Tik-79.159 Tiedon salaus ja suojaus	
Tentin 8.8.1996 ratkaisut	Tuomas Aura

1. (a) Hybridisalauksessa itse sanoma salataan symmetrisellä salausmenetelmällä ja satunnaisella istuntoavaimella. Istuntoavain salataan vastaanottajan julkisella avaimella ja lähetetään vastaanottajalle erikseen tai sanoman mukana.

   (b) CBC (Cipher Block Chaining) on lohkosalausalgoritmin käyttötapa, jossa selväkielinen lohko xorrataan edellisen salakielisen lohkon kanssa ennen salaamista algoritmilla. (Ensimmäinnen lohko xorrataan satunnaiseti valitun alustuvektorin kanssa. Hyöty on, että sama sanoma kaksi kertaa salattuna näyttää erilaiselta eikä sanomassa toistuvia osia voida havaita.)

   (c) Yksisuuntaisella hajautusfunktiolla lasketaan sanomasta vakiomittainen (esim. 160-bittinen) sormenjälki. Yksisuuntaisuus tarkoittaa, että pelkän sormenjäljen perusteella on laskennallisesti mahdotonta päätellä mitään sanoman sisällöstä. Lisäksi funktiolta vaaditaan, että on mahdotonta löytää kahta sanomaa, joilla on sama sormenjälki.

   (d) Vahva kryptografinen menetelmä on nähtävissä olevassa tulevaisuudessa turvallinen kaikkia ajateltavissa olevia hyökkääjiä vastaan, ainakin erittäin suurella todennäköisyydellä. (Kryptografisia algoritmeja muuten on paljon muitakin kuin salaus, esimerkiksi vaikka allekirjoitusalgoritmit.)

   (e) Bittivirtasalauksessa salattava bittijono xorrataan vahvalla pseudosatunnaislukugeneraattorilla tuotetun bittijonon kanssa. Salauksen avaaminen tapahtuu täsmälleen samalla tavalla. Lähettäjän ja vastaanottajan on alustettava satunnaislukugeneraattorinsa samalla avaimella. Tarvittaessa voidaan salaus suorittaa vaikka yksi bitti kerrallaan.

   (f) Subliminaalinen kanava tarkoittaa viestintätapaa, jota käytettäessä ulkopuolinen taho ei voi edes tietää, että viestejä lähetetään. Sanomat siis piilotetaan.

2. (a) $521 = 1000001001_2$.

1	$999^{2^0} \bmod 1997$		$= \mathbf{999}$
0	$999^{2^1} \bmod 1997$	$= 999^2 \bmod 1997$	$= 1498$
0	$999^{2^2} \bmod 1997$	$= 1498^2 \bmod 1997$	$= 1373$
1	$999^{2^3} \bmod 1997$	$= 1373^2 \bmod 1997$	$= \mathbf{1958}$
0	$999^{2^4} \bmod 1997$	$= 1958^2 \bmod 1997$	$= 1521$
0	$999^{2^5} \bmod 1997$	$= 1521^2 \bmod 1997$	$= 915$
0	$999^{2^6} \bmod 1997$	$= 915^2 \bmod 1997$	$= 482$
0	$999^{2^7} \bmod 1997$	$= 482^2 \bmod 1997$	$= 672$
0	$999^{2^8} \bmod 1997$	$= 672^2 \bmod 1997$	$= 262$
1	$999^{2^9} \bmod 1997$	$= 262^2 \bmod 1997$	$= \mathbf{746}$

   Oma julkinen avaimemme on $Y = g^y = 999^{521} \bmod 1997$
   $= 999^{2^9} \cdot 999^{2^3} \cdot 999^{2^0} \bmod 1997$
   $= 746 \cdot 1958 \cdot 999 \bmod 1997 = 861 \cdot 999 \bmod 1997 = \mathbf{1429}$.

   Protokollassa seuraavaksi lähetetään julkinen avain $Y = 1429$ asiamies A:lle. Tämän jälkeen molemmat osapuolet laskevat yhteisen salaisen avaimen.

