Kam kráčís, Kryptografie?

Diskuse o současné teoretické i aplikované kryptografii.

Libor Dostálek <dostalek@prf.jcu.cz>
Jan Dušátko <jan@dusatko.org>
Dominik Pantůček <dominik.pantucek@trustica.cz>
Pavel Vondruška <pavel.vondruska@crypto-world.info>

6. 10. 2018

Program

- Úvod
- Představení účastníků
- Panelová diskuse
- Dotazy z publika

Úvod

- Kryptografie je zde od dávnověku
- Kryptografie se stále rozvíjí
- Kryptografie je dnes základním pilířem digitální ekonomiky
- Kryptografie má velmi zajímavou budoucnost
- Kryptografie má různé aspekty

Kam kráčíš, Kryptografie

Diskuse o současné teoretické i aplikované kryptografii.

Libor Dostálek <dostalek@prf.jcu.cz>

Jan Dušátko <jan@dusatko.org>

Dominik Pantůček <dominik.pantucek@trustica.cz>

Pavel Vondruška <pavel.vondruska@crypto-world.info>

6. 10. 2018

Představení: Jan Dušátko

Kryptonadšenec

- Kryptografii se začal věnovat díky článkům Vlastimila Klímy v časopise Chip (1995)
- Drobné zkušenosti s IT počínaje EC 1021, Sinclair ZX Spectrum a Commodore C-64

Kryptografie:

- přehled a porovnání šifrovacích módů
- přehled a porovnání autentizačních mechanismů
- snaha o evangelizaci a propagaci kryptografie – Cryptosession
  https://cryptosession.cz

Módy užití blokových algoritmů

Generace	Popis	Vysvětlení
1	Ad-hoc	Návrh módů dle nejlepších snah autorů
2	Security proved	Doložena matematická analýza bezpečnosti
3	AE (Authenticated Encryption)	Šifrování s ověřením
4	AEAD (Authenticated Encryption with Associated Data)	Šifrování s ověřením a přidanými daty

Další členění:

Format Preserving Mode

Zajišťuje šifrování pouze zvoleného rozsahu otevřeného textu, zbytek struktury zůstává zachován.

Arbitrary Block Length (ABL)

Variabilní délka bloku, může odpovídat i délce celé zprávy.

Tweaked

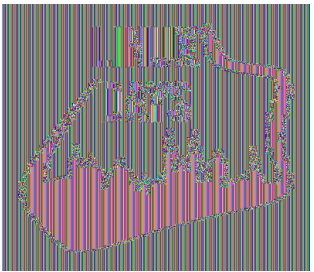
Každý blok má vlastní modifikátor.

ECB mód (nepoužívá se)

ECB (Electronic Code Book)

- každý blok je šifrován stejným klíčem
- maximální bezpečný objem 1 blok

ECB

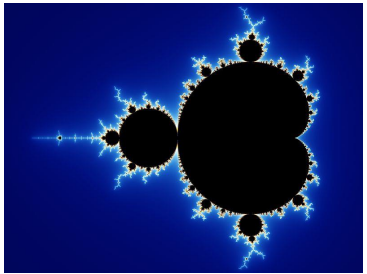


OFB mód (nepoužívá se)

OFB (Output Feedback)

- podobnost s OFB modem je možné najít při generování Juliových (Gaston Maurice Julia) nebo také Mandelbrotových (Benoit Mandelbrot) fraktálů
- velikost bezpečného objemu šifrovaných dat je nepředvídatelná

Mandelbrotův fraktál



OFB

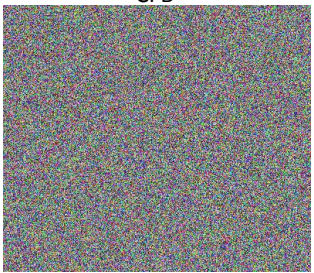
Mody CBC (používá se), CFB (nepoužívá se)

CBC (Cipher Block Chaining) a CFB (Cipher Block Feedback)

- pro výpočet odolnosti proti kolizi se používá šířka blokové šifry N
- platí, že odolnost odpovídá $(N/8)*2^{N/2}$
- 64b blok: $8*2^{64/2}$= 32GB
- 128b blok: $16*2^{128/2} = 2.7*10^{8}$TB

