Bezpečnost v informačních technologiích (KIV/BIT)

1. Úvod do předmětu - motivace, základní pojmy

Ing. Pavel Král, Ph.D.

Katedra informatiky a výpočetní techniky
Západočeská Univerzita

11. února 2015

Table of Contents

Kontakt, informace o předmětu

- Kontakt:
  - e-mail: pkral@kiv.zcu.cz
  - www: http://home.zcu.cz/ pkral
  - tel: +420 377 632 454
- Úřední hodiny:
  - ÚT 13:30-14:15
  - ST 11:00-11:45
- Informace: portál, Courseware
  - sledovat aktuality

Podmínky absolvování

- **Cvičení**: účast dobrovolná ($\times$ je vhodné na cvičení chodit $\leftarrow$ praktické procvičení odpřednášené látky)
- **Zápočet**: min. 50% možných bodů ze samostatné práce (SP) a záp. testu
  - zápočtový test - max. 20b
  - samostatná práce (SP) - max 20b
- **Odevzdání SP**:
  - **před** *řádným* termínem $\rightarrow$ bonus $+5b$
  - **v** *řádném* termínu
  - **po** *řádném* **do** *mezního* termínu $\rightarrow$ penalizace $-5b$
  - **po** *mezním* termínu $\rightarrow$ **ztráta nároku na zápočet**
- **Poznámky**:
  - Aktivita na cvičení také hodnocena
  - "Programovací" SP lépe hodnocena než prezentace ($\triangle = 25$ %)
  - "Staré" zápočty se **neuznávají**. Po domluvě s vyučujícím možno uznat body z SP. Test nutno absolvovat **znovu**!

Podmínky absolvování

Důležité termíny:

- zadání SP - **5. týden semestru**
- řádný termín zápočtového testu - **11. týden semestru**
- řádný termín odevzdání SP - **poslední týden semestru**
- mezní termín odevzdání SP - **28.5.2015**

Přednášky:

- účast dobrovolná ($\times$ vhodná)

Zkouška:

- min. 50% možných bodů z písemky - max. 40b
- body_celkem = trunc (body_ze_zápočtu $*$ 0.2) + body_ze_zkouškové_písemky

Známka	Body
1	42-49
2	34-41
3	26-33
4	0-25

Literatura

- Hanáček, P., Staudek, J. **Bezpečnost informačních systémů**, *John Wiley & Sons*, 2000, ISBN 80-238-5400-3.
- Menezes, Van Oorschot, Vanstone, **Handbook of Applied Cryptography**, *CRC Press*, 1997, ISBN: 0-8493-8523-7, http://www.cacr.math.uwaterloo.ca/hac/.
- Jiří Přibyl, Jindřich Kodl, **Ochrana dat v informatice**, *České vysoké učení technické*, 1996.
- Neil Daswani, Christoph Kern, Anita Kesavan, **Foundations of Security: What Every Programmer Needs to Know**, *Apress*, 2007
- Peter Szor, **Počítačové viry : analýza útoku a obrana**, *Zoner Press*, 2006, ISBN: 80-86815-04-8.

Cíle předmětu

- Získání přehledu v oblasti kryptografie a kryptografických algoritmů
- Seznámení s problematikou oprávnění a řízení přístupu
- Řešení bezpečnosti v operačních systémech, informačních systémech a sítích

Plán přednášek

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Šifrování s veřejným a soukromým klíčem (asymetrické šifry)
- Autentizace, autentizační protokoly
- Problém distribuce klíčů, transport a dohadování klíče
- Hashovací funkce a integrita dat
- Digitální podpisy
- Bezpečnost operačních systémů a síťových služeb; viry
- Bezpečnost informačních systémů
- Firewally (KERIO)
- Prezentace semestrálních prací
- Případové studie

Plán přednášek

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Šifrování s veřejným a soukromým klíčem (asymetrické šifry)
- Autentizace, autentizační protokoly
- Problém distribuce klíčů, transport a dohadování klíče
- Hashovací funkce a integrita dat
- Digitální podpisy
- Bezpečnost operačních systémů a síťových služeb; viry
- Bezpečnost informačních systémů
- Firewally (KERIO)
- Prezentace semestrálních prací
- Případové studie

