Aplikovaná (počítačová) kryptologie

RNDr. Vlastimil Klíma
vlastimil.klima@i.cz

ICZ

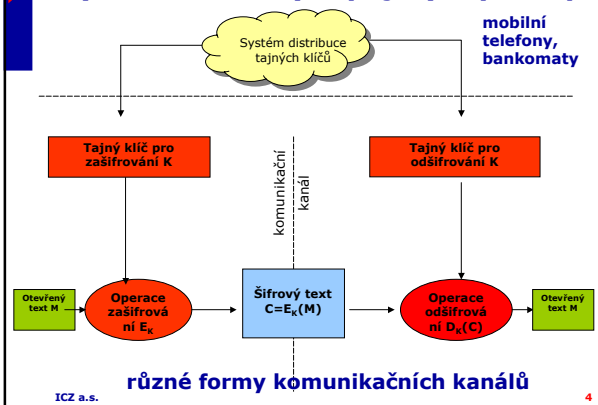
Obsah, cíl

- cíl: ve 3 přednáškách předat základní informace o moderní aplikované **symetrické** kryptografii a kryptoanalýze
- obsah: všeobecný úvod, pojmy, kryptografické a kryptoanalytické metody, proudové a blokové šifry, konkrétní šifry, operační mody, hašovací funkce a jejich použití

Základní pojmy

- kódování a šifrování *v počítačové vědě a v počítačové kryptografii*: **kódování** nepoužívá žádnou tajnou doplňkovou informaci, **šifrování** ano, tato tajná doplňková informace se nazývá **šifrovací klíč**
- **otevřený text** (OT) je informace, která se má šifrovat
- **zašifrováním** dostáváme **šifrový text** (ŠT), jeho **odšifrováním** (dešifrováním) obdržíme původní otevřený text
- **šifrový systém (šifra)** je množina dvojic zobrazení $\{E_k, D_k\}_{k \in K}$, kde **K** je prostor klíčů, **M** je prostor otevřených textů a **C** je prostor šifrových textů,
  E_k : **M** $\rightarrow$**C**: m $\rightarrow$c je šifrovací transformace,
  D_k : **C** $\rightarrow$**M**: c $\rightarrow$m je dešifrovací transformace,
  přičemž pro každé k $\in$ **K** a m $\in$ **M** platí $D_k(E_k(m)) = m$.
- **kryptografie** – věda o tvorbě šifer, **kryptoanalýza** – věda o luštění, **kryptologie** – věda o tvorbě a luštění šifer

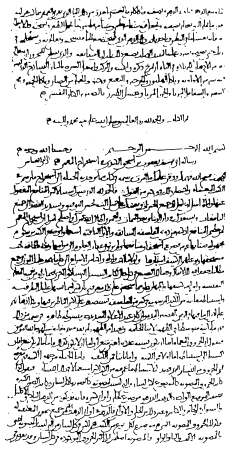
Symetrické šifry – pojmy a princip



Příklady symetrických šifer z historie

Marie Stuartovna, královna skotská a francouzská, 16.stol.

Popis luštění substituce, Al-kindí, 9.století



Substituční šifra Marie Stuartovny

a b c d e f g h i k l m n o. p q r s t u x y z

Nuly Dowbleth

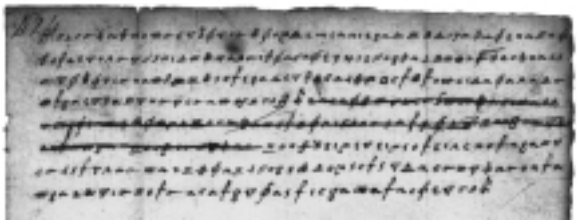
and for with that if but where as of the from by

so not when there this in wich is what say me my wyrt

send lĩe receave bearer I pray you Mte your name myne

je možno použít označení kód (historická šifra)

Šifrovaný dopis Marie Stuartovny, se souhlasem ke spiknutí a vraždě anglické královny Alžběty



