Základy moderní kryptologie – Symetrická kryptografie I.

Vlastimil Klíma

verze: 1.2

Abstrakt

Cílem třech přednášek (Symetrická kryptografie I., II. a III) je

a) ukázat, že moderní kryptologie se zabývá mnohem širším okruhem věcí než jen utajováním zpráv a jejich luštěním,
b) seznámit s některými novými myšlenkami,
c) a věnovat se více jedné části moderní kryptologie, tzv. symetrickým schématům.

Vzhledem k rozsahu těchto přednášek, které mají úvodní přehledový charakter, nebude možné postihnout ani klíčové, ani nejkrásnější myšlenky této vědy, ale jen některé nejpoužívanější. Následující texty vychází částečně z citované a doporučené literatury, jsou však nutně zatíženy subjektivním výkladem.

Doporučená literatura:

Základní příručka:
Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996, dostupné celé on-line na
http://www.cacr.math.uwaterloo.ca/hac/

Často doporučovaná alternativa:
Doug Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995

Historie:
David Kahn, *The Codebreakers*, Scribner, 1996

Internetový portál:
http://theory.lcs.mit.edu/~rivest/crypto-security.html

Kontakt a osobní stránky:
v.klima@volny.cz, http://cryptography.hyperlink.cz

Poděkování: Autor vyjadřuje poděkování společnosti LEC s.r.o., http://www.lec.cz, za podporu při psaní textu přednášky.

Obsah

1. Rozvoj kryptologie a souvislosti

Klasická kryptografie se zabývala především **šiframi**, tj. způsoby **utajení** zpráv. Patřily sem zejména šifrovací systémy jako jednoduchá záměna, jednoduchá a dvojitá transpozice, Vigenerova šifra a podobně. Často jsou nazývány historické **šifrovací systémy**.

Druhá světová válka přinesla nebývalý zájem o kryptografii i o kryptoanalýzu. O dříve zatajovaný i opomíjený obor se najednou začaly zajímat hlavy států a generální štáby armád. Není divu, kryptoanalytici jim přinášeli čisté informace z nejvyšších míst velení nepřítele, bez jediného výstřelu a bez rizika. Kryptoanalýza se stala tichou, neviditelnou a účinnou zbraní. Kvalitní kryptografie byla naopak obranným štítem, který umožnil dopravovat tajné zprávy jak do týlu nepřítele, tak na frontu. Nebylo to poprvé, kdy kryptografové a kryptoanalytici zasáhli přímo do bojů, aniž by opustili své kanceláře daleko od fronty. Fascinující historii kryptologie od dávné minulosti až do osmdesátých let minulého století popisuje jedinečná kniha Davida Kahna [8].
Ve druhé světové válce přínos kryptoanalytiků vyvrcholil. Byl tak nepřehlédnutelný a široký, že zasáhl na všech frontách a ovlivnil všechny hlavní válčící strany. Proto si po válce všechny mocnosti začaly budovat mohutná kryptografická a luštící centra, kryptografická zařízení byla zařazena do kategorie zboží dvojího užití a posuzována stejně jako vývoz tanků nebo letadel.

Obr.: Budova NSA, Fort Meade, MD, USA, http://www.nsa.gov/

Začalo se více dbát na rozvoj teorie. V rámci tohoto poválečného dění Claude E. Shannon nejprve v roce 1948 publikoval práci **A Mathematical Theory of Communication** [1], která je pokládána za základ teorie informace, a rok poté práci **Communication Theory of Secrecy Systems** [2], která je pokládána za základ moderní kryptologie. Není bez zajímavosti, že byla publikována díky nepozornosti vládních agentů, měla zůstat utajena.

Shannon využil pojmů z teorie informace k ohodnocení bezpečnosti známých šifer. Definoval entropii jazyka, vzdálenost jednoznačnosti, dokázal absolutní bezpečnost Vernamovy šifry, zavedl pojmy difúze a konfúze a ukázal, jak posuzovat a konstruovat šifrové systémy kombinací různých typů šifer. Zavedl také model komunikačního kanálu, který se používá při popisu kryptografických systémů dodnes.

Nečekané impulsy pro kryptologii přinesla počítačová revoluce v sedmdesátých letech. Nové technologické možnosti přinesly nové koncepty. Vznikly moderní blokové šifry a byl objeven princip kryptografie s veřejným klíčem [5], [6]. Ochrana dat ve státní sféře v USA si pak vynutila i vydání veřejné "státní" šifry DES [9].

Průmysl informačních a komunikačních technologií převrátil původní poválečný koncept co největšího zahalování kryptologie do státního aparátu. Kryptologie dostala nové impulsy a vymkla se státní kontrole.

V roce 1982 se konala první veřejná mezinárodní konference kryptologů a o dvacet let později se tato věda a její aplikace probírají nejméně na dvaceti mezinárodních konferencích ročně [10].

Šifrovací technologie se dostaly do domácích počítačů, mobilních telefonů, internetu a bankovnictví. Vznikla řada nových myšlenek v kryptografii i v kryptoanalýze. Na přelomu tisíciletí byly objeveny nové principy kryptoanalýzy. Dokonce se spekuluje, že se vyrovnává potenciál tajné státní vědy a veřejné kryptologie.

Na přelomu tisíciletí se také na veřejnost po 50 letech od svého vzniku dostávají odtajněné informace o luštění ve druhé světové válce. Veřejnost současně začíná postupně odhalovat skutečný cíl mohutných odposlouchávacích objektů a umístění moderních podzemních špionážních a luštících center tajných služeb. [11]

Obr.: Centrum F83, rozsáhlé podzemní pracoviště systému Echelon

Po ukončení studené války v posledním desetiletí minulého století dochází k přeměně zaměření těchto center na průmyslově orientovanou špionáž. Do této pasti padají nakonec i vlastní spojenci. Navíc se projevuje mezinárodní terorismus. Na jedné straně existují snahy o omezování kryptografie z obavy z jejího zneužití teroristy a zločinci, na druhé straně je silná snaha veřejnosti o absolutní uvolnění kryptografie z důvodu ochrany vlastního soukromí.

