



EVROPSKÁ UNIE  
Evropské strukturální a investiční fondy  
Operační program Výzkum, vývoj a vzdělávání

**MŠMT**  
MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY

# Kryptologie

*Základní pojmy, rozdělení, historie a  
pravidla*

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16\_015/0002204



Doc. Ing. Roman Šenkeřík, Ph.D. FAI,  
Ústav informatiky a umělé inteligence

# Obsah prezentace

- Obsah předmětu.
- Literatura.
- Základní pojmy.
- Historie.
- Kryptografická pravidla.
- Lehký matematický “background”
- Klíčový prostor.

# 1. Obsah předmětu

# Obsah předmětu

*Co nás čeká a nemine:*

- Úvod do Kryptologie
  - historie, rozdělení, základní pojmy, rozdělení šifer a jiné „úvodní“ formality...
- Klasická (konvenční) kryptografie
  - trocha historie aneb jak naši prarodiče šifrovali milostné a jiné vzkazy :-) A jak jim to jiní kazili a pomocí jakých nástrojů...
- Moderní kryptografie
  - nástup křemíkové doby 10101010101012?

# Obsah předmětu

*Co nás čeká a nemine:*

- Moderní nekonvenční kryptografie
  - Teorie Chaosu, Kvantová teorie, AI, Kognitivní krypto, Úvod do Fraktální geometrie a fraktálního šifrování
- Steganografie
  - Doplněk kryptografie - umění a věda v jednom pro ukrytování informací
- Kryptoanalýza
  - Základy technik luštění, útoky na šifry

## 2. Literatura

# Literatura

## ○ Klasická Kryptografie

- Pavel Vondruška - Kryptologie, šifrování a tajná písma (edice OKO) [1]
- Hanžl, Pelánek, Výborný - Šifry a hry s nimi (*aneb jak připravit hry a úkoly zbavit se nepohodlných osob na celý den*) [2]
- Jiří Janeček - Odhalená tajemství šifrovacích klíčů minulosti [3]

## ○ Moderní Kryptografie

- Fred Piper, Sean Murphy - Kryptografie, průvodce pro každého [4]
- Ondřej Bitto - Šifrování a biometrika [6]
- Josef Zelenka a kolektiv autorů – Ochrana dat, kryptologie [7]

# Literatura

- Ostatní
  - ENG literatura + webové zdroje (CZ literatury není mnoho). Více podrobností v podpůrných materiálech k předmětu KRY.
  - Spíše pro historiky, příznivce řady teorií, a „filozofy“: Simon Singh - Kniha kódů a šifer [8]
- Poznámka k internetovým zdrojům - často se vyskytuje řetězové kopírování chyb a nepřesností.



# 3. Základní pojmy

# Základní pojmy

- **KRYPTOLOGIE** - technický (vědní) obor zastřešující celkově 3 podobory a zabývající se ochranou přenosu informací.
  - Kryptologie = Kryptografie + Kryptoanalýza + Steganografie.
- **KRYPTOGRAFIE** - technický obor zabývající se tvorbou, vývojem, inovacemi, standardizacemi šifrovacích algoritmů a jejich používáním.
  - Při kryptografických protokolech informaci zašifrujeme, ale dále ji již neskrýváme (odesíláme běžnými komunikačními kanály).

# Základní pojmy

## ○ **KRYPTOANALÝZA**

- technický obor zabývající se dešifrováním zachycené komunikace, dále testováním odolnosti nových algoritmů, možnostmi útoků, odhalováním “zadních vrátek”, penetračními testy atd...

## ○ **STEGANOGRAFIE** tzv. “věda a umění v jednom balíčku”

- úkolem steganografie je “schovávání” informací, tak aby nebyly viditelné.
- Při steganografii informaci nešifrujeme, ale “pouze” ji skrýváme. Samozřejmě se doporučuje kombinovat s kryptografickými protokoly - tj, 1. zašifruji a pak 2. “schovám”.
- Ochrana informace i účastníků komunikace – kde není na první pohled „viděna“ utajená komunikace - nezajímám se.

# Základní pojmy



- **Otevřený text** (Open Text, PlainText)
  - čitelný text/data, CZ i ENG zkratka OT
- **Šifrovaný text** (Cipher Text)
  - “nečitelný” text/data, CZ zkratka ŠT, ENG zkratka CT
- **Šifry a kódy**
  - Pozor, je mezi nimi rozdíl. Pomocí šifry zprávu ukrýváme. Kód zprávu jen upravuje, aby bylo možné ji dále “fyzicky” přenést a zabezpečit proti poruchám v komunikačním kanálu.

