé světové války.

3 Vývoj po druhé světové válce

Po skončení druhé světové války si válčící strany navzájem neprozradily, které kódy soupeřů se jim podařilo prolomit a které naopak zůstaly neodhalené. Němci mimo jiné i proto ještě v šedesátých letech dvacátého století mohli při prodávání poslední verze Enigmy na blízký východ tvrdit, že je to neprolomený šifrovací systém. Díky tomu mohli Američané odposlouchávat ještě i na začátku sedmdesátých let tajné zprávy některých států pomocí technologie z druhé světové války. Největší rozmach kryptografie se započal právě v sedmdesátých letech. Do této doby byla totiž známá pouze symetrická kryptografie, od sedmdesátých let se již kryptografie dělí na symetrickou a asymetrickou.

3.1 Symetrická kryptografie

Symetrická kryptografie (v některých materiálech též konvenční kryptografie) je metoda při níž používáme stejný klíč pro zakódování tak pro rozkódování zprávy. Vstupem je tedy nějaký tajný text a klíč. Pomocí klíče se text šifrovací funkcí převede na kód, který již může být bezpečně odeslán příjemci. Příjemce potom použije dešifrovací funkci se stejným klíčem a získá tím původní tajný text. Nejdůležitější je, že jak příjemce, tak odesilatel musí mít k dispozici stejný klíč. Zde nastává problém s nutností zabezpečit samotný přenos klíče tak, aby se nedostal do cizích rukou. Pro šifrování se používají funkce, u kterých je velice obtížné a časově velmi náročné z vstupního a zakódovaného textu vygenerovat klíč. To i přes to, že vlastní kódování a rozkódování pomocí tohoto klíče je velice rychlé. Obtížnost případného zjištění klíče záleží zejména na délce klíče. Šifrovaná zpráva by měla odolat útoku hrubou silou, který předpokládá zkoušení všech možných klíčů. Pokud je klíč délky 4 bity, existuje potom pouze 2^4 (32) možných klíčů. Při průměrné rychlosti testování 4 klíče za vteřinu je tedy doba k nalezení správného klíče dílem malé chvilky. Již před řadou let se podařilo prolomit šifru DES s 56bitovým klíčem. Proto v dnešní době většina symetrických šifer pracuje se 128bitovými klíči, které mají teoretickou dobu prolomení hrubou silou vypočtený přibližně na 1000 let.



Obrázek č.8 - Schéma symetrického šifrování [4]

Mezi symetrické metody kryptografie lze vedle již zmíněného algoritmu DES zařadit jeho nástupce 3DES, BlowFish, CAST nebo CIPHER. Hlavním důvodem stálého používání symetrických šifer je hlavně rychlost, se kterou můžeme šifrovat a dešifrovat. Největší nevýhodou je potom nutnost nejprve nějakou metodou předat potřebný tajný klíč, další nevýhodou může být vysoký počet potřebných klíčů. Pro komunikaci mezi dvěma osobami stačí jeden klíč, pokud mezi sebou komunikují tři lidé, již jsou potřeba tři klíče. Při vyšším počtu osob tak již začíná být problém samotná správa tajných klíčů.

3.1.1 BlowFish

Jedná se o symetrickou blokovou šifru s velikostí bloku 64 bitů a délkou klíče nejvýše 448b. Algoritmus je tvořen dvěma částmi: částí expanze klíče a částí šifrování dat. Expanze klíčů převádí klíč na několik polí podklíčů. Šifrování dat je prováděno v šestnácti rundách. Každá runda provede permutaci závislou na klíči a poté substituci závislou jak na kódovaných datech tak i na klíči. Všechny operace použité v algoritmu jsou XOR a sčítání 32-bitových slov. Před samotných šifrováním nebo dešifrováním dat je však nutné vypočíst podklíče.

Většina blokových šifer je založena na principu Feistelovy sítě. Základní myšlenka spočívá v tom, že vstupní blok o n bitech je rozdělen na dvě stejně dlouhé části (označené pro jednoduchost L a R). Poté se definuje iterativní blokový algoritmus, kde vstup do i-té rundy je výstupem vždy rundy předcházející.

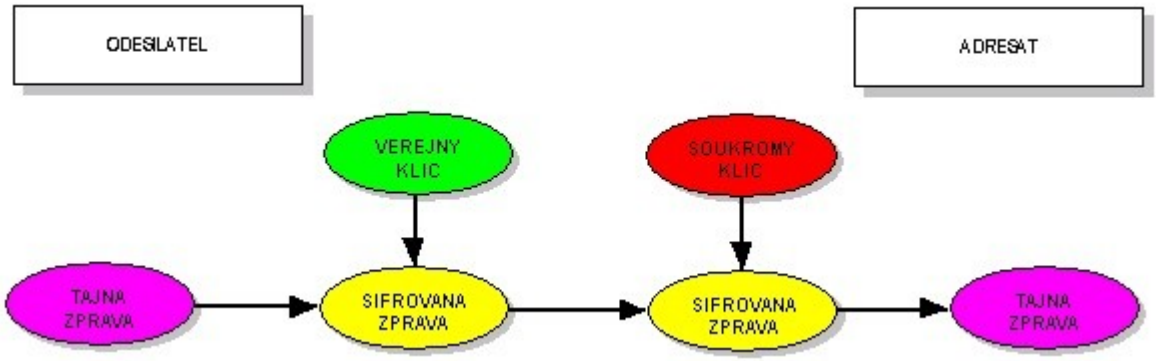
$L_i = R_{i-1}$

$R_i = L_{i-1}\ XOR\ f(R_{i-1}, K_i)$ kde K_i je podklíč použitý v i-té rundě a f je libovolná funkce.

Na stejném teoretickém principu fungují i šifry DES a CAST.