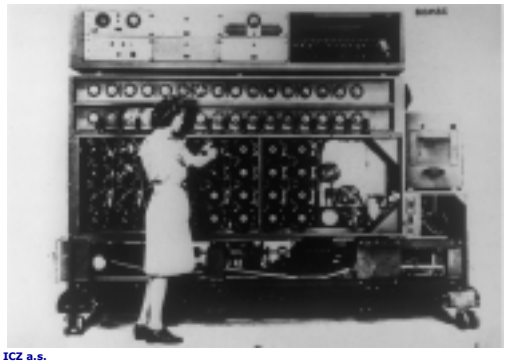
Slabé šifry jsou horší než žádné, vzbuzují falešný pocit bezpečí

Velitelské stanoviště gen. Guderiána

používání Enigmy Němci bylo značné

(na počátku II. sv.války 20 tisíc kusů)

Luštící stroj na Enigmu, Bletchley Park, Anglie



Historické šifry

- základní typy (historických) šifer, možnosti luštění, význam
  - ***Substituční***
  - ***Transpoziční***
  - ***Aditivní***
- Claude E. Shannon: Communication Theory of Secrecy Systems, Bell System Technical Journal, vol.28-4, pp. 656 - 715, 1949.

http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf

- vyjasnit si, co je systém a co klíč, jakou má klíč mohutnost, jak posuzovat šifrový systém, typy systémů, vzdálenosti jednoznačnosti apod.
- myšlenka kombinace různých typů šifer

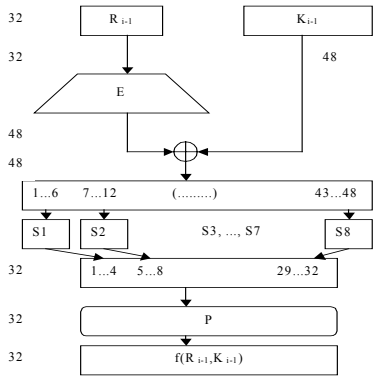
Moderní šifry

- neutajuje se šifrový systém, ale jen klíče
- pro komerční použití (ochrana obchodního tajemství, citlivých informací): veřejné a co nejširší posuzování kvality (tiger team)
- veřejné vládní, průmyslové, standardy a de facto standardy: NIST (FIPS), ANSI (X9.*), RSA (PKCS), IEEE (P1363), RFC
- standardizovány důležité stavební prvky:
  - Symetrické algoritmy (CAST, TripleDES, AES, IDEA, RC5, Blowfish)
  - Hašovací funkce (SHA-1, SHA-256, 384, 512)
  - RNG (FIPS PUB 140-2)
  - Asymetrické - podpis (RSA, DSA, ECDSA)
  - Asymetrické - výměna klíčů, dohoda na klíči (RSA, DH, ECC)

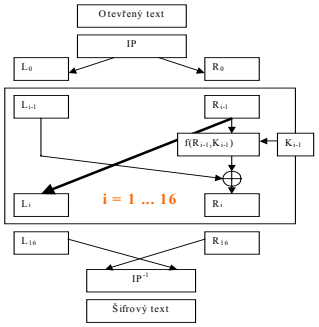
Moderní šifry

- symetrické:
  - nesrovnatelně složitější než historické, vznikají složením obvykle mnoha desítek jednoduchých šifer (stavebních bloků) - nejčastěji substitucí, transpozic a aditivních šifer

DES - funkce f(R,K) jako kombinovaná šifra, stavební prvek



DES - ilustrace, základní schéma



Moderní šifry

- asymetrické:
  - založeny na teorii čísel a operacích s velkými čísly, například m^e mod n pro m, e, n obvykle 300-600 ciferná čísla

Moderní šifry

- luštění moderních šifer je nesrovnatelně složitější než luštění historických šifer
- ve válečném konfliktu se kvalitní šifry stávají kvalitními zbraněmi, které "znehybňují" drahé nepřátelské odposlechové systémy
- kvalitní luštitelé a luštící zařízení se stávají protizbraněmi, které jsou tiché a účinné, vyřazují z činnosti drahé nepřátelské šifrovací systémy, ponechávají nepřítele v jistotě, že jeho komunikace jsou chráněny a může jimi předávat důležité informace
- závěr: "šifry" jsou považovány za zbraně oprávněně

