

Merkitse nimesi viereen, monellako luentokerralla suurinpiirtein olit läsnä ensimmäisen viikon jälkeen. (Näitä kertoja oli 11.) Jos olit mukana kurssilla joskus aiemmin, merkitse vuosiluku.

Vastaa viiteen tehtävään.

Kun olet saanut vastaukset valmiiksi, merkitse vastauspaperin alkuun tehtävien numerot siinä järjestyksessä kuin arvioit osanneesi niihin vastata, paras ensimmäiseksi, huonoin viimeiseksi. Jos arvostelu tuottaa saman järjestyksen, saat lisäpisteen.

1. Selitä juuri sen verran, että lukija vakuuttuu että tiedät mistä on kyse:
 - o julkisen avaimen varmenne
 - o pakettinnuuskinta
 - o tietosuojaja
 - o SSL, Secure Sockets Layer
 - o piilokanava
 - o hash-funktio *128, 160 b*
2. Nämäkin ovat erillisiä yhden pisteen kysymyksiä, eli varo käyttämästä liikaa aikaa:
 - o Mikä on tärkein ero kännykän SIM-kortilla ja HST-henkilökortilla olevissa kryptoavaimissa?
 - o Mitä eroa on tietoturvahyökkäyksen aiheuttamalla tuloksella ja hyökkääjää motivoivalla tuloksella?
 - o Kryptoanalyttikolla voi olla pelkän kryptotekstin lisäksi jotain lisätietoa. Mainitse jokin tyypillinen sellainen ja miten murtaaja on voinut päästä siihen käsiksi. (Algoritmi tai avain ei kelpaa tässä.)
 - o Mikä on toiminnallisuuden ja vakuuttavuuden ero Common Criteriassa?
 - o Rabinin kryptosysteemissä salatekstin purkaminen on vain neliöjuuren laskemista modulo julkisesti tunnettu luku n. Miksi vain tuon luvun n keksijä pystyy tähän?
 - o Esitä jokin peruste joko sille, että tekijänoikeus kuuluu tietoturvakurssin aihepiiriin, tai sille että se ei kuulu.
3. Mainitse ainakin kuusi erityyppistä fyysistä keinoa, joilla tietokonelaitteistoja ja niissä olevia tietoja voidaan suojata erilaisilta uhkilta. (Fyysistä ei luennoissa eikä materiaalissa määritelty selvästi, mutta sen piiriin luettiin melko laaja alue, mm. laitteistot. Bittikin on fyysistä sellaisessa yhteydessä, jossa siitä voi saada sähköiskun, pienenkin.)
4. a) Mitä muita kuin tapahtumatietoja käytetään lähteenä järjestelmissä, jotka pyrkivät havaitsemaan tietokoneisiin kohdistuvia hyökkäyksiä?
b & c) Havaitsemismenetelmien perusjako on tietämys- ja käyttäytymispohjaisiin. Luonnehdi näitä lyhyesti.
5. Kahden osapuolen yhteistä salaisuutta *ei voi* voidaan käyttää molemmin- tai toispuoliseen autentikointiin monin eri tavoin. Mikä on heikoin tuntemasi tapa (joka on käytössä) ja mikä vahvin? Esittele myös jokin kolmas tapa näiden väliltä. (Voit rajoittaa toispuoliseen autentikointiin, mutta mainitse aina kumpi osapuoli autentikoidaan kummalle. Huomaa, että salaisuutta voi pitää yhteisenä, jos se ainakin jossain vaiheessa on ollut molempien tiedossa.) *paikalliset tuntemukset*
hltä tuntemus
lappuuta
6. Oletetaan, että A ja B ovat sopineet symmetrisestä avaintensalausavaimesta K, jota he käyttävät päivittäin vaihdettavien datansalausavainten k_1, k_2, \dots salaukseen seuraavien kahden vuoden ajan.
 - a) Luettele tarpeellisia ja mahdollisia avaintenhallintaan liittyviä toimia K:n kaltaisen avaimen elinkaareissa. (3p, muut kohdat á 1p)
Mainitse kaksi tämän luettelon tapahtumaa,
 - b) jotka eivät voi kuulua saman avaimen K elinkaareen.
 - c) jollaiset eivät tyypillisesti kuulu avainten k_1, k_2 jne. elinkaareen.
 - d) Mainitse kaksi a-kohdan luettelosta puuttuvaa tointa, jotka voivat kuulua julkisen avaimen hallintointiin.