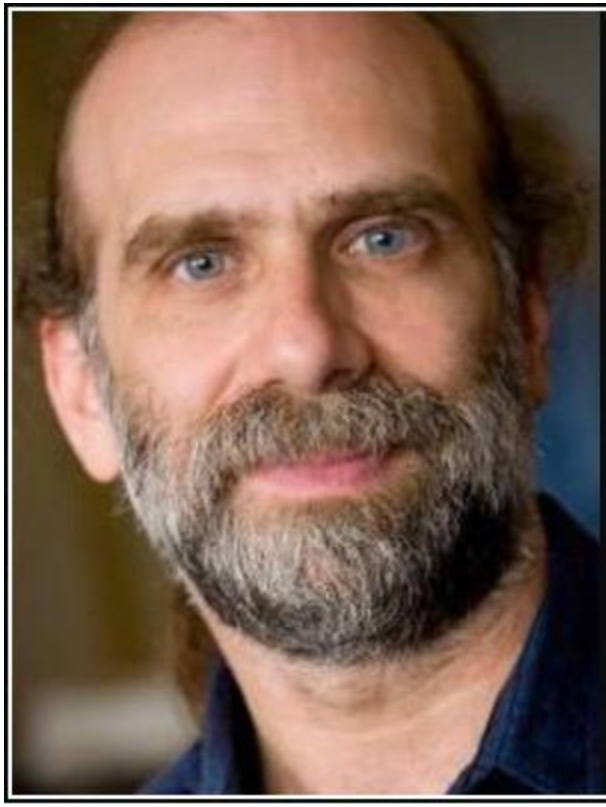
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

# Úvod do kryptologie, základní pojmy

Ing. Tomáš Vaněk, Ph.D. tomas.vanek@fel.cvut.cz



If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

— Bruce Schneier —

# Osnova – co určitě musíme stihnout

- úvod do kryptologie, základní pojmy
- moderní blokové symetrické šifry (AES)
- režimy činnosti blokových šifer (ECB,CBC,OFB,CTR,XTS)
- moderní proudové symetrické šifry
  - (RC4, A5), ChaCha, projekt eSTREAM
- asymetrické kryptosystémy
  - RSA, Diffie-Hellman, eliptické kryptosytémy (ECDSA, ECDH)
  - IBE – Identity Based Encryption
- hashovací funkce (SHA-1,2,3)
- autentizační protokoly
  - CHAP, EAP, AAA, 802.1x, RADIUS, TACACS

# Osnova – co určitě musíme stihnout

- IPsec
- SSL/TLS, DTLS
- zabezpečení el. pošty – S/MIME, PGP
- PKI (Public Key Infrastructure)
  - Certifikáty X.509, CA
- elektronický podpis, časová razítka
  - eIDAS, ZoSVDP
- zabezpečení v datových sítích
  - Ethernet, Wi-Fi, WiMAX, Bluetooth
- zabezpečení v mobilních sítích
  - GSM, UMTS, LTE, LTE-A
- zabezpečení VoIP komunikace

# Když náhodou zbude čas…

- Steganografie
- Digitální vodoznaky
- Kvantová kryptografie a postkvantová kryptografie
- Teorie informace
- Teorie výpočetní složitosti
- Generátory pseudonáhodných posloupností
- Zero-knowledge protokoly
- TOR
- Zabezpečení v IoT
- GDPR, NIS, PSD2

# Literatura k předmětu

- Menezes A, Vanstone S, van Oorschot P., Handbook of Applied Cryptography, CRC Press, 1996, volně ke stažení na http://www.cacr.math.uwaterloo.ca/hac/
- Mao W., Modern Cryptography - Theory & Practice, Prentice-Hall, 2004, ISBN: 0-13-066943-1
- Stamp M., Information Security - Principles and Practice, Wiley, 2006, ISBN: 0-471-73848-4

- Levický D., Kryptografia v informačnej bezpečnosti, elfa, 2005,ISBN:80-8086-022-X
- Burda K., Aplikovaná kryptografie, VUTIUM, 2013, ISBN: 978-80-214-4612-0

# Literatura ostatní


- Singh *S., Velká kniha kódů a šifer,* Argo, 2001,ISBN 80-86569-18-7
- Vondruška P. – Kryptologie, šifrování a tajná písma, Albatros, 2006, ISBN: 80-00-01888-8
- Pužmanová R., *Bezpečnost bezdrátové komunikace – Jak zabezpečit WiFi, Bluetooth, GPRS či 3G*, Computer Press, 2005, ISBN: 80-251-0791-4
- Peterka J., Báječný svět elektronického podpisu, předběžná verze - http://www.bajecnysvet.cz/stahnout.php
  - články na o eln. podpisu, eIDAS na *www.lupa.cz*
- Dostálek L., Vohnoutová M., Knotek M. – Velký průvodce infrastrukturou PKI a technologií elektronického podpisu, Computer Press, 2009, ISBN: 978-80-251-2619-6