# Základní pojmy

## ○ Klíč vs. Heslo

- Jaký je rozdíl? Heslo slouží pro autentizaci na základě jiného sdíleného tajemství (ID, přihl. jméno, atd...). Klíč je vstupem šifrovacího/dešifrovacího algoritmu.

## ○ Symetrický klíč vs. Asymetrický klíčový pár

- Symetrický klíč (někdy nazývaný konvenční) je pro obě operace šifrování i dešifrování je stejný
- Asymetrický klíčový pár - šifrování i dešifrování používá různé klíče.

## ○ Veřejný klíč + Privátní klíč = klíčový pár

- Veřejný je dostupný “všem” pro odeslání dat (ovšem řádně zabezpečen), privátní má pouze příjemce pro dešifrování. Pozor - podepisování používá převrácenou logiku!

# Základní pojmy

- **Abeceda textu**

- množina znaků OT/ŠT

- **Statistická charakteristika jazyka**

- „alias“ frekvenční analýza - četnost výskytu znaků v daném jazyce.
  - Někdy je označována jako tzv. „otisk prstu“ daného zdrojového jazyka zprávy
  - Každý jazyk na světě (včetně nářečí) má vlastní rozložení (distribuci) pravděpodobnosti výskytu znaků.

- **Klíčový prostor**

- Počet všech možných klíčů v daném systému (kapacita abecedy, délka klíče) představuje tzv. klíčový prostor.

# 4. Historie

# Historie

- Mnoho let př.n.l používána především steganografie - ukrývání.
- 500 př.n.l první šifra ATBASH (reverze  $A = Z$ ,  $Z = A$ ) - Hebrejské národy (Féničané).
- 400 př.n.l Řecko - první transpoziční šifry (přeházení znaků) a intenzivní používání steganografie
- 50 př.n.l Řím - Caesarova šifra
- 4. stol. - Indie Kamasutra (*je to především kniha o utajené komunikaci*)
- 10. stol. Arábie - objev frekvenční analýzy a luštění jednoduchých šifer.
- 13, 14 stol. Substituční šifry (substituce = jednoduché nahrazení znaku, ale většinou bez klíče, tj i statistické vlastnosti se substituuují – nízká odolnost vůči frekvenční analýze)



# Historie

- 15, 16 stol. První návrhy „odolných“ šifer s klíči - le chiffre indéchiffrable (není nutno překládat) - tady si Evropané všimli, že jim 500 let “někdo” pomocí frekvenční analýzy luští zprávy.
- 19 stol. prolomení šifer s klíči, intenzivní rozvoj telegrafu, první mechanické přístroje
- 1. a 2. svět válka: Rozvoj komplikovaných vojenských “polních” šifer a mechanických přístrojů (Enigma)
- 1949 - Shannonova teorie kódování a informace, dále rozvoj počítačů
- 1973 - Objev kryptografie s veřejným a privátním klíčem (asymetrická kryptografie)
- od 90 let - Rozvoj kvantové kryptografie a jiných nekonvenčních metod - chaos, AI, kognice, další matematické funkce (eliptické křivky...)

# **5. Kryptografická pravidla.**

# Kryptografická pravidla

1. Stejným klíčem by neměly být nikdy zašifrovány dva různé texty.
2. Dbát na dostatečnou délku klíče.
3. Klíč by měl být co nejméně “uhodnutelný”.
4. Pokud používáme více klíčů, ze znalosti jednoho by nemělo být možno odvodit další klíče (jména rodinných příslušníků, dětí, měsíce v roce atd..).

# Kryptografická pravidla

5. Kryptologický systém by měl být jednoduchý a přehledný, aby zbytečně neodradil uživatele.
6. Pokud je to možné kombinujeme se steganografickou technikou - kde není viditelná zpráva, není podezření a zvědavost.
7. Snaha o co největší kompresi dat - čím delší zpráva tím více materiálu pro kryptoanalýzu.

# 6. Lehký matematický “background”

# Matematický “background”

Nejčastěji používanou funkcí z oblasti kryptografické aritmetiky je jednoduchá funkce **MOD**.

Představuje zbytek po celočíselném dělení - tedy:  $y = x \text{ MOD } n$

kde:  $y$  - celočíselný zbytek,  $x$  - dělenec,  $n$  - dělitel

Příklady:

$$7 \text{ MOD } 4 = 3$$

$$5 \text{ MOD } 3 = 2$$

$$2 \text{ MOD } 3 = 2$$

Tato aritmetika nám zaručí, že výsledek (zbytek) bude vždy v rozsahu 0 až  $n-1$ , tedy je zaručena rotace vektoru (abecedy).

