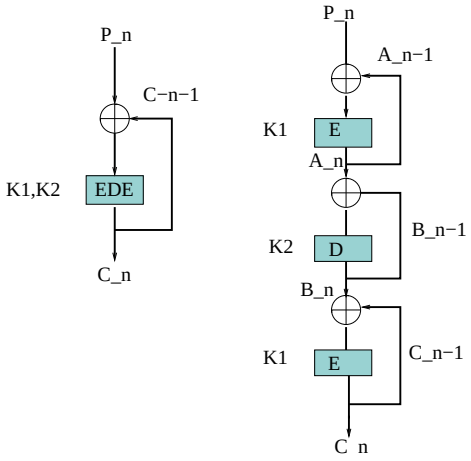
Tietoturvan perusteet, harjoitus 5, 26.-29.4. 2010

1. Tutki, mitä standardi
   NIST SP-800-88 (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)
   sanoo kovalevyjen ja muistien puhdistamisesta. Mitä tekniikkoja muistien puhdistamisessa on käytössä? Onko aina tarpeellista kirjoittaa päälle moneen kertaan?

2. Vanhempia, lyhyitä salausavaimia käyttäviä salausmenetelmiä voidaan käyttää edelleen, jos salaus tehdään kolmeen kertaan. Yleensä tällöin ensin salataan yhdellä avaimella, sitten puretaan toisella ja lopuksi vielä salataan ensimmäisellä avaimella. Näin saadaan yhteensopivuus perinteisen yhden avaimen salauksen kanssa. Miksi? Käytetään tällaisen salauksen yhteydessä CBC-ketjutusmoodia. Kuviossa 1 on esitetty kaksi vaihtoehtoa ketjutukselle tässä tilanteessa. Kummalla tavalla ketjutus kannattaisi tehdä, kun tarkastellaan a) turvallisuutta, b) tehokkuutta? Miten parantaisit kummassakin turvallisuutta, kun käytössä on vain kolme salauspiiriä ja jokin määrä XOR-operaatioita? Edelleen pitäisi käyttää vain kahta avainta.



Kuva 1: 3DES ja CBC

3. Oletetaan, että virhe on *selvätektissä*. Kuinka moneen vastaanotettuun selvätekstiin tuo virhe vaikuttaa CBC-moodissa ja CF-moodissa?

4. Luennoilla mainittiin eräs tapa torjua pienten palasten hyökkäys palomuuria vastaan. Tällöin vaadittiin, että ensimmäinen pala on riittävän iso. Jos se hylätään, niin kaikki muutkin palaset hylätään. Kuitenkin on luonteenomaista IP:lle, että palaset saattavat tulla toisessa järjestyksessä. Toisin sanoen jokin muu palanen tuleekin ennen ensimmäistä. Kuinka tällainen tilanne käsitellään?

5. Tarkastellaan seuraavaa yksinkertaista protokollaa, jossa A lähettää B:lle salatun viestin käyttäen julkisen avaimen protokollaa:

(a) $A \longrightarrow B$: $(A,\ E(PU_B, [M, A]),\ B)$

(b) $B \longrightarrow A$: $(B,\ E(PU_A, [M, B]),\ A)$

Eli ensin A lähettää viestin B:lle, jossa viestissä on lähettäjä ja vastaanottaja selväkielisenä ja lisäksi viesti M ja lähettäjä A salattuna B:n julkisella avaimella. B kuittaa samanlaisella sanomalla. Yksinkertaistetaan protokollaa hieman:

(a) $A \longrightarrow B$: $(A,\ E(PU_B, M),\ B)$

(b) $B \longrightarrow A$: $(B,\ E(PU_A, M),\ A)$

Eli salauksesta on poistettu lähettäjä. Nyt kuitenkin hyökkääjä, joka kuuntelee verkkoliikennettä ja omaa itse oman julkisen avaimen, pystyy paljastamaan viestin M sisällön. Miten?