Plán přednášek

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Šifrování s veřejným a soukromým klíčem (asymetrické šifry)
- Autentizace, autentizační protokoly
- Problém distribuce klíčů, transport a dohadování klíče
- Hashovací funkce a integrita dat
- Digitální podpisy
- Bezpečnost operačních systémů a síťových služeb; viry
- Bezpečnost informačních systémů
- Firewally (KERIO)
- Prezentace semestrálních prací
- Případové studie

Plán přednášek

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Šifrování s veřejným a soukromým klíčem (asymetrické šifry)
- Autentizace, autentizační protokoly
- Problém distribuce klíčů, transport a dohadování klíče
- Hashovací funkce a integrita dat
- Digitální podpisy
- Bezpečnost operačních systémů a síťových služeb; viry
- Bezpečnost informačních systémů
- Firewally (KERIO)
- Prezentace semestrálních prací
- Případové studie

Plán přednášek

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Šifrování s veřejným a soukromým klíčem (asymetrické šifry)
- Autentizace, autentizační protokoly
- Problém distribuce klíčů, transport a dohadování klíče
- Hashovací funkce a integrita dat
- Digitální podpisy
- Bezpečnost operačních systémů a síťových služeb; viry
- Bezpečnost informačních systémů
- Firewally (KERIO)
- Prezentace semestrálních prací
- Případové studie

Plán přednášek

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Šifrování s veřejným a soukromým klíčem (asymetrické šifry)
- Autentizace, autentizační protokoly
- Problém distribuce klíčů, transport a dohadování klíče
- Hashovací funkce a integrita dat
- Digitální podpisy
- Bezpečnost operačních systémů a síťových služeb; viry
- Bezpečnost informačních systémů
- Firewally (KERIO)
- Prezentace semestrálních prací
- Případové studie

Plán přednášek

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Šifrování s veřejným a soukromým klíčem (asymetrické šifry)
- Autentizace, autentizační protokoly
- Problém distribuce klíčů, transport a dohadování klíče
- Hashovací funkce a integrita dat
- Digitální podpisy
- Bezpečnost operačních systémů a síťových služeb; viry
- Bezpečnost informačních systémů
- Firewally (KERIO)
- Prezentace semestrálních prací
- Případové studie

Plán přednášek

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Šifrování s veřejným a soukromým klíčem (asymetrické šifry)
- Autentizace, autentizační protokoly
- Problém distribuce klíčů, transport a dohadování klíče
- Hashovací funkce a integrita dat
- Digitální podpisy
- Bezpečnost operačních systémů a síťových služeb; viry
- Bezpečnost informačních systémů
- Firewally (KERIO)
- Prezentace semestrálních prací
- Případové studie

Plán přednášek

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Šifrování s veřejným a soukromým klíčem (asymetrické šifry)
- Autentizace, autentizační protokoly
- Problém distribuce klíčů, transport a dohadování klíče
- Hashovací funkce a integrita dat
- Digitální podpisy
- Bezpečnost operačních systémů a síťových služeb; viry
- Bezpečnost informačních systémů
- Firewally (KERIO)
- Prezentace semestrálních prací
- Případové studie

Plán přednášek

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Šifrování s veřejným a soukromým klíčem (asymetrické šifry)
- Autentizace, autentizační protokoly
- Problém distribuce klíčů, transport a dohadování klíče
- Hashovací funkce a integrita dat
- Digitální podpisy
- Bezpečnost operačních systémů a síťových služeb; viry
- Bezpečnost informačních systémů
- Firewally (KERIO)
- Prezentace semestrálních prací
- Případové studie

Plán přednášek

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Šifrování s veřejným a soukromým klíčem (asymetrické šifry)
- Autentizace, autentizační protokoly
- Problém distribuce klíčů, transport a dohadování klíče
- Hashovací funkce a integrita dat
- Digitální podpisy
- Bezpečnost operačních systémů a síťových služeb; viry
- Bezpečnost informačních systémů
- Firewally (KERIO)
- Prezentace semestrálních prací
- Případové studie

Plán přednášek

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Šifrování s veřejným a soukromým klíčem (asymetrické šifry)
- Autentizace, autentizační protokoly
- Problém distribuce klíčů, transport a dohadování klíče
- Hashovací funkce a integrita dat
- Digitální podpisy
- Bezpečnost operačních systémů a síťových služeb; viry
- Bezpečnost informačních systémů
- Firewally (KERIO)
- Prezentace semestrálních prací
- Případové studie