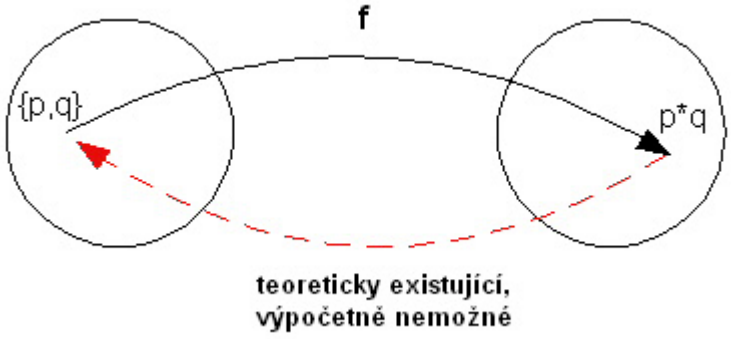
Obr.: Budova luštitelské služby v Moskvě

2. Nové myšlenky kryptografie

Počítačová revoluce přinesla řadu nových myšlenek, které jsou velmi krásné a svým způsobem fantastické [5], [6]. V tomto úvodu jich uvedeme ve zkratce jen několik.

2.1. Jednosměrné funkce

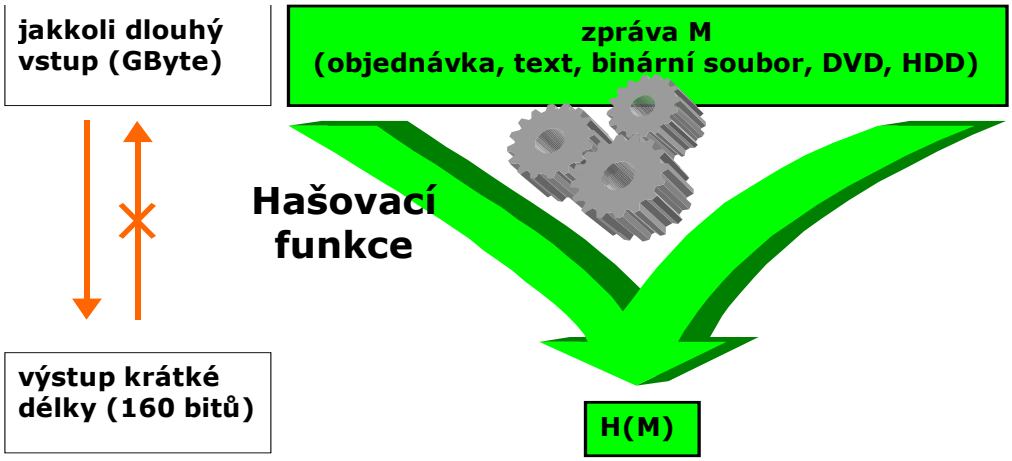
První z nich jsou **jednosměrné funkce**. Jsou to takové funkce f: X → Y, pro něž je snadné z jakékoli hodnoty x ∈ X vypočítat y = f(x), ale pro nějaký náhodně vybraný obraz y ∈ f(X) nelze (neumíme, je to pro nás výpočetně nemožné) najít její vzor x ∈ X tak, aby y = f(x). Přitom víme, že takový vzor existuje nebo jich existuje dokonce velmi mnoho. Je to třeba jako když smícháme dvě složky lepidla. Za několik vteřin vytvoří novou sloučeninu se zcela novými vazbami atomů a molekul, které nelze jednoduše rozpojit a vrátit do původní podoby. Podobně to probíhá s ohromnými čísly. Dokážeme je snadno spojit vynásobením. Číslo, které obdržíme, má však zcela jinou "molekulovou" strukturu, původní dvě složky pevně váže v nové číselné sloučenině a my v současné době neznáme dostatečně rychlou metodu jak tato čísla separovat.



Obr.: Jednosměrná funkce

2.2. Hašovací funkce

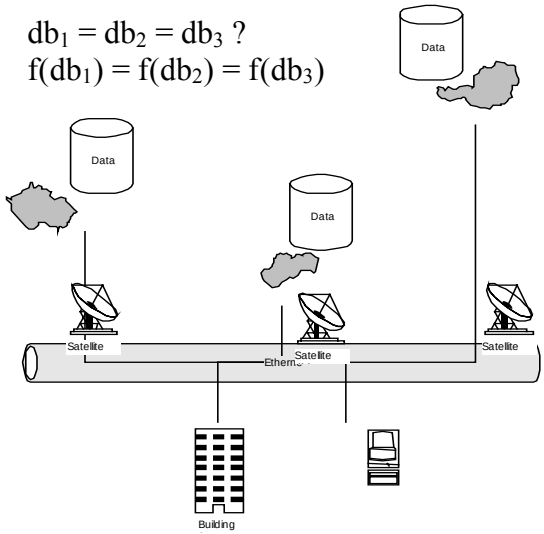
První odnoží jednosměrných funkcí jsou tzv. **hašovací funkce**, které umí vytvořit z jakkoliv velkých dat jejich identifikátor - digitální otisk dat. Data lze nyní identifikovat (a to i z právního hlediska) podle jejich digitálního otisku majícího řádově pár set bitů.



Obr.: Hašovací funkce

2.2.1. Kontrola shody databází, otisky dat

Uveďme si příklad banky, která ukládá všechna data ze všech účtů klientů do databázového systému, který je on-line zálohován, takže se vyskytuje současně na třech, geograficky vzdálených místech Evropy. V určitý okamžik je nutné zjistit, zda tyto systémy jsou opravdu totožné. Proto na určitou dobu uvedeme databáze do klidu. Nyní bychom mohli klasicky přenášet z jednoho i druhého záložního centra jednotlivé sektory pevných disků nebo záznamy v databázi do centra a porovnávat je řetězec za řetězcem. Možná za několik dní nebo týdnů bychom mohli být hotovi, v závislosti na objemu dat a přenosové kapacitě spojení. Místo toho však stačí na všech třech místech vypočítat pouze hašový obraz databází nebo jednotlivých jejich částí (sekcí apod.) f(db) a přenést tyto obrazy k porovnání do centra. Na rozdíl od jejich vzorů se jedná jen o stovky bitů. Pokud jsou hodnoty $f(db_1)$, $f(db_2)$ a $f(db_3)$ shodné, máme jistotu, že se databáze nebo jejich části neliší ani o jeden bit. Digitální otisky dat působí stejně jako otisky prstů. V řadě zemí byly digitální otisky dat z hlediska identifikace dat nepřímo legislativně postaveny na roveň otisků prstů.



Obr.: Kontrola shodnosti vzdálených rozsáhlých databází

2.2.2. Prokazování autorství

Hašovací funkce se mohou použít i k prokázání autorství například tímto způsobem. Někdo vytvoří určité dílo (například objev z určité oblasti), nechce však z určitých důvodů toto dílo zveřejnit ihned, má však obavy, aby později někdo nemohl popřít, že dílo je jeho a vzniklo už třeba před několika lety nebo měsíci. Postačí zveřejnit digitální otisk (hash) tohoto díla.