3.2 Asymetrická kryptografie

Asymetrická kryptografie využívá jiného klíče pro zakódování a jiného pro rozkódování. Dohromady se oba klíče nazývají párem klíčů. Všechna odesílaná data se šifrují pomocí veřejného klíče, přijímaná se potom dešifrují soukromým klíčem. Veřejný klíč není nazýván veřejným jen tak, pokud chcete, aby Vám někdo mohl poslat zakódovanou zprávu, musíte nejprve uveřejnit svůj veřejný klíč. Ten využije odesilatel k tomu, aby zakódoval zprávu, která je určena pouze Vám. Pro rozkódování zprávy lze potom použít pouze druhý klíč z páru, soukromý. Klíčový pár je většinou vytvářen zároveň. S délkou klíče u asymetrických metod je to trochu jinak, než u šifer symetrických. Asymetrické šifry totiž pracují se specifickými čísly, většinou to jsou prvočísla. Při pokusech o prolomení kódu je tak třeba se soustředit pouze na tato čísla a proto je třeba oproti symetrickým metodám délku klíče zvýšit natolik, aby zůstala zachována míra bezpečnosti. V dnešní době se tak běžně setkáváme s 1024bitovými nebo 2048bitovými klíči.



Obrázek č.9 - Schéma asymetrického šifrování [4]

Mezi nejznámější asymetrické algoritmy lze zařadit DH, RSA a DSA. Algoritmu RSA se podrobně věnuji v kapitole 7.Hlavními výhodami těchto metod je, že nemůže dojít k případnému vyzrazení soukromého klíče a také, že je třeba méně klíčů než u symetrických metod. Pro komunikaci s více lidmi zde stačí každému jeden pár klíčů. Hlavní nevýhodou těchto metod je jejich malá rychlost. Asymetrické metody jsou až tisíckrát pomalejší než metody symetrické. Další nezanedbatelnou nevýhodou je nutnost ověření pravosti veřejného klíče. Abyste si byly jisti, že komunikujete skutečně s tím člověkem, kterého potřebujete, je nutné, aby byl jeho veřejný klíč nějak jednoznačně označen. K tomu slouží certifikační úřady, které zjednodušeně řečeno udržují databázi osob s ověřenou totožností a jejich veřejných klíčů.

3.2.1 DH

Asymetrická šifra Diffie-Hellman je v nynější době velice používaná v open source systémech z důvodu vypršení autorských práv. Tato šifra je založena na matematickém problému výpočtu diskrétního logaritmu, tedy vypočtení hodnoty X, která splňuje G^X=M mod P, kde G a M jsou celá čísla a P je prvočíslo.

Mějme čísla M, A, B, P, G, X, Y. P musí být prvočíslo. Dalšími podmínkami jsou: M<P a Y=G^X mod P. Veřejným číslem je potom trojice [P,G,Y]. Soukromým klíčem je [X], původní zprávou potom číslo M a zašifrovaná zpráva je reprezentována dvojicí [A,B]

Klíče můžeme vytvořit takto. Náhodně najdeme prvočíslo P tak, aby bylo větší než všechny potencionální zprávy M, které bychom chtěli šifrovat. Potom zvolíme náhodná čísla G a X tak, aby obě dvě byly větší než P. Y vypočítáme podle již známého vzorce. Zašifrování zprávy M probíhá tak, že vypočteme čísla A a B podle následujících vzorců:

$A=G^X \bmod P$

$B=Y^X * M \bmod P$

Výsledná šifra bude mít tedy dvojnásobnou délku než původní zpráva. Dešifrování provedeme jednoduše tak, že M=(B/A^X) mod P

3.3 PGP

Pretty Good Privacy (dost dobré soukromí) je počítačový program, který umožňuje kódování hybridním způsobem. Funguje tak, že nejprve se vygeneruje náhodný tajný klíč, který se použije pro symetrické kódování tajné zprávy. Tento tajný klíč se zakóduje pomocí veřejného klíče asymetrické metody. Oba kódy (zakódovaný klíč a zakódovaný text zprávy) se odešlou příjemci. Ten si nejprve díky svému soukromému klíči zjistí náhodný tajný klíč a použije ho na dekódování tajné zprávy. Tento princip kombinuje ideální vlastnosti obou typu kryptografických metod. Rychlá funkčnost symetrického kódování samotné zprávy a vysoká bezpečnost předání tajného klíče díky asymetrické metodě kódování. Každý uživatel PGP tedy dostane svůj vygenerovaný klíčový pár. Pro zvýšení bezpečnosti je navíc soukromý klíč chráněný heslem, aby se ještě ztížila možnost ukradení tohoto klíče. Jako další vylepšení přišlo PGP s tím, že veřejný klíč se skládá z několika položek, které mohou přesně identifikovat vlastníka klíče.Položkou, která může pomoci s ověřením pravosti daného klíče, je podpis jiným

klíčem. Jedná se v podstatě o zaručení se za daný veřejný klíč. Pokud jiný uživatel ví, že daný klíč patří osobě jejíž ID klíč obsahuje, může tento klíč sám podepsat.

V roce 1991 spatřila světlo světa první verze PGP. Jejím autorem je americký odborník na kryptografii Philip Zimmermann. Prvním používaným asymetrickým algoritmem bylo RSA, avšak z důvodu sporů s autorskými právy se přešlo v dalších verzích na algoritmus DH. Jako symetrická metoda je potom nejčastěji použito IDEA, 3DES nebo CAST.

4 Občanský průkaz

Oproti pasu, který měl sloužit k odhalování případných zločinců, byl občanský průkaz již od prvopočátku zamýšlen pouze k identifikaci člověka. Myšlenka identifikace všech osob je mnohem mladší než identifikování viníků. Také snad proto se první zmínky o všeobecné občanské legitimaci na našem území objevily teprve v roce 1919, kdy vláda nařídila jejich zavádění. Tato legitimace však byla dobrovolná a obsahovala vedle fotografie jenom jméno, příjmení a datum narození držitele. První povinný občanský průkaz byl zaveden teprve během německé okupace a to dne 17.3.1939 nařízením říšského protektora. Podoba průkazu vycházela z obdobného dokumentu z Třetí říše. V podstatě stejný jako nařízení protektora byl zákon z roku 1948 o občanských průkazech, který zavedl povinnost mít občanský průkaz osobám v celním pohraničním pásmu.