Obsah cvičení

- praktické ověření odpřednášené látky → kopírují přednášky
- část cvičení konzultační → zejména vyřešení problémů při řešení SP
- Náplň zveřejněna vždy nejpozději den před začátkem cvičení

1. Praktické vyzkoušení základů steganografie
2. Praktické vyzkoušení základů šifrování
3. Praktické vyzkoušení základů kryptoanalýzy

Stále častější hackerské útoky v poslední době

Microsoft a Symantec překazily obří útok. Odpojily statisíce počítačů

- Společnostem Microsoft a Symantec se podařilo identifikovat škodlivý software, který nakazil podle některých odhadů až milion počítačů po celém světě. Statisíce nakažených strojů dočasně odřízly od internetu a poskytly jim zdarma antivir. ...
- http://technet.idnes.cz/microsoft-a-symantec-zastavily-obri-utok-botnet-bamital-pkt-/sw_internet.aspx?c=A130207_002339_sw_internet_kuz

Hackeři napadli twitter, mohli získat až čtvrt milionu hesel

- Sociální síť twitter čelila útoku hackerů. Vyzrazení citlivých údajů se může týkat až 250 tisíc účtů. Twitter své uživatele o nebezpečí zneužití jejich hesel okamžitě informoval. Únik citlivých informací, zřejmě do rukou čínských hackerů, avizovaly už dva americké deníky, v sobotu přidal své podezření třetí. ...
- http://technet.idnes.cz/hackeri-napadli-twitter-0wd-/sw_internet.aspx?c=A130202_163039_zahranicni_brm

Další hackerské útoky, virové hrozby

Hackeři se dostanou i k družicím, ať patří HBO, nebo americké armádě

- Počítačový zločin se dostal už i na oběžnou dráhu. V minulosti nabral podobu jen svérázného zákaznického protestu, dnes představuje nebezpečí i pro satelity provozované pod patronátem armády. ...
- http://technet.idnes.cz/hackeri-druzice-0i7-/tec_vesmir.aspx?c=A121220_161806_tec_vesmir_mla

Na Írán zaútočil počítačový vir, tvářil se jako vládní soubory

- Íránští vědci zachytili nebezpečný počítačový vir Stars a nyní ho zkoumají v laboratořích. Špionážní vir je podle nich součástí kybernetického tažení, které proti Teheránu vedou jeho nepřátelé. Loni napáchal škody na íránských jaderných zařízeních virus Stuxnet. ...
- http://zpravy.idnes.cz/na-iran-zautocil-pocitacovy-vir-tvaril-se-jako-vladni-soubory-p6l-/zahranicni.aspx?c=A110426_115124_zahranicni_stf

Další hackerské útoky, virové hrozby

Hackeři donutili ledničku a televize rozesílat spamy

- Tisíce chytrých zařízení, které byly zapojeny do botnetu, odhalila bezpečnostní firma Proofpoint. Své síly na rozesílání spamu měly takto poskytovat například ledničky, set-top boxy nebo domácí routery. ...
- http://technet.idnes.cz/hacknute-lednicky-0mv-/sw_internet.aspx?c=A140119_231435_sw_internet_vse

Prověřte a případně odstraňte špehy v PC

- K nákaze systému Windows špehovacím programem stačí chvilka nepozornosti. Objevit je a ze systému následně dostat však už tak jednoduché není. Pomoci mohou takzvané antimalwarové nástroje, které s nimi zatočí. ...
- http://technet.idnes.cz/proverte-a-pripadne-odstrante-spehy-v-pc-ffa-/software.aspx?c=A140121_150831_software_dvr

Motivace = potřeba ochrany hodnotných informací

- V jakých oblastech?