Předpověď vývoje ekonomiky v České republice roce 2004 je popsána v práci, kterou zveřejním 1.1.2005.
SHA-1(mojeprace.doc) =
A085F5701D56B55CA5843ED952546A88ED6F80D9
Alois Předvídavý, 11.11.2003

Obr.: Prokazování autorství

2.2.3. Ukládání přihlašovacích hesel

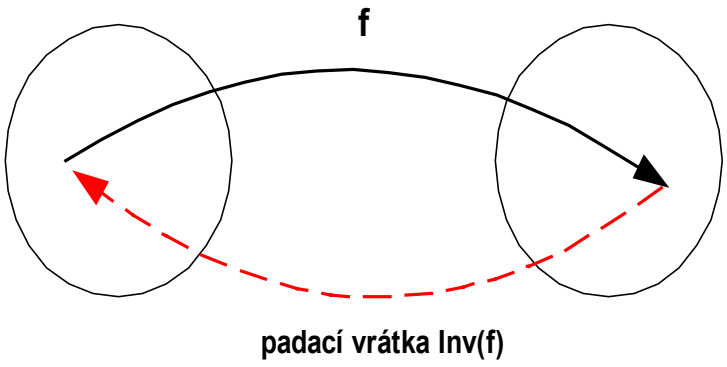
Další zajímavou aplikací hašovacích funkcí je **ukládání přihlašovacích hesel** v počítačových systémech. Hesla uživatelů, passwordy $pswd_i$, nemohou být ukládána do systémů přímo, protože by je šlo jednoduše vyhledat a zneužít. Ukládají se proto ve formě $h(pswd_i)$, kde h je hašovací funkce. Díky její jednocestnosti není z této hodnoty, uložené v systému, možné odvodit vlastní hodnotu přihlašovacího hesla $pswd_i$, vyloučíme-li snadné passwordy a slovníkový útok na ně. V reálných systémech se navíc používá metoda solení znesnadňující slovníkový útok.

uživatel	hash(password)
BÍLÁ	**A085F5701D56B55CA5843ED952546A88ED6F80D9**
NÁHLOVSKÝ	**BDE45D6S52F5640A059CD5856454E4A488B40458**
ŠÍP	**014DA256B954CF65E156200C00A127521D45A44E**
...	**...**

Obr.: Ukládání přihlašovacích hesel

2.3. Jednosměrné funkce s padacími vrátky

Druhou odnoží jednosměrných funkcí jsou **jednosměrné funkce s padacími vrátky**. Bývají také nazývány jednosměrné funkce se zadními vrátky, pokud je zřejmé, že se nejedná o pirátská vrátka do systému.



Obr.: Jednosměrné funkce s padacími vrátky

Pomůžeme si příměrem. Do hladomorny mohou být uvrženi všichni, ale jen ten, kdo zná tajný kámen, může po zatlačení na něj otevřít tajný východ. Jednosměrné funkce s padacími vrátky způsobily revoluci v moderní kryptologii. Jsou to takové jednosměrné funkce f, které lze

invertovat jen za předpokladu znalosti jejich padacích vrátek. Tato podmínka se vztahuje nejen na transformace jako celek, ale i pro jednotlivé funkční hodnoty. Je to obdoba klíče k poštovní schránce. Všichni do ní mohou vhazovat dopisy, ale jen vlastník klíče od schránky ji může vybrat a přečíst si všechny dopisy.

Padací vrátka nazýváme privátním klíčem (d), který umí funkci f invertovat, tj. systematicky umět vypočítávat vzory od předložených obrazů. Příklady s poštovní schránkou a hladomornou ukazují také vlastnost **asymetrie** - vypočítat funkční hodnotu $y = f(x)$ mohou všichni neboť je to pro všechny veřejně dostupný úkon, ale jen vlastník privátního klíče d může tuto akci invertovat, tj. vypočítat $f^{-1}(y)$.
Veřejnou cestu (E) charakterizuje *veřejný klíč* (e) a *privátní cestu* (D) ven *privátní klíč* (d). Protože jsou obě cesty různé, odpovídající funkce označujeme různě. Máme tedy transformace

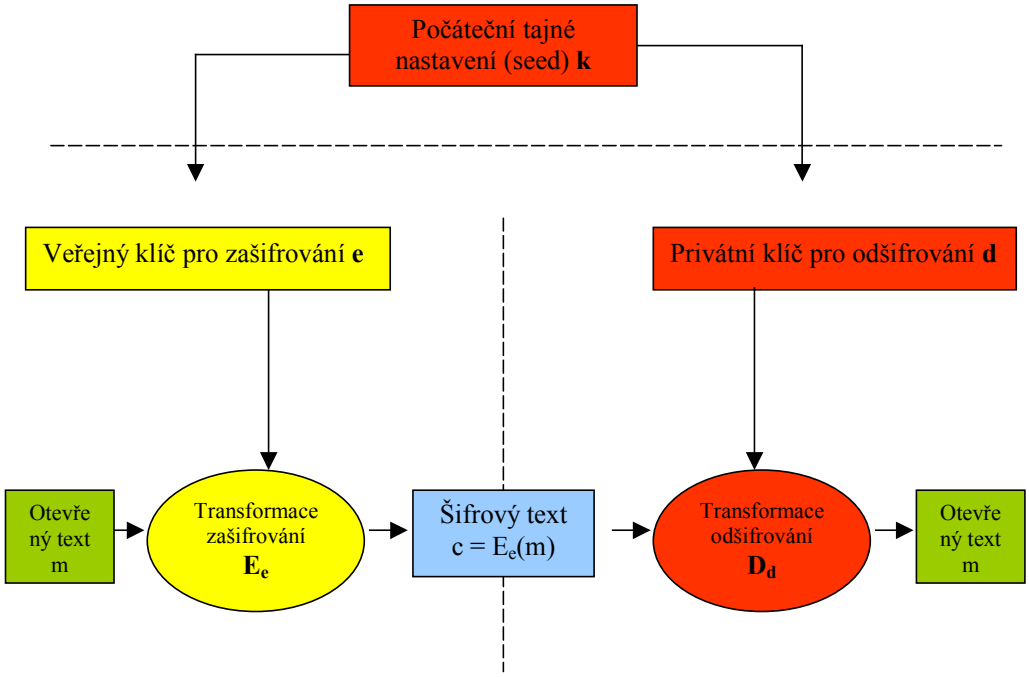
$$y = f(x) = E_e(x)$$
a
$$x = f^{-1}(y) = D_d(y).$$

U jednocestných funkcí s padacími vrátky pak platí, že pro každý (útočníkovi neznámý) klíčový pár (e, d) a pro skoro všechna y je výpočetně nemožné nalézt takové x, že $y = E_e(x)$.