Teprve v roce 1953 bylo vydáno nařízení o povinnosti vlastnit občanský průkaz všem bez výjimky. Tento první povinný průkaz byl několikastránková knížečka v červených plátěných deskách a obsahoval nejenom osobní informace o držiteli, ale také údaje o zaměstnavateli, dosaženém nejvyšším vzdělání, branném poměru, zdravotní údaje a omezení o způsobilosti k právním úkonům. Tento průkaz byl vydáván občanům při dosažení patnácti let věku a to okresním oddělením Sboru národní bezpečnosti. Postupem času se nejprve změnily desky na plastové a přibily informace o rodičích držitele. Po sametové revoluci se změnila na tři roky barva občanských průkazů z červené na hnědou.

Po rozdělení republiky již nastoupil občanský průkaz v obdobné podobě známé dodnes, tedy formou ID karty, avšak tehdy ještě s fotografií přilepovanou k plastové kartičce a orazítkované pro zajištění nevyměňování fotografií. Teprve od roku 2000 dostávají občané průkaz splňující normu ID2, přední strana obsahuje základní údaje o držiteli a také jeho tištěnou podobu a podpis držitele dokladu, všechny názvy položek na přední straně jsou poprvé označeny v českém i anglickém jazyce. Norma ID2 také nařizovala zavedení strojově čitelné oblasti. Na druhé straně průkazu se nalézají údaje o místu narození, trvalém pobytu, rodném příjmení a rodinném stavu, případně nepovinné údaje. Poslední výraznou změnou prošel občanský průkaz v roce 2005, oproti předchozí verzi jsou názvy položek přeloženy i do francouzštiny a byl přesunut údaj

o rodném čísle. Od roku 2006 je na zadní stranu jako další údaj zaznamenáno uzavření registrované partnerství a jako nepovinný údaj taky údaje o partnerovi.

Obrázek č.10 - Občanský průkaz [5]

4.1 Strojově čitelná oblast

Osobní doklady a související dokumenty jsou opatřeny strojově čitelnými informacemi usnadňujícími automatizované zpracování pomocí OCR. Takové údaje mají podobu dvou řádků textu u spodního okraje. Obsah těchto dvou řádek je definován normami, přičemž délka řádku je pro různé doklady různá. První řádek obsahuje informace o typu a podtypu doklady, vydavatelský stát, příjmení a jméno držitele, zbytek vyplněn znakem „<", samostatný výskyt znaku „<" ve jménu nebo příjmení má význam mezery. Druhý řádek je potom složek z čísla dokladu, kontrolní číslice dokladu, občanství, datum narození, kontrolní číslice k datu narození, pohlaví, platnost dokladu, kontrolní číslice k datu platnosti a volitelné pole s kontrolním znakem

Občanský průkaz čtečka pozná podle toho, že má řádek dlouhý pouze 36 znaků, označen je ID jakožto typ a podtyp dokladu. Ve druhém řádku potom jako volné pole je uvedena druhá část rodného čísla doplněná výplňovým „<<<", kontrolní znak volitelného pole ani souhrnný kontrolní znak není na občanském průkazu uveden.

Cestovní pas se od občanského průkazu liší mimo jiné i délkou řádku. Pas má řádek dlouhý 44 znaků, označován bývá pouze písmenem P a znakem „<". Ve volném poli je zapsáno rodné číslo doplněné výplňovým „<<<" následovaným kontrolním znakem volitelného pole a souhrnným kontrolním znakem.

Veškeré kontrolní znaky s výjimkou posledního souhrnného se počítají s pomocí cyklicky opakovaných vah 7, 3, 1 vypočte vážený součet. Kontrolní číslicí je zbytek po dělení deseti tohoto součtu.

```
Příklad:
Platnost do: 210622
   +----+----+----+----+----+----+
   |  2 |  1 |  0 |  6 |  2 |  2 |
---+----+----+----+----+----+----+
 * |  7 |  3 |  1 |  7 |  3 |  1 |
---+-------------------------------+
 = | 17 +  3 +  0 + 42 +  6 +  2 = 70 % 10 = 0
---+----+----+----+----+----+----+---------====
Kontrolní znak je 0
```

4.2 Budoucnost

V posledních dvou letech se zejména v Japonsku a ve Spojených státech amerických začíná testovat naprostá novinka v oblasti identifikace osob. Touto novinkou jsou elektronické čipy implantované pod kůži většinou pravé paže. Výhodami těchto čipů je nemožnost svou identifikaci někde zapomenout a naprostá jednoznačnost tohoto čipu. Jelikož je na čipu nahrána informace o jméně, příjmení, datu narození a zároveň i fotografie držitele dá se čip zfalšovat velice obtížně. Některé čipy mohou obsahovat i informace o krevní skupině držitele, případně i záznam jeho DNA. Nevýhodami jsou hlavně čtečky takovýchto čipů a možné rozbití čipu při pádu či úderu do paže. Problém se čtečkami se mi jeví jako největší. Takováto čtečka i v rukou nepovolaného člověka dokáže přečíst veškeré údaje uložené na čipu. Tato data potom může využít libovolně dle svého uvážení. Narozdíl od pasů, u kterých je takovéto čtení možné pouze na omezenou dobu při otevření Vašeho pasu, není možné nikomu zakázat, aby vedle Vás šel, přitom měl v kapse čtečku údajů a během chůze skenoval Vaše údaje z čipu. Před rozšířením této novinky je proto třeba ještě mnohé vyřešit, avšak troufám si tvrdit, že nějak takhle bude vypadat budoucnost občanských průkazů i cestovních pasů.

5 Cestovní pas

Cestovní pas je cestovní dokument, který pro konkrétního člověka vydává stát jehož je občanem. Je základním dokumentem, který je potřeba pro vstup a projíždění jinými státy.

Cestovní pasy zároveň deklarují právo na ochranu v zahraničí státem, který tento dokument vydal a vstup do země, která ho vydala. Cestovní pasy obvykle obsahují fotografii držitele, podpis, datum narození, národnost a někdy další znaky identifikující člověka. Mnoho zemí do pasů začíná zahrnovat i tištěnou strojově čitelnou oblast dokladů usnadňující zpracování. Nejnověji mohou pasy obsahovat také čip, který kromě běžných údajů může volitelně obsahovat také biometrické údaje, které usnadňují identifikaci předkladatele dokladu jako oprávněného držitele. Pokud je pro vstup do země potřeba vízum, bývá vlepeno do cestovního pasu. V jednodušších případech je vízum udělováno přímo při překračování hranic formou otisku razítka.