Motivace = potřeba ochrany hodnotných informací

- Oblasti
  - vláda
  - vojenství
  - firmy
  - organizace
  - osobní
- kartotéky $\longrightarrow$ fyzická ochrana dostatečná
- v počítačích nedostatečné
  - ochrana uvnitř systému - neautorizovaný přístup (osoby, programy)
  - ochrana v síti
    - neautorizovaný přístup
    - ochrana přenášených informací
  - ochrana před viry
- Př:

Problémy v oblasti bezpečnosti

- důvěrnost dat
- integrita dat
- autentizace
- neodmítnutelnost (nonrepudiation)
- dostupnost $\leftrightarrow$ Denials of Service (DoS) útoky
  - v rámci OS
  - po síti
  - složité řešení
- ochrana soukromí = ochrana osob před zneužitím informací o nich

Kdo má zájem škodit?

Pojmenování útočníků

- literatura o bezpečnosti *intruder* (vetřelec), *adversary* (protivník)
- vojenská literatura *enemy* (nepřítel)

Zabezpečení systému - potřeba znalostí o útočníkovi (motivace, znalosti, vybavení, ...)

- netechničtí
  - běžní uživatelé
  - "script kiddies"
- techničtí
- pokusy jednotlivců o zisk
- komerční, vládní a vojenská špionáž

Pozn.:

- Častěji dochází ke ztrátám dat náhodou (HW & SW chyby, chybná manipulace) → zálohovat!!!

Metody obrany

- **ukrytí, zašifrování** informací $\longrightarrow$ utajení přenosu
- kontroly SW
  - zabezpečení proti napadení zvenku
- kontroly HW
  - hardwarová realizace šifrování, ochrana přístupu, ověření identity,...
- administrativní, legislativní a etické kontroly
  - pravidelné změny přístupových hesel
  - zákony; problém rychlého vývoje v IT $\times$ pomalá tvorba zákonů
  - potřeba pochopení širokou veřejností
- fyzické kontroly
  - zámky na dveřích, hlídač, zálohy dat, ...

Za jakých podmínek jsou kontrolní opatření účinná?

Účinnost kontrolních opatření

- porozumění bezpečnostní problematiky
- využívání kontrolních opatření
- překrývání kontrolních opatření
- periodická inovace

Problém utajení přenosu obsahu zprávy

- Steganografie (z řec. steganos = zakryté, tajné)
  - "utajené psaní" = utajení existenci zprávy
- Kryptografie (z řec. kryptos = skrytý)
  - zakódování → útočník neschopen zjistit obsah zprávy

Historická steganografie

- jedna z prvních zmínek v Héródotově historii
  - Demeratus potřebuje tajně oznámit Spartě, že Xerxes chce napadnout Řecko
  - seškrábání vosku z tabulek, napsání na dřevo a opětovné pokrytí voskem
  - vzhled tabulek jako nepoužitých $\longrightarrow$ průchod strážemi
- vytetování zprávy na oholenou hlavu (otroka), nechat narůst vlasy, možnost přečtení až po dalším oholení.
- neviditelné inkousty
- neviditelné inkousty s technologií pro detekci

Detekce (historicky)
(viz heslo "Dechiffrování" v Riegerově Slovníku naučném II/2, Praha 1862)

Chceš-li se přesvědčiti, zdali na bílém papíře, o kterém se domýšlíš, že neviditelné písmo na sobě nese, skutečně něco psáno jest, udělej následující zkoušky v tomtéž pořádku, jak zde uvedeny jsou, po sobě:

1. Drž papír proti světlu, zdali snad písmo prosvítá (stane se to, je-li papír bílým inkoustem popsán).
2. Polož papír na arch savého papíru napojeného louhem ze dvou částí živého vápna a jedné části kamenky (auripigment) svařených ve vodě, a ponech ho tam asi půl hodiny.
3. Drž papír nad žhavým uhlím.
4. Polož ho na půl hodiny do čisté vody.
5. Usuš papír a posyp jej po obou stranách práškem z uhlí neb sazí, pak tento pomalu odfoukni.
6. Potři papír po obou stranách tence černidlem; písmo vyvstane a ukáže se černější.

Neobjeví-li se písmo po žádné z těchto zkoušek, pak není zajisté nic tam psáno.

Historická steganografie

- mikročtečky
- otevřené kódování (nulové šifry)
  - Apparently neutral's protest is thoroughly discounted and ignored. Ismen hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.
  - každé 2. písmeno slova tvoří skutečnou zprávu: "Pershing sails from NY June 1."