1	$1872^{2^0} \bmod 1997$		$= \mathbf{1872}$
0	$1872^{2^1} \bmod 1997$	$= 1872^2 \bmod 1997$	$= 1646$
0	$1872^{2^2} \bmod 1997$	$= 1646^2 \bmod 1997$	$= 1384$
1	$1872^{2^3} \bmod 1997$	$= 1384^2 \bmod 1997$	$= \mathbf{333}$
0	$1872^{2^4} \bmod 1997$	$= 333^2 \bmod 1997$	$= 1054$
0	$1872^{2^5} \bmod 1997$	$= 1054^2 \bmod 1997$	$= 584$
0	$1872^{2^6} \bmod 1997$	$= 584^2 \bmod 1997$	$= 1566$
0	$1872^{2^7} \bmod 1997$	$= 1566^2 \bmod 1997$	$= 40$
0	$1872^{2^8} \bmod 1997$	$= 40^2 \bmod 1997$	$= 1600$
1	$1872^{2^9} \bmod 1997$	$= 1600^2 \bmod 1997$	$= \mathbf{1843}$

Yhteiseksi salaiseksi avaimeksi tulee $K = g^{xy} = X^y = 1872^{521} \bmod 1997$
$= 1872^{2^9} \cdot 1872^{2^3} \cdot 1872^{2^0} \bmod 1997$
$= 1843 \cdot 333 \cdot 1872 \bmod 1997 = 640 \cdot 1872 \bmod 1997 = \mathbf{1877}$.

Arvostelu: Tehtävässä piti tuntea Diffie–Hellman-protokolla ja osata suurten lukujen potenssiin korotus. Täydet pisteet sai pienistä laskuvirheistä huolimatta, jos idea oli oikein.

(b) Autentikointi puuttuu. Osapuolet eivät voi olla varmoja, että julkinen avain kuuluu sille henkilölle, jolta se näyttää tulevan. Tämä mahdollistaa esim. *man-in-the-middle*-hyökkäyksen. Julkiset avaimet pitäisi todistaa oikeiksi esim. allekirjoituksella.

3. (a) A päättelee sanoman 2 tuoreuden nonssista N_A, jonka hän on itse generoinut ja lähettänyt sanomassa 1.

B päättelee sanoman 3 tuoreuden nonssista N_B. Sanoman 3 tärkein tehtävä on, että lähettämällä sanoman 3 A kertoo B:lle hyväksyvänsä sanoman 2, joka sisälsi kopion nonssista N_A. Näin sanoma 3 todistaa B:lle, että nonssi N_A on tuore. Koska N_A on tuore, voi B nyt päätellä, että myös sanoma 1 oli tuore. Tällä tavalla myös sanoman 1 tuoreus tuli osoitettua B:lle nonssien avulla.

Kolmisuunatisessa autentikoinnissa ei ole tarvetta huomioida aikaleimoja. Jos aikaleimoja kuitenkin käytetään, B tarkistaa sanoman 1 tuoreuden aikaleimasta T_A ja A sanoman 2 tuoreuden aikaleimasta T_B. Koska osapuolten kellot eivät yleensä ole aivan tarkasti samassa ajassa, vastaanottaja voi myös muistaa aikaleiman rinnalla lähetettävät nonssit (N_A sanomassa 1 ja N_B sanomassa 2) niin kauan kuin hän pitää aikaleimaa tuoreena. Näin vastaanottaja varmistaa, ettei hän vastaanota samaa sanomaa toista kertaa aikaleiman voimassaoloaikana.

(b) Istuntoavaimia on kaksi, jotta A ja B voivat salata lähettämänsä sanomat eri avaimilla. Kun eri suuntiin lähetettävä data salataan eri avaimella, estyvät monet toistohyökkäykset, joissa osapuolen lähettämiä sanomia lähetetään takaisin hänelle itselleen. (Pelkkä salaus eri avaimella ei kuitenkaan riitä sanomien eheyden tai alkuperän tarkistamiseen.) Käytännössä suurempi hyöty on, että kun kumpikin osapuoli generoi itse avaimensa, he voivat salata dataa valmiiksi puskuriin ja jopa lähettää toiselle jo ennen autentikoinnin päättymistä . Kahden avaimen vaihto ei maksa juuri sen enempää kuin yhdenkään, joten ei ole mitään syytä käyttää samaa avainta molempiin suuntiin.

(c) Kuten kohdassa (a) todettiin, kolmas sanoma todistaa sanoman 1 ja avaimen K_{AB} tuoreuden B:lle nonssilla. Kaksisuuntaisessa autentikoinnissa niiden tuoreus jää pelkän aikaleiman varaan.

Lisäksi B sanoman 3 saatuaan tietää, että A on vastaanottanut sanoman 2 eli A:lla on avain K_{BA}. Kaksisuuntaisessa autentikoinnissa sanoman 2 katoaminen on muulla tavalla huomioitava mahdollisena virhetilanteena.

Arvostelu: Tämä oli vaikea tehtävä, eikä kirjassa kerrota kaikkea.

