801346A SALAUSMENETELMÄT (4 op)

Loppukoe 26.11.2012 (4 tehtävää) EI LASKIMIA

1. Murra frekvenssianalyysilla Caesarin yhteenlaskumenetelmällä laadittu salakirjoitus

CZMZDNZIXMTKOZYOZSO

a) antamalla kryptaus- ja dekryptausfunktio;
b) antamalla kryptotekstin 4 viimeisen symbolin OZSO selkokielinen vastine.
Käytössä on englanninkielinen 26 kirjaiminen aakkosto ja sen koodaus luvuiksi:
a=0, b=1, c=2, d=3, e=4, f=5, g=6, h=7, i=8, j=9, k=10,l=11, m=12, n=13,
o=14, p=15, q=16, r=17, s=18, t=19, u=20, v=21, w=22, x=23, y=24, z=25.
Englanninkielen Top-6 (useimmiten esiintyvä) kirjainjoukko on
$\{\text{e,t,a,o,n,r}\} = \{4, 19, 0, 14, 13, 17\}$.

2. a) Kun tiedetään, että

$$87^2 \equiv 16^2 \pmod{n},$$

niin määrää luvun $n = 7313$ tekijät.
b) Olkoon $E(x) = ax + b, \quad E : \mathbb{Z}_n \to \mathbb{Z}_n$ affiinin järjestelmän salausfunktio ja $n = 26$.
Määritä avausfunktio D, kun
i) $E(x) = 7x + 5$;
ii) $E(x) = 4x + 10$.

3. Olkoot $p = 7$, $q = 13$, $e = e_B = 7$, vastaanottajan B parametreja RSA-salauksessa. Suorita seuraavan kaavion mukainen toiminta, kun A lähettää B:lle viestin $m = 10 \in \mathbb{Z}_{91}$.
a) Määritä kryptausfunktio E ja dekryptausfunktio D.
b) Mikä on kryptoteksti c?
c) Mikä on B:n salainen eksponentti d?
d) Anna $D(c)$:n lauseke (ei tarvi laskea).

A	Public channel	B
Secret data		Secret data
		$p, q \in \mathbb{P}_{\geq 3}, p \neq q$
$m \in \mathbb{Z}_n$		$n = n_B = pq$
Encrypting	$n = n_B, e = e_B$	$\leftarrow n_B$ to be published
$E(m) = c$		$\varphi(n) = (p-1)(q-1)$
		$e = e_B \in \mathbb{Z}^*_{\varphi(n)}$
Cryptotext $c \in \mathbb{Z}_n$ sent to B		$\leftarrow e = e_B$ to be published
$c \to$ B		$d = e^{-1} \in \mathbb{Z}^*_{\varphi(n)}$
		Decrypting
	$c \to$ B	$D(c) =$???

4. tehtävä toisella sivulla.

4. A ja B käyttävät Diffie-Hellman avaimenvaihtoa ja El-Gamal salausta ryhmässä $\mathbb{Z}_{17}^* = \langle 3 \rangle$. A:n salainen eksponentti $a = 6$ ja B:n salainen eksponentti $b = 5$.
a) Selvitä A:n ja B:n julkiset avaimet k_A, k_B sekä yhteinen avain $k_{A,B}$.
b) Dekryptaa A:n lähettämä salattu viesti $v_A = 5$.