Kryptografie a informační bezpečnost

Mgr. Kamil Malinka, Ph.D.

malinka@fit.vutbr.cz

FIT VUT

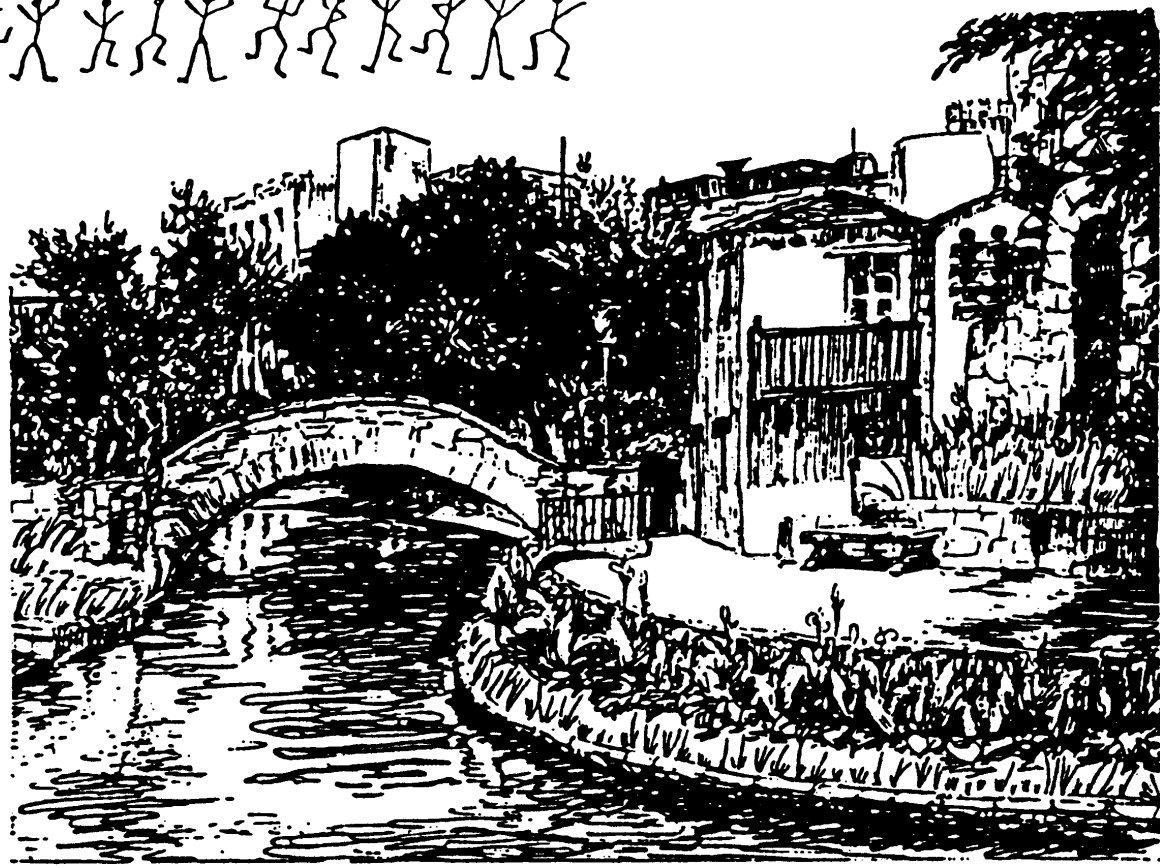
Odkazy

- Hlavní informační zdroj předmětu KIB
  - aktuality předmětu
  - http://securityfit.cz/kib/

- Je 7. prosince 1941
- 1:28 AM – je zachycena 9 minutová rádiová zpráva na trase Tokyo – Washington
- 1:37 AM – zaměstnanec ve službě na odposlouchávací stanici začíná přepisovat zprávu na dálnopisném přístroji k odeslání do Washingtonu
- Místnost 1649, ministerstvo námořnictva, Washington, oddělení OP-20-GY – bílá, žlutá a růžová kopie jsou přijaty dálnopisem a rozděleny podle používaného klíče
- Použitá šifra je rozpoznána jako PURPLE, jedná se o nejkvalitnější japonskou šifru, která byla ale oddělením OP-20-G zlomena a byly vytvořeny kopie šifrovacích rotorových strojů.
- Francis M. Brotherhood nastavil přepínače na dešifrovacím stroji podle klíče pro den 7.prosinec. Během několika minut obdrží otevřený text.
- Zpráva je v japonštině, takže je přenesena do oddělení OP-20-O je 5 AM
- „Velvyslanec laskavě předloží … naši odpověď … v 1:00 PM. .. Japonská vláda je nucena s lítostí tímto oznámit americké vládě, že vzhledem k postoji americké vlády nemůžeme jinak, než považovat za nemožné dosáhnout dohody dalším vyjednáváním.“
- Je 7 AM a je neděle, za čtyři hodiny je zpráva doručena velícím důstojníkům