Myšlenka něčeho jako je cestovní pas, vzešla již ve starověkém Egyptě. Kdy se snažili nějak vyřešit problémy s poznáváním zločinců nepatřících do příslušného města. V Egyptě se toto snažili řešit pomocí spisů psaných klínovým písmem na cihlách, ve středověku byly sepisovány do knih útrpného práva smolných či hrdelních. Jednalo se v podstatě o první verze rejstříků trestů a různé seznamy zločinců, které se opisovali a tyto opisy se posílali do spřátelených měst. Takováto opatření však nestála za mnoho. Právě snaha získání informací osobách bezpečnostními orgány vedla k zavedení všelijakých cestovních pasů nebo legitimačních papírů jejichž identifikační hodnota však před vynálezem fotografie nebyla příliš vysoká.

V zemích blízkého i dálného východu se rozhodli řešit situaci s identifikací zločinců velice neobvykle. Tresty byly rozděleny podle své nebezpečnosti do jakési tabulky. Podle této tabulky se zločincům usekl určitý prst na ruce, případně celá ruka. Podle chybějících částí těla pak mohl každý poznat, s kým má tu čest.

Ve Francii za doby Ludvíka XVI. zavedla tajná policie speciální písmo právě pro psaní do cestovních pasů. Tímto písmem, které bylo identifikováno určitou barvou, ozdobami
a liniemi, byl na průvodní list napsán stav, bydliště, státní příslušnost, vědomosti a varování před podezřelými a nebezpečnými. Vynález tisku představoval velký krok

k doplnění málo spolehlivých seznamů zločinců. Umožnil aby jejich podobizny vyřezané ve dřevě byly rozmnožovány tiskem a rozšiřovány.

První verze cestovního pasu České republiky začala být vydávána od roku 1993, jednalo se běžný v okolních státech používaný typ zelené barvy s datovou stranou umístěnou na zadní předsádce, vlepenou fotografií a názvy položek v českém a anglickém jazyce.

Poslední verze bez strojově čitelných údajů byl vydáván až do února 2007 v podstatě nezměněné formě.

Mezitím se však začaly vydávat pasy se strojově čitelnými údaji. Jeho první verze spatřila světlo světa 1.7.2000 a oproti verzi bez strojových údajů byl zbarven dočervena. Datová strana je umístěna na zadní předsádce, podoba držitele je tištěná a názvy položek jsou v českém a anglickém jazyce.

Tato forma se dochovala až do roku 2005, od 16.3 se začali vydávat nové verze s datovou stranou umístěnou na druhé straně, tištěnou podobou držitele a názvy položek uvedené v českém, anglickém a francouzském jazyce. Navíc na stranách 6 a 7 jsou uvedeny překlady názvů položek do 18 jazyků států Evropské Unie a ruského jazyka.

Tento typ však vydržel pouze necelého půldruhého roku, když 1.9. byl uveden cestovní pas s biometrickými údaji. Datovou stránku už mají umístěnou na všité polykarbonátové kartě, podoba držitele je vytvořena laserovou perforací. Názvy položek už nedoznaly změny. Od 7.3. 2009 byly k již zavedeným biometrickým údajům (digitálně zpracované fotografii občana a jeho podpisu) ještě otisky ukazováku levé a pravé ruky.

Obrázek č.11 - cestovní pas s biometrickými údaji [6]

5.1 Nosič biometrických údajů

Hned ze začátku je nutno říct, že mnohé nevýhody nosiče biometrických údajů, které zde uvádím, byly známy již před uvedením pasů s těmito nosiči. Přesto se většina států rozhodla tyto nosiče používat, protože rizika s tím spojená považují za akceptovatelné. Toto platí například pro útoky kopírováním dat, které jsou popsány již několik let mimo jiné i v dokumentaci organizace, která je standardizací elektronických pasů pověřena. Přesto byla zpráva o možnosti kopírování dat brána mnohými periodiky jako téměř revoluční novinka.

Standardizaci pasů na celosvětové úrovni má na starosti Mezinárodní organizace pro civilní letectví (ICAO), která je součástí OSN. Tato organizace vydává standard číslo 9303 popisující, jak má pas vypadat. Řada vlastností elektronických pasů je volitelná, někdy je dokonce možná volba z více variant. U nás se parametry elektronických pasů řídí nařízením Evropské Unie.

Elektronický pas se od tradičního liší zejména integrovaným bezkontaktním čipem a logem elektronického pasu na svém obalu. Čip s anténou je vložen do stránky s datovými údaji, který je na začátku pasu a je tvořena polykarbonátovou vrstvou, do které je čip zalit a do níž je také laserem gravitována černobílá fotografie držitele pasu. Čip v pase je bezkontaktní čipová karta splňující ISO 14443. Tato technologie je schopna přenášet data na vzdálenost maximálně deseti centimetrů a umožňuje využití čipových karet s paměťovou kapacitou desítek kB. Data v elektronickém pase jsou soubory v jednom adresáři. Datových souborů je maximálně 16, jsou nazývány DG1 až DG16.

DG1 obsahuje data ze strojově čitelné zóny, DG2 potom fotografii držitele pasu a DG3 je určena pro otisky prstů. V DG4 bude podle normy uložen obraz oční duhovky, pokud se k tomuto druhu biometriky někdy přejde. Kromě datových skupin obsahuje pas ještě dva soubory s metadaty. Další datové skupiny mohou obsahovat dodatečné údaje o držiteli, vydávající instituci nebo pase. Normou není určeno v jakém pořadí mají tyto doplňkové informace následovat. Soubor EF.COM obsahuje seznam přítomných datových skupin a údaje o použitých verzích. Soubor EF.SOD potom obsahuje digitální podpis dat. Soubory EF.COM, EF.SOD, DG1, DG2 a DG3 jsou povinné pro všechny pasy vydané na území Evropské Unie, mimo Evropu se ještě vyskytují místa, kde soubor DG3 povinný není, později se pokusím vysvětlit proč tomu tak je. Všechny ostatní datové skupiny jsou volitelné.

