



Caesarova šifra

Tuto šifru používal pro vojenskou komunikaci **Julius Caesar** a popsal ji v Zápiscích o válce galské (odtud je odvozen její název). Caesar používal posun o tři místa, obecně je ale **za Caesarovu šifru označováno jakékoli šifrování na principu prostého posunu písmen** o konstantní hodnotu.

1. Dešifruj následující zprávu – klíč AD

(nezapomeň, že jsou používána pouze písmena anglické abecedy, takže tam nejsou háčky a čárky)

CLWUD SRMHGHPH VSROHFQH GR GLYDGOD.

--	--	--	--	--

2. Zašifruj následující zprávu – klíč AD

SEJDEME SE VE DVĚ HODINY U MOSTU.

--	--	--	--	--	--	--

3. Dešifruj jednotlivá slova podle uvedeného klíče:

Zašifrované slovo	Klíč	Dešifrované slovo
WVJPAHJ	AH	
QRGBKYTOIK	AG	
YAZUFAD	AM	
ATKWPTKX	AT	

4. Zkus prolomit šifru (najít klíč):

RWOXAVJCRTJ SN YARVJ YANMVNC.

--	--	--	--

Hledaný klíč:

