

Šifrování dat

Minulá hodina

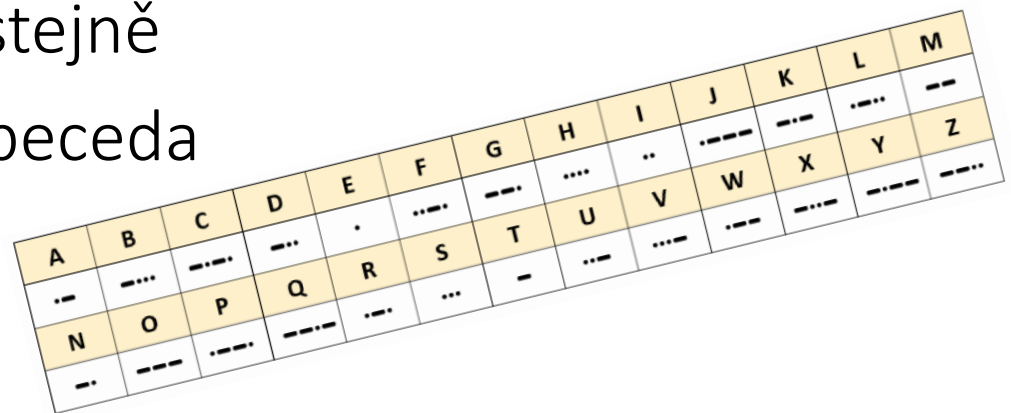
Kód =

- způsob, jak zapsat informaci tak, aby se dala zaznamenat a přenést
- Více podob

Standardizovaný kód =

- zveřejněn a používán všude stejně
- Braillovo písmo, Morseova abeceda

Dobrý kód = ?



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
-.	---	-.-.	---	...-	...	-	...-	...-	-.--	-.-.	-.-.	---

Minulá hodina

Znaková sada

32	mezera	51	3	70	F	89			
33	!	52	4	71	G				
34	"	53	5	72				110	n
35	#	54	6					111	o
36	\$	55				93]	112	p
37	%				K	94	^	113	q
38				76	L	95	_	114	r
39			:	77	M	96	`	115	s
40		59	;	78	N	97	a	116	t
41)	60	<	79	O	98	b	117	u
42	*	61	=	80	P	99	c	118	v
43	+	62	>	81	Q	100	d	119	w
44	,	63	?	82	R	101	e	120	x
45	-	64	@	83	S	102	f	121	y
46	.	65	A	84	T	103	g	122	z
47	/	66	B	85	U	104	h	123	{
48	0	67	C	86	V	105	i	124	
49	1	68	D	87	W	106	j	125	}
50	2	69	E	88	X	107	k	126	~

Co by se stalo, kdyby tyto zprávy někdo zachytil?

Lze tomu nějakým způsobem předejít?

IIIOTVIAUKA



Šifrování dat

Dokážete podle této tabulky rozluštit zprávu?

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



Stejným způsobem zašifrujte jméno vaší oblíbené filmové postavy

Jaké jsou výhody a nevýhody tohoto způsobu šifrování?

Šifrování dat

Zkuste vymyslet jiné způsoby, jak byste mohli pomocí tohoto klíče zakódovat zprávu „ahoj“

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

Šifrování dat

Pomocí následujícího klíče zašifrujte slovo: POKLAD

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
1					2					3					4					5				

Šifrování dat

Dešifrujte tuto zprávu:

L5-15-18-L3-C8

X	<i>8</i>	<i>7</i>	<i>3</i>	<i>5</i>	<i>2</i>
<i>C</i>	A	B	C	D	E
<i>I</i>	F	G	H	I	J
<i>S</i>	K	L	M	N	O
<i>L</i>	P	Q	R	S	T
<i>A</i>	U	V	X	Y	Z

Šifrování dat

Ve dvojici si doplňte do tabulky vlastní slovo a číselnou kombinaci. Následně si pošlete zašifrované slovo a dešifrujte.

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

Šifrování dat

Dešifrujte tuto zprávu:

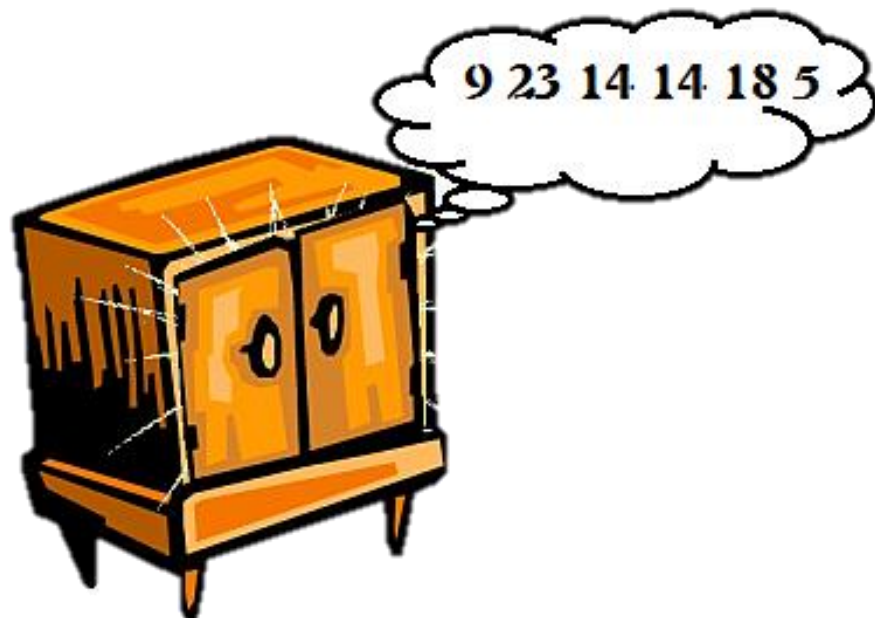
44-666-222-55-33-999



Úlohy k zamyšlení

Ve skříňce je zamčený poklad a hráč musí říct nahlas zašifrované slovo, aby ji otevřel.

Po kliknutí na dvířka skříňka řekne 6 čísel. Každé číslo je třeba nahradit písmenem. Každé písmeno abecedy odpovídá jinému číslu.



Jaké je ono kouzelné slovo?

- A) TICKET
- B) LOOSER
- C) COMMON
- D) WINNER

Úlohy k zamyšlení

Která z následujících možností **nevznikla** zašifrováním slova TEXT? Proč?

(A) · - ·· / · / ··· / - // (B) ^ ↗ ↘ ⇌ ⇓ (C) 84 69 88 84 (D) 4/3 6/1 5/1 6/1

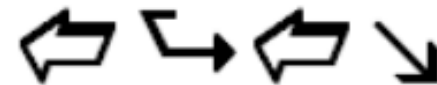
Úlohy k zamyšlení

Členové party zašifrovali svá jméno pomocí šipek. Každé písmeno abecedy je představováno speciální šipkou.

Například jméno **Ester** je zašifrováno jako:



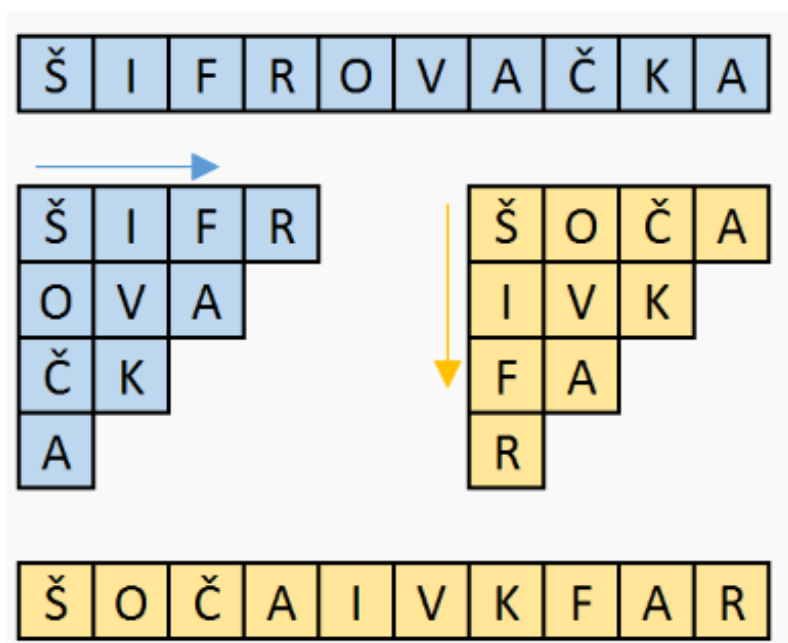
Zjisti, jaké jméno se skrývá pod následující šifrou:



- | | |
|---------|---------|
| a) NANA | c) DANA |
| b) ADAM | d) IVAN |

Katka posílá zprávu Honzovi, ale nechce, aby jí ostatní četli. Snaží se ji tedy napsat v zašifrované podobě. Rozdělí zprávu na části po 10 znacích. Každou část zašifruje touto metodou:

1. Vloží znaky do trojúhelníku, jak je znázorněno v levém modrém trojúhelníku níže.
2. Trojúhelník překlopí (vznikne pravý trojúhelník).
3. Napíše znaky v jejich novém pořadí, jak jsou zapsány v pravém žlutém trojúhelníku.



Katkou šifrovaná zpráva zní "JET?AMEKÁS".

Napiš původní zprávu.

Zdroje

Archiv úloh Bobříka informatiky:

<https://www.ibobr.cz/test/archiv>

Učebnice iMyšlení:

BERKI Jan a Jindra DRÁBKOVÁ. Základy informatiky pro 1. stupeň základní školy [online]. Liberec: Technická univerzita v Liberci, 2020. ISBN 978-80-7494-520-5. Dostupné z <https://imysleni.cz/ucebnice/zakladyinformatiky-pro-1-stupen-zs>.

BERKI Jan a Jindra DRÁBKOVÁ. Základy informatiky pro 2. stupeň základní školy [online]. Liberec: Technická univerzita v Liberci, 2020. ISBN 978-80-7494-521-2. Dostupné z <https://imysleni.cz/ucebnice/zakladyinformatiky-pro-zakladni-skoly>.