Počátky kryptologie

– kryptologie a steganografie



Historie

- Egypt – město Menet Khufu
  - substituce běžných hieroglyfů
  - cílem je upoutání čtenáře
  - příklad: 1858 nahrazeno Léta páně….
  - nejstarší dochovaná záměrná transformace textu 1900 př.n.l.
- Hebrejci – 600 př.n.l.
  - Atbaš – reciproká substituční šifra
  - nalezneme ji i v bibli: Sheshack <-> Babel
  - vzdálenost písmene od začátku abecedy -> písmeno od konce abecedy
- Sparta – 5. stol. př.n.l.
  - 1.technické zařízení – skytale
- Indie
  - kniha Artaasastra – doporučení využívat kryptoanalýzy velvyslancům
  - učebnice Kámasutra – rada ženám – osvojte si tajná písma a šifry

Historie

- Řím – přelom letopočtu
  - Caesarova šifra – popsána v Zápiscích o válce galské
  - monoalfabetická šifra – posun o 3 místa
  - využívání permutací a substitucí – dlouho účinná metoda
- Polybiova šifrovací mřížka
  - písmeno reprezentováno dvojicí znaků
  - SLOVO -> 4432355235

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y
6	Z				

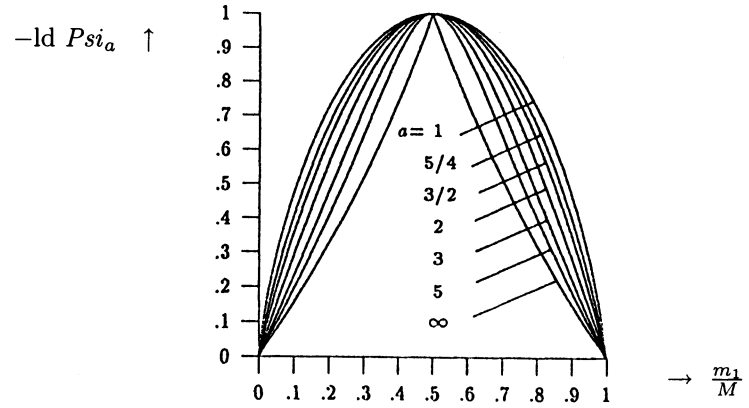
Historie

- Arábie – frekvenční analýza
- 14.stol. – bouřlivý rozvoj
  - státy najímají vlastní kryptoanalytiky
  - jejich kvalita často rozhoduje o životě a smrti – Marie Stuartovna
- 16. stol. – Vigenerova šifra
  - polyalfabetická substituce
  - řešení: bigramy, trigramy, odhad délky klíče apod.
  - souboj – logické uvažování, matematika, statistické metody

Moderní kryptografie

- Claude E. Shannon – entropie
  - míra informace, kterou zpráva obsahuje
- William F. Friedman

- Data Encryption Standard
  - publikován omylem,
  - průlom v kryptografii
  - otevření debaty



William Friedman

- Pracoval v Geneva poblíž Chicaga v laboratořích plukovníka George Fabyana
  - výzkum v oblasti chemie, biologie a akustiky
  - věřil, že Bacon byl Shakespeare
  - financování kryptoanalytického výzkumu resp. srovnávací analýzy textů obou autorů
- Friedman studovat původně genetiku (Kišiněv)
  - se svojí ženou Elizabeth Smith významně posunul kryptologii o desítky let kupředu
  - 1921 vstoupil do Signal Corps, 1929 šéfem MI8
  - byl hlavní postavou za úspěchy US kryptologie během druhé světové války

Riverbank publication No. 22 – Kappa a Chi testy (1920)

Relativní frekvence nalezení stejného písmene na stejné pozici ve dvou nezávislých textech (koincidence znaků) – **index shody**

