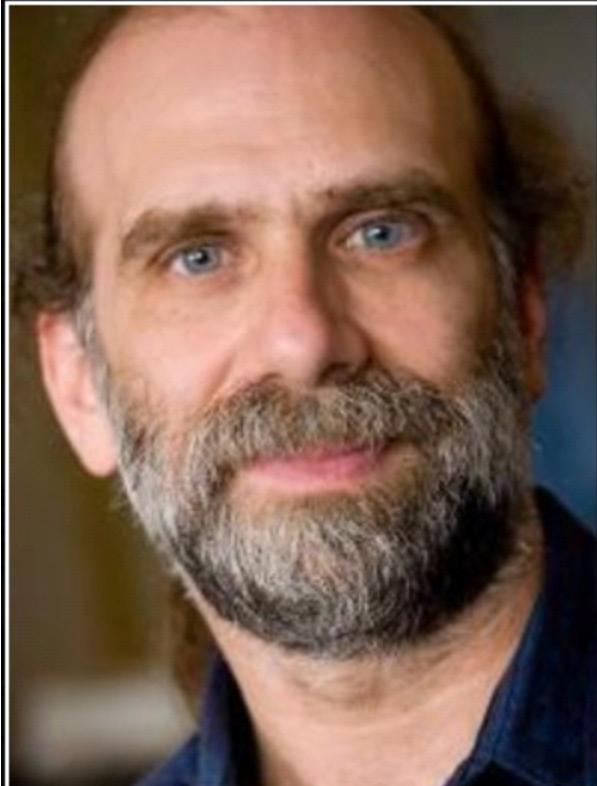


**České vysoké učení technické v Praze  
Fakulta elektrotechnická  
Katedra telekomunikační techniky**

## **Úvod do předmětu, motivace, základní pojmy**

Ing. Tomáš Vaněk, Ph.D. [tomas.vanek@fel.cvut.cz](mailto: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), ChaCha20, projekt eSTREAM
- asymetrické kryptosystémy
  - RSA, Diffie-Hellman, eliptické kryptosystémy (ECDSA, ECDH)
- hashovací funkce (SHA-1,2,3)
- Klasické autentizační protokoly
  - CHAP, EAP, AAA, IEEE 802.1x, RADIUS,
- decentralizovaná autentizace - OpenID
- autorizační protokoly - OAuth2



# Osnova – co určitě musíme stihnout

- IPsec (IKEv1, IKEv2)
- SSL/TLS, DTLS
  - **TLS 1.3**
- zabezpečení el. pošty – S/MIME, PGP
- PKI (Public Key Infrastructure)
  - Certifikáty X.509, CA
- elektronický podpis, časová razítka
- zabezpečení v datových sítích
  - Ethernet, Wi-Fi (**WPA3**), Bluetooth
- zabezpečení v mobilních sítích
  - GSM, UMTS, LTE, LTE-A
- zabezpečení VoIP komunikace



# Když náhodou zbude čas...

- IBE – Identity Based Encryption
- Steganografie
- Digitální vodoznaky
- Kvantová kryptografie a postkvantová kryptografie (PQC)
- Teorie informace
- Teorie výpočetní složitosti
- Generátory pseudonáhodných posloupností
- Zero-knowledge protokoly
- TOR
- Zabezpečení v IoT
- Legislativa
  - Národní - ZoSVDP, ZoKB
  - EU – eIDAS, GDPR, NIS, CyberSecurity Act



# Zdroje

---

## Coursera:

- <https://www.coursera.org/learn/crypto>
- <https://www.coursera.org/learn/crypto2>
- <https://www.coursera.org/specializations/introduction-applied-cryptography>
- <https://www.coursera.org/specializations/intro-cyber-security>



## 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
- Burda K., Aplikovaná kryptografie, VUTIUM, 2013, ISBN: 978-80-214-4612-0
- Burda K. "KRYPTOGRAFIE OKOLO NÁS", Edice CZ.NIC – zdarma ke stažení <https://knihy.nic.cz/>



