

Vigenèrova šifra – pracovní list

Dokážete zašifrovat vaše tajné heslo? Jak se tvoří šifry? Jak se naopak šifry mohou zpětně dešifrovat? Se všemi těmito tématy se v průběhu zpracování tohoto pracovního listu seznámíte.

Úkol č. 1

Vymyslete si vlastní tajný text, který budete následně šifrovat. Text může být ve formě tajné věty, kterou byste například chtěli poslat svým válečným spojencům. Přemýšlejte nad ním jako nad něčím, co chcete někomu předat tak, aby to nikdo jiný nerozluštil, i kdyby se mu to dostalo do rukou.

Text si запиšte sem: _____

(a nikomu jej neukazujte!)

Nyní si zkuste svůj text sami zašifrovat. Tak, aby nikdo jiný bez tajného klíče váš text nerozšifroval. Nezapomeňte ovšem na nutnost jednotného šifrování na základě klíče.

Šifrovací klíč si запиšte sem: _____

Zašifrovaný text si запиšte sem: _____

Úkol č. 2

V rámci druhého úkolu si vyměňte vaše zašifrované texty se svými spolužáky. Napište váš zašifrovaný text na kus papíru a předejte spolužákovi. Stejně tak dostanete od spolužáka jeho zašifrovaný text.

Zašifrovaný text spolužáka napište sem: _____

Zkuste tento text rozšifrovat a níže zakroužkujte jednu z možností:
Zašifrovaný text jsem rozšifroval/a. Zašifrovaný text jsem nerozšifroval/a.

Požádejte vašeho spolužáka, aby vám sdělil tajný klíč, podle kterého svůj text šifroval.

Tajný klíč si запиšte sem: _____

Zkuste text rozšifrovat znovu, tentokrát s využitím klíče, a níže zakroužkujte jednu z možností:

Zašifrovaný text jsem již rozšifroval/a.

Zašifrovaný text jsem stále nerozšifroval/a.

Rozšifrovaný tajný text запиšte sem: _____

Pokud jste šifru stále nemohli rozluštit, požádejte o radu spolužáka, který šifru vytvářel. Pokud jste šifru rozluštili, diskutujte s autorem šifry její správnost.

Úkol č. 3

V tomto úkolu se seznámíte s moderní a propracovanou možností šifrování. Tu představuje tzv. Vigenèrova šifra. Požádejte pana učitele nebo paní učitelku, aby vám sdělili odkaz na speciální stránku, na které je vytvořena interaktivní verze tohoto šifrování. Nebo naskenujte QR kód vpravo na stránce.



Na této internetové stránce se seznámte s principem tohoto typu šifrování a pokuste se zašifrovat váš tajný text podle šifrovacího klíče.

Šifrovací klíč si запиšte sem: _____

Zašifrovaný text si запиšte sem: _____

Vyměňte si váš zašifrovaný text s jiným spolužákem, sdělte mu šifrovací klíč a nechte jej, aby se pokusil váš zašifrovaný text dešifrovat. Totéž udělejte vy s textem, který získáte od spolužáka.

Zašifrovaný text spolužáka si запиšte sem: _____

Šifrovací klíč spolužáka si запиšte sem: _____

Dešifrovaný text spolužáka si запиšte sem: _____

Diskutujte s vaším spolužákem správnost vašeho i jeho dešifrovaného textu.

Podařilo se vám na základě dešifrovacího klíče správně rozluštit šifru? Napište odpověď na tuto otázku a přidejte odůvodnění: _____