# Bezpečnost v praxi je vždy otázka kompromisu

**Každý systém je tak bezpečný, jak je bezpečný jeho nejslabší článek**

# Terminologie, aneb když se budu večer nudit

Původ z řečtiny :

- **kryptós** (skrytý)
- **gráphein** (psát)
- **logos** (věda)
- před nástupem počítačů byla kryptografie řazena k lingvistice
- v současnosti kryptografie úzce využívá matematiku
- zejména oblasti: modulární aritmetika
  teorie informace
  teorie výpočetní složitosti
  teorie pravděpodobnosti
  statistika
- viz předmět A7B01MCS

# Terminologie, aneb když se budu večer nudit

**Kryptologie (Cryptology)**

- vědní obor zahrnující  kryptografii a kryptoanalýzu

**Kryptografie (Cryptography)**

- návrh a konstrukce kryptografických algoritmů a způsoby jejich využívání

**Kryptonalýza (Cryptanalysis)**

- metody získávání otevřeného textu z textu šifrového **bez znalosti klíče**
- zkoumá odolnost a zranitelnost kryptosystémů

# Terminologie, aneb když se budu večer nudit

- **Otevřený text (OT) /** Plain text (PT) – informace v čitelné podobě, která bude šifrována
- **Šifrový text** (ŠT) / Cipher text (CT) - informace, které, která je výsledkem šifrování a je čitelná pouze se znalostí nějaké „tajné“ informace
- **Šifrování** / Encryption - použití šifrovacího algoritmu
- **Dešifrování** / Decryption - získání otevřeného textu ze šifrového textu pomocí šifrovacího algoritmu a klíče
- **Klíč** / Key – parametr kryptografického algoritmu (utajovaný), bezpečnost kryptosystému závisí na bezpečnosti klíče

# Terminologie, aneb když se budu večer nudit

**Kryptografický algoritmus / Encryption algorithm**

- matematický postup, který přetváří otevřený text do takové podoby, kdy původní informace se stává nečitelnou a obráceně, postup, který přetváří šifrový text do podoby otevřeného čitelného textu.

**Klíč / Key**

- jeden ze vstupů šifrovacího algoritmu
- element, který změní obecný šifrovací algoritmus ve specifický postup šifrování

**Heslo / Password**

- řetězec znaků sloužící k ověření uživatelovy identity
- heslo může být použito přímo nebo transformováno na klíč

**Passphrase**

- použití jako heslo, ale skládá se ze sekvence slov

# Terminologie, aneb když se budu večer nudit

- **symetrická šifra** / symmetric key cryptosystem – kryptografický algoritmus, který pro šifrování i dešifrování používá tentýž klíč*
- **asymetrická šifra /** public key cryptosystem – kryptografický algoritmus, který používá dva odlišné klíče, jeden pro šifrování a jeden pro dešifrování
- **veřejný klíč /** public key – jeden z dvojice klíčů asymetrického šifrovacího algoritmu, obvykle slouží k šifrování a nemusí být utajován
- **soukromý klíč** / private key – druhý z dvojice klíčů asymetrického šifrovacího algoritmu, obvykle slouží k dešifrování a musí být vždy utajován

* není zcela přesné

# Jak NESPRÁVNĚ mluvit o kryptologii

## Neexistující slova

- enkryptace / enkrypce
- kryptování / enkryptovat / dekryptovat

## Slova s jiným významem

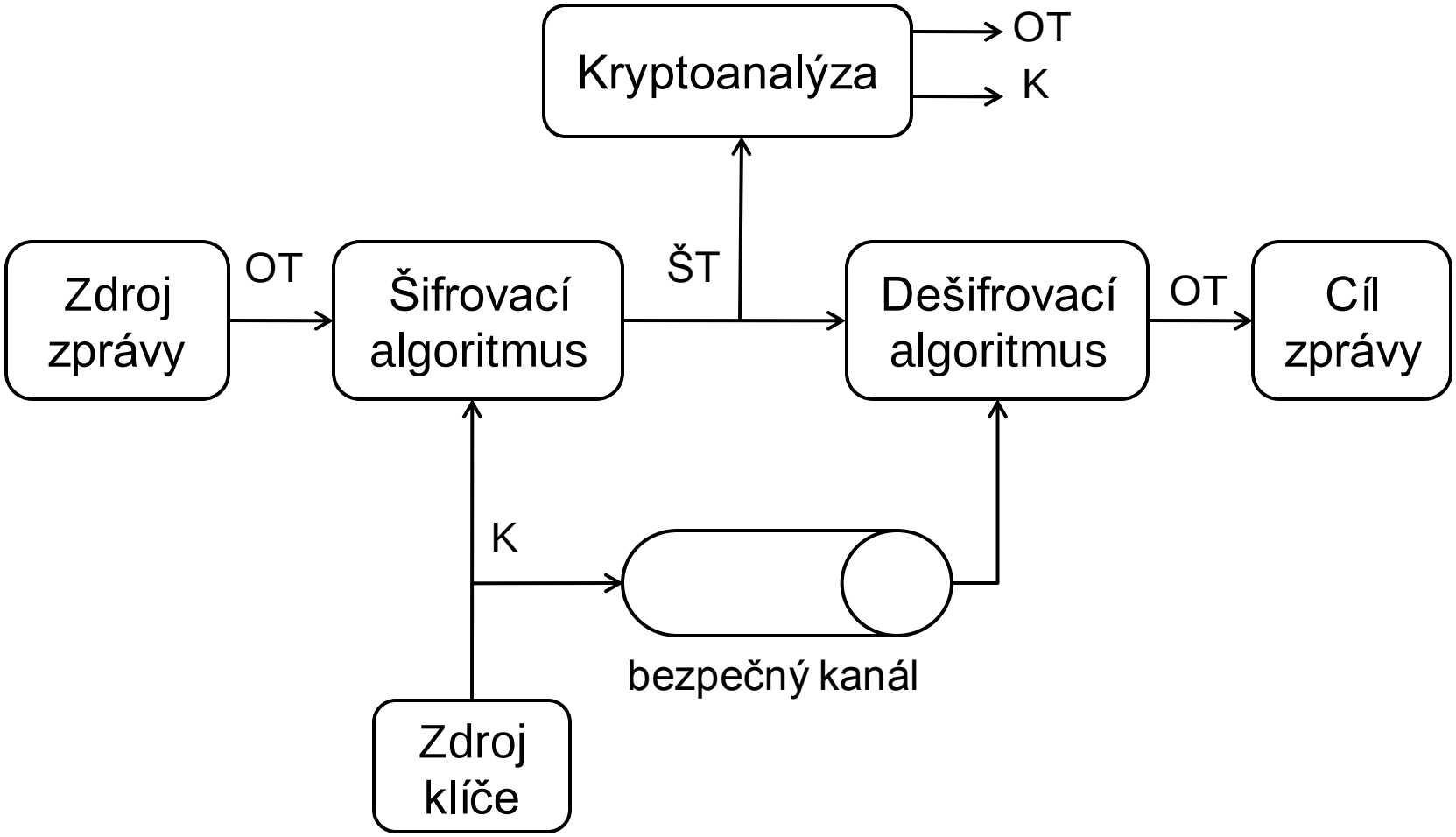
- kódování – (kódovat /dekódovat)

## Nejednoznačná terminologie

- **autentizace** (GE - *authentisierung* )
- autentifikace (FR - *authentification*)
- autentikace (EN - *authentication*) – podle vzoru communication – komunikace , méně časté