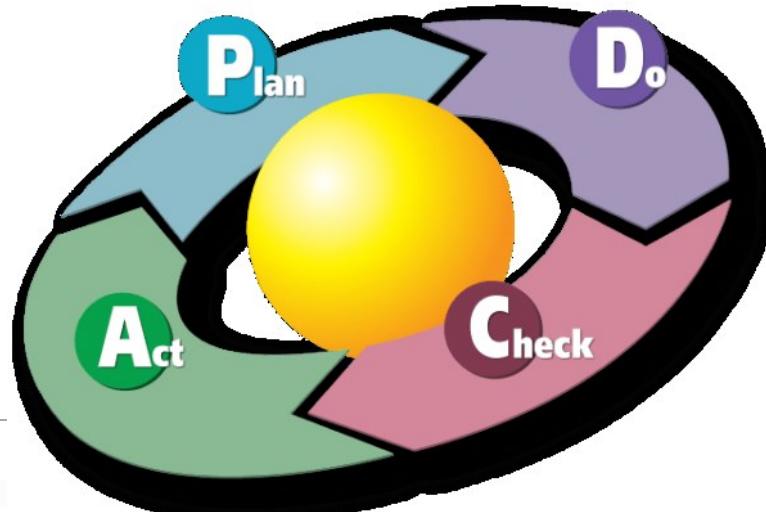
# Co je a co není informační bezpečnost

## NENÍ

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

## JE

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





# 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



# 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

## Krytonalýza (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, 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)

