

Kódování a šifrování – vzorové otázky z testu (9. třída)

Následující otázky jsou jen příklad toho, co všechno můžete najít v testu. Otázky v testu se mohou mírně lišit. Kódovací tabulku, pokud bude potřeba, dostanete společně s testem.

Nelekněte se množství otázek – často jsou si podobné a úzce spolu souvisí. Test nebude dlouhý, rozhodně ne na celou hodinu.

Odpovědi na všechny otázky najdete v prezentacích na <https://www.zsbroumovska.cz/it/>

- Jaký je rozdíl mezi kódováním a šifrováním? K čemu slouží kódování a k čemu šifrování?
- Co má každá šifra navíc oproti kódu?
- Popište stručně vlastními slovy, jak funguje Caesarova šifra
- Zašifrujte/dešifrujte zadané slovo pomocí Caesarovy šifry s klíčem 5
- Dokážeme dešifrovat zašifrované slovo i bez znalosti klíče? Jak?
- Co je to útok hrubou silou?
- Vysvětlete rozdíl mezi Caesarovou a Vigenèrovou/Vernamovou šifrou
- Co je to symetrická a co je asymetrická šifra? Vysvětlete rozdíl
- Jaká je hlavní nevýhoda symetrické šifry? Vysvětlete, jak pomůže asymetrická šifra
- Popište stručně princip asymetrické šifry
- K čemu slouží digitální podpis? Vysvětlete stručně jeho princip
- K čemu slouží certifikát?