Tik-79.159 Tiedon salaus ja suojaus	kevät 97
Laskuharjoitus 5, viikko 9	Tuomas Aura, Antti Huima

1. Miksi CBC-salausta ja CBC-MAC-eheystarkistusta ei voida tehdä samalla avaimella? (CBC-MAC: salataan viesti erillisellä avaimella CBC-moodissa ja hylätään salakielinen teksti paitsi viimeinen lohko, joka liitetään selväkielisen tekstin perään virheentarkistuskoodiksi. Sen jälkeen suoritetaan varsinainen salaus.)

2. Eräs yritys suojaa maksumääräystensä eheyden 32-bittisellä CRC-virheentarkistuskoodilla (polynomi 1 00000100 11000001 00011101 10110111) ja salaa viestiliikenteen RC4-salausalgoritmilla. Sanomien formaatti on seuraava:

tavut	sisältö
0–15	saajan tilinumero
16–19	rahasumma markkoina (32-bit uint, MSB first)
20–199	viitenumero tai viesti saajalle
200-203	CRC

   Tiedät, että yritys on juuri maksamassa sinulle viheliäisen pientä 790 markan palkkiota yhteyskaapelin maahan kaivamisesta. Miten saattaisit toimia, jos moraalisi ei olisi niin korkea?

3. Julkinen RSA-avaimesi on $(3, 4897)$ ja salainen $(3171, 4897)$. Avaa julkisella avaimellasi salattu sanoma 4109.

4. Julkinen RSA-allekirjoitusavaimesi on $(17, 1189)$.

   (a) Modulin 1189 salaiset tekijät ovat $29 \cdot 41$. Mikä on salainen allekirjoitusavaimesi?

   (b) Sanoman "Moi, mitä kuuluu?" sormenjälki sovitulla yksisuuntaisella hajautusfunktiolla laskettuna on 321. Esitä allekirjoitettu sanoma kokonaisuudessaan.

5. Miksei RSA:ssa pidä käyttää samaa modulia n useammassa avainparissa, vaikka yksityiset avaimet olisivat saman henkilön hallussa?

6. Mitä tapahtuu, kun $p|m$ tai $q|m$ RSA:ssa?