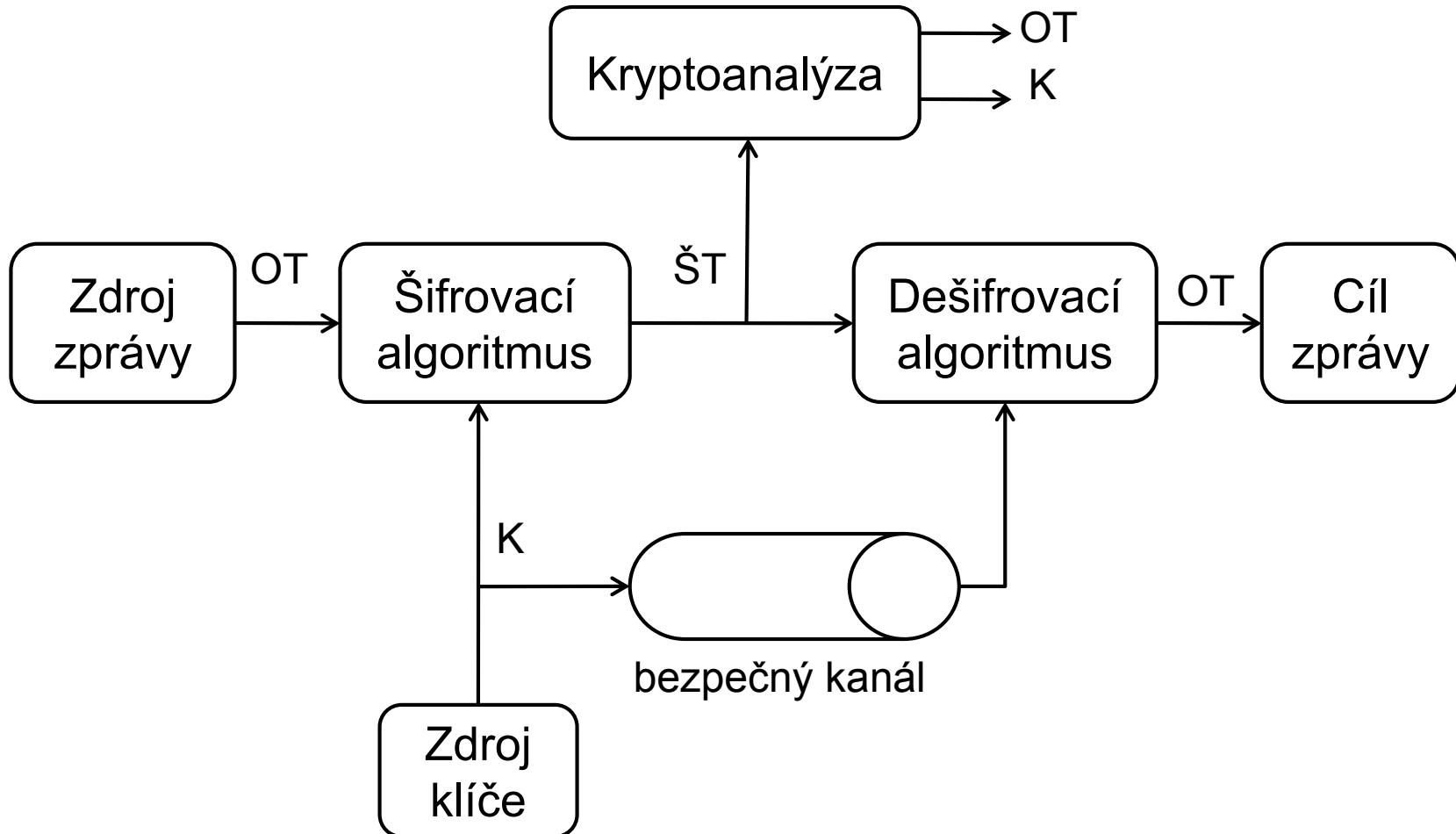
## Nejednoznačná terminologie

- **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





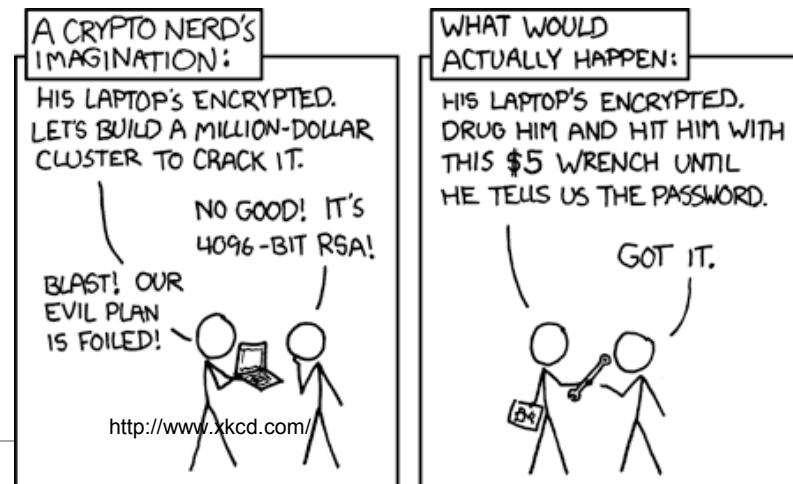
# KRYPTOANALÝZA

- 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
- Budeme řešit na cvičeních...velmi jednoduché příklady



# Terminologie - Kryptoanalýza

- útok hrubou silou (brute-force)
  - prohledání celého prostoru klíčů
  - nejjednodušší útok
  - složitost je úměrná množství klíčů
  - předpokládáme, že jsme schopni detektovat 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



# Modely útočníků

- Ciphertext-only attack (COA)
  - Útočník zná jeden nebo více šifrových textů.
- Known-plaintext attack (KPA)
  - Útočník zná jeden nebo více párů ŠT a OT.
- Chosen-plaintext attack (CPA)
  - Útočník volí otevřené texty a dovídá se šifrové texty.
- Chosen-ciphertext attack (CCA)
  - Útočník volí šifrové texty a dovídá se otevřené texty.
  - Někdy se navíc předpokládá, že útočník může zároveň volit i otevřené texty a dovídат se šifrové texty.
- Všechny šifrové texty vznikají použitím stejného klíče



## Cíle útočníků

---

- Key recovery attack
  - Určit použitý klíč.
- Plaintext recovery attack
  - Dešifrovat nějaký šifrový text.
- Zjistit jen jeden bit klíče nebo otevřeného textu nebo jiný údaj o klíči nebo otevřeném textu.
- Distinguishing attack
  - Poznat, zda se jedná o šifrový text nebo o náhodná data.
- Od dobré šifry požadujeme, aby bez znalosti klíče byla při CPA i CCA nerozlišitelná od náhodně zvoleného prostého zobrazení  $P \rightarrow C$ .