# Matematický “background”

- Dalšími významnými matematickými operacemi (především v moderní kryptografii) jsou:
  - Modulární aritmetika
  - Teorie prvočísel
  - Násobení a zpětná faktORIZACE součinu prvočísel
  - Problém diskretního logaritmu
  - Číselné síťové pole
- Detaily k výše uvedeným problémům jsou uvedeny v odpovídajících lekcích.

# 7. Klíčový prostor



# Klíčový prostor

- Je třeba dodržovat základní kryptografická pravidla - vyhnout se “slabým klíčům” či snadno uhodnutelných.
- Nejstarší a nejjednodušší (*Monoalfabetické substituční*) šifry v podstatě nepoužívají klíč - klíčem je substituční abeceda. Pro počet možných substitucí tedy platí **Permutace n prvků substituční abecedy** - tedy počet možných seřazení množiny o n prvcích bez opakování.

$$P(n) = n!$$

# Klíčový prostor

- Pro většinu ostatních šifer a počet všech možností klíče platí Variace s opakováním - tedy výběr podmnožiny o  $k$  prvcích z konečné množiny o  $n$  prvcích a záleží tedy na pořadí!!!
- Pozor nemůžeme použít statistický prvek *kombinace* - zde nezáleží na pořadí!!

$$V'_k(n) = n^k$$

# Klíčový prostor - příklad

- ENG abeceda má 26 znaků
- CZ abeceda má 42 znaků!!
- Počet možných klíčů pro klíč o délce 8 znaků (26 znaků abecedy a - z):  
 $26^8 = 2.09 \cdot 10^{11}$
- Počet možných klíčů pro klíč o délce 8 znaků (26 znaků abecedy a - z + 26 znaků abecedy A - Z):  $52^8 = 5.35 \cdot 10^{13}$
- Počet možných substitucí pro anglickou abecedu (26 znaků):  $26! = 4.03 \cdot 10^{26}$
- Počet možných substitucí pro českou abecedu (42 znaků):  $42! = 1.41 \cdot 10^{51}$
- Počet možných klíčů pro Vernamovu šifru o délce 160 znaků - SMS: (26 znaků abecedy - náhodný klíč o délce 160 znaků):  $26^{160} = 2.49 \cdot 10^{226}$

# Klíčový prostor - příklad

- Počty možných klíčů pro moderní symetrické šifry (DES, 3DES, AES...) - binární reprezentace klíče - tedy abecedu 2 počet bitů:
- 56 bitů (DES):  $2^{56} = 7.21 \cdot 10^{16}$
- 128 bitů (AES):  $2^{128} = 3.4 \cdot 10^{38}$
- 168 bitů (3DES):  $2^{168} = 3.74 \cdot 10^{50}$
- 192 bitů (AES):  $2^{192} = 6.28 \cdot 10^{57}$
- 256 bitů (AES):  $2^{256} = 1.16 \cdot 10^{77}$
- 512 bitů (AES):  $2^{512} = 1.34 \cdot 10^{154}$

# Seznam odkazů

- [1] VONDRUŠKA, Pavel. Kryptologie, šifrování a tajná písma. Ilustroval Bára BUCHALOVÁ. Praha: Albatros, 2006. Oko (Albatros). ISBN 80-00-01888-8.
- [2] HANŽL, Tomáš, Radek PELÁNEK a Ondřej VÝBORNÝ. Šifry a hry s nimi: kolektivní outdoorové hry se šiframi. Praha: Portál, 2007. ISBN 978-80-7367-196-9.
- [3] JANEČEK, Jiří. Odhalená tajemství šifrovacích klíčů minulosti: ruční šifry. Praha: Naše vojsko, 1994. Mozaika (Naše vojsko). ISBN 80-206-0462-6.
- [4] PIPER, F. C. a Sean MURPHY. Kryptografie. Praha: Dokořán, 2006. Průvodce pro každého. ISBN 80-7363-074-c
- [6] BITTO, Ondřej. Šifrování a biometrika, aneb, Tajemné bity a dotyky. Kralice na Hané: Computer Media, 2005. ISBN 80-86686-48-5.
- [7] ZELENKA, Josef. Ochrana dat: kryptologie. Hradec Králové: Gaudeamus, 2003. ISBN 80-7041-737-4.
- [8] SINGH, Simon. Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii. 2. vyd. v českém jazyce. Přeložil Dita ECKHARDTOVÁ, přeložil Petr KOUBSKÝ. Praha: Dokořán, 2009. Aliter (Argo: Dokořán). ISBN 978-80-7363-268-7.



EVROPSKÁ UNIE  
Evropské strukturální a investiční fondy  
Operační program Výzkum, vývoj a vzdělávání

**MŠMT**  
MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY

# Děkuji za pozornost

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16\_015/0002204



Doc. Ing. Roman Šenkeřík, Ph.D. FAI,  
Ústav informatiky a umělé inteligence