

# 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

17. února 2016

# Table of Contents

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obraný

Steganografie

Kryptografie

Druhy útoků

- 1 Administrativní záležitosti
- 2 Úvod - motivace, problémy, metody obrany
- 3 Steganografie
- 4 Kryptografie
- 5 Druhy útoků

# Kontakt, informace o předmětu

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Kontakt:
  - e-mail: [pkral@kiv.zcu.cz](mailto: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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obransy

Steganografie

Kryptografie

Druhy útoků

- **Cvičení:** účast dobrovolná (  $\times$  je vhodné na cvičení chodit  
← praktické procvičení odpřednášené látky)
- **Zápočet:** min. 60% možných bodů ze samostatné práce (SP) a záp. testu
  - zápočtový test - max. 20b
  - samostatná práce (SP) - max 20b
- **Odevzdání SP:**
  - **před** *řádným* termínem → bonus +5b
  - **v** *řádném* termínu
  - **po** *řádném do mezního* termínu → penalizace -5b
  - **po** *mezním* termínu → **ztráta nároku na zápočet**
- **Poznámky:**
  - Aktivita na cvičení také hodnocena
  - “Programovací” SP lépe hodnocena než prezentace ( $\Delta = 25\%$ )
  - “Staré” zápočty se **neuznávají**. Po domluvě s vyučujícím možno uznat body z SP. Test nutno absolvovat **znovu!**

# Podmínky absolvování

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

## 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 - **26.5.2016**

## Přednášky:

- účast dobrovolná ( × vhodná)

## Zkouška:

	Známka	Body
■ min. 60% možných bodů z písemky - max. 40b	1	42-49
	2	34-41
■ body_celkem = trunc (body_ze_zápočtu * 0.2) + body_ze_zkouškové_písemky	3	26-33
	4	0-25

- 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 Příbyl, 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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)
- Prezence semestrálních prací
- Případové studie

# Plán přednášek

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- Úvod do předmětu - motivace, základní pojmy
- Ochrana informací šifrou, typy šifer, použití, příklady
- Moderní symetrická kryptografie
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- 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 phishingové útoky v poslední době

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

## Falešná záplata na Flash Player chce zmást uživatele produktů Apple

- Na počítače a notebooky s operačním systémem OS X míří nový trik útočníků, kteří chtějí proniknout na cizí systémy. Využívají k tomu falešnou hlášku o aktualizaci přehrávače Adobe Flash.
- [http://technet.idnes.cz/falesna-zaplata-na-flash-player-chce-zmast-uzivatele-produktu-apple-kratke-zpravy.aspx?c=A160209\\_101840\\_tec-kratke-zpravy\\_vse](http://technet.idnes.cz/falesna-zaplata-na-flash-player-chce-zmast-uzivatele-produktu-apple-kratke-zpravy.aspx?c=A160209_101840_tec-kratke-zpravy_vse)

## Pozor na falešnou reklamu mBank. Z Facebooku vede přímo k podvodníkům

- Podvodná reklama na údajně nové internetové bankovníctví mBank se snaží nalákat klienty této banky k návštěvě falešných stránek.
- [http://technet.idnes.cz/mbank-podvod-c9f-/sw\\_internet.aspx?c=A160203\\_181752\\_sw\\_internet\\_vse](http://technet.idnes.cz/mbank-podvod-c9f-/sw_internet.aspx?c=A160203_181752_sw_internet_vse)

## 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](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-zahranicni.aspx?c=A110426\\_115124\\_zahranicni\\_stf](http://zpravy.idnes.cz/na-iran-zautocil-pocitacovy-vir-tvaril-se-jako-vladni-soubory-zahranicni.aspx?c=A110426_115124_zahranicni_stf)

## 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-lednický-0mv-/sw\\_internet.aspx?c=A140119\\_231435\\_sw\\_internet\\_vse](http://technet.idnes.cz/hacknute-lednický-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](http://technet.idnes.cz/proverte-a-pripadne-odstrante-spehy-v-pc-ffa-/software.aspx?c=A140121_150831_software_dvr)



# Motivace = potřeba ochrany hodnotných informací

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

## ■ V jakých oblastech?

# Motivace = potřeba ochrany hodnotných informací

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obrany

Steganografie

Kryptografie

Druhy útoků

- Oblasti
  - vláda
  - vojenství
  - firmy
  - organizace
  - osobní
- kartotéky → 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- důvěrnost dat
- integrita dat
- autentizace
- neodmítnutelnost (nonrepudiation)
- dostupnost ↔ 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 útočnickovi (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!!!