# 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 (holandský 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

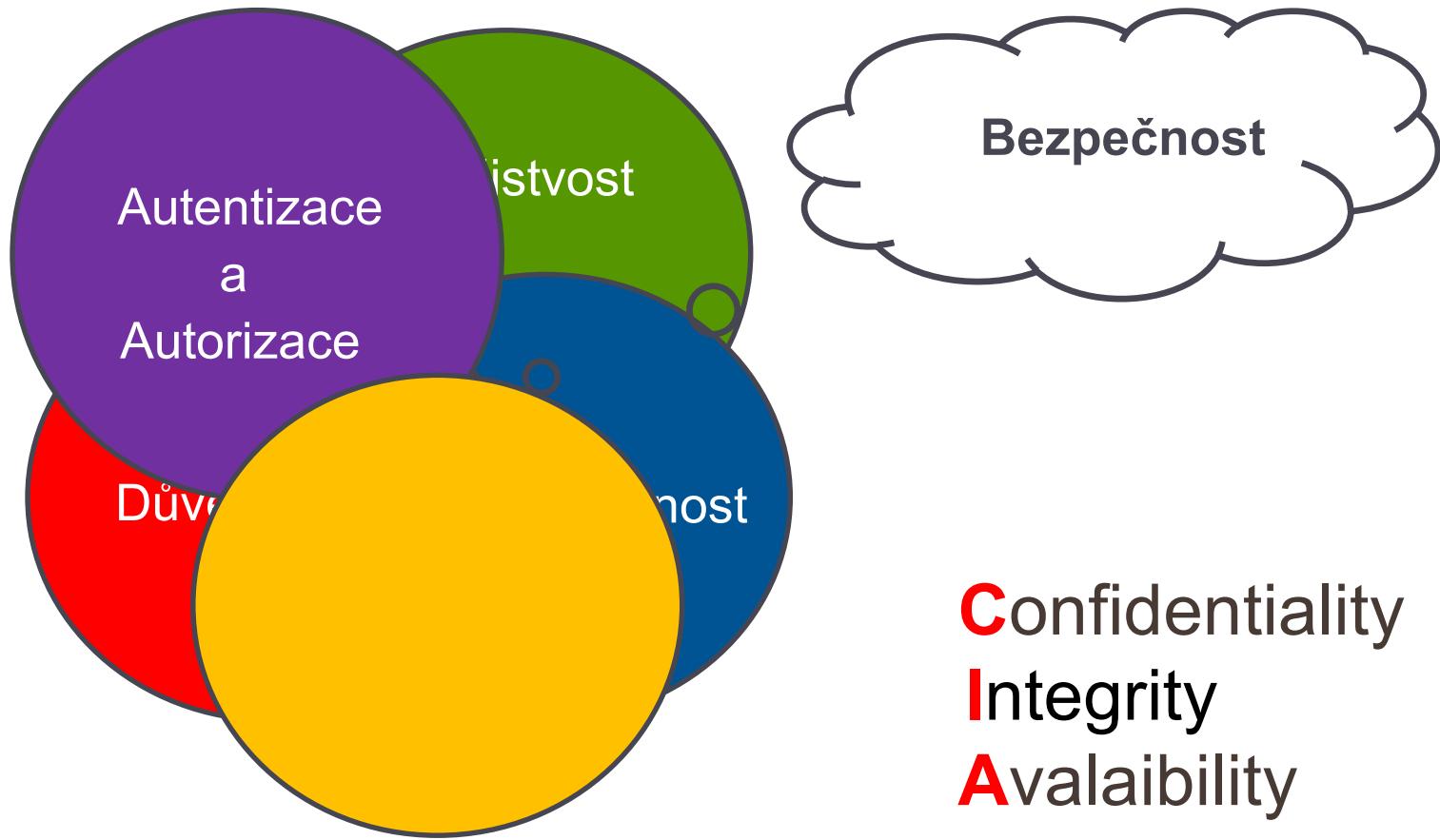
- V dnešní době je většina informací vytvářena, udržována, a přenášena v elektronické podobě.
- Informace mohou být cílem různých útoků, které souvisí s elektronickou povahou dat a proto je přenášená data nezbytné chránit.
- Existuje několik základních cílů, které je potřeba splnit, aby byl systém manipulující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

