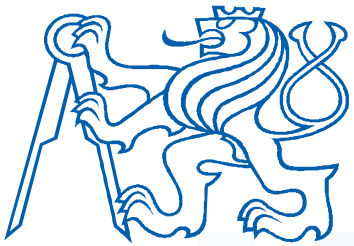
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

A7B32KBE 1. přednáška

Úvod do kryptologie, základní pojmy

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



Osnova

- úvod do kryptologie, základní pojmy, historický vývoj
- teorie informace
- teorie výpočetní složitosti
- moderní blokové symetrické kryptosystémy – AES, RC6, MARS, Blowfish, Camelia,…
- režimy činnosti blokových šifer – ECB,CBC,OFB,CFB,CTR, XTR
- moderní proudové symetrické kryptosystémy – RC4, A5, E0, projekt eSTREAM
- asymetrické kryptosystémy - IFP, DLP, ECDLP
- hashovací funkce - MD5, SHA-1, SHA-2, Whirlpool, Tiger
- bezpečnostní problémy hashovacích funkcí, projekt SHA-3
- generátory pseudonáhodných posloupností

Osnova

- autentizační protokoly - RADIUS, Kerberos, DIAMETER, Tacacs
- všesměrové autentizační protokoly – BiBA, TESLA, TIK
- protokoly s nulovým rozšířením informace – Fiat-Shamir
- IPsec (AH,ESP,IKE, ISAKMP)
- SSL/TLS, WTLS, DTLS
- Steganografie
- Digitální vodoznaky
- Kvantová kryptografie
- Zabezpečení protokolů pro VoIP komunikaci - SIP, H.323, IAX, Skype
- Zabezpečení v datových sítích – IEEE 802.3, IEEE 802.11, IEEE 802.15, IEEE 802.16

Osnova

- Zabezpečení v mobilních sítí GSM, UMTS
- Elektronický podpis
- Časová razítka
- Certifikační autority

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/
- Levický D., Kryptografia v informačnej bezpečnosti, elfa, 2005,ISBN:80-8086-022-X
- 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

Literatura ostatní

- Přibyl J.: *Informační bezpečnost a utajování zpráv,* ČVUT, 2004, ISBN: 80-01-02863-1
- Dostálek L. a kol., *Velký průvodce protokoly TCP/IP - Bezpečnost,* Computer Press, 2003, ISBN: 80-7226-849-X
- 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

"If you think cryptography can solve your problem, then you don't understand your problem and you don't understand cryptography."

Bruce Schneier

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 pojmy

Kryptologie (Cryptology)

- vědní obor zahrnující kryptografii a kryptoanalýzu

Kryptografie (Cryptography)

- návrh a konstrukce kryptografických algoritmů a způsoby jejich využívání

Kryptonalýza (Cryptanalysis)

- zabývá se metodami získávání otevřeného textu z textu šifrového **bez znalosti klíče**
- zkoumá odolnost a zranitelnost kryptosystémů

Základní pojmy

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

- **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

Kryptografický algoritmus (šifrovací algoritmus, kryptosystém, šifra / cryptographic algorithm, encryption algorithm, cryptosystem, cipher)

- 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 nebo transformováno na klíč