CBC

CFB



Mody CCM, GCM – čítačové módy s ochranou

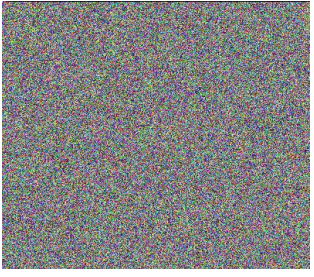
GCM (Galois Counter Mode) a CCM (Counter mode with Cipher Chaining Mode-MAC)

- změna klíčů pro GCM doporučena nejdéle po 2^{32}Bloků – 16 Bloků ~ 64 GB dat
- změna klíčů pro CCM doporučena nejdéle po 2^{32} Bloků – 1Bblok ~ 64 GB dat
- autentizační tag je pro CCM i GCM 128b
- autentizační tag pro CCM_8 má délku pouze 64b

LINUX DAYS

GCM

CCM

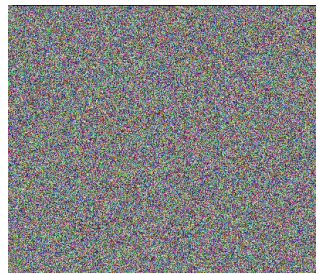


Mody IAPM, OCB – oblíbené komunitou

IAPM (Integrity Aware Parallelization Mode) a OCB (Offset Code Book)

- OCB je založen na IAPM.
- inicializační vektor (IV) se používá pro generování syntetického čítače (IAPM), což znamená možnost šifrovat maximálně 2^{64} bloků
- změna klíčů pro IAPM i OCB doporučena nejdéle po 2^{32}B =64GB dat

IAPM



OCB

Mod XTS a EME^2 – šifrování disků

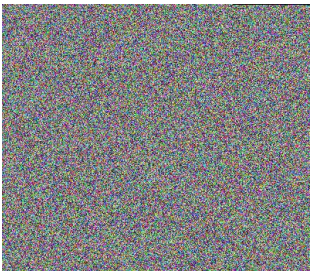
XTS (XEX-based tweaked-codebook mode with ciphertext stealing)

- nemá kontrolu integrity, proto standard vynucuje použití spolu s HMAC
- vyžaduje dvojnásobnou délku klíče
- vyžaduje 2 volání algoritmu na zpracování jednoho bloku dat

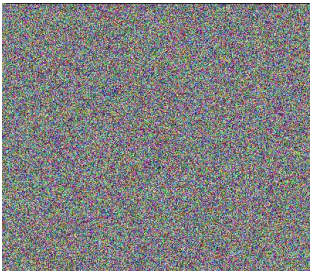
EME^2 (ECB-Mix-ECB with AEAD)

- jedná se o AEAD algoritmus s variabilní délkou bloku (ABL)
- interně vyžaduje 2,5 volání algoritmu na zpracování jednoho bloku dat
- vyžaduje trojnásobnou délku klíče

XTS



EME^2



Přehled

				Bezpečný objem pro algoritmy	
Název	**Generace**	**Použití**	**Vznik**	**bloky 64-bit**	**bloky 128-bit**
ECB	ad-hoc	obecné[1]	není známo	1 blok	1 blok
OFB	ad-hoc	obecné	1980	Nepředvídatelný	nepředvídatelný
CBC	ad-hoc	obecné	1976	2^{32}	2^{64}
CFB	ad-hoc	obecné	1980	2^{32}	2^{64}
CTR	ad-hoc	obecné	1979	2^{32} -1 blok	2^{32} -1 blok
CCM	AEAD	obecné	2011	N/A	2^{32} -1 blok
GCM	AEAD	obecné	2005	N/A	2^{32}-16 bloků
IAPM	AEAD	obecné	2000	N/A	2^{32} -1 blok
OCB	AEAD	obecné	2001	N/A	2^{32} -1 blok
XTS	druhá generace	disky	2007	N/A	Neznámé
EME²	AEAD/ABL	disky	2004	N/A	Neznámé
ChaCha20	*proudová šifra*	*obecné*			*256GB*

Kam kráčíš, Kryptografie

Diskuse o současné teoretické i aplikované kryptografii.

