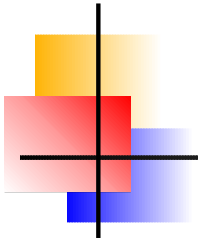
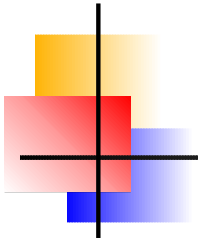


Z histórie kryptografie

Stanislav Palúch

University of Žlina/Department of Mathematical Methods

26. septembra 2016



Najstaršie historické pramene

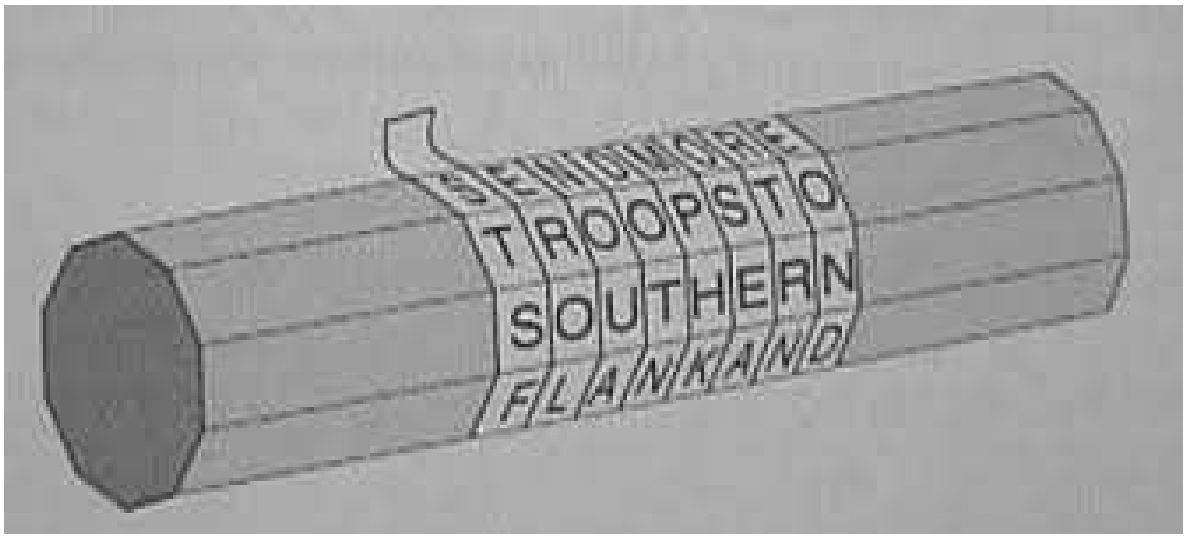
1900 pred Kristom
Egyptskí pisári použili neštandardné hieroglyfické symboly namiesto obvyklých hieroglyfov, čo sa považuje za prvé doložené použitie kryptografie. [Kahn str. 71]

1500 pred Kristom
Tabuľka z Mezopotámie so zašifrovanou formulou na výrobu glazúrovanej keramiky [Kahn str. 75]

600 - 500 pred Kristom
Hebrejci používali primitívnu šifru ATBAŠ založenú na nahradení prvého znaku abecedy posledným, druhého predposledným atď. [Kahn str. 82]

Grécko a Sparta

500 pred Kristom – Grécko a Sparta – skytalé



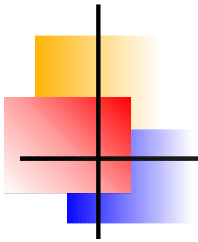
Ceasarova šifra

100 - 44 pred Kristom – Julius Ceasar

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	Z
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	C

C	E	A	S	A	R
F	H	D	V	D	U

Šifra bola na svoju dobu nerozlúštiteľná,
kým ju neprezradili
Ceasarovi bývalí spojenci (Cicero),
ktorí prešli k jeho nepriateľom.

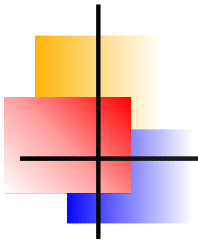


Indické a arabské korene kryptografie

medzi 1. - 4.storočím n.l.
Kámasútra: 44. umenie: Pochopiť písanie šifier a slov na utajenie vecí.