Passphrase

- použití jako heslo, ale skládá se ze sekvence slov

Terminologie

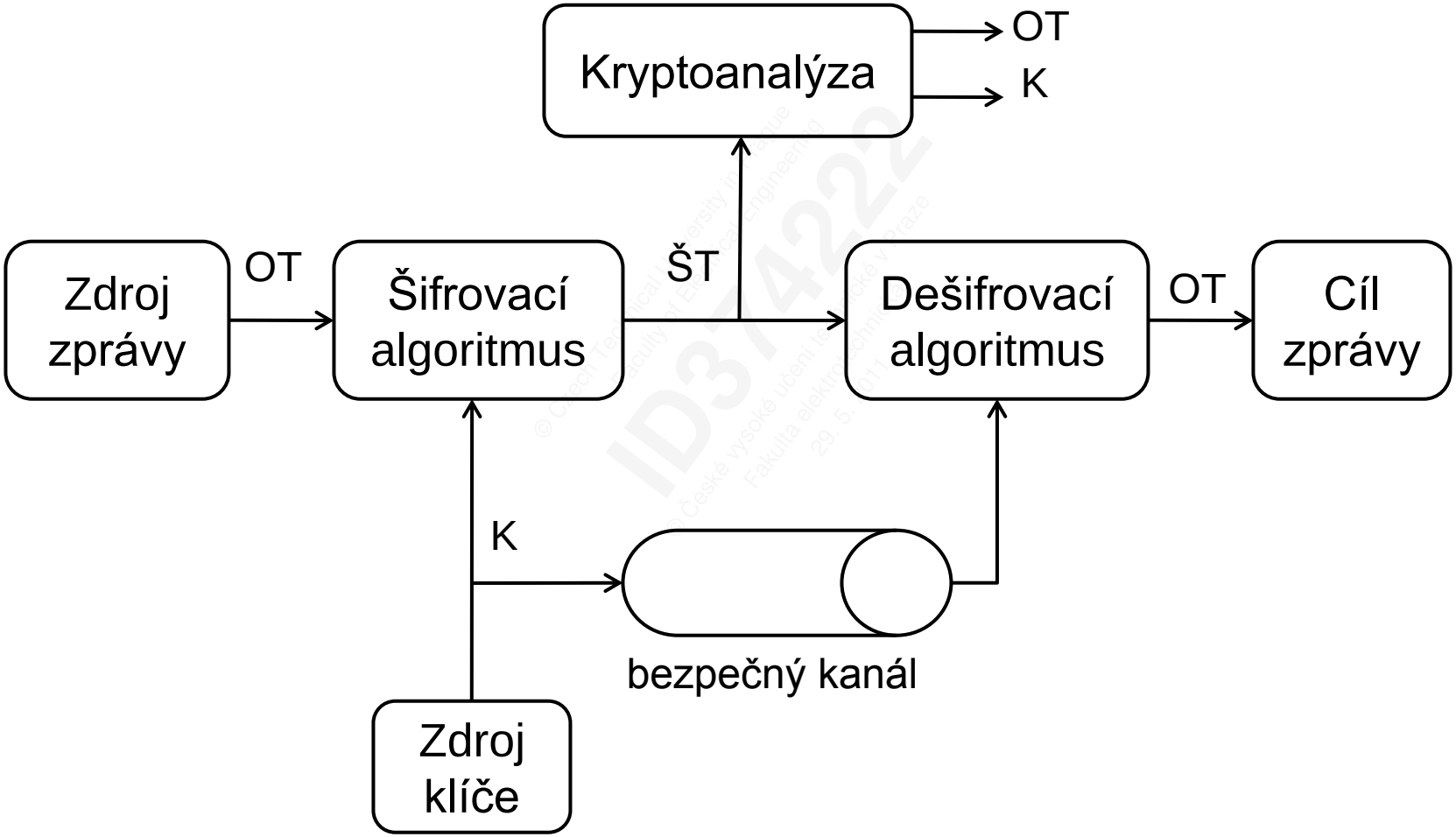
- **symetrická šifra** / symmetric key cryptosystem – kryptografický algoritmus, který pro šifrování i dešifrování používá tentýž klíč*
- **asymetrická šifra /** public key cryptosystem – kryptografický algoritmus, který používá dva odlišné klíče, jeden pro šifrování a jeden pro dešifrování
- **veřejný 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

Terminologie

- Šifra se používá k šifrování otevřeného textu
- Výsledkem šifrování je šifrový text (ŠT)
- Dešifrováním získáme zpět ze šifrového textu text otevřený.
- Klíč slouží k jedinečnému nastavení šifrovacího algoritmu.
- Symetrický kryptosystém používá stejný klíč k šifrování i dešifrování.
- Asymetrický kryptosystém používá šifrování a dešifrování dva různé klíče - veřejný klíč a soukromý klíč.

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

Kryptoanalýza - kategorie útoků na kryptosystém

Útok se znalostí	Útočník má k dispozici	
Pouze ŠT	- ŠT + šifrovací algoritmus	Pasivní útočník
Pouze ŠT a OT	- ŠT + šifrovací algoritmus - jeden nebo více párů ŠT-OT svázaných klíčem K	
Vybraných OT	- ŠT + šifrovací algoritmus - kryptoanalytikem vybrané OT spolu s odpovídajícími zašifrovanými ŠT	Diferenciální kryptoanalýza

Kryptoanalýza

Útok se znalostí	Útočník má k dispozici	
Adaptivních vybraných OT	- ŠT + šifrovací algoritmus - kryptoanalytikem vybrané OT spolu s odpovídajícími zašifrovanými ŠT - kryptoanalytik může OT modifikovat na základě výsledků předchozího šifrování	Aktivní útočník - nestojí vně systému, ale je jeho součástí
Vybraných ŠT	- ŠT - algoritmus - údajné ŠT zvolené kryptoanalytikem a k němu příslušející dešifrované OT	Algoritmy veřejného klíče
Vybraných OT a ŠT	- ŠT + šifrovací algoritmus - kryptoanalytikem vybrané OT spolu s odpovídajícími zašifrovanými ŠT - údajné ŠT zvolené kryptoanalytikem a k němu příslušející dešifrované OT	