Libor Dostálek <dostalek@prf.jcu.cz>
Jan Dušátko <jan@dusatko.org>
Dominik Pantůček <dominik.pantucek@trustica.cz>
Pavel Vondruška <pavel.vondruska@crypto-world.info>

6. 10. 2018

Představení: Pavel Vondruška

1) MFF UK (vystudoval a od roku 2005 přednáším)
2) Kryptolog a kryptoanalytik … (… ☺ ….)
3) Elektronický podpis (ÚOOÚ …)
4) Certifikační autorita
5) Crypto-World 1999-2014
6) Nyní: Senior specialista bezpečnosti pro řízení PKI a bezpečnostní ředitel pro ochranu utajovaných informací ve společnosti CETIN
7) SSKB (člen výboru)
8) (eIDAS… MV ČR /)

CETIN ČESKÁ TELEKOMUNIKAČNÍ INFRASTRUKTURA

Vítejte na crypto-world.info

Crypto-World | Crypto - News | Security - News

Kniha o šifrování

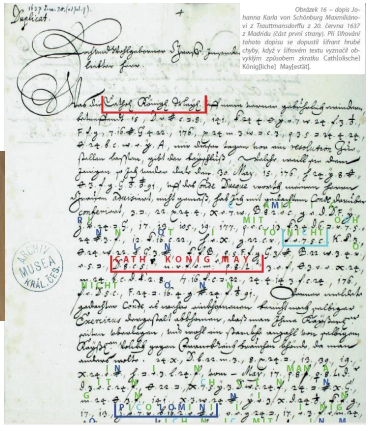
Crypto-World
ISSN 1801-2140

1001101001 = ???
dlrow-otpyrc= ???

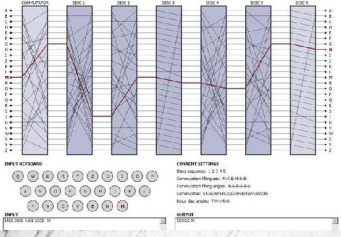
SOUTĚŽE

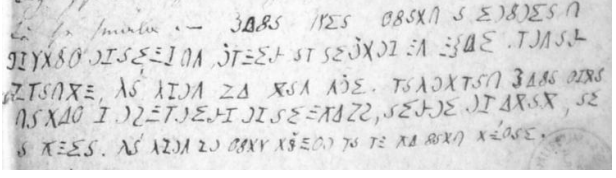
Soutěže 2000-2013

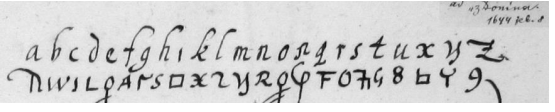
Dálnopisný stroj D-302 „Dalibor“ vyráběný ve Zbrojovce Brno



Obrázek 16 – dopis Johanna Karla von Schönburg Waxenštejn-ví z Trautmansdorfu z 20. června 1637 z Madridu (část první strany). Při šifrování tohoto dopisu se dopustil chyby, když v šifrovém textu vynechal obvyklým způsobem zkratku Catholicissimi Königl[iche] Mayf[estät].







ECSC 2018 - European Cyber Security Challenge

Evropské finále kybernetické soutěže (ECSC) se uskuteční ve dnech 14. až 18. října 2018 v Londýně.. Letošní ročník organizovala UK Cybersecurity Challenge pod záštitou Evropské agentury ENISA. Evropského finále se zúčastní 20 národních týmů z celé Evropy.

Kdo vlastně „chce“ kryptografii - 2000

1) NBÚ , Zákon č. 148/198 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, UI, http://www.nbu.cz/
2) ÚOOÚ, Zákon o elektronickém podpisu 227/2000 Sb. (Směrnice 1999/93/ES) http://uoou.cz/
3) ÚOOÚ, Zákon o ochraně osobních údajů 101/2000 Sb. http://uoou.cz/
4) MPO, Zákon o telekomunikacích 151/2000 Sb. http://www.mpo.cz/
5) MPO, Zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, dosavadní závaznost norem ČSN byla ukončena k 31.12.1999, tvorbou pověřen Český normalizační institut