Kroneckerův symbol

$$\delta(x,y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases} .$$

$$Kappa(T,T') = \sum_{\mu=1}^{M} \delta(t_\mu, t'_\mu)/M$$

Index shody je různý pro různé jazyky

Určením frekvence znaků v šifře jsme schopni zjistit jazyk zprávy

Index shody	
Angličtina	0,0676
Francouština	0,0801
Němčina	0,0824
Italština	0,0754
Španělština	0,0769
Ruština	0,0470
Čeština	0,0577
Slovenština	0,0581
Náhodný text	0,0385=1:26

```
1 Indeedthereexistsaparticularinvariantofatextunder
  Astonishinglygivenamonoalphabeticallyencryptedcry
         +                                       +
1 monoalphabeticencryptionwhichisdiscussedinthefollowing
  ptotextitiseasiertosaywhetheritisinEnglishFrenchorGerm
                                  +              +
1 andarelatedinvariantofapairoftextswhichiseven
  anthantodecryptitThisisalsotrueforplaintextth
  ++       +                      +
1 invariantunderapolyalphabeticencryptionofbothtexts
  ereisareliablemethodtotestasufficientlylongtextfor
                                                 +
```

M=206, delta=9 kappa(T,T’) = 9/206 = 0,043

Kappa a Chi testy

Kappa-Chi theorem – průměrný index koincidence

$$\frac{1}{M}\sum_{\rho=0}^{M-1} Kappa(T^{(\rho)}, T') = Chi(T, T') \ .$$

Chi značí skalární součin (Solomon Kullback, 1935) – m_i je absolutní frekvence výskytu znaku *i* v textu.

$$Chi(T, T') = (\sum_{i=1}^{N} m_i \cdot m'_i)/M^2 \ .$$

Pro výpočet průměrného indexu koincidence dvou textů tak stačí znát počty výskytů jednotlivých písmen v obou textech. Použití Kappa-Chi k odhadu délky klíče – spočítání pro různé délky klíče a vybrání nejvhodnější tedy nejbližší abecedě.

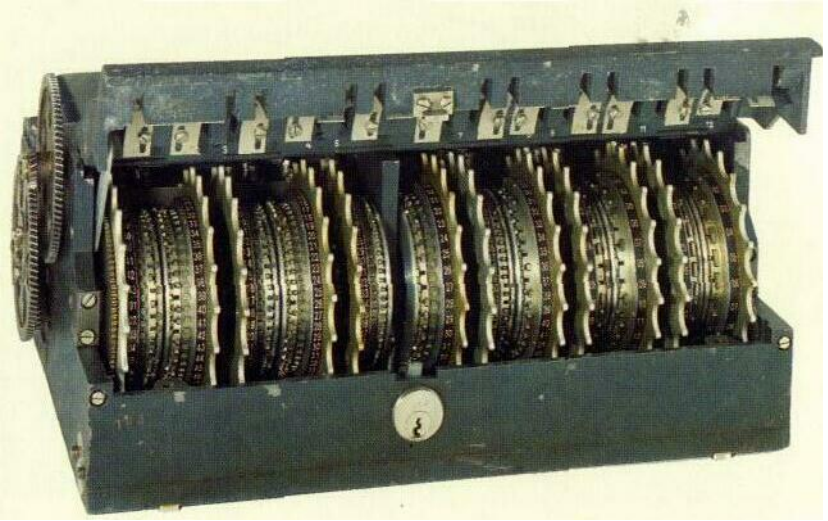
WW II.

- Druhá světová válka byla velkou událostí z pohledu kryptografie
- Velké investice vyústily ve velký rozvoj
- Mnoho příkladů úspěšné kryproanalýzy (s velkými důsledky…)
- Množina šifer se stupňovanou složitostí – kryptoanalýza začíná na nejjednodušší variantě a koncepci poté využijeme na složitější varianty (viz. Polsko - Enigma)
- Nutno si uvědomit neexistenci počítačů!
- Kódové knihy
  - řazení kódových slov podle abecedy, slova v abecedním řazení blízko u sebe mají podobné kódy -> možnost odhadu prvních písmen apod.
- Polní šifry
  - vyžadovali zručnost – vysoké požadavky vedly k ignoraci šifer (nepoužívání nebo chybovost), nízké požadavky nezaručovali bezpečnost
  - Chyby usnadňují kryptoanalýzu!
- Šifry založené na utajení jejich mechanismu – dříve či později dojde k prozrazení a kolapsu celého systému
- Dnešní kryptologie stojí na Kerckhofově principu