725-790 n.l.
Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi
napísal knihu o kryptografii inšpirovanú jeho lúštením šifier pre byzanského cisára.
Jeho riešenie bolo založené na znalosti otvoreného textu, čo je štandardná kryptoanalytická metóda.

1226 n.l.
Archívne nálezy pochádzajúce z tohoto roku ukazujú, že
v Benátkách bola používana kryptografia, kde bodky a krúžky nahradzovali zvláštnym spôsobom slová a písmena.



Gabrieli di Lavinde

1379 n.l.
Gabrieli di Lavinde

Vytvoril systém pozostávajúci s úplnej substitučnej abecedy rozšírenej o dvojpísmenové kódy pre cca dve desiatky najfrekventovanejších slov alebo mien.

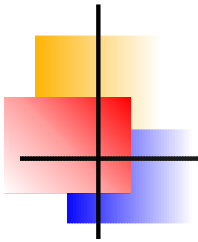
Navyše tiež tzv. klamače, nevýznamové skupiny písmen, ktoré mali sťažiť kryptoanalýzu zašifrovaných textov.

Tento princíp sa používal takmer 450 rokov, napriek tomu, že už boli k dispozícii aj silnejšie metódy.

Leon Battista Alberti

1466-1467
Leon Battista Alberti

napísal 25 stranovú prácu
– prvú prácu napísanú v západnej Európe –
venovanú kryptoanalýze.
Dielo obsahuje výklad kryptoanalytických postupov na základe jazykových znalostí, roztriedenie systémov šifrovania na substitúciu a transpozíciu, objav polyalfabetickej substitúcie a šifrovanie kódov.



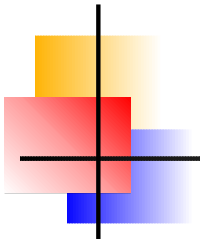
Johannes Trithemius

1518 n.l. Johannes Trithemius (benediktínsky mních)
prvá tlačená kniha s kryptologickou náplňou.

Vymyslel šifru, pri ktorej sa každý znak priameho textu zašifroval podľa ďalšieho riadku Trithemiusovej tabuľky.

Trithemiusova tabuľka

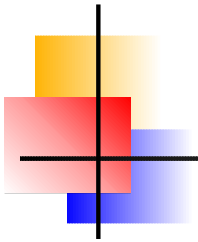
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	J	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	A



A

	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	Z
A	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	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	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
D	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	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	J	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	A

$$\mathrm{T} + \mathrm{M} \to \mathrm{F}$$



A

1553 n.l. Giovanni Battista Belas (taliansku šľachtic)

vyšla brožúra "La cifra" popisujúca kryptosystém, ktorého základom je tajný kód.

Tajným kódom je tu slovo, príp. veta, ktorá sa opakovane píše nad otvorený text.

Každé písmeno otvoreného textu je potom šifrované riadkom Trithemiusovej tabuľky určenej písmenom nad ním.
(Šifra založená na tomto princípe sa neprávom pripisuje Vigenèrovi)

Blaise de Vigenère

1586
Vyšla kniha „Traicté des Chiffres“, kde navrhuje systém, v ktorom aj samotná správa je kľúčom.

S	V	J	E	D	N	O	M	J	E	J	P	O	U	Z	I	T	I	P	O	S	T	U	P	U	J
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
v	j	e	d	n	o	m	j	e	j	p	o	u	z	i	t	i	p	o	s	t	u	p	u		
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	
N	E	N	H	Q	B	A	V	N	N	Y	D	I	T	H	B	B	X	D	G	L	N	J	J		

Príklad použitý z
Grošek, O, Porubský, Š: Šifrovanie. Algoritmy, metódu, prax. 1992 - Grada.
ISBN 80-85424-62-2

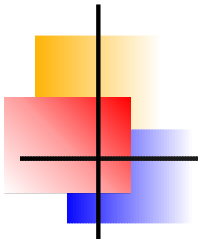
1586 n.l.
Listy sprisahancov proti Alžbete prechádzajú rukami kryptoanalytika Thomasa Phelippesa.