Import/Export šifer - ČR a USA

- **ČR:** import/export: Wassenaarská dohoda o vývozní kontrole klasických zbraní a zboží dvojího použití, http://www.wassenaar.org, Ministerstvo průmyslu a obchodu ČR
- **USA:** dříve restrikce do 56b, vývoz dnes poměrně liberální, výjimky 7 zemí (Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria)
- konzistentní s Wassenaarskou dohodou
- **poslední revize 6.6.2002 a minoritní 03/2003**
- liberalizován vývoz silných šifer (nad 64 bitů), u výrobků masové spotřeby téměř neomezeně (30 denní "review")
- Bureau of Industry and Security (BIS), dříve Bureau of Export Administration (BXA), v rámci ministerstva obchodu USA

Elektronická špionáž

- část systémů z doby studené války přeměněna na ekonomickou špionáž
- k jejich provalení vedly miliardové obchodní ztráty (nejen v Evropě)
- Evropa:
  - Něm. firma, vysokorychlostní vlaky, 3 500 000 000 DM
  - Thomson-CSF, radarový systém, 1 400 000 000 USD
  - Airbus Industrie , letecká technika, 1 000 000 000 USD
- vyšetřování Evropským parlamentem
- www.europarl.eu.int/

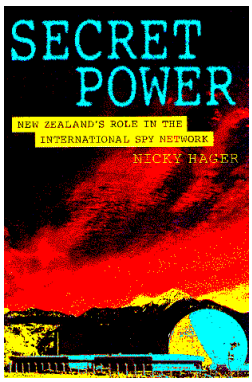
Odposlechové systémy

- v komerčním světě šifry a další kryptografické techniky chrání důležité informace, obchodní tajemství, počítačové sítě,... jejich kvalita by měla odpovídat ceně dat, která chrání.
- ve světovém měřítku je jen malé množství komerčních dat přenášeno v zašifrovaném tvaru a kvalitně
- zbytek není šifrován vůbec nebo nekvalitní šifrou (slabé klíče, pevné klíče apod.).
- důsledek: systémy odposlechu a sběru informací jsou "zahlceny"

Echelon

Echelon je celosvětový odposlechový a vyhodnocovací systém

http://archive.aclu.org/echelonwatch/resources.html



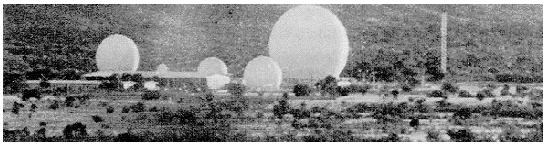
Od kolegy z dovolené na Krétě...

Echelon

Vřesoviště F83

Echelon - další prvky

radiové komunikace, diplomatické spoje, podmořské kabely, regionální - národní satelitní systémy,...



NSA

Moskva

výpočetní centrum ruské tajné služby s podzemním luštitelským městečkem, Moskva

Šifrování z obecně bezpečnostního hlediska

- uložená data – hrozba **okopírování nebo zcizení** nosiče (HDD, notebooky, PC, diskety)
- přenášená data - hrozba **odposlechu**
- šifrování je nové bezpečnostní opatření k zajištění *důvěrnosti*
  - mnohdy jediné možné skutečně účinné opatření
  - šifrovací klíče se lépe spravují a chrání než vlastní data
  - lze je ukládat do předmětů, uživatel si nemusí klíče pamatovat, ani znát
- šifrování je nové bezpečnostní opatření, vyžaduje odbornost (vyvrtat si zuby svépomocí nebo jít za zubařem ?)
- šifrování *nezajišťuje integritu* (vžitý omyl "šifrování řeší bezpečnost"),
- **aktivní narušení dat nebo jiné působení** na komunikačním kanálu resp. paměťovém médiu - je nutné použít kombinaci kryptografických technik

Kryptografie: základní kategorie kryptografických funkcí a jejich užití

techniky:

- symetrické šifry
  - proudové a blokové šifry
- asymetrické šifry (schémata)
  - pro šifrování klíčů, výměnu klíčů, dohodu na klíči
  - pro digitální podpis (s obnovou zprávy, s dodatkem)
- generátory náhodných čísel (RNG)
- hašovací funkce
- kryptografické kontrolní součty (MAC, HMAC)

služby:

- důvěrnost
- integrita
- autentizace původu dat, subjektů
- nepopiratelnost

Terminologie

- problém s tvorbou nových českých ekvivalentů anglických termínů
- správně: šifrování, zašifrovat, odšifrovat, šifrovat, šifrér (člověk), šifrátor (stroj), šifrovací zařízení, šifra, šifrovací algoritmus, ...
  - chybně: kryptování, enkrypce, enkryptace, zaenkryptovat, kryptace, kryptátor, kryptér, dekryptovací instituce
- správně: autentizace
  - chybně: autentifikace, autentikace

Kryptoanalýza - Úvod

- historie kryptoanalýzy
  - většina šifer až do poloviny 20. stol. rozluštěna, část mladších také
- naivní představy o luštění a kryptoanalýze přetrvávají
  - ze šifrového textu, bez popisu kryptosystému, nekonečné změny, naivní cíle, nemasové použití, lidová tvořivost
- současné cíle kryptoanalýzy
  - nejen OT, ale klíč, informace o částech nebo vlastnostech OT, K, nalezení slabých klíčů, různé vztahy (komplementárnost) apod.
- typy útoků - základní klasifikace **COA** (Ciphertext-Only Attack), **KPA** (Known-Plaintext Attack), **CPA** (Chosen-Plaintext Attack), **CCA** (Chosen-Ciphertext Attack)

Kryptoanalýza - metody

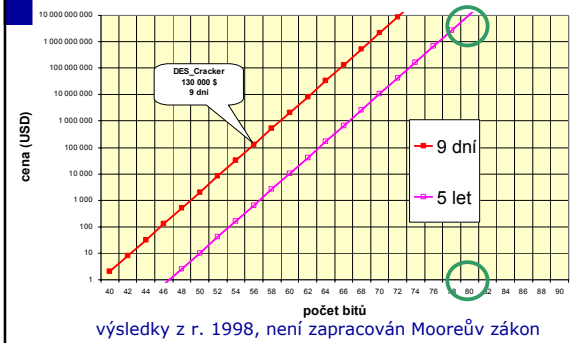
- hrubou silou
  - rostou SW i HW možnosti,
  - objednání luštění e-mailem,...

Útok hrubou silou - luštění DES

- **17. 7. 1998** sestrojen „DES-cracker"
- cena 210 000 USD
  - 130 000 za HW
- je možné si ho koupit nebo sestrojit
  - (objednání luštění e-mailem)
- 29 desek se 64 zákaznickými čipy
- 90 MLD klíčů/sec.
- DES challenge III - 22 hodin (19.1.1999, viz http://www.rsasecurity.com/rsalabs/challenges/des3/index.html)
- maximální doba luštění - 9 dní

Luštící stroj na DES

Velikost klíče a možnosti luštění z hlediska ceny a času - námět k nekonečné diskusi



výsledky z r. 1998, není zapracován Mooreův zákon

Velikost klíče a možnosti luštění z hlediska počtu operací

	jedinec	firma	tajná služba	lidé	???
počítače / čipy	1 PC	10^3 čipů	10^5 čipů	10^8 čipů	10^{51} čipů
zkoušek klíčů/s	10^4	10^6	10^9	10^{12}	10^{19}
čas na útok v sec.	týden (10^6)	měsíc (10^7)	rok (10^8)	100 let (10^{10})	1000 let (10^{11})
celk. počet operací	10^{10}	10^{16}	10^{22}	10^{30}	10^{81}
délka klíče v bitech	34	54	73	100	269

vývoz DES NSA AES

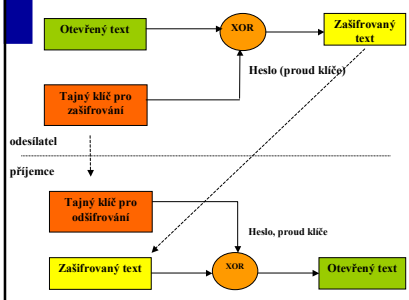
RC5 - 64

- v rámci soutěže společnosti RSA, RC5-64 challenge, na webu RSA
- 26.9.2002 nalezen 64bitový klíč
- 4 roky, 331.252 dobrovolníků, organizace skupinou Distributed.net
- z webu stáhnutí klienta, zkouší klíče z přidělené množiny, prohledáno 85% klíčového prostoru
- skupina z ČR mezi 20 nejagilnějšími
- "The unknown message is: Some things are better left unread"

