# Article information:

Tietoturvallisuuden perusteet: Oppitunti 6: Salauksen historiaa: Johdanto salakirjoituksen historiaan
[https://moodle.metropolia.fi/mod/lesson/view.php?id=6195=156=no](https://moodle.metropolia.fi/mod/lesson/view.php?id=6195&pageid=156&startlastseen=no)

# Article summary:

1: Salakirjoitusta on käytetty kolmena historiallisena aikakautena: manuaalisen salakirjoituksen aikakausi, koneellisen salakirjoituksen aikakausi ja digitaalisen salakirjoituksen aikakausi.

2: Salakirjoitus jaetaan kahteen pääryhmään: steganografiaan, jossa viesti on näkymätön, ja kryptografiaan, jossa viesti on vaikeasti tulkittavissa.

3: Historiassa tunnetaan erilaisia salakirjoitusmenetelmiä, kuten skytale, Polybiuksen menetelmä, Atbash-koodi ja Caesarin koodi. Näitä menetelmiä voidaan murtamalla selvittää salattu viesti.

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

Artikkelin otsikko Tietoturvallisuuden perusteet: Oppitunti 6: Salauksen historiaa: Johdanto salakirjoituksen historiaan antaa ymmärtää, että artikkeli käsittelee salakirjoituksen historiaa ja tietoturvallisuuden perusteita. Otsikko on selkeä ja antaa lukijalle käsityksen siitä, mitä odottaa artikkelin sisällöstä.

Artikkelin alussa mainitaan, että aiheesta on esitetty myös edellisen kurssin PowerPoint-esityksessä. Tämä viittaa siihen, että artikkeli voi olla tiivistelmä tai jatkoa aiemmalle materiaalille. Olisi hyödyllistä saada lisätietoja siitä, miten tämä artikkeli liittyy aiempaan materiaaliin ja miten se täydentää sitä.

Artikkelissa esitellään kolme historiallista ajanjaksoa, joissa salakirjoitusta on käytetty. Näiden ajanjaksojen kuvaaminen antaa hyvän yleiskuvan salakirjoituksen kehityksestä ajan myötä. Kuitenkin olisi hyödyllistä saada lisätietoja siitä, millaisia menetelmiä ja tekniikoita käytettiin kussakin ajanjaksossa.

Artikkelissa mainitaan myös steganografia ja kryptografia salakirjoituksen pääryhminä. Tämä jakaminen auttaa ymmärtämään salakirjoituksen eri lähestymistapoja. Olisi kuitenkin hyödyllistä saada lisätietoja siitä, miten nämä kaksi ryhmää eroavat toisistaan ja millaisia menetelmiä ne sisältävät.

Artikkelissa esitellään useita historiallisia esimerkkejä salakirjoituksen käytöstä, kuten muinaisen Egyptin hieroglyfit ja Kreikan spartalaisten skytale-laitteen käyttö. Nämä esimerkit havainnollistavat hyvin salakirjoituksen käyttöä eri aikoina. Kuitenkin olisi hyödyllistä saada lisätietoja siitä, miten nämä menetelmät toimivat ja millaisia haasteita niiden murtaminen aiheutti.

Artikkelissa mainitaan myös Atbash-koodi ja Caesarin koodi salakirjoitusmenetelminä. Näiden menetelmien kuvaaminen antaa lukijalle käsityksen siitä, miten yksinkertaisia salakirjoitusmenetelmiä on kehitetty ajan myötä. Olisi kuitenkin hyödyllistä saada lisätietoja siitä, miten nämä menetelmät toimivat ja millaisia haasteita niiden murtaminen aiheutti.

Artikkelissa ei tarjota tieteellisiä lähteitä tai viitteitä väitteille tai esitetyille faktoille. Tämä heikentää artikkelin luotettavuutta ja uskottavuutta. Olisi hyödyllistä saada tarkempia tietoja siitä, mistä tiedot on saatu ja millaisia lähteitä niiden taustalla on.

Artikkelissa ei myöskään käsitellä mahdollisia riskejä tai haasteita, joita salakirjoituksen käyttöön liittyy. Tietoturvallisuuden näkökulmasta olisi tärkeää keskustella myös siitä, miten salakirjoitusta voidaan käyttää väärin tai murtaminen voi aiheuttaa haittaa. Tämä puute voi antaa yksipuolisen kuvan salakirjoituksen eduista ja jättää lukijan ilman täydellistä ymmärrystä aiheesta.

Artikkeli ei myöskään käsittele vasta-argumentteja tai eri näkökulmia salakirjoituksen historiaan. Olisi hyödyllistä kuulla myös kriittisiä näkökulmia tai erilaisia mielipiteitä aiheesta, jotta lukija saisi kokonaisvaltaisemman käsityksen salakirjoituksen historiasta.

Yhteenvetona voidaan todeta, että artikkeli tarjoaa perustiedot salakirjoituksen historiasta ja esittelee joitain esimerkkejä menetelmistä. Kuitenkin artikkeli kärsii puutteista lähteiden viittaamisessa, puuttuvista yksityiskohdista ja vasta-argumenttien puuttumisesta. Lisäksi artikkeli ei käsittele mahdollisia riskejä tai haasteita salakirjoituksen käytössä. Parantamalla näitä puutteita artikkeli voisi tarjota lukijalleen kattavamman ja tasapuolisemman kuvan salakirjoituksen historiasta.

# Topics for further research:

* Salakirjoituksen menetelmät ja tekniikat eri ajanjaksoina
* Steganografian ja kryptografian eroavaisuudet ja käyttökohteet
* Salakirjoituksen murtamisen haasteet ja riskit
* Salakirjoituksen käytön väärinkäytön mahdollisuudet
* Salakirjoituksen historiaan liittyvät vasta-argumentit ja eri näkökulmat
* Tietoturvallisuuden perusteet ja salakirjoituksen rooli siinä

# Report location:

<https://www.fullpicture.app/item/3c36d997373814c5b54fa514c530d714>