Poznámka: Pro ta y, které si útočník vytvoří sám, neboť pro libovolné x může vypočítat $y = E_e(x)$, je pochopitelně schopen inverzi $x = f^{-1}(y)$ určit. Také pro určité klíčové páry, které si vytvoří sám, je schopen z transformace E_e odvodit D_d. Definice proto musí obsahovat kvalitativní **neschopnost útočníka systematicky invertovat** zvolené nebo zadané obrazy jednosměrné funkce s padacími vrátky.

2.4. Asymetrické kryptografické systémy

První aplikací jednocestných funkcí s padacími vrátky jsou **asymetrické kryptografické systémy**, z nichž nejprve uvedeme **šifrovací systémy s veřejným klíčem**. U historických **symetrických šifrovacích systémů** bylo nutné na obě strany komunikačního kanálu dopravit stejné klíče – odesílateli klíč pro zašifrování a příjemci (tentýž) pro odšifrování. U asymetrických kryptosystémů (kryptosystémů s veřejným klíčem), které jsou určeny pro šifrování, je možné klíč pro zašifrování poslat neutajeně nebo ho rovnou uveřejnit v telefonním seznamu. V tajnosti se uchovává jen klíč privátní. V praxi to funguje tak, že uživatel si oba dva klíče, které nazýváme klíčový pár, vygeneruje a veřejný klíč poskytne potenciálním komunikujícím stranám. Poté je už schopen od kohokoliv přijímat zašifrované zprávy, které je schopen rozšifrovat za použití privátního klíče. Ostatní uživatelé znají jen jednosměrnou funkci E_e a pro libovolnou zprávu x umí vytvořit $c = E_e(x)$, tj. zašifrovat ji. Nikdo, kromě příjemce, však neumí invertovat zachycený šifrový text, protože nezná padací vrátka.



Obr.: Asymetrický šifrovací systém

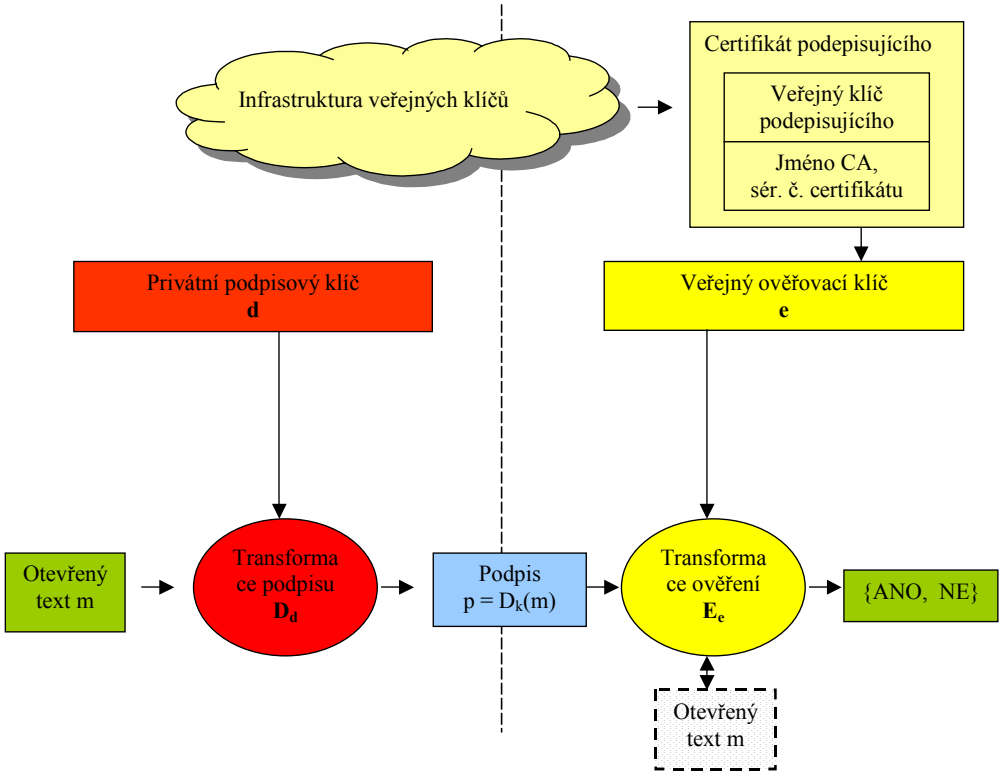
2.5. Digitální podpisy

Další aplikací jednocestných funkcí s padacími vrátky jsou digitální podpisy (obecně kryptografické systémy pro digitální podpis). V případě operací šifrování a odšifrování platilo $D_dE_e = I$. Uvažujme na okamžik, že transformace E_e a D_d jsou komutativní (nemusí tomu tak vždy být), tj. $E_eD_d = I$ a vysvětlíme princip digitálního podpisu.

Mějme nějaký dokument (smlouvu apod.) *m* a příslušný kryptosystém s veřejným klíčem (E_e, D_d). Dokument *m* podepíšeme tím, když k němu připojíme hodnotu podpisu $p = D_d(m)$. Proč? Každý si může veřejnou transformací E_e ověřit, že $E_e(p) = E_eD_d(m) = m$, tj. že *m* a *p* patří k sobě. Přitom hodnotu *p* z *m* mohl vytvořit pouze vlastník padacích vrátek - privátního podpisového klíče *d*. Aby to fungovalo správně, musí být ještě zajištěno, že transformace (E_e, D_d) patří opravdu danému člověku. Toto ujištění obvykle poskytuje nezávislá třetí strana, certifikační autorita, která spojuje identitu uživatele s jeho transformací E_e (tj. s jeho veřejným klíčem).

Poznamenejme na okraj, že i v této ilustraci principu digitálního podpisu musí *m* mít určitý formát (nemůže to být náhodný řetězec), jinak by útočník mohl pro libovolně zvolené *r* prezentovat $E_e(r)$ jako zprávu *m* a hodnotu *r* jako její podpis *p*, neboť platí $E_e(p) = m$.