Kryptoanalýza

- útok hrubou silou (brute-force)
- prohledání celého prostoru klíčů
- nejjednodušší útok
- složitost je úměrná množství klíčů
- předpokládáme, že jsme schopni detekovat nalezení OT
- vzorec pro odhad pravděpodobnosti úspěchu útoku hrubou silou

$$\text{Prob}(x) = \frac{\text{čas platnosti hesla} \bullet \text{počet odhadů za jednotku času}}{(\text{velikost abecedy})^{\text{délka hesla}}}$$

- rubber-hose (pendreková) 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

Kryptoanalýza – postranní kanály

- „alternativní“ způsoby útoků na kryptosystém
- neútočí se na samotný algoritmus, ale jeho implementaci

Klasické postranní kanály:

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

- lze realizovat i adaptivní postranní kanály

Nepodmíněná a výpočetní bezpečnost

Nepodmíněná bezpečnost

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

Výpočetní bezpečnost

- Cena za prolomení šifry přesahuje cenu chráněné informace
- Čas nutný k prolomení šifry přesahuje dobu životnosti chráněné informace

Kerchoffův princip

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

Základní předpoklad při konstrukci kryptosystémů:

- útočník zná celý kryptosystém
- pouze klíč je tajný
- kryptografické algoritmy nejsou tajné

Proč by měl tento předpoklad platit ?

- utajované algoritmy nikdy nezůstanou navždy tajné
- praxe ukazuje, že v utajovaných algoritmech jsou po odhalení často nalezeny bezpečnostní chyby
- je lepší odhalit chyby dříve nežli později…

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/

Základní pojmy - Autentizace

- 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

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

Základní pojmy - Utajení

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

Základní pojmy - Integrita

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

Základní pojmy - Nepopiratelnost

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.

Prostředky používané k dosažení základních cílů:

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

Kódy

- jedna z metod klasické kryptografie
- systém pro ukrytí smyslu zprávy, nahrazující slovo nebo skupinu slov jiným znakem nebo skupinou znaků
- základní princip kódu - nahrazování delších slovních spojení (věty) kratšími (slova).
- seznam nahrazení obsahuje **kódová kniha**
- kódová kniha obsahuje odpovídající si dvojice OT a ŠT
- **Příklad kódu:** pošlete banány = ráno zaútočte

KÓD ≠ ŠIFRA

Šifry - klasické šifry

- 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

- Produktové šifry
  - Šifra obsahující jak substituční tak transpoziční část

Šifry - symetrické algoritmy

Proudové šifry (Stream ciphers)

- pracují na principu Vernamovy šifry
- relativně krátký klíč
- z klíče je odvozen dlouhý proud klíče (keystream)
- proud klíče se pak používá jako heslo do Vernamovy šifry

+ rychlost
+ snadnější implementace v HW
+ malé šíření chyb

- malá úroveň difuze
- náchylné k úmyslným modifikacím

Šifry - symetrické algoritmy

Blokové šifry (Block ciphers)

- klíč blokové šifry určuje konkrétní kódovou knihu, podle které se bude šifrovat
- každý klíč vede k jiné kódové knize
- používají jak konfuzi, tak difuzi

+ difuze
+ imunita vůči narušení
+ lze je provozovat i jako proudové (CFB,OFB, CCMP)

- zpoždění
- šíření chyb

Šifry - asymetrické algoritmy

Tři základní skupiny podle příslušného „těžkého problému“ na jehož obtížnosti závisí bezpečnost celého kryptosystému.

- **Integer Factorization Problem (IFP)**
- **Discrete Logaritm Problem (DLP)**
- **Elliptic Curves DL Problem (ECDLP)**

Hashovací funkce

Vstup: posloupnost libovolné délky

Výstup: posloupnost konstantní délky (typicky stovky bitů)

nazývá se - haš, haše, hash, hashový kód, otisk zprávy

Známé hashovací funkce: MD-5, SHA-1, SHA-2, RIPEMD-160, Whirlpool…

Použití: detekce narušení integrity

Historie

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

Kámasútra

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

Skytale

- 7 st. př.n.l.
- 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
- $C_i = E(P_i + 3) \mod 26$
  $P_i = D(C_i - 3) \mod 26$