Historická steganografie

- mikročtečky
- otevřené kódování (nulové šifry)
  - Apparently neutral's protest is thoroughly discounted and ignored. Ismen hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.
  - každé 2. písmeno slova tvoří skutečnou zprávu: "Pershing sails from NY June 1."

Současná steganografie

- vysílání v rozptýleném spektru (spread spektrum)
- informace ukrytá do souboru s obrázkem, videem nebo zvukem (modifikace nejméně významných bitů $\longrightarrow$ změna nepostřehnutelná)

- Původní obrázek se skrytým obrázkem (vlevo); vložený skrytý obrázek (vpravo)

Další využití steganografie

- *utajení komunikace*
- zajištění autorských práv (digitálně uložená hudba, video, ...)

Kryptografie (šifrování)

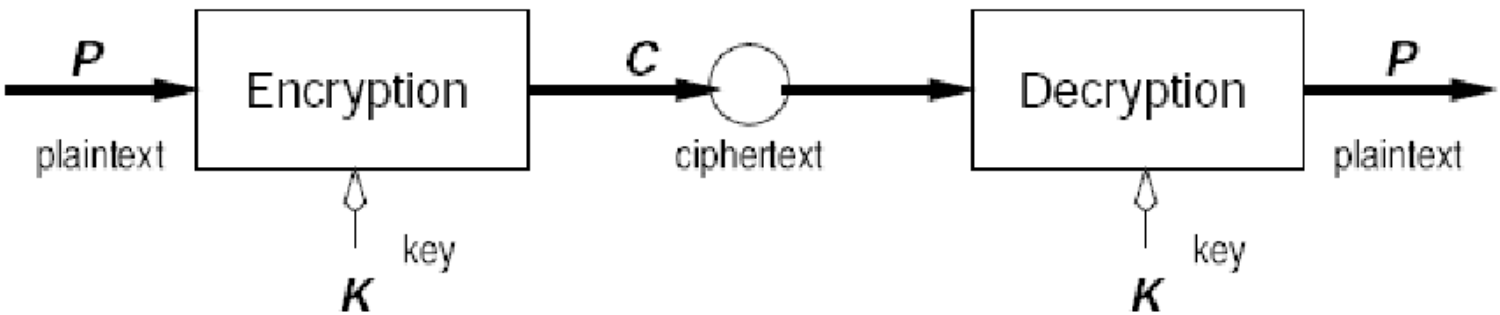
- termín *šifrování* - vznik z francouzského slova "chiffre"
- začátek ve starém Egyptě
- vývoj šifer zejména díky vojenskému využití
  - přidělení zprávy vojákovi, zašifrování, odeslání
  - množství zpráv $\longrightarrow$ množství šifrantů $\longrightarrow$ problém přechodu na jinou metodu (učení mnoha lidí) $\longrightarrow$ parametrizace šifrovací metody klíčem

Záladní model šifrování (a dešifrování)

= algoritmus (funkce), který převádí čitelnou zprávu neboli prostý text (plaintext) na její nečitelnou podobu neboli šifrový text (ciphertext, kryptogram)

- vstup = otevřený text - P
- transformace pomocí šifrovací funkce E; parametrizace klíčem K
- výstup = šifrový text - C, $C = E_K(P)$
- odeslání šifrového textu
- dešifrování pomocí dešifrovací funkce D: P, $P = D_K(C)$