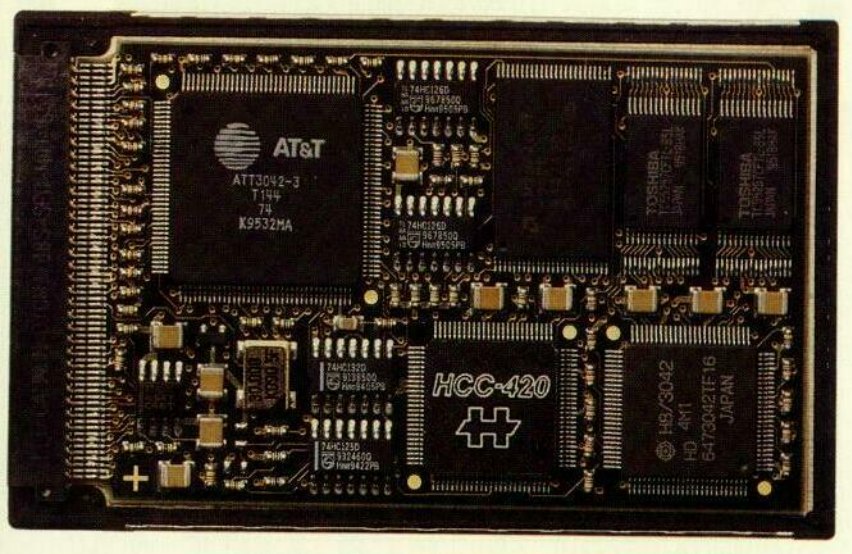
WW II. - Enigma

- Pro bezpečnost kryptografického schématu je zásadní způsob jeho užívání
- Enigma byla velmi silnou šifrou
- Její zlomení bylo umožněno pouze chybami v jejím používání. Nepomohlo ani postupné zesilování mechanismu.
- Anglická kryptoanalýza byla založena na vlastnosti Enigmy – písmeno nemohlo být zašifrováno samo na sebe
- Umožnilo nalézt klíč z tzv. cribs
- *Podrobnosti na* ***www.bletchleypark.org.uk***
- Bletchley Park
  - silná skupina anglické kryptoanalýzy
  - Konstrukce první Bomby pro lámání Enigmy