**http://interval.cz/clanky/hrichy-pro-sileneho-korektora-autentizace-autentikace-nebo-autentifikace/**

# Terminologie - klasický (Shannonův) model kryptosystému

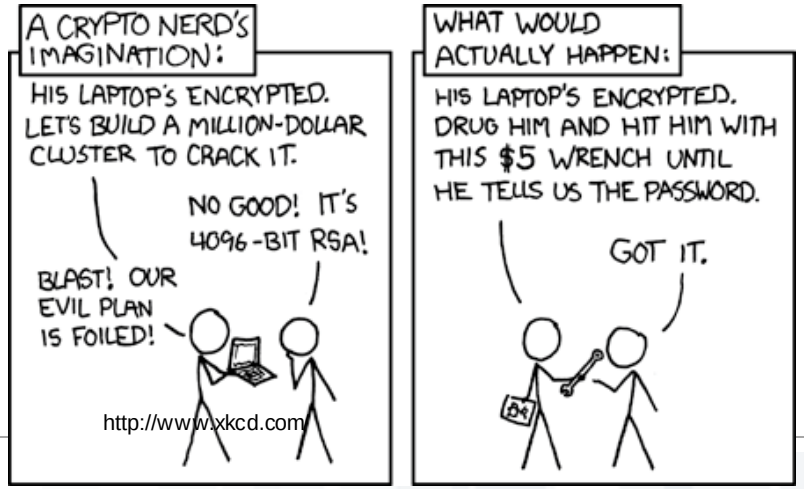


# Terminologie - Kryptoanalýza

- Věda o hledání slabých míst a/nebo prolamování matematických metod informační bezpečnosti
- Cílem je získání OT bez znalosti *klíče* (případně proces získání klíče nebo obojího).
- Kryptosystém lze prolomit využitím bezpečnostní chyby v:
  - šifrovacím algoritmu
  - komunikačním protokolu využívajícím daný šifrovací algoritmus
  - schématu pro správu klíčů

# Terminologie - Kryptoanalýza

- útok hrubou silou (brute-force )
  - prohledání celého prostoru klíčů
  - nejjednodušší útok
  - složitost je úměrná množství klíčů
  - předpokládáme, že jsme schopni detekovat nalezení OT
- pendreková (rubber-hose) kryptoanalýza
- korupční kryptoanalýza
- social engineering



# Kryptoanalýza – útok hrubou silou

| Délka klíče [b] | Prostor klíčů | Čas nutný k prohledání prostoru klíčů rychlostí 1 klíč/μs | Čas nutný k prohledání prostoru klíčů rychlostí $10^6$ klíčů/μs |
|---|---|---|---|
| 32 | $2^{32} = 4{,}3 \times 10^9$ | 71,6 minut | 4,3 ms |
| 56 | $2^{56} = 7{,}2 \times 10^{16}$ | 2284 let | 20,02 hodin |
| 128 | $2^{128} = 3{,}4 \times 10^{38}$ | $1{,}08 \times 10^{25}$ let | $1{,}08 \times 10^{18}$ let |
| 168 | $2^{168} = 3{,}7 \times 10^{50}$ | $1{,}2 \times 10^{37}$ let | $1{,}2 \times 10^{30}$ let |
| náhodná permutace 26 znaků | $26! = 4 \times 10^{26}$ | $6{,}4 \times 10^{12}$ let | $6{,}4 \times 10^{6}$ let |

# Terminologie - kryptoanalýza postranními kanály

- „alternativní“ způsoby útoků na kryptosystémů
- neútočí se na samotný algoritmus, ale jeho fyzickou implementaci
- zachycení informace v průběhu zpracování

Klasické postranní kanály:

- **Timing analysis** – útok založený na analýze doby trvání různých matematických operací
- **Power monitoring analysis** – viz předchozí případ, ale sleduje se spotřeba
- **Radiation monitoring analysis** - sleduje se vyzařování v různých částech E-M spektra
- **Fault analysis** – získávání informací z chybových hlášení…

- lze realizovat i adaptivní postranní kanály

# Kerckhoffův princip – poslední důležitá poučka

**„Utajení šifrovacího algoritmu nesmí sloužit jako opatření nahrazující nebo garantující kvalitu šifrovacího systému.“**

- 1883 Auguste Kerckhoff (holadnský kryptograf)
- Základní předpoklad při konstrukci kryptosystémů
  - útočník zná celý kryptosystém
  - kryptografické algoritmy nejsou tajné, pouze klíč je tajný
- Proč by měl tento předpoklad platit ?
  - utajované algoritmy nikdy nezůstanou tajné navždy
  - praxe ukazuje, že v utajovaných algoritmech jsou po odhalení často nalezeny bezpečnostní chyby
  - je lepší odhalit chyby dříve nežli později…

