

## Nápovědy – III.kolo

### Soutěž 2007 - třetí kolo, pokračování příběhu Štěpána Schmidta

---

14.10.2007

<http://crypto-world.info/news/index.php?prispovek=6136&sekce=s>

#### Soutěž 2007 - nápověda č.6

Obecná nápověda pro zadávání slov, kterými se prokazuje, že řešitel úlohu třetího kola rozluštil...

III/1: Obraz?

III/2: P1

III/3: Jakému strýci?

III/4: Odkud?

III/5: (3)

III/6: (3)

(vždy je správnou odpovědí jen jedno slovo, toto slovo je obsaženo v otevřeném textu a vždy se zadává bez diakritiky a velkými písmeny)

### Soutěž 2007 - nápověda č.7

---

15.10.2007

<http://crypto-world.info/news/index.php?prispovek=6146&sekce=s>

V pozůstalosti Štěpána Schmidta se mezi různými matematickými texty objevily i dvě tabulky s neznámým obsahem.

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
?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
ST	OV	NI	VA	NE	EN	PO	RA	RO	SE	OU	CH	PR	RN	ND	NH										
?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?										
STR		FRIDRICH		AUGUST		VALKY		VOJENSKA		RADA		SLEZKO													
?		11		12		2		31		32		4													

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
?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
ST	OV	PO	RA	RO	SE	OU	CH	MARIE			TEREZIE			PETR		KATERINA									
?	?	?	?	?	?	?	?	1			2			3		4									

## Soutěž 2007 - nápověda č.8

---

16.10.2007

<http://crypto-world.info/news/index.php?prispevek=6156&sekce=s>

### **Třetí** varianta šifrovaného textu **obležení Prahy**

12 CH x 14 m N ch N s 27 4 m T N b I d g 1 m 1 21 d 24 N 12 19 i M 16 P 3  
ch S 1 I e x 1 s CH 13 b d z 23 f t 19 CH g L R 20 16 d A h S n e c N s 15  
d 20 t M 10 e h Q T b f L 16 d 23 n f n f 2 23 11 d h M ch Q 3 6 a 2 A g 21  
t L 11 CH 16 N B f s m f 1 4 N a Q d 23 25 B 24 CH A f l f L 4 4 H K 27 1  
10 d 21 15 R r n L S 17 P 3 24 6 N T y f CH 4 N 15 1 C CH L b 25 23 2 r d J  
d a M 11 R 10 CH 18 P M t H n 2 15 10 2 i L a 26 B ch M 15 c 27 K G l f 18  
Q 2 t e K e 14 27 1 n H j M J H 4 R 13 ch 2 a 20 b S P 21 j 27 j s e Q 26 S  
y 24 H B d l e z 19 s L K e s 4 Q z CH A f 20 k L S j p 2 K M 23 20 k M R j  
N O S m R n d 16 O 1 24 f 15 11 3 k 19 d l 3 14 6 M l f 21 J N L 4 y 24 d 6  
S L 5 23 25 C g N 6 S 21 d a J G z G 20 H J m f O 2 j M R 21 j e M 6 6 G K  
26 24 f 5 f l d 8 d l d P 2 K e 13 4 1 T m e 15 P M z ch M 6 I G 12 21 13 f  
19 f 22 26 12 H t 11 CH 14 22 21 t O CH A 2 T t i l s 20 d 19 n CH 13 H R k  
N K CH n 2 2 c 25 B h N 15 n 2 4 2 I d T 5 O z e K G 18 Q 2 h R 23 N a J d  
y d l G 18 Q L r M x e 11 e n 1 19 e 23 N 10 21 j M 16 M C f t m d 19 G I l  
f 10 20 G K x d 4 L S D 3 s 20 a M y G 17 M 13 L A CH 22 f 24 G t d z 19 s  
22 G 16 P M t L n 3 21 d 22 M 12 f l 19 i 3 O 2 6 2 22 25 17 Q 3 C N 23 2 J  
l m M 24 27 18 K 1 m b G t 24 25 3 c 25 A h N 14 m f 17 O CH s f J e x B f  
K 1 x m CH B G I H c CH s 22 S z 3 g 1 12 G 14 e S t L i d 13 12 CH z 5 27  
n 1 16 O 1 23 f j P G 4 J N 1 s 1 k M a i J CH C H 15 e 21 r Q d 5 P 3 j N  
S 21 k f 1 P 14 3 6 27 17 P N t M n 1 O G y S 11 H 23 d J H t e J T 14 11 H  
z 5 25 21 M S 21 s P f 6 H s 5 M t 25 4 n d N 4 5 CH J 26 S 24 f 19 n G A d  
i S t I G O f 11 3 x a L y CH 14 G I L 19 r CH 18 Q S 21 k 25 i R Q E G P r  
D O H d 4 O H A g t M g M 12 13 f l 3 6 P R g 25 23 i 24 d s n T K f r 3 18  
3 1 f s CH 19 H C 21 e 4 14 20 e s 16 1 4 f 19 1 s 20 e 4 15

## Soutěž 2007 - nápověda č.9

---

18.10.2007

<http://crypto-world.info/news/index.php?prispevek=6169&sekce=s>

V pozůstalosti Steplinga jsem našel vzpomínku na to, jak mu Štěpán Schmidt popisoval jednu anglickou šifru...

## Ze vzpomínek Steplinga

Jednou, když jsem navštívil svého přítele Štěpána v lázních Bad Ischlu vyprávěl mi o velmi zajímavých transpozičních šifrách.

Štěpán napsal do levého sloupce otevřený text a do pravého sloupce šifrový text po transpozici.

MAR	R A M
MARI	R A I M
MARIE	R A I M E
MARIE T	R A I T M E
MARIE TE	R E A I T M E
MARIE TER	R E A I T R M E
MARIE TERE	R E A I T R M E E
MARIE TEREZ	R E A I T R Z M E E
MARIE TEREZI	R E I A I T R Z M E E

„Asi nevidíš pravidlo jak se text transformuje?“ , zeptal se mě.

„Ano, je těžké si jej uvědomit“ pokračoval Štěpán.

„V tomto konkrétním případě se text vepíše do níže uvedené tabulky na místa označená hvězdičkami. Jakmile text vepíšeš, dostaneš šifrový text tak, že jednoduše opíšeš znaky nejprve z prvního řádku tabulky, pak z druhého a nakonec třetího.

		*		*						*			
	*		*		*		*		*		*		
*						*		*				*	

Tedy např. MARIE TEREZIE = R E I A I T R Z E M E E

		R				E				I			
	A		I		T		R		Z		E		
M				E				E				*	

Klíčem k této šifře je tedy domluvená tabulka (počet řádků) a způsob zápisu textu do této tabulky. Šifru vynalezli Angličané a protože jim psaní do sloupců v tabulce připomíná laťky v plotu, nazvali tuto šifru „podle plotu“ (Rail fence cipher). Angličané se domnívají, že je to poměrně bezpečná šifra, ale mýlí se ! Nedávno jsem jednu takovou dokázal rozluštit.“