Tik-79.159 Tiedon salaus ja suojaus	kevät 97
Laskuharjoitus 8, viikko 12	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 on pieni ja sanoman arvo pieni, ei potenssiin korotus ylitä n:ää.
   (b) Multiplikatiivisuuden vuoksi havaitaan salakielestä, jos yksi salattu sanoma on kahden edellisen tulo.
   (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. Sotilasorganisaatio haluaa salata kaiken tietoliikenteen, mutta myös arkistoida tietyn koneen kautta kulkevan datan niin, että sen sisältöä pystytään riittävin valtuuksin tarvittaessa tutkimaan. Kuinka järjestät salauksen?

3. 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?

4. Kansainvälisissä sopimuksissa on usein pykälä, jonka mukaan ne astuvat voimaan vasta kaikkien osapuolien vahvistettua sopimuksen. Kuinka samaa menetelmää voidaan käyttää hyväksi sopimuksia sähköisesti allekirjoitettaessa?

5. Dokumenttien ja tapahtumien sitominen nykyhetkeen tai tiettyyn ajanhetkeen menneisyydessä tai tulevaisuudessa on ongelmallista. Miten voidaan varmistua seuraavista seikoista?
   (a) Allekirjoitus on tuore eli laadittu äskettäin.
   (b) Myöhemmin voidaan todeta, että dokumentti oli olemassa jo hetkellä T.
   (c) Myöhemmin voidaan todeta, että dokumenttia ei ollut olemassa vielä hetkellä T.
   (d) Allekirjoittaja ei voi itse päivätä allekirjoitusta menneisyyteen eikä tulevaisuuteen.
   (e) Salaisuus paljastuu vasta tulevaisuudessa hetkellä T, vaikka alkuperäistä kirjoittajaa ei enää olisi järjestelmässä.

   Pohdi ratkaisuvaihtoehtojen luotettavuutta ja kustannuksia, esim. sanomien määrää eri osapuolten välillä ja luotetun osapuolen tai laitteen tarvetta.

6. Mitä tapahtuu ElGamal-allekirjoituksessa, jos
   (a) kantaluvun g generoima sykli on lyhyt (eli g:n aste $\mathbb{Z}_p^*$:ssä on pieni)
   (b) salainen parametri k paljastuu
   (c) samaa salaista parametria k käytetään kaksi kertaa
   (d) sanomista ei lasketa yksisuuntaista funktiota ennen allekirjoittamista
   (e) allekirjoitusta (a, b) tarkistettaessa ei tutkita ehtoa $1 \leq a \leq p-1$ (p on moduli)?

   (Huomaa, että Schneier ei mainitse asioita 6a, 6d ja 6e.)