Tik-79.159 Tiedon salaus ja suojaus	kevät 97
Laskuharjoitus 6, viikko 10	Tuomas Aura, Antti Huima

1. Julkinen RSA-avaimesi on $(3, 4897)$ ja salainen $(3171, 4897)$. Luet luultavasti itse allekirjoittamasi sanoman $2345, 689$, missä 2345 on sanoma ja 689 allekirjoitus. Tarkista julkisen avaimen avulla, onko allekirjoitus aito.

2. 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.	$A \longrightarrow B$	$E_K(M)$	

3. Diffie–Hellman-parametrien arvoiksi on sovittu $n = 2207$ ja $g = 5$. (Varoitus: lukuarvot ovat todellisuutta ajatellen liian pieniä.) Vastaanotat A:lta sähköpostitse **asianmukaisesti allekirjoitetussa** sanomassa hänen julkisen DH-avaimensa $X = 1872$. Arvot omaksi salaiseksi avaimeksesi $y = 521$.

   - Millä sanomilla avaintenvaihtoprotokolla jatkuu?
   - Mikä tulee yhteiseksi salaiseksi avainmateriaaliksi?

4. Generoi (pseudo)satunnainen alkuluku p: valitse (pseudo)satunnainen kokonaisluku ja etsi propabilistisella Miller–Rabin-testillä (Schneier s.259) seuraava sitä suurempi alkuluku. Vakuutu luvun jaottomuudesta vähintään todennäköisyydellä 99 %. (Havainnollisuuden vuoksi laske sopivan pienillä luvuilla.)

5. Olkoon p edellisessä tehtävässä 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.)

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