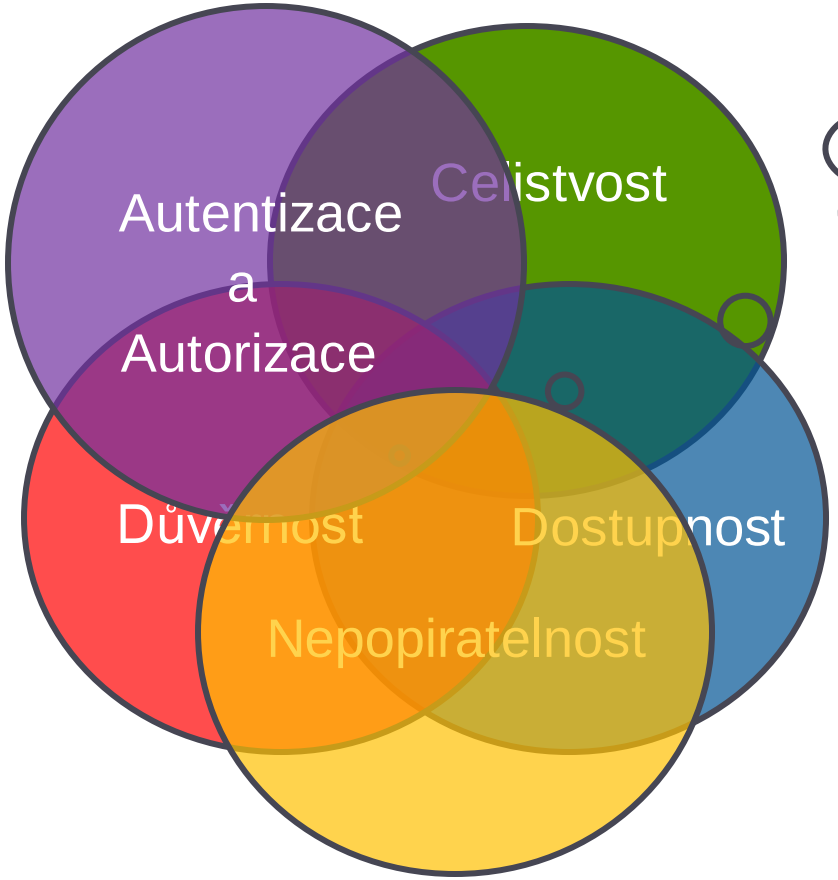
# Základní pojmy

- V dnešní době je většina informací vytvářena, udržována, a přenášena v elektronické podobě.
- Informace mohou být cílem různých útoků, které souvisí s elektronickou povahou dat a proto je přenášená data nezbytné chránit.
- Existuje několik základních cílů, které je potřeba splnit, aby byl systém manipulující s (elektronickými) daty považován za důvěryhodný.

**Jaké jsou základní cíle?**

Tyto cíle pomáhá plnit vědní disciplína – **kryptografie**.

# Základní cíle informační bezpečnosti




**Bezpečnost**

**C**onfidentiality
**I**ntegrity
**A**valaibility

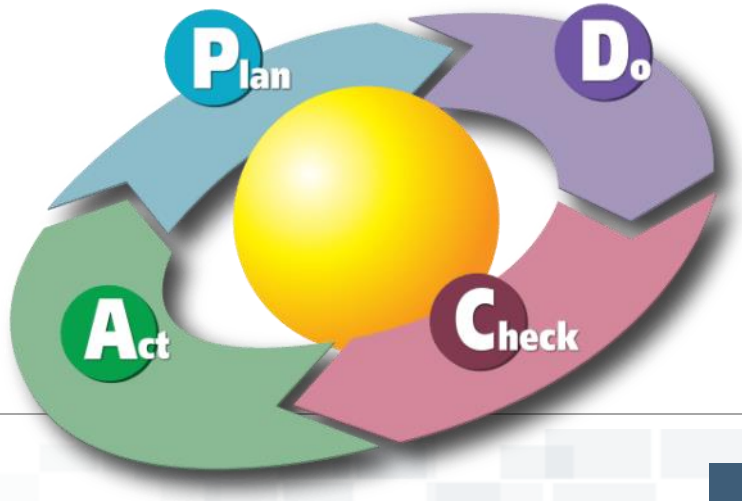
# Co je a co není informační bezpečnost

**NENÍ**

- Produkt
- Trvalý stav
- Jednorázová záležitost typu „Nastav a zahoď klíč“

JE

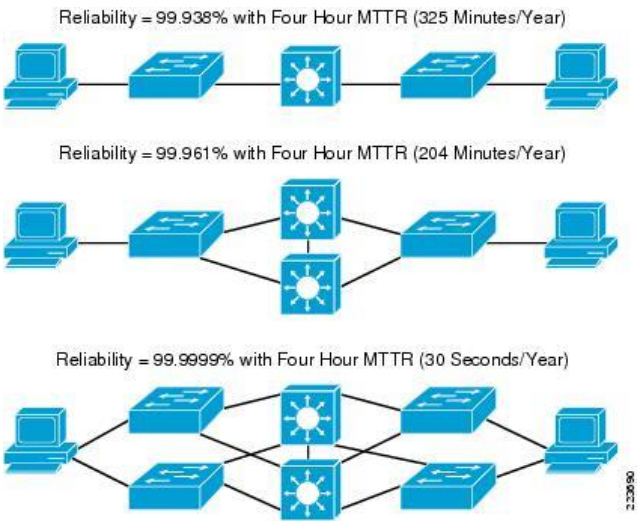
- Proces
- Nikdy nekončící cyklus
  - Plánování (analýza)
  - Implementace
  - Testování
  - Vyhodnocování



