Opettajan sähköposti: jouko.teeriaho@lapinamk.fi

SALAUSMENETEL-MÄT OSA 2

Soveltava osa

KURSSIN ESITTELY

Salausmenetelmien osan 2 materiaali Moodlessa

TEORIA

- 6 videoluentoa, sekä niihin liittyvät luentokalvot
- muutama tutorvideo laskuihin liittyen
- 2 pdf – liitettä syventävää materiaalia

OSAN 2 SUORITUS

- Osa 2 suoritetaan **etätehtävillä (57 kpl)**, jotka palautetaan Moodlessa olevaan palautuslaatikkoon.

- Etätehtävistä 43 on sanallisia tehtäviä.

  Vastaukset löytyvät luennoista. Lyhyet vastaukset riittävät

- Etätehtävistä 14 on laskutehtäviä .

  Laskuissa käytetään Exceliä ja **WolframAlpha.com** laskinta luennoissa ja tutorvideoissa kuvatulla tavalla

Osan 2 arviointi

Osa 2 arvioidaan asteikolla 0 - 5
(tarkkuudet kuten 3,5 , 2+ tai 4- mahdollisia)

Pisteiden ja arvosanojen vastaavuudet:
29 p = 1
34 p = 2
40 p = 3
45 p = 4
51 p = 5

Koko kurssin arvosana saadaan yhdistämällä osan 1 (matematiikkaosuus) ja osan 2 (soveltava osa) arvosanat. Molempien osien painokerroin = 50%.

Videoluentojen sisältö

1. Salauksen peruskäsitteet, Klassiset salaukset
2. Modernit salausmenetelmät. Jono- ja lohkosalaus
3. PK- salaus. Esimerkkinä RSA
4. Key exchange, tiivisteet , digitaalinen allekirjoitus
5. PK infrastruktuuri, varmenteet, autentikointi
6. Kryptoanalyysi, muita kryptografian sovelluksia