Pracovní list číslo 2: Polyalfabetická substituce

Z minulého listu víme, že slabým místem monoalfabetické substituce je zachování frekvence znaků. Tomu se můžeme vyhnout zobrazováním každého písmena na různé znaky v závislosti na jeho poloze v textu. Tento princip se nazývá polyalfabetická substituce - používáme totiž několik šifrovacích abeced.
Nejznámějším příkladem polyalfabetické substituce je *Vigenèrova šifra.* Tato šifra je složena z několika Caesarových šifer – jednotlivé šifrovací abecedy jsou prosté posuny. Volba posunu pro zašifrování daného písmena závisí na poloze písmena v textu. Pro snadnější zapamatovatelnost jsou tyto posuny určeny pomocí klíče (hesla). Šifrování provádíme následovně: zapíšeme si pod text zprávy a dostatečně krát zopakovaný klíč a tyto dva řádky „sečteme“ dle *Vigenèrova šifra* (viz *Vigenèrova čtverec* – konec pracovního listu). Uveďme příklad:

z i j v y r o v n a n e t r o c h u s e u c a t r o c h u p r e m y s l e j a k a z d y d e n
p e t r k l i c p e t r k l i c p e t r k l i c p e t r k l i c p e t r k l i c p e t r k l i

O M C M I C W X C E G V D C W E W Y L V E N I V G S V Y E A Z G B C L C O U I M P D W P N P V

t r o c h u m a l u j a k r e s l i a z p i v e j a t a n c u j a h r a j s i a p r a c u j
c p e t r k l i c p e t r k l i c p e t r k l i c p e t r k l i c p e t r k l i c p e t r k

V G S V Y E X I N J N T B B P A N X E S G S G M L P X T E M F R C W V T A C T I R G E V L T

Rozšifrování se provádí analogicky, tentokrát od zašifrované zprávy „odčítáme“ klíčové slovo. Vigenèrova šifra již výrazně srovná frekvence znaků v šifrované zprávě, a čím je delší klíč delší, tím jsou frekvence vyrovnanější a šifra bezpečnější. Vigenèrova šifra byla poměrně dlouho považována za nerozluštitelnou, ale i ona má své slabé místo. Je jím opakování klíče. Čím je klíč delší, tím méně se opakuje a tím je také těžší rozšifrování.
Další možností je použít klíč pouze k „nastartování“ substituce a dále šifrovat zprávu dle sebe sama:

z i j v y r o v n a n e t r o c h u s e u c a t r o c h u p r e m y s l e j a k a z d y d e n
p e t r k l i c z i j v y r o v n a n e t r o c h u s e u c a t r o c h u p r e m y s l e j a

O M C M I C W X M I W Z R I C X U U F I N T O V Y I U L O R R X D M U S Y Y R O M X V J H N N

Abychom však dostali opravdu bezpečnou šifru, je potřeba používat nekonečný náhodný klíč, respektive klíč stejně dlouhý jako samotná zpráva. Je také třeba tento klíč použít pouze jednou. Tato šifra je známá jako *jednorázová tabulka.* Zřejmou nevýhodou tohoto přístupu je nutnost předání rozsáhlého klíče mezi Alici a bobem, respektive předání celé sady klíčů - každý klíč použijeme pouze jednou. Je několik možností, jak takové klíče získat:

- Tabulky náhodných čísel: Alice i Bob mají stejnou knihu náhodných čísel. Alice při šifrování uvede, kterou stránku použila k zašifrování. Stránky se ihned po použití zničí.
- Telefonní seznam: pokud vezmeme telefonní seznam, postupujeme abecedně a z každého čísla vezmeme poslední dvě cifry, výsledná posloupnost bude mít

Mgr. Irena HENCOVÁ, MBA, LL. M. 725 037 081
irena.hencova@ddmporuba.cz

dostatečně náhodný charakter. V tomto případě je potřeba, aby Alice i bob měli stejný telefonní seznam. Alice pak pouze uvede, u kterého jména začíná.

- Iracionální čísla: číslice v desetinném rozvoji iracionálních čísel jako například π či e mají také dostatečně náhodný charakter.