- **ukrytí, zašifrování** informací → 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 × pomalá tvorba zákonů
  - potřeba pochopení širokou veřejností
- fyzické kontroly
  - zámky na dveřích, hlídač, zálohy dat, ...

# Za jakých podmínek jsou kontrolní opatření účinná?

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obraný

Steganografie

Kryptografie

Druhy útoků

# Účinnost kontrolních opatření

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

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

# Problém utajení přenosu obsahu zprávy

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

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



# Historická steganografie

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- 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 → 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)

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

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 svého 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 od foukni.
- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- 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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

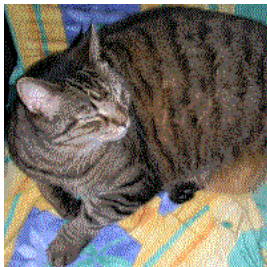
Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

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



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

# Další využití steganografie

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

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

# Kryptografie (šifrování)

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

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

# Základní model šifrování (a dešifrování)

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

= 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 šifrovaného textu
- dešifrování pomocí dešifrovací funkce  $D$ :  $P$ ,  $P = D_K(C)$



# Schéma šifrování a dešifrování

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

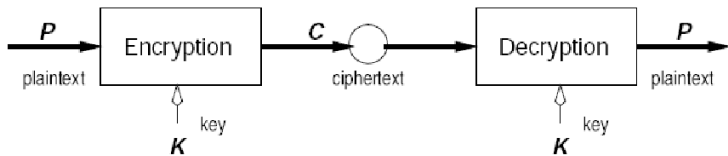
Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků



# Modely útoků

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

- útočník - přístup k šifrovanému textu = odposlech
- → zkopírování kryptogramu  $C$
- neznalost klíče  $K$  a šifrovací funkce
- = pasivní odposlech
- aktivní odposlech = možnost vložení vlastní zprávy

# Schéma šifrování a dešifrování s útokem (odposlech)

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

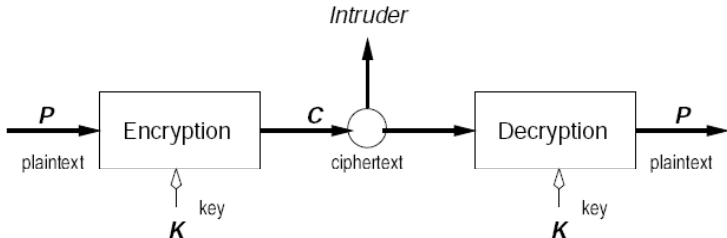
Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obraný

Steganografie

Kryptografie

Druhy útoků



# Několik málo termínů

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

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

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

$\rightarrow$  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 → k dispozici šifrované a otevřené texty; hledání klíče  $K$  (příp. algoritmus)

# Další druhy útoků

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

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)

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

Úvod -  
motivace,  
problémy,  
metody  
obran

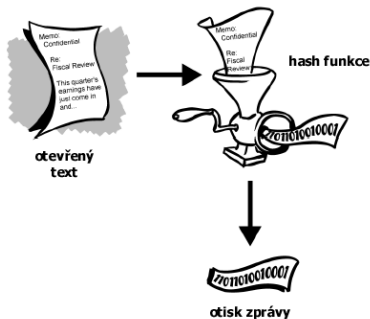
Steganografie

Kryptografie

Druhy útoků

=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

Bezpečnost v  
informačních  
technologiích  
(KIV/BIT)

Ing. Pavel  
Král, Ph.D.

Administrativní  
záležitosti

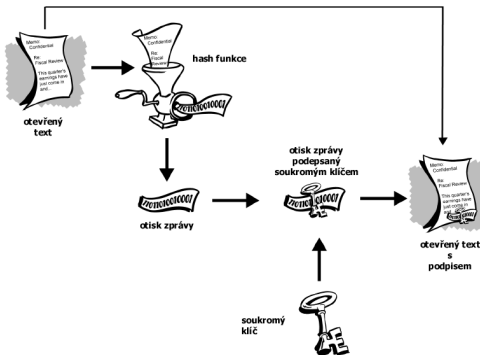
Úvod -  
motivace,  
problémy,  
metody  
obran

Steganografie

Kryptografie

Druhy útoků

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



Příjemce:

- ověření podpisu (rozšifrování hashe) pomocí veřejného klíče autora