5.2 Přístup k datům

V základní verzi nejsou data v elektronických pasech z hlediska důvěrnosti nijak chráněna, proto může s čipem komunikovat kdokoliv vlastnící příslušnou čtečku. Komunikace s čipem také není nijak šifrována, takže je možný i odposlech probíhající komunikace. Takové pasy však vyvolaly řadu debat o bezpečnosti osobních dat. Jedním z vymyšlených vylepšení je stínění pasu například zabalením do hliníkového přebalu. Tato metoda je použita u amerických pasů. Zabráníte tím nevědomé komunikaci s čipem avšak nemůžete zabránit odposlechu. Stínění navíc ztěžuje legitimní komunikaci a při mírném otevření pasu již není zcela účinné.

Jinou možností obrany vůči čtení je autentizace čtečky. Nejedná se ovšem o autentizaci v klasické verzi, protože autentizační data nejsou tajná, jedná se spíše jenom o informaci, že čtečka zná určité informace vytištěné v pase. To by mělo prokázat možnost fyzického přístupu k pasu. Spolu s následným šifrováním komunikace je zajištěná i obrana vůči odposlechu. Vyřešit však je potřeba skutečnost, že pas musí být čitelný pohraničníky všech zemí světa. Řešením je, že autentizační údaje jsou získány hašováním určitých údajů ve strojově čitelné zóně. Takto může přistupovat k datům v pase kdokoliv kdo má pas v ruce a může v něm číst data, má přístup i k údajům na čipu. Řeší se tak přistup k datům v zavřeném pase v kapse neznámého člověka, ale přístup k datům není omezen pouze na pohraničníky, ale číst data mohou například i hoteliéři. Tento způsob ochrany dat v pasech se nazývá základní řízení přístupu BAC, který je celosvětovým volitelným ochranným prvkem. Pasy členských zemí však musí BAC implementovat povinně.

5.3 Integrita dat a autenticita čipu

Integrita dat je zajištěna digitálním podpisem dat. Digitální podpis je umístěn v souboru EF.SOD a jedná se o klasickou strukturu typu SignedData. Každý stát má svou certifikační autoritu, která vydává certifikáty složkám, které vydávají pasy. Jedná se o podepisovače dokumentů. Samotná data jsou podepsána těmito podepisovači. Pro ověření podpisu musíme mít certifikát příslušné země, ten musíme získat důvěryhodnou cestou od dané země a zároveň i certifikát podepisovače dokumentů, který se nachází přímo v pase. Podepsaná data tvoří speciální strukturu obsahující heše všech přítomných DG souborů v pase. Tímto způsobem je možné ověřit integritu každého souboru samostatně. Podpisové mechanismy použité v elektronických pasech jsou RSA, DSA a ECDSA. Použitelné hašovací funkce jsou SHA-1, SHA-224, SHA-256, SHA-

384 a SHA-512. Digitální podpis dat v pase je jedním z klíčových bezpečnostních prvků elektronických pasů. Při podepisování dat si země může vybrat podpisové schéma, které jí vyhovuje z hlediska implementace. Při ověřování podpisu je pochopitelně nutné podporovat všechny varianty. Ověřování podpisu je relativně bezproblémová věc, komplikacemi může být velké množství algoritmů, které je třeba implementovat, získávání správných kořenových certifikátů všech zemí a datové skupiny u nichž jsou možné legitimní změny. Problém se získáváním kořenových adresářů se již tři roky marně snaží vyřešit ICAO pomocí adresářové služby, která však stále ještě neobsahuje všechny země. Legitimní změny můžeme zaregistrovat například u souboru DG16, který obsahuje adresy příbuzných pro případ informování o nehodě držitele, takové datové skupiny by se potom neměly podepisovat. Je zřejmé, že digitální podpis nemůže zabránit vytváření identických kopií dat. Z toho důvodu není možné spoléhat pouze na data z čipu, ale je třeba při kontrole cestovního dokladu věnovat pozornost i klasickým ochranným mechanismům pasu a souladu vytištěných dat s daty uvedenými v čipu. Zabránit kopírování dat však můžeme i za pomoci kryptografie a odolnosti vůči narušení. V takovém případe je v čipu uložen asymetrický pár klíčů. Zatímco veřejný klíč je volně čitelný ze souboru DG15, soukromý klíč není z čipu relativně získatelný a je pouze možno ověřit, zda jej má čip k dispozici. Tento postup se nazývá aktivní implementace a je volitelným prvkem elektronických pasů. V této možnosti se naše pasy liší od evropských, narozdíl od stanov EU naše předpisy AA implementují.

5.4 BAC

Základní řízení přístupu je mechanismus bránící čtení dat z čipu bez znalosti autentizačních klíčů. Tyto klíče jsou odvozeny z dat vytištěných ve strojově čitelné zóně. Konkrétně se jedná o číslo dokumentu, datum narození držitele a datum vypršení platnosti pasu. Všechny tyto údaje se nacházejí na druhém řádku čtecí zóny. Nebyly vybrány zcela náhodně, jsou to právě ty údaje, které obsahují kontrolní číslici. To se děje z toho důvodu že i OCR bývá chybové a proto je preference polí s kontrolní číslicí pochopitelná. Tyto tři údaje se v ASCII formě zřetězí a hašují se algoritmem SHA-1. Z tohoto haše se dalším hašováním pomocí 112 bitové 3DES odvodí klíče pro šifrování a autentizaci. Následně dojde k ustavení sdíleného klíče sezení a následná komunikace je zabezpečena. Toto je klasická vzájemná autentizace, která je považována za bezpečnou, pokud jsou klíče tajné. V případě pasů ale nejde o tajnost klasickou, protože klíče jsou odvoditelné z dat napsaných v pase, nicméně i zde je vhodné zabránit náhodnému uhodnutí klíče. U pasů je však toto mírně problematické, protože data, ze

kterých jsou klíče odvozeny nemají příliš velké rozpětí. Možnost prolomení však zmenšuje nutnost být maximálně deset centimetrů od čipu. Od 1.1.2010 již budou muset být údaje pro hašování hašovány pomocí algoritmu SHA-2 a zároveň od tohoto data bude stanovena nejmenší délka klíče RSA algoritmu na 2048 bitů.