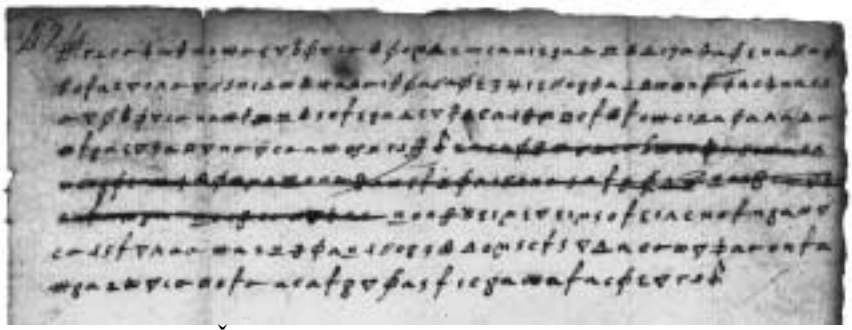
V obecnějších schématech digitálního podpisu aplikujeme veřejnou transformaci E_e na dvojici (*m*, *p*) a obdržíme nikoli data (*m*) jako v předchozím výkladu, ale pouze prvek z množiny {Ano, Ne}, tj. rozhodnutí, zda podpis je platný nebo neplatný. Tak pracují schémata digitálního podpisu s dodatkem. Pokud je výsledkem přímo zpráva *m*, jsou to tzv. schémata digitálního podpisu s obnovou zprávy. Transformace E_e a D_d nemusí být vždy zašifrovací a odšifrovací transformace. V případech schémat digitálních podpisů hovoříme o **transformaci podepisovací** a **transformaci ověřovací**.



Obr.: Asymetrický systém pro podepisování zpráv

2.6. Nepopiratelnost

Digitální podpisy mají také onu praktickou vlastnost, že při případném sporu může třetí nezávislá strana rozhodnout, zda podpis je platný nebo nikoli, aniž by musela znát jakékoliv privátní klíče. To v éře symetrické kryptografie nebylo možné. Například u přijaté šifrované zprávy nebylo možné prokázat, zda ji skutečně vytvořil odesílatel nebo si ji vymyslel příjemce. Z důvodu symetrie případný soudce nemá možnost ani se znalostí tajného klíče rozhodnout, kdo zprávu vytvořil. Tuto službu je však možné i u symetrických technik zajistit pomocí nezávislé třetí strany. Obecně ověření toho, zda se nějaká akce stala nebo ne, nezávislou třetí stranou, se nazývá nepopiratelnost.
Na obrázku vidíme zachycený šifrovaný dopis Marie Stuartovny. Luštitel, který znal šifrovací klíč, vložil závěrečnou část zprávy, žádající sdělení jmen a adres spiklenců, spolupracujících s Marií Stuartovnou. Na základě toho byli spiklenci odhaleni.



Obr.: Šifrovaný dopis Marie Stuartovny [13]

Zajištění integrity přenášených (šifrovaných) zpráv je kupodivu velkým praktickým problémem mnoha moderních systémů a přetrvává do současnosti, stejně jako mýtus, že šifrování řeší všechny problémy bezpečnosti.

2.7. Další myšlenky moderní kryptografie

Zajímavých myšlenek moderní kryptografie je mnohem více, než jsme zmínili, určitě sem patří také výměna tajného klíče na nechráněném komunikačním kanálu, systém sdíleného tajemství, hraní karetních her na dálku bez možnosti podvádění, současný podpis smlouvy smluvními stranami najednou, protokoly výměny klíčů, vzájemné autentizace, průkaz nějaké znalosti bez jejího odhalení apod.

3. Moderní kryptografie a bezpečnostní cíle

Moderní kryptografie, kterou můžeme datovat od sedmdesátých let dvacátého století, se zabývá i jinými službami (než je pouhé utajení), které se uplatňují v oblasti komunikačních a počítačových technologií, a to nejen ve vládním (jako dříve), ale i v soukromém sektoru.

3.1. Bezpečnostní cíle

Moderní kryptografie zajišťuje následující **bezpečnostní cíle**:

- **Důvěrnost dat** – tj. utajení informace před neoprávněnými uživateli. Existuje řada přístupů, jak zajistit důvěrnost dat. Například řízením fyzického přístupu k datům nebo kryptografickými metodami, kdy se data převedou do nesrozumitelné podoby šifrováním.
- **Integrita dat** – tj. zajištění, aby data nebyla úmyslně nebo neúmyslně změněna neoprávněným uživatelem, například pozměněním, vložením, smazáním části dat nebo jejich zopakováním ve zprávě apod.
- **Autentizace entit** - ověřuje proklamovanou identitu daných entit (uživatele, počítače, zařízení, programu, procesu apod.).
- **Autentizace dat** - ověřuje proklamovanou identitu dat, tj. například jejich obsah, čas jejich vzniku, jejich původ apod. Vedlejším produktem autentizace dat je zajištění jejich integrity.
- **Nepopiratelnost** – zajišťuje, aby daný subjekt nemohl později popřít to, co předtím vykonal. Je-li zajištěna nepopiratelnost, pak v případě sporu dvou stran může díky ní třetí (nezávislá) strana rozhodnout o tom, zda daný úkon proběhl nebo ne. Nepopiratelnost může být mnoha typů, například se rozeznává nepopiratelnost týkající se vytvoření zprávy (ochrana proti tvrzení původce, že zprávu nevytvořil), dále nepopiratelnost odeslání, podání, přenosu a příjmu zprávy.
- **Řízení přístupu** – tj. zajištění, že pouze oprávněné subjekty mají přístup k definovaným objektům (zdrojům)
- A další

3.2. Základní kryptografické služby

Mezi základní kryptografické služby patří **důvěrnost, integrita, autentizace a nepopiratelnost**. Pomocí nich se dá zajistit většina bezpečnostních cílů.

Poznamenejme, že uživatelem nemusí být vždy osoba, v kontextu konkrétního informačního nebo komunikačního systému to může být program nebo proces, zprávou nemusí být e-mail, ale může to být libovolný soubor dat, program, položka v databázi apod.

3.3. Kryptografické nástroje

Moderní kryptografie má pro zajištění **bezpečnostních cílů** řadu kryptografických nástrojů, které rozšířily původně jediný cíl – utajení a jediný nástroj - šifry. Mezi **kryptografické nástroje (kryptografické mechanismy)** patří:

- Šifrovací systémy
- Hašovací funkce
- Generátory náhodných znaků
- Autentizační kódy zpráv a klíčované hašové autentizační kódy zpráv
- Šifry s veřejným klíčem
- Schémata digitálních podpisů
- Schémata výměny klíčů nebo dohody na klíči
- Schémata sdíleného tajemství
- Autentizační a identifikační schémata
- A další

3.4. Informačně bezpečnostní služba

Informačně bezpečnostní služba je metoda zajištění určitého bezpečnostního cíle. Například integrita přenášených dat na komunikačním kanálu je bezpečnostní *cíl* a metoda jeho zajištění je bezpečnostní *služba*. Tato bezpečnostní služba se může zajistit různými kryptografickými *nástroji*, například digitálním podpisem, autentizačním kódem zprávy nebo klíčovaným hašovým autentizačním kódem.

