Zadání šifer pro velikonoční výlet (kategorie 2)

Pár základních pravidel úvodem: Při šifrování jsem používal zásadně anglickou abecedu, tedy 26 písmen bez diakritiky (pro jistotu – CH v tomto systému představují dvě písmena). Kdyby to někde bylo jinak, bude to uvedeno. Některé šifrované texty jsou v souladu s pravidly radiotelegrafie rozděleny do skupin po pěti písmenech, ale na rozdíl od vojenských šifer nejsou doplňována chybějící písmena.

Pokud dojde na Polybiův čtverec, je použitý v původní podobě, kde se písmeno I shoduje s písmenem J. Kdybyste bádali nad tím proč, tak proto, že čtverec má 25 pozic, ale pracujeme s 26 písmeny. Polybiův čtverec sám šifrou není, je to stejný případ jako Morseova abeceda; ale pokud použijeme klíč, je to zajímavější.

Za každý správně dešifrovaný text dostanete bod (drobné chyby toleruji, ale nesmí měnit smysl textu). Pokud je text otázkou, další bod dostanete za správnou odpověď. Celé řešení pošlete na mou adresu do 15. dubna. Na kotevním webu pak najdete správné odpovědi a také Vaše pořadí. Všechny použité šifry najdete v souboru šifer z Pražských strašidel, který je také na kotevním webu. Pokud byste tápali, téměř vše se dá dohledat (strýček google v tomto případě opravdu ví skoro všechno) a pokud ne, na webu Kotvy se během příštího týdne objeví nějaká nápověda. Dotazy a protesty můžete poslat na mého emila, ale pozor – otázka „jak se řeší toto?“ automaticky odečítá bod(y). (*Protesty anulují všechny body pět let dopředu…* ☺)

Šifra první:

Japonka. K řešení potřebujete úkol 1; u japonky musíte znát počet řádků a počet sloupců. Jedno číslo dostanete jako součet počtu schodů a počtu vodorovných trámů rozhledny, druhé pak když od výsledku odečtete počet svislých (šikmých) trámů. Ale na to, které číslo určuje řádky a které sloupce budete muset přijít sami. Výsledek je citát a je použitá naše abeceda s diakritikou a interpunkční znaménka počítejte jako znak.

L L T Z Á Ž Ř E , J Ř V U Ů V E E A Ů , N V M B A V Í M S O V M L S I Ě E . Y K A H Ě T L K J V T K K K V Ť L L Ř L Á E R E E Á D D O Ů B E A Í , V M Á S M V Y Y L L Y V L V Z Á .

Šifra druhá:

Polybiův čtverec, klíč v druhém úkolu.

14–15–35–12–14–11–44–22–34–44–24–31–41–24–21–35–45–24–21–13–14–24–14–24–13–14–24–31–24–24–14–45–22–44–24–12–22–42–22–12–13–45–24–44–13–12

Šifra třetí:

Je celkem jednoduchá, klíčem je číslo z posledního, tedy osmého úkolu. Ale dejte pozor, na šifrovaný text to číslo budete muset použít tolikrát, kolik je ono samo. Pozor na to, že tu mohla být použitá kombinace metod šifrování:

[2]S I L B O C N N I P M Y A K J C I L R G Y P M C U I A Y Z Z P C L P A M C S O L U I ! Y

Šifra čtvrtá:

Caesar; klíč podle úkolu 7.

R U F I A J Q F P A N A G U W N E Y G U G P A N A L N E P A G W F E Z K R H P W R U R L N W V A

Šifra pátá:

Vigenérův polyalfabetický systém; klíč v úkolu 6 (pro zjednodušení přiložena Vigenérova tabulka). Šifrován je pouze text citátu, takže za jeden bod. Ale druhý bod dostanete, pokud zjistíte, kdo je autorem citátu, a třetí prémiový bod pokud najdete, ze které knihy text pochází.

M V P L Q W R V Y Z B B P O B R P U N Z A U J P L H

Šifra šestá a poslední:

Nepotřebujete žádný klíč, jen trochu selského rozumu…

CeN tU RI oPUb lIu s hon Or i usJ EoS eL JEmu žrO vNON e nín E jEn v cElé LeG iI AlE VCE LÉ mŘÍm ěA iga liI

Vigenérova šifra

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