5.5 AA

Cílem aktivní autentizace je ověřit, zda je čip v pase autentický. Pomocí protokolu výzva-odpověď se ověřuje, zda má pas k dispozici správný soukromý klíč. Asymetrický pár klíčů pro aktivní autentizaci je specifický pro každý pas. Čtečka ověřuje digitální podpis pasu na haši podepsaném soukromým klíčem pasu. Za předpokladu odolnosti vůči narušení čipu, správnosti implementace či odolnosti vůči útokům postranními kanály je výsledkem bezpečné ověření autenticity čipu. Problémem aktivní autentizace je, že výzva, která se posílá k pasu k podepsání, není zcela náhodná, ale kóduje mimo jiné i čas a místo. Pokud by nějaká země uchovávala výzvy a odpovědi jako důkaz o tom, že se daný člověk nacházel na daném čase a na určitém místě. V praxi však takový důkaz musí čelit faktu, že pas podepíše kdekoliv a kdykoliv jakoukoliv výzvu a vypovídací hodnota odpovědí je tedy malá. Navíc by bylo mnohem jednodušší sledovat data pohybu mobilního telefonu, který je vysledovatelný s mnohem větší přesností a pravidelností. I tak je ale existence tohoto možného útoku důvodem proč třeba Německo nebo Francie ve svých pasech aktivní autentizaci neimplementovalo.

5.6 Problémy s otisky prstů

Od března letošního roku se začali do čipů v cestovních pasech přidávat i informace o otiscích prstů. Od té doby se již ukázaly mnohé nedostatky tohoto pokusu o další zpřesnění identifikace držitele. Jedním z problémů je samotný sběr otisků. Při zkušebních pokusech s porovnáním otisků prstů z policejních záznamů a otisků, které se dělají do pasů byla počítačem vypočtená shoda sotva u 20% pokusů. Hlavním důvodem takto nízkého čísla je fakt, že v policejních záznamech je otisk tvořený pomocí otočení celé půlky prstu, zatímco otisk do pasu je vytvořen přiložením prstu na čtečku. Takovýto otisk je jenom těžko srovnatelný s policejním typem, pokud se provede pouze jednou. Proto se třeba ve Španělsku rozhodli provádět sejmutí otisku třikrát po sobě a vybírají pouze nejlepší otisk. Tímto zlepšili shodnost na více než 85%. Dalším problémem jsou však samotné elektronické čtečky otisků. Když se tato zařízení dostala do běžného prodeje, varoval původní vynálezce, že čtečka není a nikdy nebude natolik

přesná, aby se podle ní dalo s velkou přesností zajistit rozlišení dvou lidí od sebe. Postupem času se přesnost čteček zlepšila, přesto však dosud není hodno na tato zařízení naprosto spoléhat.

6 Elektronický podpis

Podpis nás provází v podstatě celý život. Už na základní škole, když nás naučí psát, je jednou z prvních znalostí, které nám předají, umění podepsat se celým jménem. V dospělosti se potom náš podpis většinou modifikuje jenom na příjmení a je ovlivněn našimi podepisovacími návyky. Tyto druhy podpisu mají jeden společný bod, k jejich vytvoření potřebujeme vlastní ruku, kousek papíru a psací nástroj. Nyní je však již několik let součástí našich zákonu podpis elektronický. U něj již podpis nevytváříme sami, ale udělá to za nás speciální software nainstalovaný na počítači. Elektronický podpis přinesl mnoho výhod. Nedají se najít dva stejné a nelze ho napodobit, stačí se jednou elektronicky podepsat a není potřeba na různých místech vyplňovat formuláře s osobními údaji. Velikou nevýhodou je nejasnost a nejednoznačnost uvedení elektronického podpisu do českých potažmo i evropských zákonů. Pokud si totiž člověk chce elektronický podpis pořídit, zjistí, že ho musí každý rok obnovovat a navíc že ho v podstatě nemá ani kde použít. Při zavádění elektronického podpisu se předpokládalo, že by mohl být používán při veškerém jednání se státními úřady. Realita v tuto chvíli vypadá tak, že jediná opravdová možnost, kdy využít v kontaktu se státní zprávou elektronický podpis je možnost podepsat své daňové přiznání. Přiznejme si, že jenom kvůli jedné listině nemá cenu vydávat každoročně peníze na obnovu elektronického podpisu. Další myšlenkou byla možnost, že by se pomocí elektronického podpisu dalo zjednodušit elektronické obchodování, kdy by odpadla nutnost vypisovat pokaždé svoje údaje, které navíc ani nemusí být pravdivé. Každý svůj uzavřený obchod byste jednoduše podepsali svým elektronickým podpisem a tím byste stvrdili, že objednávku skutečně vyřizujete a potvrzujete. Ovšem zde se dostáváme do začarovaného kruhu. Dokud nebude dostatek lidí používajících elektronický podpis, nevyplatí se elektronickým obchodům implementovat řešení pro elektronický podpis.

6.1 Elektronický versus digitální podpis

Někdo by mohl říct, že mezi digitálním a elektronickým podpisem nejsou žádné rozdíly a že záleží jenom na dané zemi, kterou terminologii zvolí. Tak třeba v USA se mluví o digitálním podpisu, zatímco evropské země většinou používají termín elektronický podpis. Rozdíl mezi těmito dvěma označeními je však mnohem markantnější. Elektronický podpis je obecný, technologicky neutrální termín, který se vztahuje na

množství různých metod, kterými může člověk potvrdit autenticitu elektronického dokumentu. Přestože jsou všechny elektronické dokumenty digitální, mohou se vyskytovat v různých formách a mohou být vytvořeny různými technologiemi. Jako příklady elektronického podpisu tak lze uvést třeba i jméno odesilatele v závěru mailu, digitalizovanou podobu ručního podpisu připojenou k elektronickému dokumentu, tajný kód nebo PIN sloužící k tomu, aby adresát poznal odesilatele, dále třeba i otisk prstu nebo sken sítnice a nakonec digitální podpis vytvořený použitím asymetrické kryptografie. Digitální podpis je termín pro technologicky specifikovaný typ elektronického podpisu. K podepsání dokumentu využívá asymetrické šifrování. Elektronický podpis je tak v podstatě obecnější pojem a kromě samotného digitálního podpisu v sobě zahrnuje i jiné aspekty využití různých metod.

