ZÁKLADY KRYPTOLOGIE

KRYPTOLOGIE

= nauka o šifrování

Důvody šifrování

- zabezpečení dat a tajných informací (choulostivá data o osobách, vědecké objevy, hesla, …)
- tajná korespondence (např. válečné depeše, milostná psaníčka, …)

Pohled do historie

Skytala

Odvětví kryptologie

- Kryptografie
- Steganografie
- Kryptoanalýza

Steganografie

- *steganos* = schovaný, *graphein* = psát
- utajování existence tajných zpráv

- př.: Histiaios a oholená hlava; použití zprávy jako opasku, …

Některé steganografické metody

Neviditelný inkoust

Některé steganografické metody

Ukrytí textu ve změti písmen:

- Skákal pes přes oves, přes zelenou louku, šel za ním myslivec, péro na klobouku.

(kapesník)

- Martin Olbracht ušel kus Ameriky.

(mouka)

Některé steganografické metody

Ukrytí textu do obrázku

Kryptografie

- *kryptos* = skrytý
- změna podoby textu
- domluvená pravidla šifrování účastníků komunikace

- př.: Skytala (tyče o stejném průměru)

Kryptoanalýza

- luštění tajných zpráv bez znalosti šifrovacího klíče
- nutná výborná znalost jazyka, poznatků z oblasti kryptologie, dostatek trpělivosti

Základní pojmy

- **šifra** = nahrazování písmen textu jinými písmeny, číslicemi nebo znaky
- např: SOBOTA → 1814114190
- **kód** = slovo, číslo nebo symbol, které nahrazuje nějaké jiné slovo nebo skupinu slov
- **otevřený text** = srozumitelný text psaný v běžném jazyce, který chceme zašifrovat

Základní pojmy

- **šifrový text** = text po zašifrování, jeví se jako náhodná kombinace znaků
- **klíč** = souhrn pravidel, podle kterých probíhá šifrování; musí ho znát příjemce a odesílatel; před ostatními ale musí být bezpečně utajen
- např.: užití symbolů:

- **šifrovací algoritmus** = postup vytváření šifrového textu

Základní pojmy

- **šifrování** = převedení otevřeného textu pomocí klíče a šifrovacího algoritmu na šifrový text
- **dešifrování** = převedení ŠT na OT, příjemce zprávy musí znát klíč i algoritmus, který použil odesílatel
- **luštění** = převedení ŠT na OT bez znalosti klíče a pravidel
- **kódování** = převod textu do podoby vhodné pro vysílání elektrických, zvukových nebo optických signálů (Morseovka, binární kód)

Základy šifrování

SUBSTITUČNÍ ŠIFRY

- nejrozšířenější
- záměna znaků OT za znaky šifrové abecedy (písmena, čísla, symboly, …)

TRANSPOZIČNÍ ŠIFRY

- změna pořadí znaků v OT podle určitých pravidel
- počet a tvar znaků OT je stejný jako u ŠT

Substituční šifry

- Jednoduchá záměna = jediná šifrovací abeceda
- Převodová tabulka:

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

- př.: OT: Sabina

ŠT: HZYRMZ

Substituční tabulky

OT:	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
ŠA	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
OT:	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
ŠA	X	S	A	D	Z	R	F	P	J	W	C	Q	T	E	Y	M	B	K	H	N	O	U	G	L	V	I
OT:	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
ŠA	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
OT:	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
ŠA:	⇨	⇦	⇨	⇦	⇨	←	→	↑	↓	↖	↗	↙	↘	↔	↕	▲	▼	△	▽	◀	▶	◁	▷	◣	◢	◤

Dešifrování

- Stejný princip jako u šifrování, ale opačný postup hledání znaků

OT:	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
ŠA:	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

- př.: ŠT: V VKWHYLGLT

  OT: PODPAREZEM → pod pařezem

Transpoziční šifry

- Text psaný pozpátku
- př.: OT: HAJKOVA
  ŠT: AVOKJAH
- Střídání první a poslední pozice
- př.: OT: heslo je klokan → 13 pozic
  ŠT: H S _ E L K N A O K J L E
  O

Transpoziční šifry

- Zápis „ob tři“ pozice:

  OT: TRANSPOZICE → 11 pozic

  ŠT: T N O C R S Z E A P I

- Šifrovací systém podle plotu:

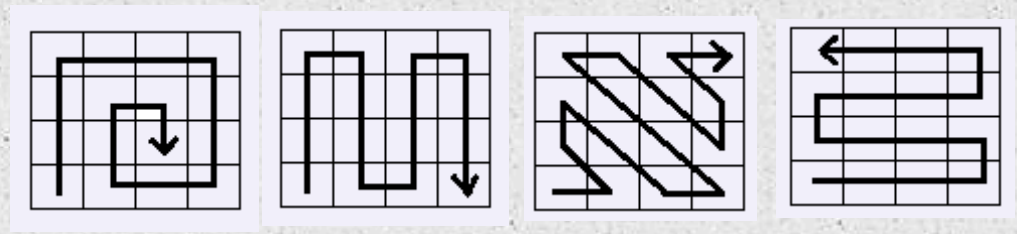
  OT: hledej kolem studny

H				E				L				T				Y
	L		D		J		O		E		S		U		N	
		E				K				M				D		

ŠT: HELTY LDJOE SUNEK MD

Další transpoziční tabulky

- Zápis znaků OT do tabulky po směru šipek → ŠT čteme po řádcích



- př.:

L	O	J	E
S	T	A	O
E	U	N	R
H	G	N	A

ŠT: LOJES TAOEU

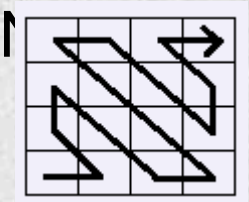
NRHGNA

Dešifrování

- u jednoduchých transpozic čteme text podle dohodnutého pravidla
- u tabulkových transpozic musíme nejprve připravit vhodnou tabulku, zapsat do ní ŠT po řádcích a OT přečíst podle předem dohodnutého pravidla

Dešifrování

- př.: ŠT: KHRNI SROOE EAYVZ STNSE



→ 25 znaků → tabulka 5x5

K	H	R	N	I
S	R	O	O	E
E	A	Y	V	Z
S	T	N	S	E
N	A	A	J	J

V

OT: naše tajná skrýš je ohrožení

Zdroje

- PELÁNEK, Radek. *Hlavolamikon: [sbírka hlavolamů, hádanek, šifer a logických úloh]*. Brno: Computer Press, 2014. ISBN 978-80-251-4303-2.
- HÁJKOVÁ, S. *Luštění transpozičních šifer s podporou počítače*. Hradec Králové, 2014. Bakalářská práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí bakalářské práce PhDr. Michal Musílek, Ph.D. 41 s.