Schéma šifrování a dešifrování

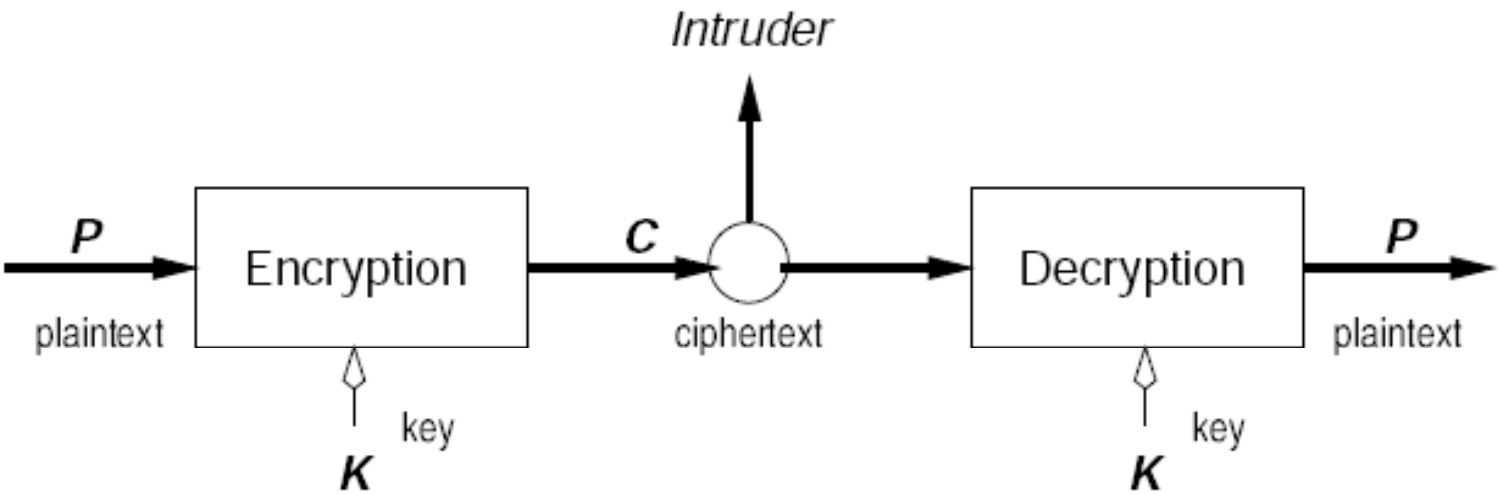


Modely útoků

- útočník - přístup k šifrovému textu = odposlech
- $\longrightarrow$ zkopírování kryptogramu C
- neznalost klíče K a šifrovací funkce
- = pasivní odposlech

- aktivní odposlech = možnost vložení vlastní zprávy

Schéma šifrování a dešifrování s útokem (odposlech)



Několik málo termínů

- Kryptografie = věda o návrhu šifer
- Kryptoanalýza = věda o luštění zašifrovaných zpráv
- Kryptologie = Kryptografie + Kryptoanalýza

Kryptoanalýza

- *Kerckhoffův princip* - jeden ze základních předpokladů úspěšného utajení dat
  - utajení a bezpečnost zašifrovaných dat nesmí záležet na utajení šifrovacího postupu ← kryptoanalytik může znát šifrovací metodu
  - vymyslet, otestovat a zavést metodu velmi náročné → utajení málo pravděpodobné
- v souč. době předpoklad masového rozšíření šifer – možnost analýzy odposlechu šifrovacími čipy nebo pomocí software

→ důležitost role **klíče** = řetězec znaků; možnost změn dle potřeby
Výsledný model = veřejně známá metoda parametrizována tajným klíčem K

Základní druhy útoků (dle odposlechu)

- Ciphertext only attack (útok přímo na šifrovaný text) - k dispozici pouze šifrový text
- Known plaintext attack (útok se znalostí otevřeného textu) - znalost části otevřeného textu
- Chosen plaintext attack - znalost *zvoleného* otevřeného textu
- Adaptive chosen plaintext attack (adaptivní metoda luštění s možností volby otevřených textů)
- Chosen ciphertext attack (útok s možností výběru šifrované zprávy) - dešifrování několika zpráv $\longrightarrow$ k dispozici šifrované a otevřené texty; hledání klíče K (příp. algoritmus)