6.2 Zaručený elektronický podpis

Právě mimo jiné kvůli nejednoznačnosti pojmů zavedl český právní systém pojem zaručeného elektronického podpisu. Jedná se v podstatě o elektronický podpis v takové formě, která zpravidla kryptografickými metodami, zaručuje i integritu dokumentu a autentizaci podepsaného. Pro některé účely je navíc ještě vyžadován zaručený elektronický podpis založený na kvalifikovaném certifikátu. Hlavní rozdíl mezi prostým a zaručeným elektronickým podpisem je v podstatě stejný jako rozdíl mezi úředně neověřeným a ověřeným vlastnoručním podpisem. Zaručený elektronický podpis dokumentu zajišťuje autenticitu (původnost identity subjektu), integritu (po podepsání nebyl dokument změněn), nepopiratelnost a může obsahovat i časové razítko, které prokáže datum a čas podepsání dokumentu.

6.3 Jak elektronický podpis funguje

Zaručený elektronický podpis je atypickým příkladem asymetrické kryptografie. Obvyklý postup by byl, že bychom vzali veřejný klíč příjemce, zašifrovali bychom dokument a příjemce by byl poté jediný, kdo by dokázal pomocí svého tajného klíče dokument přečíst. Nám však jde o něco naprosto jiného. Jedná se nám pouze o to, že dokument byl podepsán skutečně námi. Proto vezmeme pouze otisk (hash) dokumentu, tento otisk zašifrujeme svým tajným klíčem, čímž vznikne podpis. Ověření podpisu se potom odehrává tak, že pomocí našeho veřejného klíče dešifrujeme hash a poté ho porovnáme s námi vytvořeným otiskem podepsaného dokumentu. Pokud si oba hashe odpovídají, pak je podpis ověřen a dokument je považován za důvěryhodný. Autor

potom nemůže popřít své autorství, neboť k jeho tajnému klíči nemá nikdo jiný přístup. Pokud by byl dokument po podepsání ještě změněn, pozná se to potom právě podle odlišností v otiscích.

7 Rozbor šifry RSA

Jedna z nejdéle používaných asymetrických kryptografických algoritmů se jmenuje RSA. V roce 1977 byl navržen Ronaldem L. Rivestem, Adi Shamirem a Leonardem Adlemanem na Massachusetts Institute of Technology. Iniciály navrhovatelů daly vzniknout jménu algoritmu. Algoritmus jako takový je založený na velice jednoduché úvaze. Vynásobíme dvě dlouhá prvočísla. Tento součin bez znalosti alespoň jednoho z prvočísel je v podstatě prakticky nerozložitelný zpět na původní prvočísla. V podstatě stejný systém popsal již v roce 1973 britský matematik Cocks. Jelikož by však bylo pro jeho řešení nutné použít drahou výpočetní techniku pro uvedení algoritmu do praxe, nebyl jeho systém uznán jako použitelný pro veřejnost. Jeho výzkum byl navíc až do roku 1997 tajen z důvodu označení jako přísně tajné.

7.1 Tvorba klíčů, šifrování

Tvorba klíčů spočívá v tom, že se zvolí dvě různá velká náhodná prvočísla P a Q. Následně spočítáme jejich součin

$N= P*Q$

Poté spočítáme hodnotu Eulerovy funkce

$\varphi(N) = (P - 1)(Q - 1)$

Zvolíme celé číslo E menší než $\varphi(N)$. Zároveň však E a $\varphi(N)$ musejí být nesoudělné. Nalezneme číslo D, pro které platí

$D*E \equiv 1 \pmod{\varphi(N)}$.

Pokud je E prvočíslo tak

$D = (1+r*\varphi(N))/E$, kde $r = [(E-1)\varphi(n)^{(E-2)}]$.

Veřejným klíčem je dvojice (N, E), přičemž N je označováno jako modul a E jako šifrovací exponent. Soukromý klíč potom tvoří dvojice (N, D), kde D se označuje také jako dešifrovací exponent. Je nutno ještě podotknout, že klíče jsou v praxi uchovávány v mírně upravené formě, která umožňuje trochu rychlejší zpracování.

Pokud chceme zaslat zprávu Z, je tato zpráva převedena na číslo M. Šifrovým textem odpovídajícím této zprávě je potom číslo C.

$C=M^E \bmod N$

Tento šifrovaný text je poté zaslán nezabezpečeným kanálem. Pro dešifrování zprávy stačí provést výpočet:

$M=C^D \bmod N$.

Fakt, že tímto výpočtem získáme původní zprávu, je důsledkem následující rovnosti:

$C^D \equiv (M^E)^D \equiv M^{ED} \pmod N$.

A jelikož:

$E*D \equiv 1 \pmod{P-1}$ a $E*D \equiv 1 \pmod{Q-1}$,

Díky malé Fermatově větě platí, že:

$M^{ED} \equiv M \pmod P$ a zároveň $M^{ED} \equiv M \pmod Q$

Jelikož p a q jsou různá prvočísla, pomocí čínské věty o zbytcích je dáno:

$M^{ED} \equiv M \pmod{PQ}$. Tudíž $C^D \equiv M \bmod N$.

Příklad:
Pro jednoduchost vybírám extrémně malá čísla, v praxi se využívají o mnoho řádů větší prvočísla.
P = 61 (první prvočíslo)
Q = 53 (druhé prvočíslo)
$N = P*Q$ = 3233 (modul, veřejný)
E = 17 (veřejný, šifrovací exponent)
D = 2753 (soukromý, dešifrovací exponent)
Pro zašifrování zprávy 123 probíhá výpočet:
šifruj(123) = $123^{17} \bmod 3233 = 855$
Pro dešifrování pak:
dešifruj(855) = $855^{2753} \bmod 3233 = 123$

7.2 Bezpečnost algoritmu

Zabezpečení šifrovacího systému RSA je založeno na dvou prozatím neřešitelných problémech. Prvním problémem je problém faktorizace dvou velmi vysokých čísel. Plné dešifrování RSA šifrovaného textu je nyní známými technikami nemožné, jelikož není znám algoritmus, který by dokázal tento problém vyřešit. Druhým problémem je potom nazýván RSA problém. Spočívá v tom, že nedokážeme získat e-tý kořen modulu množiny n, obnovení hodnoty m jako $M^E=C \bmod N$, kde (E, N) jsou RSA veřejné klíče a C je RSA šifrovaný text.

