ZÁKLADY KRYPTOGRAFIE

1. **Matematické základy kryptografie**
   Terminologie v kryptografii, vlastnosti prvočísel, generování prvočísel, testy prvočíselnosti, modulární aritmetika, grupy, testování generátorů multiplikativní grupy, malá Fermatova věta, Eulerova věta, Euklidův algoritmus, Eulerova funkce, časová a paměťová složitost, třídy složitosti, rozšířený Euklidův algoritmus, Čínská věta o zbytcích, rychlé modulární mocnění, eliptické křivky.

2. **Asymetrická kryptografie**
   Principy asymetrického šifrování a digitálního podpisu, problém faktorizace, problém diskrétního logaritmu, RSA kryptosystém, DSA kryptosystém, ustanovení klíče pomocí Diffie-Hellmanova protokolu, certifikáty a PKI (infrastruktura veřejného klíče), ECDH protokol a jeho výhody oproti DH, doporučené velikosti klíčů a parametrů pro asymetrické kryptosystémy.

3. **Symetrická kryptografie**
   Dokonalá šifra, proudové šifry, blokové šifry, Feistelovo schéma, algoritmus DES, algoritmus AES, operační módy blokové šifry (CBC a GCM), hashovací funkce (obecné principy), doporučené velikosti klíčů a parametrů pro symetrické kryptosystémy.

4. **Autentizace**
   Základní prvky v autentizaci, AAA protokoly, protokoly typu výzva-odpověď, asymetrické protokoly, protokoly RADIUS, Kerberos a NTLM, protokoly SSL a TLS (základní principy), hashovací funkce LM Hash a NT Hash, protokoly s nulovou znalostí, protokoly s ochranou soukromí, atributová autentizace, prokazatelná bezpečnost.