# Základní pojmy - Dostupnost

- EN - Avalaibility
- zajištění, že informace je pro **oprávněné** uživatele přístupná v okamžiku její potřeby
- uvádí se v %
  - např. dostupnost 99,999% znamená výpadek 5 minut za rok

- Kdo je, ale **oprávněný** uživatel?
  - Autentizace
  - Autorizace



# Základní pojmy - Autentizace

- EN - Authentication
- Proces ověření identity entity (člověk, program, systém).
- Dvě možné formy
  - Verifikace - entita se aktivně identifikuje, systém pouze potvrdí shodu
  - Identifikace - systém aktivně vyhledá v databázi odpovídající záznam
- Může být vzájemná nebo jednostranná.

# Základní pojmy - Autorizace

- EN - Authorization
- Oprávnění přístupu k systémovým zdrojům.
- V průběhu autorizace se určuje k jakým zdrojům má uživatel přístup.

# Základní pojmy – Utajení, Důvěrnost

- EN – Confidentiality
- Informace je dosažitelná pouze autorizovaným subjektům.
- Utajení zajišťují šifrovací (kryptografické) algoritmy

# Základní pojmy - Integrita

- EN - Integrity
- Vlastnost systému zajišťující, že přenášená informace nebyla zničena, ztracena nebo modifikována, resp. schopnost detekce takovéto změny.

# Základní pojmy - Nepopiratelnost

- EN – Non-repudation
- Subjekt nemůže důvěryhodně popřít své minulé požadavky nebo činy.

CAT RECEIPT HEADER MESSAGE 4
CAT RECEIPT HEADER MESSAGE 5
CAT RECEIPT HEADER MESSAGE 6
CAT RECEIPT HEADER MESSAGE 7

TR TYPE AUTHSALE
MERCHNT# 401200002060
ORDER# 0404
REF# 00000328
PAYMENT SUPERCARD
CARD# XXXXXXXXXXXX8959
EXP.DATE 10/00
AUTH.# 0

SUBTOTAL 12.48

TOTAL AMOUNT 100.25

SIGNATURE

I agree to pay the total amount according to the card issuer agreement.

1stcopy=Merchnt 2ndcopy=Customer
Ann T. CSHR
0095 17:38 SEP 22'00 H/S#04

Příklad:

Při placení platební kartou podpisem (nebo také znalostí PINu) stvrzujete, že jste skutečně čerpali danou službu/zboží. V budoucnosti pak tento fakt nemůžete popírat.

Prostředky používané k dosažení základních cílů:

- šifrovací algoritmy
- hashovací funkce, MAC/HMAC
- kryptografické protokoly
- časová razítka (známky)
- digitální podpisy

# Informační bezpečnost – čeho chceme dosáhnout…

Nepodmíněná bezpečnost

- Šifru nelze prolomit bez ohledu na dostupné množství výpočetního výkonu, protože ŠT neposkytuje dostatek informací nutných k jednoznačnému rozpoznání odpovídajícího OT

Podmíněná bezpečnost

- Šifru nelze prolomit, protože nemáme k dispozici dostatečné prostředky (čas, výpočetní výkon).
- **Prokazatelná bezpečnost**
  - Problém, na kterém je šifra založena spadá do třídy NP.
- **Výpočetní bezpečnost**
  - Cena za prolomení šifry přesahuje cenu chráněné informace.
  - Čas nutný k prolomení šifry přesahuje dobu životnosti chráněné informace.

# Šifry – klasické šifry (cvičení)

- Substituční šifry
  - Monoalfabetické šifry
    - Césarova šifra
    - Affiní šifra
  - Polygrafické šifry
  - Polyalfabetické šifry
  - Playfair
  - Jednorázový heslář (One-Time Pad)
- Transpoziční šifry (Permutace)
  - Blokové (sloupcové) transpozice
  - Cardanova mřížka
  - Rail Fence

- Kombinované šifry (product cipher)
  - C. Shannon
  - šifra obsahující jak substituční, tak transpoziční část
  - větší bezpečnost

# Šifry – moderní algoritmy (přednášky)

- Symetrické
  - Proudové
  - Blokové
- Asymetrické
  - Integer Factorization Problem (IFP)
  - Discrete Logarithm Problem (DLP)
  - Elliptic Curve Discrete Logarithm Problem (ECDLP)
  - Další moderní kryptosystémy
    - Kryptografie založená na mřížkách – Lattice based
    - Kryptografie založená na bilineárním párování – Weil pairing
    - Homomorfní šifrování