Jestliže bude n 256 bitů a kratší dokážeme ho dnešní technikou prolomit během několika hodin na běžném osobním počítači. V roce 1999 byl dokázán průlom RSA algoritmu při n 512 bitů. Útok probíhal pomocí velké počítačové sítě obsahující několik

set osobních počítačů. Zatím nejdále se odborníci dostali v roce 2005, kdy bylo prolomeno RSA šifrování s použitím 663 bitových klíčů, RSA klíče jsou však typicky dlouhé 1024 – 2048 bitů. Již tehdy se objevovaly názory některých expertů tvrdící, že během pěti let bude prolomen i 1024 bitů dlouhý klíč. Doposud se tyto predikce nepotvrdily a zatím neexistují ani zvěsti o tom, že by se tak mohlo v horizontu pěti let stát.

Abych však čitatele trochu zneklidnil, existují v dnešní době již dvě popsané možnosti, jak by toho průlomu mohlo být dosaženo. Jedním je teoretické hardwarové zařízení jménem TWIRL popsané Shamirem a Tromerem v roce 2003. Zároveň však ve spisu bylo napsáno, že stroj nebude moci být sestrojen dříve než se podaří vynalézt mnohem rychlejší a schopnější čipy. Dalším možným ohrožením je Shorův algoritmus, který publikovat Peter Shor v roce 1993. Shor v něm dokazuje, že kvantový počítač by mohl vykonávat faktorizaci v dostupném čase. Avšak vzhledem k problémům realizace principů kvantového počítání se nedá počítat, že by zašifrovaná data mohla být v dohledné době tímto algoritmem ohrožena.

7.3 Výhody a nevýhody

Obecnou nevýhodou asymetrického šifrování , algoritmus RSA nevyjímaje, je jeho nízká rychlost šifrování a dešifrování. Největší výhodou je v tuto chvíli praktická neprolomitelnost. Tuto výhodu lze ještě pojistit při použití klíčů o délce 2048 bitů, případně 4096 bitů.

Závěr

Původním cílem práce bylo seznámit čtenáře s novinkami v oblasti elektronických průkazů totožnosti. Během shánění materiálů jsem však dospěl k závěru, že jen málokdo by zcela porozuměl celému mému textu bez předchozích základních znalostí kryptografie. Proto jsem své cíle přehodnotil a úvodní část své práce věnoval krátkému shrnutí historie kryptografie, teprve v další části jsem se věnoval občanskému průkazu, cestovnímu pasu a elektronickému podpisu. V poslední části byly nastíněny některé aspekty tvorby asymetrického algoritmu s přihlédnutím na čtenáře – začátečníka. Po přečtení textu několika laiky jsem doufám schopen říci, že se mi cíle podařilo splnit.

Literatura

[1] TILL, Michal. *Historie kryptografie I.* [online].
2000-2002 [cit. 2009-08-10].
Dostupný z WWW: <http://www.krypta.cz/articles.php?ID=55>.

[2] *Cryptography* [online].
2006 [cit. 2009-08-10].
Dostupný z WWW: <http://en.wikipedia.org/wiki/Cryptography>.

[3] *Kryptografie* [online].
2008 [cit. 2009-08-01].
Dostupný z WWW: <http://cs.wikipedia.org/wiki/Kryptografie>.

[4] *Stručný úvod do kryptografie* [online].
2001 [cit. 2009-08-16].
Dostupný z WWW: <http://krypto.krokonet.com/>.

[5] *Občanský průkaz* [online].
2007 [cit. 2009-07-20].
Dostupný z WWW: < http://cs.wikipedia.org/wiki/Občanský_průkaz>.

[6] *Cestovní pas* [online].
2007 [cit. 2009-07-20]
Dostupný z WWW: < http://cs.wikipedia.org/wiki/Cestovní_pas>.

[7] *Elektronický podpis* [online].
2007 [cit. 2009-07-20]
Dostupný z WWW: < http://cs.wikipedia.org/wiki/Elektronický_podpis>.

[8] *Zákon 227/2000 Sb. o elektronickém podpisu* [online].
2008 [cit. 2009-08-20].
Dostupný z WWW: <http://portal.gov.cz/wps/portal/_s.155/701?
kam=zakon&c=227/2000>.

[9] *MRZ - strojově čitelná zóna dokladů* [online].
2004 [cit. 2009-07-20].
Dostupný z WWW: <http://blog.vyvojar.cz/bst/archive/2006/10/16/MRZ.aspx>.

[10] RAŠEK, L. *Elektronické cestovní doklady: část 1*.
Crypto-World. 2006, roč. 8, č. 10, s. 4-18.
Dostupný z WWW: <http://cryptoworld.info/casop8/crypto10_06.pdf>.

[11] RAŠEK, L. *Elektronické cestovní doklady: část 2*.
Crypto-World. 2006, roč. 8, č. 11, s. 17-24.
Dostupný z WWW: <http://cryptoworld.info/casop8/crypto11_06.pdf>.

[12] SINGH, Simon. *Kniha kódů a šifer*.
Petr Koubský. [s.l.]: [s.n.], 2003. 384 s.
ISBN 80-86569-18-7.

[13] Biometric capture: The German fingerprint initiative.
In *ICAO MRTD Report*. [s.l.] : [s.n.], 2009. s. 24-30.

[14] GROŠEK, Otokar, PORUBSKÝ, Štefan. *Šifrovanie - Algoritmy, metódy, prax*.
[s.l.]: [s.n.], 1992. 272 s.
ISBN 80-85424-62-2.