

1. Jaký je rozdíl mezi symetrickým a asymetrickým kryptografickým šifrovacím systémem?
2. Zařadte následující šifrovací algoritmy mezi symetrické nebo asymetrické systémy: 3DES, AES, RSA, DES, El-Gammal, Twofish, CAST, ECC, DSA.
3. Nainstalujte si na svůj počítač aplikaci Wireshark (nebo jinou podobnou), seznamte se s jejím ovládáním a účelem. Zkuste provést krátkou analýzu - zachytávání paketů ve vaší síti. Udělejte screenshot a přiložte jej do vašeho dokumentu.
4. Krátce charakterizujte jaký je rozdíl mezi protokoly http a https, a které porty využívají?
5. Co to je a k čemu se používá SSL a CA (Certificate Authority)?
6. Najděte alespoň 3 mobilní nebo desktopové aplikace, které fungují jako trezor a generátor hesel. Krátce aplikace charakterizujte.
7. Co je to Firewall? Jak lze nastavit například ve vaší domácí síti?
8. Co je to VPN, jaké výhody přináší uživateli? Uveďte alespoň 3 různé služby, které poskytují VPN?
9. Krátce charakterizujte následné pojmy: malware, spam, ransomware, hoax, phishing, polymorfní počítačový virus. 10. Co je to 2-faktorová autentifikace? Kde konkrétně ji používáte vy? Pokud ji nikde nepoužíváte, pak si ji někde zaveďte a do dokumentu to popište.