# Kryptografie v průběhu času několik zajímavostí

První zaznamenaný výskyt slova **kryptografie** je v knize sira Thomase Browna „The garden of Cyrus“ z roku 1658.

http://penelope.uchicago.edu/gardennoframes/gardenn.html
http://en.wikipedia.org/wiki/The_Garden_of_Cyrus

# Káma sútra

- popisuje 64 umění, která by měla ovládat každá žena
- 44. a 45. z nich je „mlecchita-viklapa“
  neboli “ umění porozumění a psaní textu v šifrách “
- popis dvou různých kryprosystémů
  - „kauţiliyam“
  - „m-ladejiya“

# Skytale

- 7 st. př.n.l.
- z řečtiny - hůl
- nástroj realizující transpoziční šifru
- skládal se z tyče o daném poloměru a pruhu papíru, který byl na ni navinutý
- Řekové používali tento způsob komunikace během válečných tažení
- klíč = poloměr tyče

# Césarova šifra

- jedna z nejznámějších a nejjednodušších šifer
- dnes jednoduše prolomitelná
- monoalfabetická substituční šifra
- kryptoanalýza pomocí frekvenční analýzy
- $C_i = E(P_i + 3) \bmod 26$
  $P_i = D(C_i - 3) \bmod 26$

# Césarova šifra - příklad

- Otevřený text: cesarovasifra

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y |
| D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |

- Šifrový text: FHVDURYDVLIUD

- Pouze posun o 3 se nazývá “Césarova šifra”

# Další starověké šifry

- Mezopotámie
  - 1500 př. n.l.
  - destička s technologickým popisem výroby glazury
- Polybiův čtverec
- Hebrejské šifry
  - Atbash
  - Albam
  - Atbah
- Čína
  - nepožívala kryptografii
  - skoro nikdo neuměl číst a psát
  - zprávy smotané do kuličky se obalily voskem a ukryly na tělě

# Středověká kryptologie

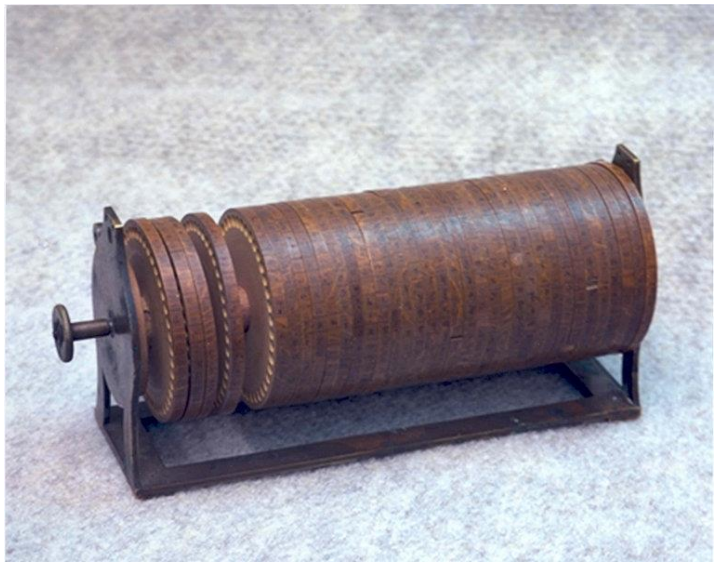
- 855 n.l. Abú Bakr Ahmad
  - arabský matematik
  - popis  několika šifrových systémů (jednoduchá záměna)
  - jeden používán ještě v 2.pol. 18.st.
- 9. století n.l.
  - Abú Júsuf Ja'qub ibn Išáq al-Kindí
  - arabský všestranný vědec (matematik,fyzik, hudebník…)
  - první popis FA
  - "*Rukopis o dešifrování tajených zpráv*"

# Nomenklátor

- oblíbený systém používaný ve středověku
- základ tvoří symboly reprezentující znaky abecedy, které jsou dále rozšířeny o
- další symboly reprezentujících slova (částečná kódová kniha)
- klamače (nulové znaky)
- zdvojující symboly