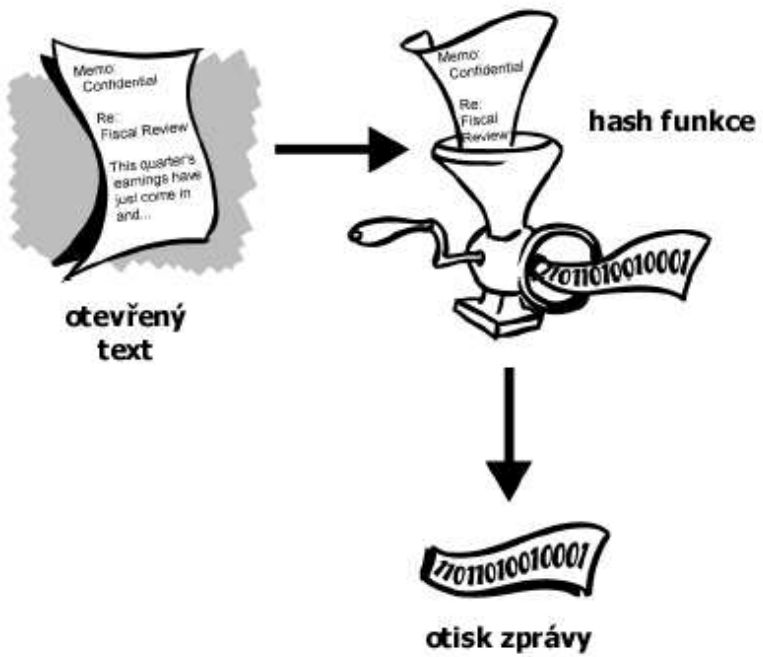
Další druhy útoků

- Brute force attack (útok hrubou silou)
- Side channel attack (útok postranními kanály)
- Agency/Purchase-key attack (agenturní/korupční kryptoanalýza)
- Rubber-hose attack (pendreková kryptoanalýza)

Kontrolní součet (Hash)

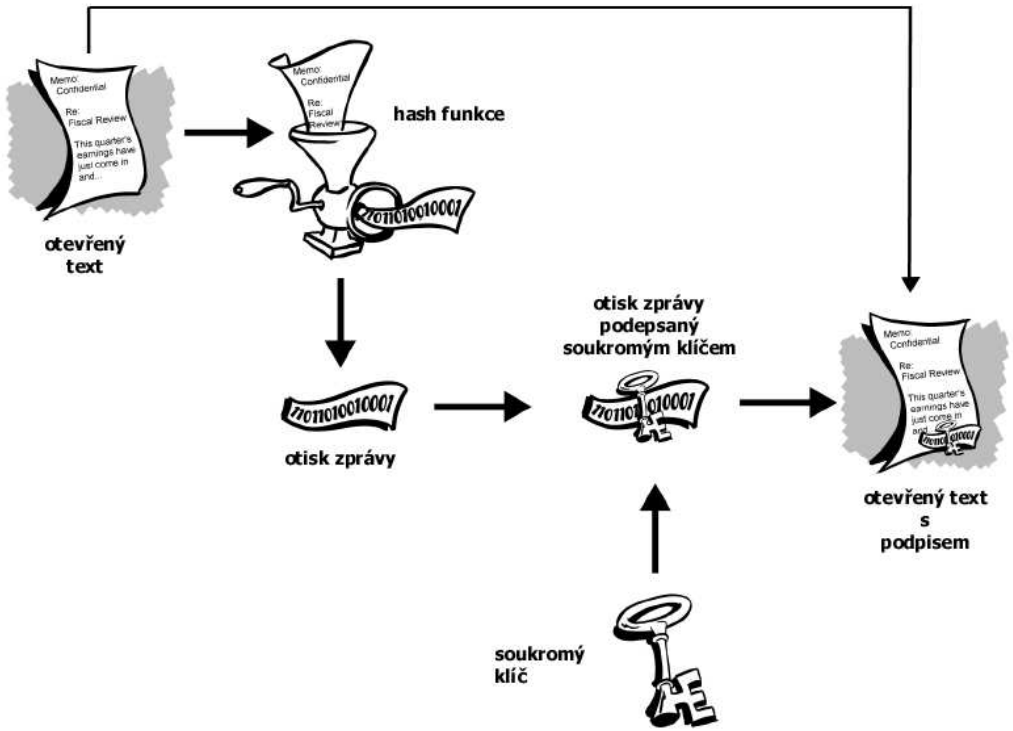
=jednocestná funkce, která z libovolně dlouhého textu vyrobí krátký řetězec konst. délky

- Př: 16B (MD5), 20B (SHA-1)
- použití: otisk prstu dat (fingerprint), bezpečné ukládání hesel (linux - MD5), el. podpis, atd.
- naprosto stejné dva dokumenty → shodný hash (otisk)



Elektronický podpis

- analogie klasického podpisu v el. komunikaci
- založen na kontrolním součtu a vlastnostech asymetrické kryptografie



Příjemce:

- ověření podpisu (rozšifrování hashe) pomocí veřejného klíče autora