21. Jednoduché šifrovací algoritmy (Ceasarova šifra, VIC)

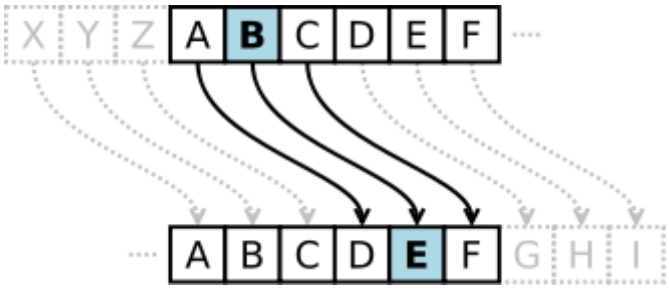
Šifra

Jakýkoli převod otevřeného textu na uzavřený (nečitelný pro běžného uživatele). Přečíst šifru lze na základě znalosti nějaké zvláštní informace, typicky klíče.

CAESAROVA ŠIFRA

Tuto šifru použil poprvé César. Zmínil se o ní ve svých Zápiscích o galské válce.

Šifrování spočívá v tom, že se abeceda posune o zadaný počet písmen.



Tabulka má tedy 2 řádky

A	B	C	D	E	F	…	…	Y	Z
D	E	F	G	H	I	…	…	B	C

POSUN = 3

Zašifrování:

```
((ZNAK – 'A' + ROTACE)%26) + 'A'
```

První znak

Posun

Počet písmen abecedy

Rozšifrování:

```
((ZNAK – 'A' + (26-ROTACE))%26) + 'A'
```

Proto, aby nebylo možné se dostat do záporných čísel

Co se týká bezpečnosti, je tento algoritmus na velmi nízké úrovni, protože nehledě na to jaký je posun, pomocí hrubé síly nejhůře na 25 kroků lze získat správný výsledek.

VIC- ŠIFRA

- Ruská šifra z 50. Let 20. Století (jedna z nekomplikovanějších ručních šifer)
- Mechanismus na dešifrování nebyl nikdy objeven
- Způsob dešifrování by vyzrazen

Důležité

- Permutace čísel 0 – 9
- Šifrovací klíč
  - Tři slova oddělená mezerami (každé písmeno právě jednou)
  - Včetně mezer

	0	1	2	3	4	5	6	7	8	9
	J	D	U		N	A		S	E	X
3	B	C	F	G	H	I	K	L	M	O
6	P	Q	R	T	V	W	Y	Z	_	α

ŠIFROVAT se začíná a končí znakem α tj. 96, mezi nímž je kódovaný text.
EIS WAS HERE – 8357 6557 348628