**Jaké jsou základní cíle?**

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



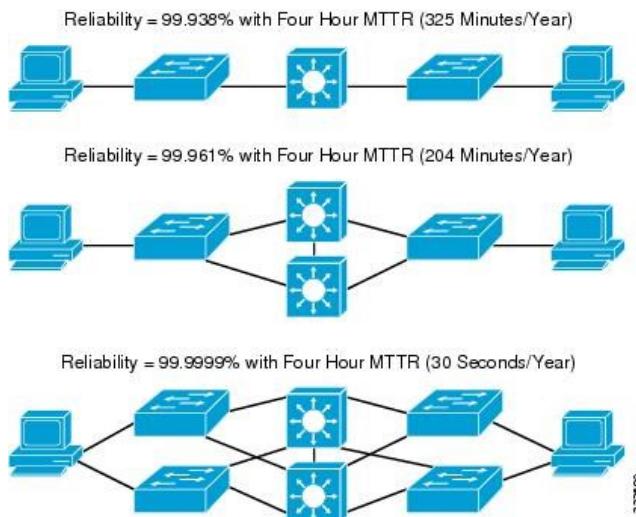
# Základní cíle informační bezpečnosti





# Základní pojmy - Dostupnost

- EN - Availability
- 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.

Příklad: CHAP, EAP, 802.1x



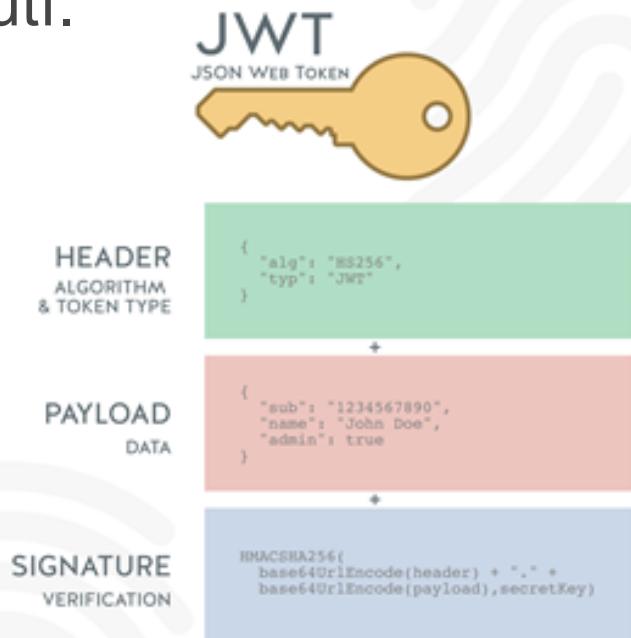


# Základní pojmy - Autorizace

- EN - Authorization
- Oprávnění přístupu k systémovým zdrojům.
- V průběhu autorizace se určuje k jakým zdrojům má uživatel přístup.
  - Výsledkem je povolení či zamítnutí.