3.5. Definice moderní kryptografie

Moderní kryptografii můžeme v širším významu definovat jako studium matematických metod pro zajištění informační bezpečnosti.
Metod pro zajištění informační bezpečnosti je celá řada, například fyzické, personální, technické, administrativní apod. Kryptografie hraje důležitou roli, ale nikoli jedinou.

3.6. Pojmy kryptografický systém, algoritmus, zobrazení a transformace

V klasické kryptografii splývaly pojmy kryptografický systém, kryptografický algoritmus a kryptografická transformace, neboť v rámci jedné služby (zajištění důvěrnosti dat) nemělo příliš velký smysl tyto pojmy rozlišovat. Rozlišování a definice těchto pojmů není v současné době ještě ustálená, zejména se spojují pojmy systém a algoritmus, což v konkrétním kontextu může být jedno a totéž. Obecně bychom tyto pojmy mohli rozlišit následovně od nejnižší úrovně k nejvyšší.

<table>
<tr><th colspan="4">Transformace, zobrazení, algoritmus, pravidla a kryptosystém</th></tr>
<tr><td>transformace zašifrování
$E_{k(i)}$: M → C: m → m xor k(i)</td><td>zobrazení E</td><td rowspan="2">algoritmus
proudové šifry
(G, E, D)</td><td rowspan="2">kryptografický systém
šifrování dat proudovou šifrou</td></tr>
<tr><td>transformace dešifrování
$D_{k(i)}$: M → C: m → m xor k(i)</td><td>zobrazení D</td></tr>
<tr><td>transformace generátoru G:
v daném čase t nebo z daného klíče k vygeneruje posloupnost klíčů
G(t, k) = {k(1), k(2),...}</td><td>transformace G</td><td></td></tr>
<tr><td>pravidla: Klíčová posloupnost je posloupností náhodných nezávislých veličin, nabývajících hodnot 0 a 1 se stejnou pravděpodobností 0.5, každá z vygenerovaných posloupností se použije k šifrování otevřeného textu pouze jednou a má stejnou délku jako otevřený text</td><td>pravidla</td><td>pravidla</td><td></td></tr>
</table>

Obr.: Příklad pojmů kryptografický systém, algoritmus, zobrazení a transformace u proudové šifry

3.6.1. Kryptografická transformace

Kryptografická transformace (funkce, operace) je *funkce*, definující zpracování dat pomocí daného konkrétního klíče.

3.6.2. Kryptografické zobrazení

Kryptografické zobrazení je zobrazení, které každému klíči nebo jinému parametru kryptografického systému přiřadí konkrétní kryptografickou transformaci.

Příklad: U kryptografického nástroje šifrování dat máme pro konkrétní klíč *e* *kryptografickou transformaci zašifrování* dat E_e: m → E_e(m), tj. způsob zašifrování dat pomocí daného konkrétního klíče (e) a *kryptografickou transformaci dešifrování* dat D_d: c → D_d(c), tj. způsob dešifrování dat pomocí daného konkrétního klíče (d). U symetrických systémů je e = d = k, u asymetrických je klíčový pár (e, d) generován *transformací* G, která každému tajnému počátečnímu nastavení (seed) k přiřadí klíčový pár (e, d). V případě kryptografického nástroje digitálního podpisu máme pro konkrétní privátní klíč (d) *kryptografickou transformaci vytvoření podpisu* D_d: m → p = D_d(m) a pro konkrétní veřejný klíč (e) *kryptografickou transformaci ověření podpisu* E_e, například E_e: (m, p) → {ANO, NE}.

3.6.3. Kryptografický algoritmus

Kryptografický algoritmus je souhrn všech kryptografických *zobrazení* a *transformací* daného kryptosystému.

Příklad: U symetrického kryptografického systému šifrování je to dvojice zobrazení (E, D), které konkrétnímu klíči k přiřazují konkrétní transformaci zašifrování a dešifrování, E: k → E_k a D: k → D_k.

V případě digitálního podpisu je to trojice (G, S, V), přičemž

- transformace G je generátor, který pro každé tajné počáteční nastavení (seed) *k* vytváří klíčový pár veřejného a privátního klíče (e, d),
- zobrazení *S* každému privátnímu klíči *d* přiřadí konkrétní transformaci vytvoření podpisu S_d a
- zobrazení *V* každému veřejnému klíči *e* přiřadí transformaci ověření podpisu V_e.

3.6.4. Kryptografický systém

Kryptografický systém (kryptosystém, kryptografické schéma, kryptoschéma) je matematická metoda, zajišťující některou informačně bezpečnostní službu. Kryptosystém zahrnuje celý proces zpracování dat a klíče a všechny jeho okolnosti, zahrnující všechny relevantní kryptografické *algoritmy, zobrazení, transformace a pravidla*, které daný kryptosystém používá a řídí se jimi.

Příklad: V případě šifrování dat patří do kryptosystému zejména způsob generování a použití šifrovacích klíčů a definice kryptografického algoritmu šifrování dat. V případě digitálního podpisu dat je to způsob generování klíčů a definice kryptografického algoritmu vytvoření digitálního podpisu a kryptografického algoritmu verifikace podpisu. Dále například u Vernamova kryptografického systému máme transformaci zašifrování E_k a transformaci dešifrování D_k. Kryptografický algoritmus je tvořen trojicí (G, E, D), kde G je transformace generování hesla (klíče), a navíc *pravidlem*, jak tvořit a používat klíč (vygenerovaný klíč musí být náhodný a k šifrování se může použít pouze jednou).

4. Kryptoanalýza

4.1. Definice kryptoanalýzy

Moderní kryptoanalýzu můžeme v širším významu definovat jako vědu o hledání slabin nebo prolamování matematických metod informační bezpečnosti.
Kryptoanalýza prošla zajímavým vývojem nejen ve své historii, ale zejména v posledním desetiletí.