Kdo vlastně „chce“ kryptografii - 2018

1) NBÚ , Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, UI, http://www.nbu.cz/
2) MV ČR, nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, které je známo pod zkráceným názvem „nařízení eIDAS“ a také související právní úpravě oblasti služeb vytvářejících důvěru dle zákona č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce. http://www.mvcr.cz/ , http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx
3) NÚKIB, Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), https://www.govcert.cz/
4) ÚOOÚ, Nařízení (EU) 2016/679 (GDPR), 25.5.2018, http://uoou.cz/
5) MPO, Předpis č. 127/2005 Sb., Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) https://www.mpo.cz/cz/e-komunikace-a-posta/elektronicke-komunikace/narodni-legislativa-a-predpisy/zakon-o-elektronickych-komunikacich--37746/
6) **Zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů** byl mnohokrát novelizován, poslední změna je účinná od 1.9.2017, zabezpečení tvorby norem převzal od 1.1.2009 Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ)

https://www.enisa.europa.eu/news/enisa-news/cross-recognition-of-national-eid-schemes-in-the-eu

enisa European Union Agency for Network and Information Security

TOPICS NEWS PUBLICATIONS EVENT 10

NEWS ITEM

Cross recognition of national eID schemes in the EU: one-step forward

As from 29 September 2018, the eIDAS Regulation creates new impetus across EU Member States (MS) as the latter will be obliged to recognise national systems of other MS, which have been notified to the European Commission and comply with eIDAS.

Published on September 29, 2018

ECRYPT CSA

H2020-ICT-2014 – Project 645421

ECRYPT – CSA

ECRYPT – Coordination & Support Action

D5.4

Algorithms, Key Size and Protocols Report (2018)

Due date of deliverable: 28 February 2018
Actual submission date: 28 February 2018

Příloha č. 3 k vyhlášce č. …/2018

Minimální požadavky na kryptografické algoritmy

(1) Symetrické algoritmy

a) Blokové a proudové šifry

1. Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů Triple Data Encryption Standard (3DES) s využitím délky klíčů 168 bitů, omezené použití jen se zatížením klíče menším než 10 GB, postupně přecházet na AES.
2. Twofish s využitím délky klíčů 128 až 256 bitů.
3. Serpent s využitím délky klíčů 128, 192, 256 bitů.
4. Camellia s využitím délky klíčů 128, 192 a 256 bitů.
5. SNOW 2.0, SNOW 3G s využitím délky klíčů 128, 256 bitů.
6. ChaCha20.

(2) Asymetrické algoritmy

a) Pro technologii digitálního podpisu

1. Digital Signature Algorithm (DSA) s využitím délky klíčů 3072 bitů a více, délky parametru cyklické podgrupy 256 bitů a více.
2. Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 256 bitů a více.
3. Rivest-Shamir-Adleman Probablistic Signature Scheme (RSA-PSS) s využitím délky klíčů 3072 bitů a více.
4. **Elliptic Curve Schnorr Signature Algorithm (EC-Shnorr) s využitím délky klíče 256 bitů a více**

NÚKIB, Zákon č. 181/2014 Sb. zákon o kybernetické bezpečnosti, **316/2014 - Vyhláška** o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

Post-quantum cryptography …

…. Two NSA Algorithms Rejected by the ISO The ISO has rejected two symmetric encryption algorithms: SIMON and SPECK. These algorithms were both designed by the NSA and made public in 2013. They are optimized for small and low-cost processors like IoT devices. https://eprint.iacr.org/2013/404.pdf

Kam kráčíš, Kryptografie

Diskuse o současné teoretické i aplikované kryptografii.

Libor Dostálek <dostalek@prf.jcu.cz>
Jan Dušátko <jan@dusatko.org>
Dominik Pantůček <dominik.pantucek@trustica.cz>
Pavel Vondruška <pavel.vondruska@crypto-world.info>

6. 10. 2018

Představení: Dominik Pantůček

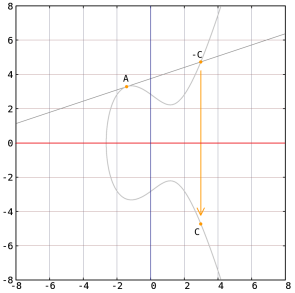
- Teesside University, Trustica
- Grafy: vizualizace, prohledávání
- Matematika: algebra, geometrie, analýza
- Programování: c++, ruby, racket (cokoliv se závorkami)
- Hudba: kompozice, housle, klavír, ukulele, zpěv

- Kryptografie:
  - Problém diskrétního logaritmu (Diffie, Hellman, Schnorr)
  - Eliptické křivky (Weierstrass, Edwards, Montgomery)
  - Návrh a kritika kryptosystémů
  - Vývoj kryptografických zařízení
- Ostatní: nutí Honzu Dušátka do studia matematiky

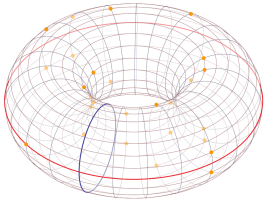
- 2013: Sítě nejsou dokonalé
- 2014: Vyvineme řešení
- 2015: Nevyvineme
- 2017: Vyvineme kryptografický token
- 2018: Vyvinuli jsme a vyrábíme kryptografický token
- Pretty Good Privacy!