## Příklad: OAuth2

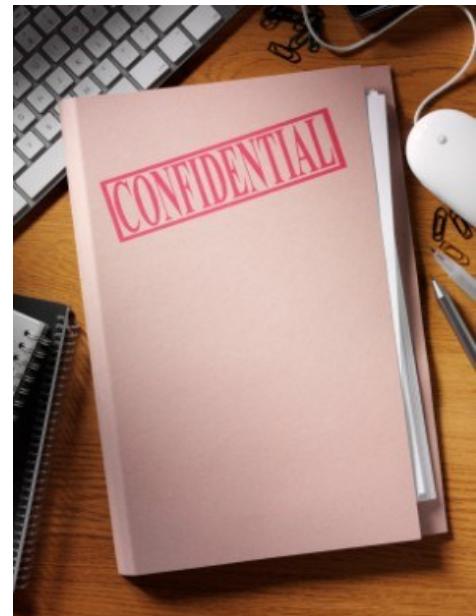
Autorizaci téměř vždy  
předchází autentizace!





## Základní pojmy – Utajení, Důvěrnost

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





# Šifry – rozdělení

## 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 – rozdělení

## 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



## Základní pojmy - Integrita

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

Příklad: SHA-3, Whirlpool



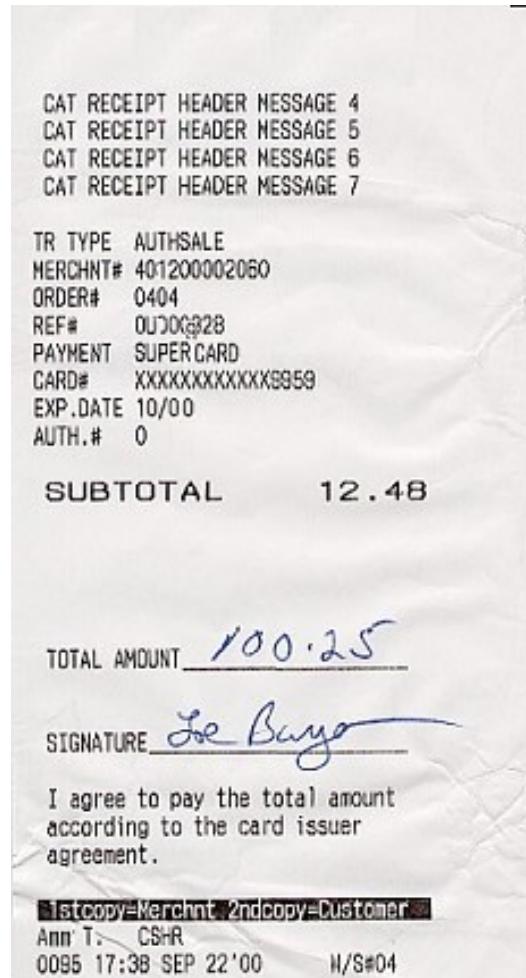


## Základní pojmy - Nepopiratelnost

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

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.





# 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.



# Kryptografie v průběhu času několik zajímavostí





---

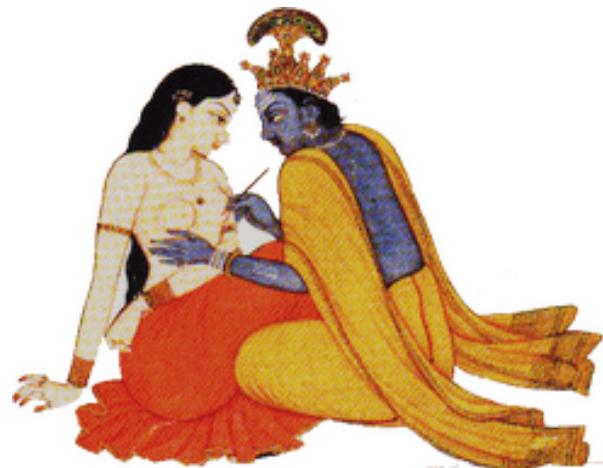
První zaznamenaný výskyt slova **kryptografie** je v knize sira Thomase Browna „The garden of Cyrus“ z roku 1658.