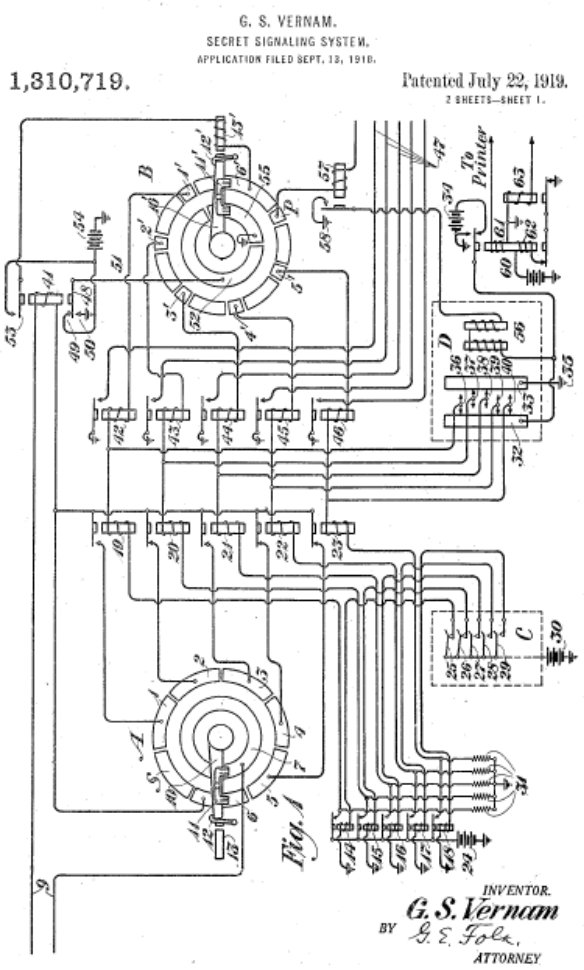
# Jeffersonův válec - 1790

- Thomas Jefferson
- 36 válečků nasunutých na osu
- po obvodu jednotlivých válečků jsou různým způsobem zapsané abecedy.
- celkem 36! x 26! ~ $1{,}5*10^{68}$ kombinací



# Vernamova šifra (One-time Pad)

- Gilbert Vernam, 1917
- zaměstnanec AT&T
- jediný absolutně bezpečný kryptosystém
- původní verze pracovala s děrnou páskou
- matematický důkaz provedl C. E. Shannon v roce 1949
- používal se pro zabezpečení horké linky mezi Moskvou a Washingtonem
- problém s generováním a distribucí klíče



# One-time Pad - požadavky nutné pro správnou funkci

**Klíč je minimálně stejně dlouhý jako přenášená zpráva.**

- jiné šifrovací systémy používají kratší klíče, což znamená, že počet možných klíčů je menší než počet možných zpráv
- kratší klíč umožňuje útok hrubou silou

**Klíč je dokonale náhodný.**

- nelze použít klasické počítačové generátory pseudonáhodných posloupností
- nejvhodnější je užití fyzikálních metod, například tepelného šumu nebo ještě lépe kvantových procesů (poločas rozpadu atd.)

# One-time Pad - požadavky nutné pro správnou funkci

**Klíč nelze použít opakovaně.**

Tato podmínka je vychází z předchozí, protože opakovaný klíč není náhodný. Dostane-li útočník do ruky dvě zprávy zašifrované stejným klíčem, má často velmi snadnou cestu k rozluštění.

**Klíč zná pouze odesílatel a příjemce.**

**Šifrový text neposkytuje žádnou informaci o otevřeném textu.**

Porušení libovolného z těchto požadavků umožní útočníkovi odhalit tajný text. Při dodržení těchto podmínek nelze takto zašifrovaný text dešifrovat ani útokem hrubou silou. Jeho výsledkem budou všechny možné zprávy dané délky, mezi nimiž nepoznáme tu, která byla odeslána.

# One-time Pad

**Šifrování:** Znak otevřeného textu se přičítá na znak hesla pomocí operace XOR

**Dešifrování:** Znak šifrového textu se přičítá na znak hesla pomocí operace XOR

# Vernamova šifra v praxi

**Project VENONA**

- sovětští agenti posílali zprávy z USA do SSSR především o vývoj jaderné bomby,…
- 1941-1950 poslali tisíce zpráv
- sovětští agenti do USA dopravili „one-time pad“, který používali jako zdroj hesel
- opakování hesel ale způsobili možnost rozluštění ze strany amerických kryptoanalytiků
- v průběhu let 1948-1980 se jich podařilo většinu rozluštit

**http://en.wikipedia.org/wiki/Venona**

# Vývoj po 2 sv. válce

- Claude Shannon – teorie informace
- rychlý rozvoj výpočetní techniky
- Data Encryption Standard (DES), 70. léta
- kryptosystémy veřejného klíče, 2.pol. 70. let
- Advanced Encryption Standard (AES), 2001
- kryptografie opouští svět diplomacie, tajných služeb a armády a stává se součástí běžného života

# Dotazy