- Konečné těleso $GF(p)$, čísla od 0 do $p-1$
- $a \equiv g^s \mod p$, například $2^5 \equiv 9 \mod 23$, neboť $2^5 = 32$ a $\frac{32}{23} = 1 + \frac{9}{23}$
- Exponenciací generátoru g se tvoří grupa, skupina čísel, která se opakuje
- Problém diskrétního logaritmu: známe a, známe g, zjistit $s =?$ je velmi obtížné
- S pomocí této grupy umíme díky existenci tohoto problému:
  - Provést bezpečnou výměnu klíčů – Diffie-Hellman
  - Vytvořit i ověřit digitální podpis – Schnorrův algoritmus (např. DSA)
- Drobný háček: Nejsou to všechna čísla $\in \langle 2, p-1 \rangle$
- Pro grupu o velikosti cca 2^{256} potřebujeme $p \approx 2^{1024}$
- To je moc...

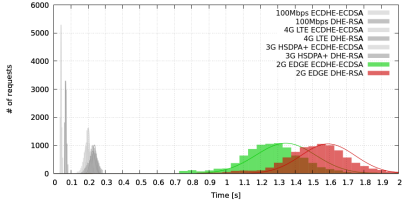
- Eliptické křivky – množiny bodů v rovině, které splňují:
  - $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
  - $y^2 = x^3 + ax + b$
  - $ax^2 + y^2 = 1 + dx^2y^2$
  - $by^2 = x^3 + ax^2 + x$
- Lze definovat operace:
  - Sčítání bodů: $C = A + B$
  - Zdvojení bodu: $C = A + A$
  - Násobení bodu skalárem: $P = G \cdot s$
- Bod – generátor – tvoří grupu bodů, tak jako v $GF(p)$
- Problém diskrétního logaritmu na eliptické křivce:
  - Známe A, známe G, zjistit s =? je velmi obtížné
- To už zde bylo...



- Počítače neumí pracovat se spojitými hodnotami
- Nevadí, použijeme 2D konečné těleso $GF(p)$
- Eliptické křivky – body na anuloidu, které splňují:
  - $y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 \mod p$
  - $y^2 \equiv x^3 + ax + b \mod p$
  - $ax^2 + y^2 \equiv 1 + dx^2y^2 \mod p$
  - $by^2 \equiv x^3 + ax^2 + x \mod p$
- Počet bodů grupy $\approx$ velikost $GF(p)$ – tedy p
- To tu ještě nebylo...



- Telekomunikační sítě občas nemají dobrý den
- Eliptické křivky jsou rychlejší



- Eliptické křivky jsou bezpečnější ...
  - ... nezávisle na NSA.

- Eliptické křivky mají mnoho zajímavostí
- Problém: Poslední dobou *se* hodně mluví o kvantových počítačích
- Řešení: Kryptografické algoritmy na základě podobností eliptických křivek
- Kvantové počítače ...
  - ... ale no tak.

Chcete je?

Kam kráčíš, Kryptografie

Diskuse o současné teoretické i aplikované kryptografii.

Libor Dostálek <dostalek@prf.jcu.cz>
Jan Dušátko <jan@dusatko.org>
Dominik Pantůček <dominik.pantucek@trustica.cz>
Pavel Vondruška <pavel.vondruska@crypto-world.info>

6. 10. 2018

Problém anonymního přístupu v SSL/TLS

Libor Dostálek

3 typy autentizace klienta v TLS

BEZ AUTENTIZACE KLIENTA VŮBEC

- Poskytování veřejných informací

Bezproblémové

BEZ AUTENTIZACE NA ÚROVNI TLS

- Autentizace kienta na úrovní HTTP, resp. aplikace
- Samostatná autentizace kleinta
- Oddělení bezpečnostní vrstvy TLS a autentizace klienta

