Tik-79.159 Tiedon salaus ja suojaus	kevät 98
Laskuharjoitus 8, viikko 13	Tuomas Aura, Antti Huima

1. Miten PKCS #1 RSA-standardi (ftp.rsa.com tai ftp.funet.fi) huomioi seuraavat ongelmat:
   (a) Jos julkinen RSA-eksponentti ja sanoma ovat pieniä, ei potenssiin korotus ylitä n:ää.
   (b) RSA:n multiplikatiivisuus.
   (c) *Forward search attack*: jos mahdollisia selväkieliä on vähän, voi hyökkääjä salata kaikki ne julkisella avaimella ja verrata salakieleen.
   (d) Hyökkääjä generoi satunnaisen allekirjoituksen ja laskee siitä julkisella avaimella vastaavan satunnaisen sanoman.

2. Tiedonsiirrossa tavoitteena on usein ns. *perfect forward secrecy (pfs)*, eli että salattua sanomaa ei voi jälkikäteen selvittää edes osapuolten yksityiset avaimet tunteva taho. Esitä menetelmä, jolla tähän päästään. (Vihje: salaa istuntoavain istuntokohtaisella julkisella avaimella ja vasta tätä vastaava yksityinen avain vastaanottajan julkisella avaimella.) Onko *pfs* mahdollista sähköpostille? PGP:ssä? Miten *pfs* ja avainten varmuuskopiointi tai *key recovery* suhtautuvat ajatuksina toisiinsa?

3. Valitaan n alkion joukosta satunnaisesti kaksi osajoukkoa, joissa on k ja l alkiota. Millä todennäköisyydellä joukoilla on vähintään yksi yhteinen alkio? Jos $k = l$, kuinka suuria osajoukkojen pitää olla, että todennäköisyys yhteisen alkion löytymiselle on vähintään 50 %?

4. Keräät useiden Unix-koneiden `/etc/passwd` -tiedostoista yhteensä 100000 salattua 8-merkkistä salasanaa. Nopea mikrotietokone kokeilee 700 000 DES-avainta sekunnissa. Yhden salasanan salaamiseen vaaditaan 25 DES-iteraatiota. Kuinka pitkään joudut odottamaan, että saat 50 % todennäköisyydellä yhden salasanan murrettua.
   (a) suolaa ei käytetä ja salasanat koostuvat vain pienistä kirjaimista (26 kpl)
   (b) suolaa ei käytetä ja salasanat sisältävät kaikkia mahdollisia 7-bittisiä merkkejä
   (c) 12-bittistä suolaa käytetään normaalisti ja salasanat sisältävät kaikkia mahdollisia 7-bittisiä merkkejä
   (d) salasanat sisältävät 10 satunnaista 7-bittistä merkiä ja suolana on käyttäjätunnus sekä järjestelmän nimi. (Tämä ei enää vastaa Unix-salasanoja, mutta oletetaan yhden salasanan kokeilun hinta samaksi kuin edellisissä kohdissa.)

   Kuinka paljon unixin crypt(3)-komennon suola vaikuttaa salasanan ratkaisemiseen vaadittavaan työhön, kun järjestelmässä on k käyttäjää? Mikä olisi paras pituus suolalle? Mitä tapahtuu, jos suola generoidaan heikolla satunnaislukugeneraattorilla?

5. Aikaleimoihin ja osapuolten yhteiseen salaiseen avaimeen perustuvassa tunnistusprotokollassa lähetetään vain yksi sanoma:

   $$\boxed{1.\quad A \longrightarrow B \quad T_A,\ MAC_K(T_A, B).}$$

   Mitkä hyökkäykset ovat mahdollisia, jos tilapäisesti
   (a) B:n kello on jäljessä (c) A:n kello on jäljessä
   (b) B:n kello on edellä (d) A:n kello on edellä.

6. Seuraavat kaksi insidenssimatriisia kuvaavat isomorfisia graafeja. Uskotko? Jos et, tule itse laskareihin vakuuttumaan asiasta. Älä luota kaverisi muistiinpanoihin!

$$G_1 = \begin{bmatrix} 0&1&0&0&0&1&1&1&0&0\\ 1&1&0&1&0&0&0&0&0&1\\ 0&0&1&1&1&1&1&1&1&0\\ 0&1&1&0&0&1&1&0&1&0\\ 0&0&1&0&1&0&0&1&1&0\\ 1&0&1&1&0&1&0&0&0&1\\ 1&0&1&1&0&0&0&0&0&0\\ 1&0&1&0&1&0&0&0&0&1\\ 0&0&1&1&1&0&0&0&0&1\\ 0&1&0&0&0&1&0&1&1&0 \end{bmatrix} \qquad G_2 = \begin{bmatrix} 1&0&0&1&1&1&0&0&0&0\\ 0&1&0&1&1&1&0&0&0&1\\ 0&0&1&0&0&0&1&0&1&1\\ 1&1&0&0&0&0&1&1&0&0\\ 1&1&0&0&0&0&0&1&1&1\\ 1&1&0&0&0&0&1&0&1&0\\ 0&0&1&1&0&1&0&0&0&1\\ 0&0&0&1&1&0&0&0&0&1\\ 0&0&1&0&1&1&0&0&0&1\\ 0&1&1&0&1&0&1&1&1&1 \end{bmatrix}$$