Tik-79.159 Tiedon salaus ja suojaus	kevät 98
Laskuharjoitus 7, viikko 12	Tuomas Aura, Antti Huima

1. Mitkä seuraavista Diffie–Hellman- ja RSA-protokollista turvaavat sanoman M luottamuksellisuuden? (entä aitouden?)

(a)

1.	$A \longrightarrow B$	g^x
2.	$B \longrightarrow A$	g^y
		Istuntoavain $K = h(g^{xy})$
3.	$A \longrightarrow B$	$E_K(M)$

(b)

1.	$A \longrightarrow B$	$g^x,\ S_A(g^x)$
2.	$B \longrightarrow A$	$g^y,\ S_B(g^y)$
		Istuntoavain $K = h(g^{xy})$
3.	$A \longrightarrow B$	$E_K(M)$

(c)

1.	$A \longrightarrow B$	g^x
2.	$B \longrightarrow A$	g^y
		Istuntoavain $K = h(g^{xy})$
3.	$A \longrightarrow B$	$E_K(M, S_A(h(K)))$

(d)

1.	$A \longrightarrow B$	g^x
2.	$B \longrightarrow A$	$g^y, E_K(S_B(g^y))$
		Istuntoavain $K = h(g^{xy})$
3.	$A \longrightarrow B$	$E_K(M, S_A(g^x))$

(e)

1.	$A \longrightarrow B$	K_A^+	(julkinen RSA-avain)
2.	$B \longrightarrow A$	$E_A(K)$	(salaus K_A^+:lla)
3.	$A \longrightarrow B$	$E_K(M)$	

2. Diffie–Hellman-parametrien arvoiksi on sovittu $n = 2207$ ja $g = 5$. (Varoitus: lukuarvot ovat todellisuutta ajatellen liian pieniä.) Vastaanotat A:lta **allekirjoitetussa** sanomassa hänen julkisen DH-avaimensa $X = 1872$. Tarkistat allekirjoituksen julkisella avaimella, jonka tiedät kuuluvan A:lle. Allekirjoitus on aito. Arvot omaksi salaiseksi avaimeksesi $y = 521$.

   (a) Millä sanomilla avaintenvaihtoprotokolla jatkuu? (muista allekirjoitus!)

   (b) Mikä tulee yhteiseksi salaiseksi avainmateriaaliksi?

   (c) Miksi sanomien pitää olla allekirjoitettuja?

3. Olkoon p edellisessä harjoituksessa Miller–Rabin-testillä löytämäsi alkuluku. Tutki, onko $n = 2p+1$ myös alkuluku. Jos on, niin n on Diffie-Hellmannin moduliksi erinomainen sopiva **turvallinen alkuluku**.

   Jos n ei ole turvallinen alkuluku, valitse uusi p, kunnes se on. (Vihje: käytä ohjelmoitavaa apuvälinettä.)

4. Olkoon n edellisessä tehtävässä löytämäsi DH-moduli. Etsi (mielellään pieni) generaattori mod n DH-kantaluvuksi g.

5. Valitaan ElGamalissa $p = 2357$, $g = 2$ ja $x = 1751$. Mikä on julkinen ja mikä salainen avain? Allekirjoita sormenjälki $h(M) = 1463$ ja tarkista allekirjoitus.

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.)