4. Lagrange-kynnysrakenne on laskettu tuntemattomasta polynomista $y \equiv ax+M \pmod{37813}$. Polynomilta tunnetaan pisteet $(2, 19525)$ ja $(4, 1583)$. Saadaan yhtälöt

$$a \cdot 2 + M \equiv 19535$$
$$a \cdot 4 + M \equiv 1583.$$

Ratkaistaan M:

$$\begin{aligned}(4a+M)-2(2a+m) &\equiv 1583-19535\\ -M &\equiv -37487\\ M &\equiv 37487.\end{aligned}$$

Salainen sanoma on siis 37487. ($a \equiv 28837$.)

Arvostelu: Laskun olivat osanneet lähes kaikki sitä yrittäneet.

5. RSA on julkisen avaimen sala- ja allekirjoitusalgoritmi. Turvallisuuden oletetaan riippuvan suurten lukujen tekijöihin jaon vaikeudesta. Kokonaisten sanomien sijaan RSA:lla salataan istuntoavaimia ja allekirjoitetaan sormenjälkiä. Paljon muutakin voi kertoa.

   Arvostelu: Täyteen 6 pisteeseen vaadittiin myös algoritmin virheetön kuvaus.

6. Vain mielikuvitus rajoittaa kryptografian käyttöä käyttäjän tunnistamisessa. Seuraavassa tärkeimpiä huomioita:

   - Käyttäjän autentikointi perustuu johonkin käyttäjän tietämään salaisuuteen tai käyttäjän hallussa olevaan fyysiseen esineeseen. Kryptografiassa salaisuus on usein avain eli salainen satunnainen bittijono.
   - Pelkkä salasanan kysyminen tai lista vaihtuvia salasanoja ei ole kryptografiaa. Unix-järjestelmissä salasanoista tallennetaan julkiseen tiedostoon yksisuuntaisella funktiolla laskettu sormenjälki. Joskus verkon yli lähetetävä salasana myös salakirjoitetaan.
   - Kryptografian älykkäämpi käyttö edellyttää, että käyttäjällä on luotettu päätelaite, jossa on riittävä laskentateho. Yksinkertaisinta on, että käyttäjä päätelaitteineen allekirjoittaa kaikki lähettämänsä sanomat ja sisällyttää niihin jonkin todisteen tuoreudesta, esim. aikaleiman tai järjestysnumeron.
   - Varsinaiset tunnistusalgoritmit ovat yleensä nollatietotodituksia, joissa tunnistaja ei saa mitään muuta tietoa kuin, että haluttu henkilö todella on juuri nyt yhteyden toisessa päässä.
   - Tunnistukseen tulisi liittyä istuntoavaimen vaihto ja istuntoavainta tulisi käyttää istunnon kaikkien sanomien eheyden varmistamiseen. Jos käyttäjä vain tunnistetaan istunnon aluksi, voi hyökkääjä muutella sanomia.
   - Käytännössä päätelaite ei useinkaan ole luotettu eikä istunnon eheyttä suojata. Tällöin voidaan käyttää yksinkertaista haaste–vaste-tunnistusta. Joskus haasteena toimii kellonaika ja vaste lasketaan yksisuuntaisella funktiolla avaimesta ja ajasta. Tuloksena on kellon mukaan muuttuvaa salasanaa.
   - Yleensä käyttäjä halutaan tunnistaa, jotta hänelle voitaisiin tarjota jokin palvelu. Palvelun tarjoajaa ei välttämättä kiinnosta atentikoinin suorittaminen, joten tunnistus kannattaa eriyttää omaksi palvelukseen. Esimerkiksi Kerberos-järjestelmässä on erillinen luotettu palvelin, joka todistaa käyttäjän henkilöllisyyden.
   - Laajassa järjestemässä ei yksi luotettu autentikointipalvelin riitä. Tällöin joudutaan miettimään, mihin palvelimiin kukin voi luottaa. ISO X.509-standardissa ongelma on ratkaistu autentikointihierarkialla, jossa ylemmät tahot todistavat alempien identiteetin erityisillä allekirjoitetuilla sertifikaateilla.

Arvostelu: Esseen kirjoittaminen näyttää olevan vaikeaa. Harva vastaus oli lukukelpoinen kokonaisuus, joten yksittäisistä avainsanoista sai pisteitä. Yhden järjestelmän teknisistä yksityiskohdista jaarittelu tai kaupallisten tuotteiden luetteleminen on tarpeetonta, jos niihin liittyvät yleisemmät periaatteet unohtuvat.