4.2. Kerckhoffsovy principy a „Security through obscurity“

S rozšiřováním šifrového spojení, zejména ve válečných konfliktech, se ukazovalo, že není možné příliš často měnit šifrovací systémy, dopravovat je na frontu a zaškolovat v používání nových šifer obsluhy. Vývoj vedl k tomu, že se používal jeden nebo několik málo šifrovacích systémů, a to poměrně dlouhou dobu, a měnily se pouze klíče. Ty pak byly dopravovány na koncová pracoviště. Často to byly tzv. denní klíče, které se používaly daný den, přičemž najednou se distribuovaly obvykle klíče na celý měsíc. Při masivním používání jednoho šifrovacího systému nebyl proto problém, aby se protivník o systému dozvěděl od zajatců, ukořistěním šifrovacích prostředků nebo písemných materiálů.
V roce 1883 definoval v knize Vojenská kryptografie holandský kryptolog Auguste Kerckhoffs řadu požadavků, které by měl šifrovací systém splňovat [4]. Tyto požadavky jsou známy jako tzv. Kerckhoffsovy principy a nejznámějším z nich je ten, že se předpokládá, že protivník zná šifrovací systém a nezná pouze šifrovací klíče.

Ještě nyní se však objevují přístupy, že se šifrovací algoritmy tají. Takovému přístupu se říká "security through obscurity", český ekvivalent se zatím nevžil, možná bychom řekli "bezpečnost založená na neznalosti (nevědomosti, zatemnění)". Utajení vlastního šifrovacího

systému je možné využít jako doplňkového bezpečnostního opatření. Aplikuje se například u šifrovacích systémů ozbrojených sil, ale v žádném případě nesmí sloužit jako opatření nahrazující nebo garantující kvalitu šifrování nebo ochrany. V současné době se vžilo pravidlo, že u systémů, které jsou určeny pro širší veřejnost, by měl být popis šifrovacího systému veřejný.

4.3. Pasivní, aktivní a adaptivní útoky

Historicky se uvažovaly útoky pouze se znalostí šifrového textu jeho zachycením nebo odposlechem (například na radiovém kanálu). S rozvojem moderních komunikačních a počítačových systémů přibyla řada nových možností. Útočník již nemusí být pouze **pasivní**, tj. sledovat komunikační kanál, ale může aktivně zasahovat do šifrového textu a dokonce i do vlastní komunikace, komunikaci může sám vyvolat, přerušit, znovu poslat starou šifrovanou zprávu, zprávu pozdržet, odstranit nebo naopak vsunout část šifrového textu do zprávy apod. Tyto útoky se nazývají **aktivní**. Aktivní útoky se dále rozvinuly do tzv. **adaptivních útoků**. Útočník v nich může korigovat svůj postup za chodu podle toho, jaké dostává výsledky. Například může posílat šifrové texty serveru a podle jeho odpovědí měnit následující texty i strategii. Praxe ukázala, že je reálné uvažovat různorodé možnosti útočníků. Tím, že útočníci už nemusí být vně nějakého počítačového systému, se otevírá pro ně řada možností jak v kvalitě, tak v kvantitě. Například zaměstnanci, pracující s nějakým informačním systémem, mohou být útočníky, jsou přitom oprávněni používat šifrovací klíče (mohou spouštět operace E_k a D_k), i když je neznají a ke klíčům nemají přímý přístup. Mohou systému předkládat svá otevřená a zašifrovaná data a od systému očekávat reakci, mohou provádět často velmi mnoho operací. Jako útočníci mají rozmanité možnosti, se kterými musí tvůrci bezpečnostních ochran počítat.

4.4. Postranní kanály

Další možnosti přinesly tzv. **postranní kanály**. Jejich objevitelé odhlédli od **matematických modelů** kryptografických systémů a zaměřili se na jejich **praktickou konkrétní fyzickou realizaci**. Ukázalo se, že například analýza spotřeby času, energie, chybová hlášení nebo elektromagnetické vyzařování konkrétních zařízení apod. dávají útočníkovi dost postranních informací k úspěšnému luštění klíčů nebo otevřených textů. Budoucnost mají před sebou **aktivní útoky postranními kanály**, tj. vyvolávání těchto kanálů vlastní činností útočníka. Dříve by bylo možné stěží předpokládat, že protivníka, jemuž luštíme šifrogram, můžeme zapojit do luštění tím, že mu postupně zašleme několik milionů šifrových textů a požádáme ho, aby nám vždy odpověděl, jestli po dešifrování obdržel nějaký smysluplný text. Přesně tak dnes pracuje několik útoků postranními kanály na protokoly SSL/TLS, které jsou součástí ochran internetového bankovnictví [14].

4.5. Základní typy útoků

Přirozeným požadavkem na bezpečnost šifrovacího systému bylo, aby útočník nemohl ze znalosti šifrovacího textu rozluštit otevřený text. Později se požadavky zpřísnily a nyní se uvažuje, že šifrovací systém by měl odolat několika typům útoků. Mezi základní patří:

- útok se znalostí šifrového textu,
- útok se znalostí otevřeného textu,
- útok s možností volit otevřený text,
- adaptivní útoky s možností volby otevřeného textu nebo šifrového textu.

4.6. Rostoucí možnosti útočníků

Celosvětové propojení počítačů do veřejné sítě také umožnilo spojení desetitisíců účastníků do luštitelských akcí pomocí distribuovaných výpočtů. Docílilo se velkého výpočetního výkonu pro kryptoanalýzu například při faktorizaci RSA a útoky hrubou silou na algoritmy

DES a RC5-64. S tímto faktorem je nutné počítat jako s reálnou veličinou při hodnocení možností případných současných útočníků.

Dále je zajímavé zjištění, že luštící práce nemusí útočník provádět přímo, ale může si je objednat jako službu například e-mailem. Umožňuje to anonymita internetu.

4.6.1. DES-Cracker

Příkladem nových možností luštění je DES-Cracker. Je to stroj, který byl zkonstruován péčí dobrovolníků v červenci roku 1998 proto, aby ukázal, že šifrovací standard DES je zastaralý a lze ho luštit hrubou silou, tj. zkusit daný šifrový text odšifrovat pomocí všech jeho 2^{56} možných klíčů. DES-Cracker prohledává klíčový prostor pomocí speciálních čipů, které pracují paralelně. Každý z nich má z řídícího procesoru přidělenu část klíčového prostoru. Čipy pracují autonomně a na řídící čip se obrací jen v případě nalezení správného klíče nebo při skončení prohledávání přiděleného prostoru. Čím více čipů je použito, tím rychleji je klíč nalezen. DES-Cracker, používá několik stojanů, ve kterých je zasunuto 29 desek, každá s 64 čipy. Toto množství čipů je schopno provést 90 miliard zkoušek klíčů za sekundu, což umožňuje prohledat celý klíčový prostor v garantované době 9 dní. Čistá cena HW stála asi byla 130 000 USD a vývoj celého stroje, sponzorovaný mj. organizací EFF, stál asi 210 000 USD. Prakticky byl DES-Cracker nasazen na luštění DES několikrát. Například v rámci soutěže DES-Challenge III byl za pomoci DES-Crackeru neznámý klíč DES zjištěn za 22 hodin. Historie kolem DES a DES-Crackeru je velmi zajímavá a společně s technickým popisem DES-Crackeru ji můžete nalézt na stránce organizace EFF [3].

