**EHDOTUS OPINNÄYTETYÖN AIHEEKSI PVM. 25.9.2023**

|  |  |  |
| --- | --- | --- |
| **Opinnäytetyön tekijä/tekijät (Opinnäytetyön tekijä(t) täyttää/täyttävät)** | | |
| Nimi/Nimet: | Roope Salminen | |
| Opiskelijatunnus/-tunnukset: | 2107630 | |
| Ryhmätunnus: | TLTITVT21SV | |
| Sähköposti: | Roope.Salminen@student.lab.fi | |
| Puhelin: | +358407482047 | |
| **Lyhyt kuvaus opinnäytetyön aiheesta** | | |
| Lohkosalauksen perusteet: termit, käsitteet, ECB ja CBC moodit. | | |
| **Lyhyt kuvaus opinnäytetyön tavoitteesta ja merkityksestä/hyödynnettävyydestä** | | |
| Tavoitteena tuoda lohkosalauksen periaatteet tutuksi. Perustellaan miksi salausmenetelmää implementoidessa moodin valinnalla voi olla suuri merkitys tietoturvan kannalta. | | |
| **Lyhyt kuvaus opinnäytetyössä käytettävistä menetelmistä** | | |
| Teoriaosuus käy läpi oleellisimmat käsitteet ja termit kuten esim. bitti, tavu, lohko, XOR-operaatio, symmetrinen salaus, ECB ja CBC moodit sekä niiden heikkoudet. Tavoitteena saada käytännön osioon jonkinlaista demonstraatiota Pythonilla käyttäen mahdollisesti Feistel verkkoa salausmetodissa. | | |
| **Yhteistyökumppanin yhteystiedot** | | |
| Yritys/organisaatio/hanke: | Kirjoita tekstiä napsauttamalla tätä. | |
| Yhteyshenkilö/ohjaaja: | Kirjoita tekstiä napsauttamalla tätä. | |
| Sähköposti: | Kirjoita tekstiä napsauttamalla tätä. | |
| Puhelin: | Kirjoita tekstiä napsauttamalla tätä. | |
| Osoite: | Kirjoita tekstiä napsauttamalla tätä. | |
| **Opinnäytetyön aikataulu** | | |
| Versio 1 valmis maanantai 30.10.2023 Versio 2 valmis maanantai 13.11.2023  Lopullinen versio valmis keskiviikko 13.12.2023 | | |
|  | | |
| **Aiheen hyväksyminen (Aiheen hyväksyjä täyttää)** | |  |
| Opinnäytetyön ohjaaja: | Kirjoita tekstiä napsauttamalla tätä. | |
| Paikka ja aika | Kirjoita tekstiä napsauttamalla tätä. Kirjoita päivämäärä napsauttamalla tai napauttamalla tätä. | |
| Allekirjoitus ja  nimenselvennys: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Kirjoita tekstiä napsauttamalla tätä. | |

Päivitetty 25.5.2020