<http://penelope.uchicago.edu/gardennoframes/gardenn.html>  
[http://en.wikipedia.org/wiki/The\\_Garden\\_of\\_Cyrus](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 kryptosystémů
  - „kauṭiliyam“
  - „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 prolamitelná
- monoalfabetická substituční šifra
- kryptoanalýza pomocí frekvenční analýzy
- $C_i = E(P_i + 3) \text{ mod } 26$
- $P_i = D(C_i - 3) \text{ mod } 26$





## Jeffersonův válec - 1790

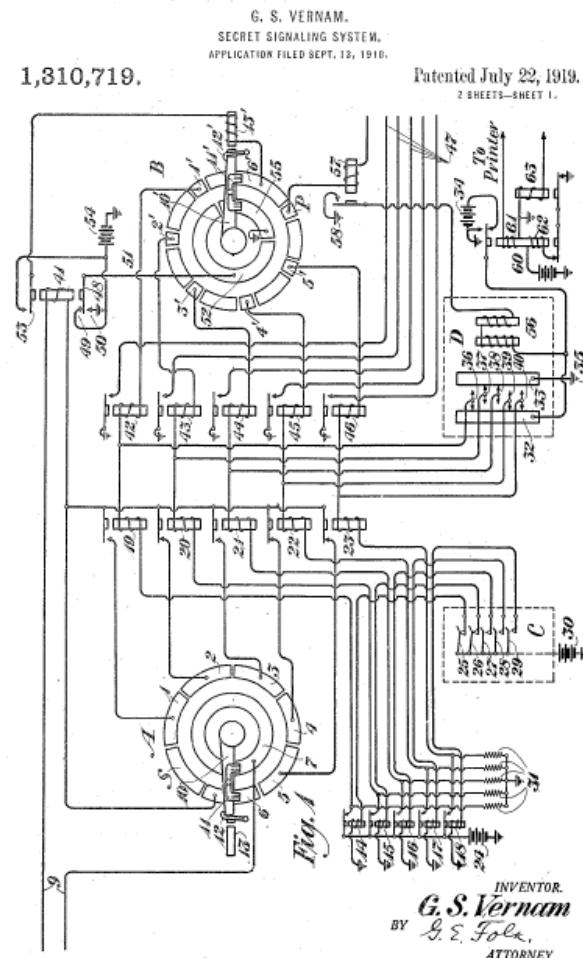
- Thomas Jefferson
- 36 válečků nasunutých na osu
- po obvodu jednotlivých válečků jsou různým způsobem zapsané abecedy.
- celkem  $36! \times 26! \sim 1,5 \cdot 10^{68}$  kombinací





# 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

### Klíč nelze použít opakováně.

- podmínka vychází z předchozí, protože opakováný klíč není náhodný
- dostane-li útočník do ruky dvě zprávy zašifrované stejným klíčem, má často velmi snadnou cestu k rozluštění



## 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 – princip

1/3

**Šifrování:  $OT \oplus Klíč = ŠT$**

	k	i	l	l	h	i	t	l	e	r
OT:	011	010	100	100	001	010	111	100	000	101
klíč:	101	111	000	101	111	100	000	101	110	000
ŠT:	110	101	100	001	110	110	111	001	110	101
	s	r	l	h	s	s	t	h	s	r

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111



## Vernamova šifra – princip

2/3

Zpráva zachycena a útočník předpokládá použití klíče „**klíč**“, který není shodný s původním:

	s	r		h	s	s	t	h	s	r
ŠT:	110	101	100	001	110	110	111	001	110	101
klíč:	111	101	110	101	111	100	000	101	110	000
OT:	001	000	010	100	001	010	111	100	000	101
	h	e	i		h	i	t		e	r

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111



## Vernamova šifra – princip

3/3

Příjemce zachytí zprávu a domnívá se že klíč je „klíč“:

	s	r		h	s	s	t	h	s	r
ŠT:	110	101	100	001	110	110	111	001	110	101
klíč:	111	101	000	011	101	110	001	011	101	101
OT:	001	000	100	010	011	000	110	010	011	000
	h	e		i	k	e	s	i	k	e

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111



## Vernamova šifra – princip

---

- Modrý klíč – Kill Hitler
- Červený klíč – Heil Hitler
- Oranžový klíč – He likes Ike

**Oázka: Lze poznat, který z textů je ten pravý?**



# Dotazy

---