K listu zo 17.júla bolo dokonca pripísaná (správne zakódavná) požiadavka na upresnenie mien šiestich spojencov, ktorí mali zavraždiť Alžbetu.

1589 n.l. – Francúzsko
Francois Viète (1540-1603) (právnik a matematik, považovaný za zakladateľa algebry).
Jeden z prvých matematikov pôsobiacich v šifrovacích službách.

Poradca hugenotského kráľa Henryho IV. bojujúceho proti katolíkom a Španielom.

Rozlúštil šifry spojencov i mnohé šifry Benátčanov.



Antoine Rossignol

Antoine Rossignol (1599 - 1682) francúczsky matematik.
Neskôr sa stal základom šifrovacej kancelária kardinála Richelieu.

Apríl 1628
Opevnené juhofrancúzske mestečko Realmont držané hugenotmi bolo obliehané kráľovkými vojskami.

A. Rossignol rozúštil zachytenú hugenotskú správu žiadajúcu o pomoc.
Rozlúštenú správu vrátili do Realmontu, na čo jeho obyvatelia obratom vzdali.

sir Francis Bacon – biliterálna šifra

1623 sir Francis Bacon
popísal vo svojom diele
"De Augmentis Scientarum"
biliterálnu šifru,
známu v dnešnej dobe ako
5-bitové binárne kódovanie.

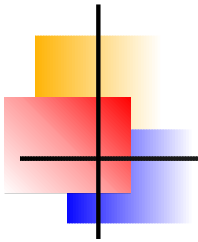
A	B	C	D	E	F
aaaaa	aaaab	aaaba	aaabb	aabaa	aabab
G	H	I	K	L	M
aabba	aabbb	abaaa	abaab	ababa	ababb
N	O	P	Q	R	S
abbaa	abbab	abbba	abbbb	baaaa	baaab
T	V	W	X	Y	Z
baaba	baabb	babaa	babab	babba	babbb

Friedrich W. Kasiski, Auguste Keckhoffs

1863 Friedrich W. Kasiski (dôstojník pruskej armády) uverejňuje metódu na riešenie polyalfabetickej šifry

1883 Auguste Keckhoffs (1935 - 1903) – kniha La Cryptografie militaire
Kerckhoffs našiel metódu, ako rozlúštiť všeobecnú polyalfabetickú šifru s neperiodickým kľúčom, ak tento bol použitý niekoľkokrát.

1. systém má byť, keď nie teoreticky, tak aspoň prakticky nerozlúštiteľný
2. odhalenie systému nesmie spôsobiť ťažkosti korešpondentom
3. šifrovací kľúč má byť ľahko zapamätateľný a ľahko zmenený
4. zašifrovaný text sa má dať prenášať ďalekopisom
5. šifrovací aparát alebo dokument má byť prenosný a obsluhovateľný jednou osobou
6. šifrovací systém má byť ľahký, bez dlhého zoznamu pravidiel a bez prepiatych nárokov na duševnú činnosť



Vývoj kryptografie v 20. storočí

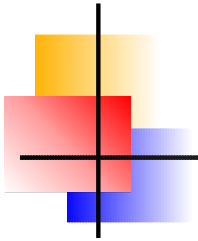
V r. 1919 Hugo Alexander Koch
zapísal svoj patent šifrovacieho stroja založeného na rotoroch.

V r. 1923
predal patent Arthurovi Scherbiusovi, nemeckému inžinierovi, ktorý ho vylepšil a nazval Enigma.

Počas 2. svetovej vojny bola používaná v rôznych variáciách predovšetkým nemeckou armádou.

V r. 1976 Whitfield Diffie a Martin Hellman publikujú
"New Directions in Cryptography"
zavádzajúcu pojem kryptosystému verejného kľúča
(nazývanou aj asymetrická kryptografia).

V r. 1977 oznámili Ronald L. Rivest, Adi Shamir a Leonard M. Adleman objav prvého konkrétneho kryptosystému s verejným kľúčom – RSA.



