

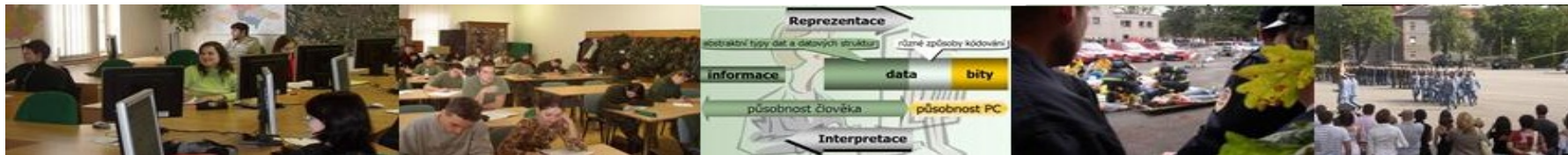
Applied informatics

Secure storage of information, its
encoding in the selected software
environment.

ZEMÁNEK, Z. - PLUSKAL, D. - SMETANA, B.

Secure storage of information, its encoding in the selected software environment

1. Secure storage of information
2. Privacy encryption
3. Presentation of examples of data protection for your case study.
4. Assignments



Aims of the exercise

1. Provide students with basic information about the secure storage of information.
2. Clarify data encryption.
3. Insert sample data protection in your case study.

Viruses

While some viruses can be intentionally destructive (eg delete files on disk), many other viruses are relatively harmless or merely annoying. For some viruses, destructive code starts with a delay.

Life of so-called "zombie" (example):

1. The author of the virus manages to infect a user's PC.
2. Viruses on infected computers continuously log on to IRC server and create a network of compromised computers (botnet).
3. Spammer pays virus writers fee for the use of the network.
4. Spammer sends instructions using the IRC channel
5. Compromised computers send spam.

Cryptography

1. Current computer science cryptography can not do without.
2. Proper use allows secure operation of computer systems and their applications.
3. Basic skills are also applicable in other areas.
4. They are often based on interesting theories and their application in practice.

Kerckhoffs principle

❑ Security of encryption system must not depend on the secrecy of the algorithm, but only on the secrecy of the key.

Transposition ciphers

Simple transpositions

writing backwards

- Only change the order of the letters, not their appearance

Front / Rear

- Writes one letter from the front, one from end

permeation

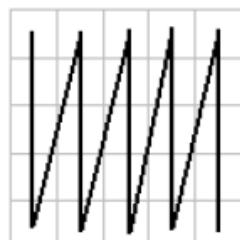
- Text is divided into two halves. Start first with odd positions and write the letter of the first half, and then fill even positions with the letters of the second half of the text.

by fence

- Text is divided into two groups - the first will contain all odd letters and the second all even letters. Ciphertext is formed by joining the first and second groups. [3]

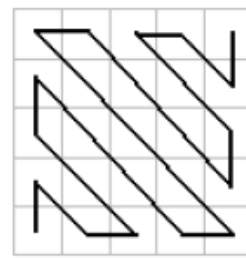
Tables

□ The text is written in different ways to the table, and then the lines are copied. [3]



T	P	E	M	R
R	O	Z	O	I
A	Z	A	C	Z
N	I	P	I	K
S	C	O	M	Y

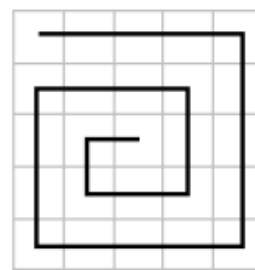
TPEMR ROZOI AZACZ NIPIK SCOMY



O	M	I	Z	Y
O	P	O	R	K
P	Z	A	C	M
R	S	I	Z	I
T	A	N	C	E

OMIZY OPORK PZACM RSIZE TANCE

Text: TRANSPOZICE POMOCI MRIZKY



Y	K	Z	I	R
C	I	Z	O	M
E	R	T	P	I
Z	A	N	S	C
A	P	O	M	O

YKZIR CIZOM ERTPI ZANSC APOMO

Transposition by key

- ❑ An encrypted message is written to table columns of the table and we write the keyword above the table.
- ❑ After the columns are sorted by the letters in alphabetical order of the keyword, the cipher text will read line by line. [3]

Text: TRANSPOZICE POMOCI MRIZKY

S	I	F	R	A	A	F	I	R	S
T	P	E	M	R	R	E	P	M	T
R	O	Z	O	I	I	Z	O	O	R
A	Z	A	C	Z	Z	A	Z	C	A
N	I	P	I	K	K	P	I	I	N
S	C	O	M	Y	Y	O	C	M	S

REPMT IZOR ZAZCA KPIIN YOCMS

Substitution ciphers

- ❑ Substitution is replacing letter by another letter, or character of a cipher alphabet.
 - Monoalphabetic - the entire text is encrypted using a single cryptographic alphabet, i.e. each letter is replaced with same character.
 - Homophony - some letters (usually the most frequently used) can be represented by more than one character.
 - Polyalphabetic - each letter of the alphabet encrypts differently (according to a key).
 - Bigram (trigram, polygram, ...) - the characters of the text (bigram - two characters) is replaced by another group of letters of ciphertext of the same number of letters.
 - Digraphic - each letter is replaced with a pair of characters. [3]

Caesar cipher

□ In the first row: the whole alphabet, in the second row: shifted alphabet (in our case, according to the key $A = T$).

Copyright (c) 1999 Les Éditions Albert René / Goscinny-Uderzo



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
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

OXGB OBWB OBVB

veni vidi vici

Caesar with a keyword

- ❑ The first line is the normal alphabet.
- ❑ The second: write the keyword first (do not repeat any letter twice and enter the remaining letters of the alphabet). The longer the keyword, the more characters will be garbled. [3]

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

Text: Pomocné slovo - Rqoqgpi anqvq

Reversed alphabet

❑ Cipher alphabet is reversed :

A=Z, Z=A, B=Y and Y=B etc.

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

Text: Prevracena abeceda

Cipher: KIVEIZXVMZ ZYVXVWZ

Assignments

1. Team leader and members test the encryption capabilities of the text and the selected paragraph encrypted by the chosen method and insert into the case study.
2. Describe a typical common virus infection (expected length: 1 page A4)

Resources:

1. Typy poškození dat. *<i>Http://www.datahelp.cz</i>* [online]. 2010 [cit. 2013-12-13]. Dostupné z: <http://www.datahelp.cz/zachrana-dat/typy-poskozeni-dat/>
2. Hlídací pes 2002 2.04. *Http://www.slunecnice.cz* [online]. 2013 [cit. 2013-12-16]. Dostupné z: <http://www.slunecnice.cz/sw/hlidaci-pes/>
3. Kryptografie. *Http://cs.wikipedia.org* [online]. 2013 [cit. 2013-12-16]. Dostupné z: <http://cs.wikipedia.org/wiki/Kryptografie>