Obr.: DES-Cracker

4.6.2. Nové formy útoků

Trochu podivně zní věta, že další zajímavou stránkou současných šifer je, že bývají realizovány počítači. Tento jednoduchý fakt totiž přináší útočníkům značné možnosti, pokud právě tyto počítače zapojí do luštění. Uvedeme dva příklady.
Při útoku na zašifrované spojení pod protokolem SSL [14] bylo využito faktu, že pokus o navázání spojení vyhodnocuje SSL server. Každý, kdo se chce se serverem spojit, zasílá mu v rámci protokolu SSL zprávu určitého formátu zašifrovanou veřejným klíčem serveru. Server tuto zprávu odšifruje a kontroluje správnost formátu. Pokud je správný, reaguje nějak a pokud je špatný reaguje jinak. Bylo ukázáno, že tato informace útočníkovi stačí k úspěšnému útoku na cizí zašifrovaný text, pokud má možnost provést několik milionů takových dotazů. Je to příklad adaptivního útoku s možností volby šifrového textu. Záleží jen na rychlosti serveru, za jak dlouho na tolik dotazů odpoví. S použitím SSL akcelerátorů, které jsou běžně dostupné na trhu to může trvat pouhou hodinu.

Podobně to probíhá v případě útoků na čipové karty. Čipová karta je také pouhý počítač, stroj, který vykonává příkazy, dané jeho operačním systémem. Pokud to není operace ověření PINu, v drtivé většině případů neregistruje, zda takových příkazů vykoná jednotky nebo miliony. Tímto způsobem bylo možné útočit na čipové karty pro mobilní telefony (SIM karty) [15]. U historických šifer by bylo těžké si představit, že by útočník mohl poslat nepříteli několik milionů šifrogramů a očekávat na ně reakci, byť reakci typu ano / ne.

5. Typy bezpečnosti kryptografických systémů

Šifry mají sloužit k zajištění utajení zpráv, je tedy přirozený požadavek, aby útočník nemohl otevřený text získat, a to na základě jakéhokoliv reálného útoku, tj. například výše uvedenými čtyřmi základními typy útoků. Protože typů útoků přibývá, požadavky na systémy ochrany dat se zvyšují – měly by odolat jakémukoliv známému typu útoku. Proto nejspolehlivější míra bezpečnosti je založená na informačně-teoretickém přístupu.

5.1. Nepodmíněná bezpečnost a absolutní bezpečnost

Řekneme, že *kryptografický systém* je **nepodmíněně bezpečný**, jestliže zůstává bezpečný i přes to, že útočník může mít k dispozici neomezené materiální prostředky k luštění. Důvodem nepodmíněné bezpečností je to, že luštitel nemá k jeho luštění dostatek *informací*.

U *šifrovacích* systémů nazýváme tuto vlastnost **absolutní bezpečnost** (perfect secrecy). Pojem zavedl C.E Shannon a dokázal, že Vernamova šifra je absolutně bezpečná. Drtivá většina kryptografických systémů tuto vlastnost nemá.

5.2. Dokazatelná bezpečnost

Řekneme, že kryptografický systém je **dokazatelně bezpečný**, jestliže jeho prolomení je (v zásadě, přibližně, řádově) stejně náročné, jako řešení známého problému, jehož složitost je velmi vysoká (například problém faktorizace nebo problém diskrétního logaritmu).

5.3. Výpočetní bezpečnost

Řekneme, že kryptografický systém je **výpočetně bezpečný**, jestliže jeho prolomení je s použitím nejefektivnějších známých útoků natolik složité, že převyšuje výpočetní možnosti a zdroje útočníka.
V současné době se za výpočetně bezpečné pro komerční účely považují systémy s výpočetní složitostí minimálně X operací, kde X se pohybuje v intervalu $<2^{80}, 2^{128}>$. Pro vojenské použití se většinou požaduje hranice $X = 2^{256}$.

6. Kryptologie

Poté, co jsme poznali, čím se zabývá kryptografie a kryptoanalýza, můžeme definovat kryptologii.
Kryptologie je věda, skládající se z kryptografie a kryptoanalýzy.

7. Literatura

[1] Claude E. Shannon, *A Mathematical Theory of Communication*, The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948
http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf

[2] Claude E. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, vol.28-4, pp. 656 - 715, 1949,
http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf

[3] Domácí stránka DES-Crackeru na webu organizace EFF: http://www.eff.org/descracker/

[4] Auguste Kerckhoffs, *La cryptographie militaire*, Journal des sciences militaires, vol. IX, pp. 5 – 38, January 1883, pp. 161 – 191, February 1883

[5] Whitfield Diffie and Martin Hellman, *New directions in Cryptography, IEEE Transactions on Information Theory*, Vol. 22, No. 6, 1976, pp. 644 - 654

[6] Ronald L. Rivest, Adi Shamir and Leonard M. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, Vol. 21, No. 2 (Feb. 1978), pp. 120 – 126

[7] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996, dostupné celé on-line na
http://www.cacr.math.uwaterloo.ca/hac/

[8] David Kahn, *The Codebreakers*, Scribner, 1996

[9] DES, *Data Encryption Standard*, FIPS PUB 46-3, October 1999,
http://csrc.nist.gov/CryptoToolkit/tkencryption.html

[10] International Association for Cryptologic Research, nezisková vědecká organizace,
http://www.iacr.org/

[11] Systém Echelon, http://www.heise.de/tp/english/inhalt/te/6929/1.html

[12] Dorothy Denning, *Cryptography and Data Security*, Addison-Wesley, 1982

[13] Simon Singh: *Kniha kódů a šifer*, český překlad, Argo a Dokořán, 2003,
http://www.simonsingh.net/Crypto_Corner.html

[14] Vlastimil Klíma, Ondřej Pokorný, Tomáš Rosa, *Attacking RSA-based Sessions in SSL/TLS*, Workshop on Cryptographic Hardware and Embedded Systems CHES 2003, Cologne, Germany, September 7 - 10, Lecture Notes in Computer Science, Vol. 2779, pp. 426 - 440, Springer-Verlag, 2003, http://eprint.iacr.org/2003/052/

[15] Klonování SIM karet, http://www.isaac.cs.berkeley.edu/isaac/gsm.html