Vývoj kryptografie v 20. storočí

1975 - Publikovaný kryptografický systém DES – Data Encryption Standard vyvinutý v IBM.
Systém DES mal 64 bitový blok a 56 bitový kľúč.

1994 - bolo faktorizované 129-ciferné číslo RSA-129. Podľa odhadu tvorcov RSA z roku 1977 mala táto činnosť trvať 4.10^6 rokov.

1997 - bol rozúštený 56-bitovýkľúč k DES pomocou distribuovaného výpočtu na Internete.

1998 - bolo publikované zosilnenie algoritmu 3-DES (triple DES) založené na trojnásobnom použití algoritmju DES s troma kľúčmi.

Vývoj kryptografie v 20. storočí

V r. 1990 Xuejia Lai a James Massey zo Švajčiarska vydali článok "A Proposal for a New Block Encryption Standard",

ktorý obsahoval návrh šifrovacieho algoritmu International Data Encryption Algorithm (IDEA) a mal nahradiť DES.

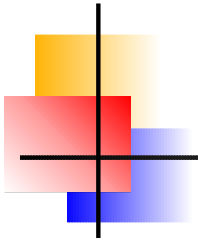
IDEA má 64 bitový blok a 128 bitový kľúč.
Pretože IDEA bola patentovaná, nerozšírila sa.
V súčasnosti sa 64-bitová dĺžka bloku pokladá za slabinu.

V r. 1991 Phil Zimmermann zverejnil jeho prvú verziu PGP (Pretty Good Privacy).

PGP je šifrovací program, ktorým sa dá zabezpečiť bezpečný prenos e-pošty, ale taktiež telefonovanie cez Internet.

Využíva algoritmy RSA a IDEA.

Aj v súčsnosti tento program na Internete používa značné množstvo používateľov, čo je umocnené skutočnosťou, že pre súkromné účely je zadarmo.

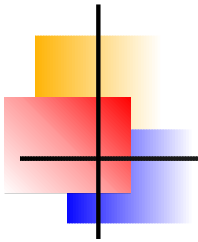


Najnovšie výsledky kryptografie

V r . 1994 bolo faktorizované 129-ciferné číslo RSA-129. Podľa profesora Rivesta, jedného z tvorcov RSA, mala táto činnosť trva 4.10^{16} rokov.

V r. 1997 Bol rozlúštený 56-bitový kľúč k DES pomocou Internetu, podobne ako v roku 1994 u RSA.

V r. 2000 šifrovací štandard DES bol, po takmer štvorročnej verejnej súťaži, nahradený belgickou šifrou Rijndael.
Blokovú š1ifru Rijndael prihlásili do súťaže známi kryptológovia Joan Daemen a Vincent Rijmen.



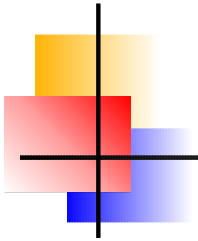
Kryptografia

Kryptografia je štúdium matematických techník na ochra nu a utajenie informácie.
Niekedy sa používa ja termín Kryptológia, ktorá sa delí na

- Kryptografiu – vynachádzanie šifrovacích systémov a
- Kryptoanalýzu – študujúcu útoky voči šifrovacím systémom.

Úlohy kryptografie

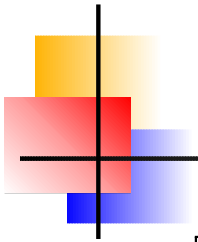
- Utajenie informácie
- Zaistenie integrity údajov – zaistenie proti zmene správy
- Autentifikácia – zaistenie, že správa pochádza od určitého pôvodcu
- Identifikácia – zaistenie, že komunikujem stým s kým chcem
- Neodškriepiteľný digitálny podpis
- Steganografia – ukrytie správy v inom údajovom súbore



Kryptografia

Ďalšie problémy, ktoré rieši kryptografia

- výmen kľúčov
- zdieľanie kľúčov
- elektronické peniaze
- anonymné hlasovacie procedúry
- atď.



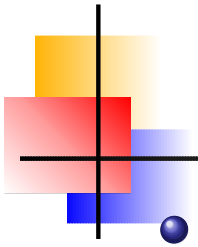
Kryptosystém

Priamy text – Plaintext $\rightarrow$ Zašifrovaný text – Ciphertext

Kryptosystém je usporiadaná štvorica $(\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathcal{T})$ kde

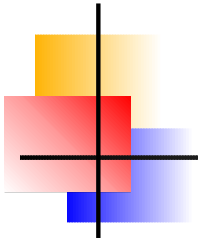
- $\mathcal{K}$ je množina kľúčov
- $\mathcal{M}$ je množina priamych textov
- $\mathcal{C}$ je množina zašifrovaných textov
- $\mathcal{T}$ je zobrazenie $\mathcal{T} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$, ktoré každej dvojici $K \in \mathcal{K}$, $M \in \mathcal{M}$ priradí zašifrovanú správu $C \in \mathcal{C}$ a také, že
  ak $\mathcal{T}(K, M) = C$ a $\mathcal{T}(K, M') = C$, potom $M = M'$.
  (Existuje teda inverzné zobrazenie $\mathcal{T}^{-1}(K, C) = M$.)

Značenie $\mathcal{T}(K, M) = E_K(M)$, $\mathcal{T}^{-1}(K, C) = D_K(C)$.



Typy kryptografických systémov

- **Symetrická kryptografia** – na šifrovanie i na dešifrovanie sa používa ten istý kľúč.
- **Nesymetrická kryptografia** – kryptografia s verejným kľúčom.
  Na šifrovanie sa používa tzv. verejný kľúč. Prijímateľ správu dešifruje svojím tajným kľúčom. Z verejného kľúča nie je možné odvodiť tajný kľúč.
- **Substitučná šifra** – nahrádza znak alebo reťazec znakov iným znakom resp. iným reťazcom.
- **Transpozičná šifra** – znaky ostávajú, mení poradie znakov
- **Monoalfabetická šifra** – šifruje sa znak po znaku, každý znak rovnakým zobrazením
- **Polyalfabetická šifra** – Šifrujú sa k-tice znakov, každý znak v k-tici iným kľúčom
- **Bloková šifra** – šifrujú sa celé bloky priameho textu
- **Prúdová šifra** – šifruje sa znak po znaku, každý znak iným kľúčom, prúd kľúčov je rovnako dlhý ako šifrovaný text

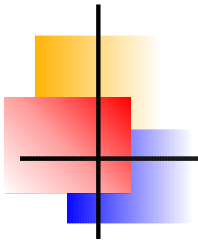


Čo ostalo z Kerckhoffových zásad

1. Prezradenie šifrovacieho algoritmu nesmie ohroziť bezpečnosť systému
2. Bezpečnosť spočíva iba v utajení kľúča

Bruce Schneier: Existujú dva typy kryptografie:

1. Tá, ktorá zabráni vašej mladše setričke čítať vaše listy
2. Tá, ktorá zabráni ústrednej spravodajskej sužbe čítať vaše súbory

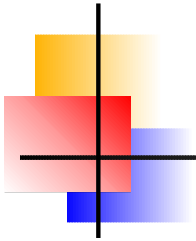


Kryptografické útoky.

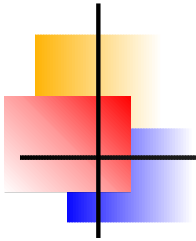
Útok na kryptografický systém je postup, ktorý odhalí priamehy text (alebo aspoň jeho časť) alebo doknca zistí šifrovací kľúč.

Typy kryptografických útokov

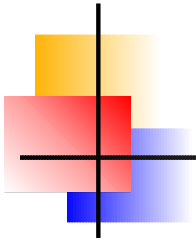
- Brute force attack
- Ciphertext only attack
- Known plaintext attack
- Chosen plaintext attack
- Chosen ciphertext attack
- Dictionary attack
- Rubber hose attack



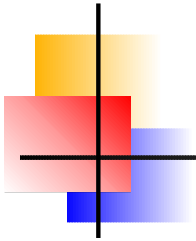
A



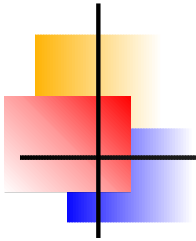
A



A



A



A