British TYPEX



Lorenz SZ 42 *Schlüsselzusatz*

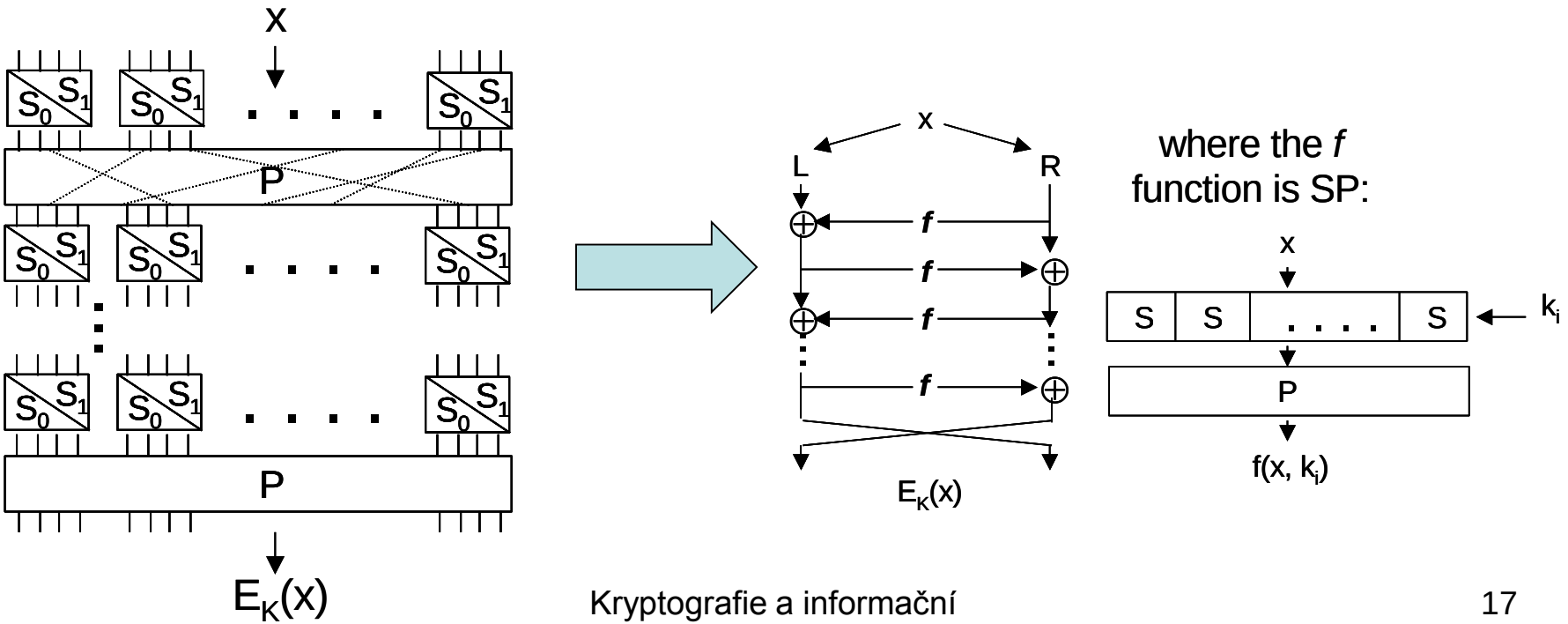


Crypto board, Crypto AG, 1996

Obrázky pocházejí z knihy
Decrypted Secrets by Friedrich L. Bauer

Lucifer/DES

- 1976 (IBM, úprava NSA), standardem do 2001
- absolutní průlom v kryptografii



- teorie jazyků
- teorie čísel
- algebra – teorie grup
- kombinatorická logika
- teorie složitosti
- ergodická teorie – statistické vlastnosti skupin
- teorie informace
- …

Kryptologie

- Komunikační protokoly
- software engineering
- programovací jazyky
- formáty dat
- operační systémy
- náhodná čísla
- distribuované systémy
- počítačové architektury
- …

Informační bezpečnost

See things differently from designers

Protokoly

- Autentizace
- Bezpečná výměna dat

- Různé druhy útoků:
  - Přehráním, odrazem, muž uprostřed, vkládání chyb, …
- Needham-Schroeder

$$A \rightarrow B: A, B, (N_A, A)PK_B$$

$$B \rightarrow A: B, A, (N_A, N_B)PK_A$$

$$A \rightarrow B: A, B, (N_B)PK_B$$

Autentizace

- co víš
- co máš
- co jsi

- Protokoly jsou velmi podobné

Digitální podpis

- Problémové oblasti
  - kryptografie
  - protokoly
  - engineering
  - administrativa / procedury
  - archivování

Opravdu asymetrická kryptografie pomáhá?

Soukromí

- big brother vs. občané

- kryptografie a její místo v zabezpečení IS (3-4)
  - výpočetní složitost a proč nás zajímá v kryptografii
  - základní stavební bloky a jak je používáme
  - proč kryptografie sama nic nevyřeší
  - pár algoritmů a jak jsme k nim došli, laická kryptografie
- autentizace(2)
  - jsem, mám, znám (hesla, PINy, certifikáty, otisky, výzva-odpověď, karty)
- elektronický podpis(2)
  - k čemu je dobrý, proč nefunguje, proč není samospasitelný
  - časová razítka, ověřování, podpis jako důkaz, archivace
- soukromí(2)
  - proč je soukromí tak důležité, ubicomp
  - anonymizování a traffic analysis, pseudonymy
- všechno ostatní(2)
  - hardening cryptography (bezpečná zařízení), správa klíčů, bezpečný přenos dat, když jde o peníze, důvěra (eBay)

Zdroje pro další studium

R. Anderson – Security Engineering

B. Schneier – Beyond Fear, Secrets and Lies

H. X. Mel –Cryptography Decrypted

B. Schneier – Applied Cryptography

Menezes – Handbook of Applied Cryptography

D. Kahn – Codebreakers

F. L. Bauer – Decrypted Secrets

O. Goldreich – Foundations of Cryptography (I & II)

S. Singh - Kniha kódů a šifer. Tajná komunikace od starého Egypta po kvantovou kryptografii