Metody kryptoanalýzy – teoretické

- analytické, statistické (jednoduchá záměna a frekvenční charakteristiky, RC4, entropie klíče,...)
- chyby v implementacích v důsledku neznalosti nebo nepozornosti (kvalitní stavební bloky, ale nesprávně použité, zanesení chyby při realizaci)
- postranní kanály – nežádoucí "vyzáření" informace (elekromagnetické, napěťově-proudové, časové, chyby neúmyslné, chyby záměrně vyvolané apod.), velmi nebezpečné, nečekané výsledky, mladý obor

Proudové šifry a operace ⊕ (xor)



b	h	b ⊕ h
0	0	0
0	1	1
1	0	1
1	1	0

⊕ = diference bitů
negace(b) = b´ = b ⊕ 1
b ⊕ b = 0
b ⊕ b´ = 1

ŠT = OT ⊕ H:
OT: ..... 1 0 0 1 1 0....
H: ..... 1 1 0 1 0 1....
ŠT: ..... 0 1 0 0 1 1...

ŠT ⊕ H = (OT ⊕ H) ⊕ H = OT

- **odšifrování stejné jako zašifrování ?**
- **šifruje to ?** ŠT = 0 ⇒ OT a H jsou stejné (nevíme ale jaké, **H je tajné**)
  ŠT = 1 ⇒ OT a H jsou různé (nevíme ale jaké, **H je tajné**)

Kryptoanalýza a proudové šifry

- proudové šifry (stejně jako obecně všechny symetrické šifry) nezajišťují integritu

OT1: ..... kontrakt na dodávku pšenice. Cena je 5 000 000,- USD. Splatn....
H: ..... kasůfkaiqpoirksdaůirtpqiwerůasktqpioerqůkdjairqpiraskgaůirup....
ŠT1: ..... áílkjěšdgjkqwšpéítůšaeígqškčjtéiqšštqegqšdlgšrlflůšleglladgwá...

.....(změna xor 234 na ŠT)

ŠT2: ..... áílkjěšdgjkqwšpéítůšaeígqškčjtéiqšštqeq78dlgšrlflůšleglladgwá...
H: ..... kasůfkaiqpoirksdaůirtpqiwerůasktqpioerqůkdjairqpiraskgaůirup....
OT2: ..... kontrakt na dodávku pšenice. Cena je 5 234 000,- USD. Splatn....

dešifrováním změněného šifrového textu (ŠT1 ⊕ Δ) obdržíme
(ŠT1 ⊕ Δ) ⊕ H = (OT1 ⊕ H ⊕ Δ) ⊕ H = OT1 ⊕ Δ

Kryptoanalýza a proudové šifry

- kritické je dvojí použití hesla

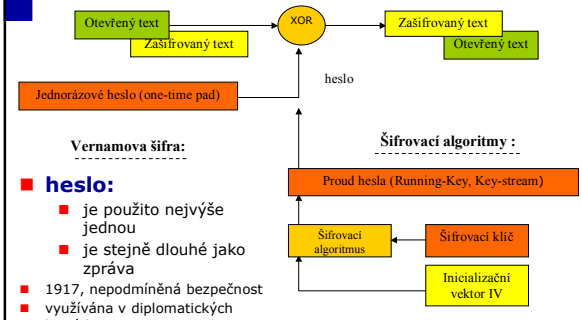
OT1: ..... schůzka skupiny Balkán se bude konat v Praze někdy v prosinci....
H: ..... kasůfkaiqpoirksdaůirtpqiwerůasktqpioerqůkdjairqpiraskgaůirup....
ŠT1: ..... áilkjěšdgjkqwšpéitůšaeígqškčjtéiqšštqegqšdlgšrlflůšleglladgwá...

OT2: ..... místě bude dohodnuta nová trasa, krytí skupiny Balkán bude za...
H: ..... kasůfkaiqpoirksdaůirtpqiwerůasktqpioerqůkdjairqpiraskgaůirup....
ŠT2: ..... ělůáčtnpydnqtpúagmawígjdůilkuqwgsvůpáwkěykčýabpdáščhqů...

