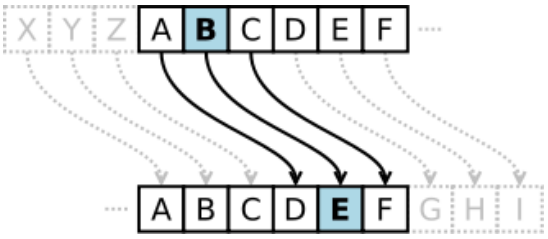
Téma 21: Jednoduché šifrovací algoritmy

Šifra je jakýkoliv převod nějakého pro nás dobře čitelného textu na uzavřený, který není čitelný pro běžného uživatele. Přečíst šifru lze na základě znalosti nějaké zvláštní informace, typicky klíče.

Princip Caesarovy šifry je založen na tom, že každé písmeno zprávy je během šifrování zaměněno za písmeno, které se abecedně nachází o pevně určený počet míst dále.

Počet možných variant klíče této šifry je o jedna menší než počet písmen (znaků) v použité abecedě. Zvolíme-li hodnotu posunu stejnou, jako je počet znaků použité abecedy, bude zašifrovaná zpráva identická s předlohou. Vyšším posunem, například posunem s klíčem o jedna větší, než je počet písmen (znaků) abecedy, dostaneme zašifrovanou zprávu odpovídající prostému posunu o klíč jedna, takže použití klíče hodnoty vyšší než počet znaků abecedy nemá kryptografický význam.



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

Posun = 3

Zašifrování:

((ZNAK – ´prvni_znak_abecedy´ + ROTACE) % ´pocet_znaku_abecedy´) + ´prvni_znak_abecedy´

Rozšifrování:

((ZNAK - ´prvni_znak_abecedy´ + (´pocet_znaku_abecedy´ - ROTACE)) % ´pocet_znaku_abecedy´) + ´prvni_znak_abecedy´

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

VIC šifra je ruská šifra z 50. let 20. století. Je to jedna z nejkomplikovanějších ručních šifer. Mechanismus na dešifrování nebyl nikdy objeven. Pro objevení musel být způsob dešifrování vyzrazen. Pro vytvoření šifry je potřeba permutace čísel 0 – 9 a šifrovací klíč (tři slova oddělená dvěma mezerami, každé písmeno musí být v třech slovech obsaženo právě jednou). Dále musíme znát počet znaků abecedy (nejčastěji 26 znaků).

Následuje typický studentský příklad:

	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