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 těle

Středověká kryptologie

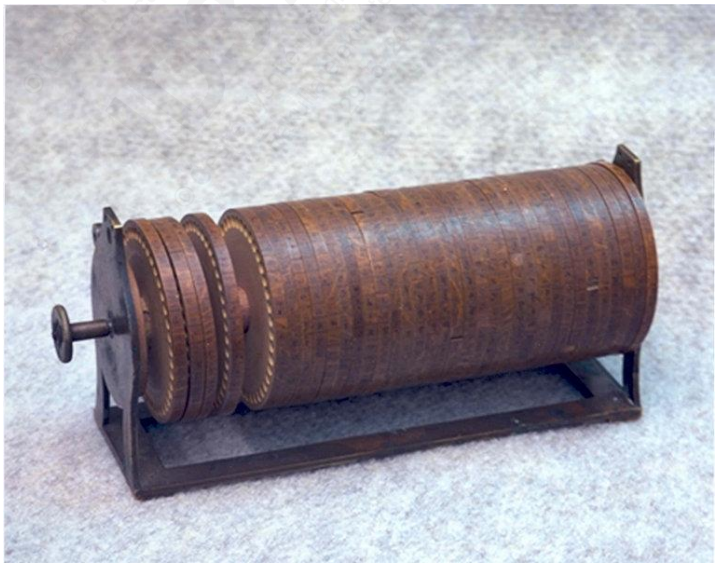
- 855 n.l. Abú Bakr Ahmad
  - arabský matematik
  - popis několika šifrových systémů (jednoduchá záměna)
  - jeden používán ještě v 2.pol koncem 18.st.
- 9. století n.l.
  - Abú Júsuf Ja'qub ibn Išáq al-Kindí
  - arabský všestranný vědec (matematik,fyzik, hudebník…)
  - první popis FA
  - "*Rukopis o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

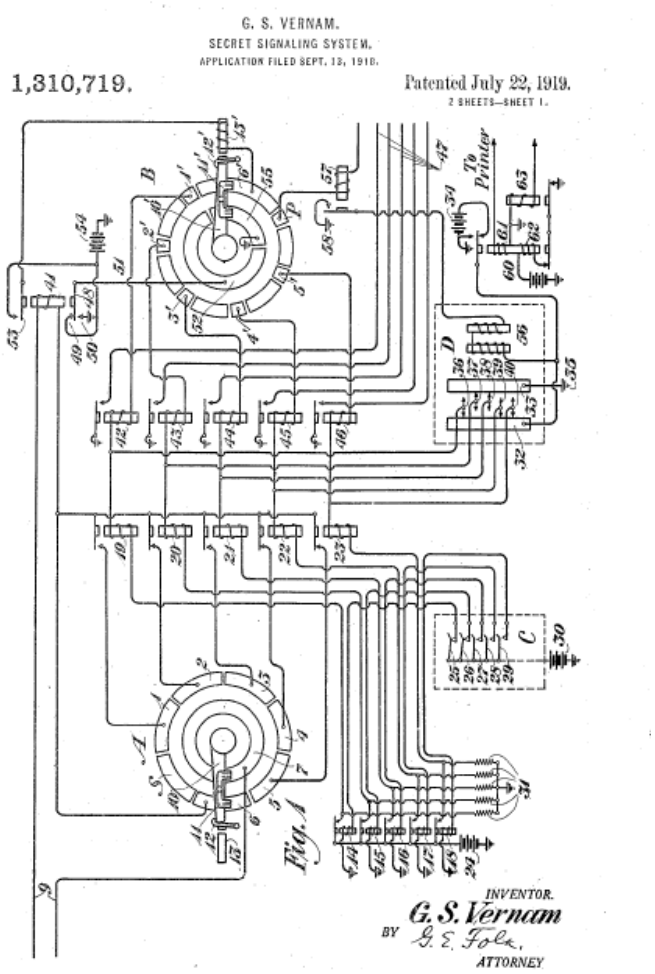
Jeffersonův válec - 1790

- 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 – princip 1/3

Šifrování: OT ⊕ Klíč = ŠT

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

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

Vernamova šifra – princip

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

	s	r	l	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	**l**	**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 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

2. sv. válka - NAVAJO

- řeč indiánů kmene NAVAJO u americké námořní pěchoty k předávání tajných zpráv rádiem
- velmi málo mluvčích
- nepodařilo se nikdy prolomit
- používán ještě ve válce v Severní Koreji i dokonce i ve Vietnamu
- zveřejněno až koncem 60.let

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