ŠT1 ⊕ ŠT2 (= OT1 ⊕ H) xor (OT2 ⊕ H) = OT1 ⊕ OT2 =
.....ůjdphtaghačwfpáíweůksnbyxnůaeptqšátaihjvyvymvukflbzrhelkl...
OT1: ..... Balkán ..... Balkán ..... čkdy v p.....
OT2: .....dháů§s.....dnuta no..... Balkán .....

- lze ze šifrových textů poznat dvojí použití hesla ?
  - texty v ASCII

Proudové šifry: Vernamova šifra vs. generátory hesla



- **heslo:**
  - je použito nejvýše jednou
  - je stejně dlouhé jako zpráva
- 1917, nepodmíněná bezpečnost
- využívána v diplomatických kruzích

Proudové a blokové šifry : bezpečnost

- teoretická bezpečnost zaměněna za výpočetní bezpečnost (na bázi složitosti algoritmu)
  - umožňuje vícenásobné použití klíče (s jiným IV), ale rizika:
    - úroveň bezpečnosti je závislá na síle protivníka
    - geniální objev může zhatit značnou část současné kryptografie

RC4 – základní údaje

- nejpoužívanější proudová šifra na internetu (SSL, S/MIME)
- 2-4 krát rychlejší než nejpoužívanější blokové šifry
- Ronald Rivest, 1987, obchodní tajemství firmy RSA
- 1994 - popis zveřejněn hackerem
- délka periody je ve střední hodnotě rovna 2^{1699}
- nevyužívá IV, na každé šifrování používá nový (náhodný) klíč, přenášen asymetricky
- klíč může mít délku 1 až 256 bajtů, nejčastěji 40 nebo 128 bitů

RC4 – příprava klíčové tabulky

- šifrovací klíč (zarovnaný na bajty) cyklicky vepisujeme do pole K(0),K(1), …, K(255)
- zvolíme identickou počáteční permutaci S, tj. S(i) = i, i = 0...255 a promícháme jí prostřednictvím hodnot K(i):

```
j = 0
for i = 0 to 255          //všechny operace v modulu 256
{
    j = (j + S(i) + K(i))
    S(i) <--> S(j)
}
```


RC4 – šifrovací schéma

- generování hesla h(i) :

```
x = y = 0
for i = 0 to n
{
        x = x + 1       //všechny operace v modulu 256
        y = y + S(x)
        S(x) <--> S(y)
        h(i) =  S (S(x) + S(y))
}
```

- heslo se xoruje na otevřený text nebo šifrový text

RC4 – bezpečnost

- tzv. broadcast varianta má druhý bajt nulový s pravděpodobností 2/256 místo 1/256, viz Mantin-Shamir Distinguisher (2001)
- Ross, 1995, třída slabých klíčů. Pokud klíč má vlastnost, že (K[0] + K[1]) = 0, potom pst(K[2]+3 = h[0]) ≈ 13.8% .
- v protokolu WEP (Wired Equivalent Privacy pro ochranu komunikace bezdrátových sítí, standard 802.11) bylo použito chybné mixování hlavního klíče s konstantami (IV || K), známými útočníkovi - to vede k odhalení hlavního klíče K - obrana je použít hašování v přípravě klíče
- jsou známy další práce, odhalující další vlastnosti RC4, nerovnoměrné rozložení 1.,2.,bajtu a jejich bigramů (2002, Pudovkina) apod., dosavadní obranou je nepoužít prvních 512 (3072) bajtů hesla

Literatura a další zdroje

Archiv článků a prezentací na téma kryptografie a bezpečnost
http://www.decros.cz/bezpecnost/_kryptografie.html
Stránka NIST, normy, dokumenty k AES aj.:
http://csrc.nist.gov/encryption/aes/aes_home.htm
Zdrojové kódy šifer
ftp://ftp.funet.fi/pub/crypt/cryptography/
Bezpečnostní a kryptografický portál
http://www.cs.auckland.ac.nz/~pgut001/links.html

O autorovi

- MFFUK, 1976 - 1981
- 1981 - 1992 v ozbrojených složkách
- 1993 - 2003 v soukromém sektoru, ICT
- kryptolog, ICZ a.s.
- projekty, přednášky, publikace na

http://cryptography.hyperlink.cz

- archiv primárně uložen na

http://www.decros.cz/bezpecnost/_kryptografie.html