Informačná bezpečnosť - otázky 1 až 5

1. Komponenty informačnej bezpečnosti a charakteristika jednotlivých komponentov

Informačná bezpečnosť pozostáva z hlavných komponentov:

- Dôvernosť (Confidentiality): informácie sú prístupné len oprávneným osobám.
- Integrita (Integrity): informácie neboli neautorizovane zmenené.
- Dostupnosť (Availability): informácie sú prístupné, keď sú potrebné.
- Autentickosť (Authenticity): pravosť pôvodu informácie.
- Neodmietnuteľnosť (Non-repudiation): nemožnosť poprieť vykonanie akcie.

2. Model konvenčného kryptografického systému a jeho opis

Používa rovnaký kľúč pre šifrovanie aj dešifrovanie. Základné prvky:

- Plaintext, šifrovací algoritmus, tajný kľúč, ciphertext, dešifrovací algoritmus.

Bezpečnosť závisí od utajenia kľúča.

3. Klasifikácia kryptografických systémov a šifier

- Podľa typu operácií: substitučné, transpozičné, kombinované.
- Podľa typu kľúčov: symetrické a asymetrické.
- Podľa spôsobu spracovania: blokové a prúdové šifry.

4. Kryptoanalýza a bezpečnosť kryptografických algoritmov + Kerckhoffov princíp

Kryptoanalýza je analýza kryptosystému s cieľom jeho prelomenia. Kerckhoffov princíp: bezpečnosť závisí od tajnosti kľúča, nie algoritmu.

5. Základná klasifikácia útokov + vysvetlenie útoku zo stredu (man in the middle)

- Pasívne (sledovanie), aktívne (zmena správ), MITM – útočník zachytáva a modifikuje komunikáciu medzi dvoma stranami.