Šifry 2 - řešení

1. Ve videu se mluví o tzv. transpozičním šifrování. Tento způsob šifrování zachovává soubor použitých písmen textu, který chceme zašifrovat, avšak zamění (promíchá) jejich pořadí dohodnutým způsobem. K přeházení písmen můžeme například použít tabulku se třemi sloupci. Otevřený text zapisujeme do tabulky po sloupcích, zašifrovanou zprávu čteme po řádcích. Na obr. 1 je ukázka zašifrování textu „TRANSPOZICNI SIFRA NENI BEZPECNA“ a výsledná šifra.

T	N	I
R	I	B
A	S	E
N	I	Z
S	F	P
P	R	E
O	A	C
Z	N	N
I	E	A
C	N	

TNIRI BASEN IZSFP PREOA CZNNI EACN

Obr. 1.

a) Zašifrujte stejný text, ale pomocí tabulky s pěti sloupci.

b) Dešifrujte následující text, o kterém víte, že byl zašifrován transpoziční šifrou (tabulkou o 10 sloupcích).

KKKYU ECTKP DJMBK TOTTR YEAYA AJOOI ZDKLA KECMP UNOAB MAOUA

ZOUKY ANNVD CUKDB BEEME LJAYY YMNNC OETZL TAIOH VTAKA TBJHJ

EABOJ OYAAE

a) Šifrovaný text má 29 písmen. Vzhledem k tomu, že tabulka má mít 5 sloupců, tak musí mít 6 řádků (5 × 6 = 30), tj. text budeme zapisovat do tabulky na obr. 2. Postupně (po sloupcích) zapíšeme do připravené tabulky text, který chceme zašifrovat.

Obr. 2

T	O	S	E	P
R	Z	I	N	E
A	I	F	I	C
N	C	R	B	N
S	N	A	E	A
P	I	N	Z	

Obr. 3

Z tabulky na obr. 3 čteme po řádcích zašifrovaný text:

TOSEP RZINE AIFIC NCRBN SNAEA PINZ

b) Do tabulky o 10 sloupcích postupně po řádcích zapisujeme zašifrovaný text a dostaneme tabulku na obr. 4.

K	K	K	Y	U	E	C	T	K	P
D	J	M	B	K	T	O	T	T	R
Y	E	A	Y	A	A	J	O	O	I
Z	D	K	L	A	K	E	C	M	P
U	N	O	A	B	M	A	O	U	A
Z	O	U	K	Y	A	N	N	V	D
C	U	K	D	B	B	E	E	M	E
L	J	A	Y	Y	Y	M	N	N	C
O	E	T	Z	L	T	A	I	O	H
V	T	A	K	A	T	B	J	H	J
E	A	B	O	J	O	Y	A	A	E

Obr. 4

Z této tabulky po sloupcích čteme ukrytý text. Vidíme, že šifra skrývá slavný citát Jana Wericha.

„Když už člověk jednou je, tak má koukat aby byl. A když kouká, aby byl, a je, tak má být to, co je, a nemá být to, co není, jak tomu v mnoha případech je.“

2. V předchozí úloze jsme znali počet sloupců šifrovací tabulky. Pokud tuto informaci nemáme, stačí postupně zkoušet různé rozměry tabulky tak dlouho, dokud nedostaneme smysluplný text. To je důvod, proč není transpoziční šifra považovaná za bezpečnou. Snadné vylepšení poskytuje použití tajného klíče, který vepíšeme do záhlaví tabulky. Po zapsání textu uspořádáme sloupce tabulky abecedně podle písmen klíče. Šifrovanou zprávu pak čteme po řádcích.

   a) Zašifrujte text „DNES JE KRASNY DEN“ klíčem SOK.

   b) Jaký text ukrývá zpráva „OKZKU YEOVJ NSRSYT“ zašifrovaná klíčem SEDM?

a) Vzhledem k tomu, že heslo má tři písmena a šifrovaný text obsahuje 15 znaků, bude mít šifrovací tabulka tři sloupce a pět řádků. Do záhlaví tabulky napíšeme klíč a máme připravenou tabulku pro šifrování (obr. 6). Zapíšeme do tabulky text, který chceme zašifrovat (obr. 7), abecedně uspořádáme sloupce (obr. 8).

S	O	K

Obr. 6

S	O	K
D	E	N
N	K	Y
E	R	D
S	A	E
J	S	N

Obr. 7

K	O	S
N	E	D
Y	K	N
D	R	E
E	A	S
N	S	J

Obr. 8

Z obr. 8 po řádcích dostaneme zašifrovanou zprávu:

NEDYK NDREE ASNSJ

b) Jednotlivé kroky provádíme v opačném pořadí, než v bodě a). Nejprve vytvoříme tabulku se záhlavím s abecedím uspořádáním sloupců (obr. 9) a to této tabulky napíšeme zašifrovaný text (obr. 10). Přeházeme sloupce tak, aby v záhlaví tabulky byl smluvený klíč (obr. 11) a po sloupcích přečteme z tabukly skrytý text:

D	E	M	S

Obr. 9

D	E	M	S
O	K	Z	K
U	Y	E	O
V	J	N	S
R	S	Y	T

Obr. 10

S	E	D	M
K	K	O	Z
O	Y	U	E
S	J	V	N
T	S	R	Y

Obr. 11

„Kostky jsou vrženy“