PROBLÉM

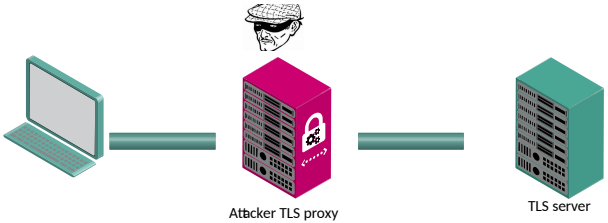
- Bohužel je toto nejčastější případ autentizace klienta

VYUŽITÍ AUTENTIZACE KLIENTA V TLS

- tzv. neanonymní TLS někdy též mTLS
- Zpravidla se používá autentizace osobním certifikátem

Bezproblémové

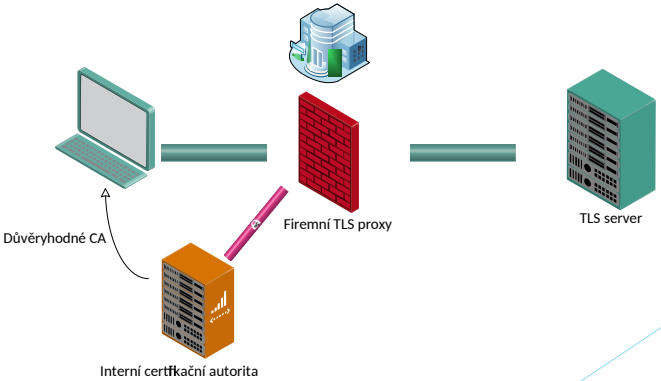
BEZ AUTENTIZACE NA ÚROVNI TLS



Řeknete: Attacker používá certifikát vydaný nedůvěryhodnou CA

Data Leakage Protection – TLS inspection

- Ochrana proti úniku informací
- Antivirová ochrana



Závěr

- Pokud máte firemní počítač, tak se podívejte, kdo vydal certifikát pro Facebook, Aktualne.cz atp.
- Přihlašujete se např. jménem a heslem z takového počítače do elektronického bankovnictví ????
- Nedíváte se náhodou v práci na divné weby ????

Panelová diskuse

- Kerckhoffsův princip
- Zadní vrátka v kryptografii
- Inventura certifikátů
- Kvantové počítače

August Kerckhoffs (19.ledna 1835 – 9.srpna 1903) byl holandský lingvista a kryptolog, profesor jazyků na École des Hautes Études Commerciales.

1. Systém by měl být prakticky nenapadnutelný, v ideálním případě ho nesmí být možné ohrozit ani teoreticky.
2. **Návrh systému nesmí vyžadovat utajení tohoto návrhu. Případný únik architektury tak neohrožuje bezpečnost komunikace.**
3. Klíč by měl být jednoduše zapamatovatelný, nejlépe bez poznámek, a měl by být snadno měnitelný.
4. Kryptogramy by měly být vysílány telegrafem.
5. Přístroje nebo dokumenty by měly být přenosné a obsluhované jednou osobou
6. Systém by měl být jednoduchý, nesmí vyžadovat složitá pravidla nebo intelektuální zátěž.

Panelová diskuse: Zadní vrátka v kryptografii?

- Zvýšení bezpečnosti?
- Boj proti terorismu??
- Skutečnost je jiná:

- Šifrování je výpočetně náročné.
- Zbytečné šifrování je drahé topení.

- Utajení je časově omezené.
- Důvěra ve falešnou bezpečnost.

Panelová diskuse: Inventura certifikátů

- Klíče: soukromý $\rightarrow$ veřejný
- Certifikát: veřejný klíč, další údaje, podpis
- Certifikační autorita, hierarchie, cesta
- Revokace certifikátů: CRL, OCSP
- Ověření: DNSSEC, DANE, CAA
- Certificate transparency
- Kvalifikované
- Pečeť, značka
- Autentizace, šifrování, ověření podpisu
- Důvěryhodnost certifikátů
- SSL/TLS

- Klasické vs. kvantové – bit vs. qubit
- Provázaný stav qubitů
- Kvantové žíhání
- Shorův algoritmus

Bezpečnostní ekvivalent	Velikost klíčů [bity]			Potřebných qubitů		
	ECC	RSA	DSA, DH	ECC	RSA	DSA, DH
80	160	1024	1024 / 160	1281	2049	2049
112	224	2048	2048 / 224	1793	4097	4097
128	256	3072	3072 / 256	2049	6145	6145

Dotazy z publika

Děkujeme za pozornost ... a ROT13 již opravdu nepoužívejte.