Náhodný charakter klíče je opravdu důležitý. Jakákoli pravidelnost klíče může posloužit k rozluštění šifry. Například použití textu knihy jako dlouhého klíče je nedostatečné. Základní postup luštění je následující. Nejdříve předpokládáme, že celý klíč sestává z nějakého frekventovaného slova či fragmentu, například trojice písmen „pro“. Pokusíme se pomocí tohoto klíče zprávu zašifrovat. Většinou nám vyjde nesmysl, ale pokud se někde objeví něco smysluplného, může to znamenat, že na daném místě klíč obsahuje „pro“. Na daném místě se pokusíme odhadnout předcházející či následující písmena zprávy a pomocí nich zase rozluštit část klíče. Takto postupujeme dál a současně luštíme obsah klíče a zprávy.
Podobně se dá postupovat, pokud bychom jeden klíč, třebas i náhodný, použili k zašifrování dvou smysluplných zpráv. Dokonce i daleko menší pravidelnosti mohou vést k rozluštění šifry. Ruským agentům, kteří tuto šifru používali, vyráběli tabulky náhodných čísel sekretářky na psacích strojích. Při psaní podvědomě docela často střídaly levou a pravou ruku - tedy posloupnost 18392 se vyskytovala pravděpodobněji než 13212. Tato drobnost umožnila Američanům některé zprávy rozluštit.

ŠIFRY – řešením rčení/citáty slavných

Příklad 1 (délka klíče 3)

GIZRP QKIPR GGQUE WYTXD BUPZL LANHQ SLUWY XHXDX BKUIW SLUWY XHUFU YFLLA NMQWU YQUEW YTXDE DG

Příklad 2 (Heslo má 4 znaky)

XTFVY SMIYQ BOGMD SZJVD PSRZU IUUFI QEHHV TZKYN DSLJZ UFZIM MYPHZ TEIBV ZACUU JRCCL FBMIK AFDVS GCQBV KYZGI MIYQZ DPSRZ THVZX MCAWM QOCTV DPVRV TCQIO QDAOM THIQB ANBRL ZAVZQ GJUEQ TINXF TMNSU VWUPV LRTZL PNZOR TDDEI YWGAY VRSQL KIIIC IYAKV JARMJ XIENB FNZXI ENBRV VDURD BQEOM THIWC OBQTK TACOU QKDEA ZSKWC EXVFS ORVPJ SIOXQ CEEAZ AOCUI UQAAF AZLDL JKTTV PNQFD FCUTV BFVDZ R

Příklad 3

ORPOC HJTPA ERDCL XBJEP ACAHB BOEZM DCMLM UJNSC IVMGF MVRJM THSCE NPQNH KMMCU AEGBF VIPWA QUUJR JTTHK MZLFQ JDLSB MMZSH OPPRW FRHOS MRPMA UOUTF OVZDE YAQJQ AGOST FHRRD OWZLF QAGFD JGARD QFDZQ UFTBU UBMWV ZYJLV LJBDB OYSWM FASPE LBCPB BMIGY LSYEZ FFNSZ BXAHV MCIOY TEVKV CEQPW YMEFV LLNVP ZBACE SUCOM IVJWV JZUEQ WTYSS LNRIU DYBGR RTJRT BJVXK TZTPK KFFLK STKIP AUKPF JTLNM KPPDE PBMIY AKOKP FVLPT HREUE YAVMD

Dům dětí a mládeže
Ostrava-Poruba
příspěvková organizace

středisko DDM Polská
Polská 1624/4, Ostrava – Poruba 708 00
www.ddmporuba.cz

Přezdívka	**Jméno**	**Příjmení**	**Věk** (např. 10 let)	**Kontakt**

Název	**Řešení šifry**	**Počet bodů**
Příklad 1		
Příklad 2		
Příklad 3		

Vigenèrova čtverec

	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	I	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	W	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	W	X	Y

Mgr. Irena HENCOVÁ, MBA, LL. M. 725 037 081
irena.hencova@ddmporuba.cz

OSTRAVA!!!