Todistus

Kryptografia

Käyttäjä **s2200855@edu.bc.fi** on suorittanut **100%** osiosta **Kryptografia**.

100 %

Kuvaus:

Kryptografian historiasta nykykäyttöön, salauksen perusteet, teknologiat, sovellukset ja niiden vaikutus turvallisuuteen.

Suoritetut moduulit:

- Mitä on kryptografia? Peruskäsitteet ja käyttötarkoitukset
- Caesar-salaus: Ikivanha koodi, joka muutti viestinnän
- Enigma-kone: Miten toisen maailmansodan koodinmurtajat avasivat sodan suurimman arvoituksen
- Tarkastussummat

- Mitä ovat hajautusfunktiot (hash) ja mihin niitä käytetään?
- Kryptografisten tiivisteiden murtaminen: Kuinka se toimii?
- MD5-tiiviste - rikkinäinen klassikko
- PBKDF2, BCrypt, SCrypt ja Argon2
- SHA2 vs SHA3 vs PBKDF2 vs bcrypt vs SCrypt vs Argon2: Mikä valita salasanan tallentamiseen?
- Mikä on MAC ja mihin sitä tarvitaan?
- Erilaisia MAC algoritmeja
- Satunnaisluvut kryptografiassa
- Mitä on symmetrinen kryptografia?
- Block Cipherit
- DES, 3DES ja AES
- Stream Cipherit
- Alustusvektori (IV) ja sen haavoittuvuudet kryptografiassa
- Mitä on asymmetrinen kryptografia?
- Digitaaliset allekirjoitukset
- Avaintenvaihtoalgoritmit
- Koodausmenetelmät
- TLS (Transport Layer Security): Internetin turvallisuuden perusta
- Varmenteet: Digitaalisen luottamuksen rakennuspalikat
- Julkisen avaimen infrastruktuuri (PKI): Digitaalisen luottamuksen perusta
- TLS:n rakennuspalikat: Cipher Suitet
- SSL/TLS uhat
- Mitä on avainten hallinta ja miksi se on tärkeää?
- Avaintenhallinta Pilvipalveluissa: AWS, GCP ja Azure

- On-Premise avaintenhallinta HashiCorp Vaultin avulla
- CertBot ja varmenteiden automaattinen uusiminen
- HSM-moduulit
- TPM-moduulit
- SSL/TLS asetusten auditointi Qualysin SSL labs -skannerilla
- SSH-asetusten auditointi Nmapilla
- CyberChef - Selainpohjainen kryptografinen sveitsiläinen linkkuveitsi