801346A SALAUSMENETELMÄT (4 op)

Loppukoe 29.10.2012 (4 tehtävää) EI LASKIMIA

1. Murra frekvenssianalyysilla Caesarin yhteenlaskumenetelmällä laadittu salakirjoitus

ALYUNYMNWIGGIHXCPCMIL

a) antamalla kryptausavain;
b) antamalla kryptotekstin 5 viimeisen symbolin PCMIL 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) Olkoot $a \in \mathbb{Z}_n^*$, $b \in \mathbb{Z}_n$, missä $n \in \mathbb{Z}_{\geq 2}$. Osoita, että salausfunktio

$$E(x) = ax + b, \quad E : \mathbb{Z}_n \to \mathbb{Z}_n$$

on bijektio.
b+c) Olkoon $n = 26$. Määritä avausfunktio D, kun salausfunktio on
b) $E(x) = 11x + 5$;
c) $E(x) = 13x + 10$.

3. Olkoot $p = 7$, $q = 13$, $e = e_B = 5$, 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) Määrää $D(c)$.

A Secret data	Public channel	B 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) Olkoon $n \in \mathbb{Z}^+$ annettu ja $A := \lceil \sqrt{n} \rceil$. Laskemalla kongruensseja

$$(A \pm k)^2 \equiv \quad (\text{mod } n), \quad k = 0, \pm 1, ...$$

määritä luvun $n = 403$ tekijät, kun $A = 21$.

b) A ja B käyttävät Diffie-Hellman avaimenvaihtoa ryhmässä $\mathbb{Z}_{17}^* = \langle 3 \rangle$. A:n salainen eksponentti $a = 7$ ja B:n salainen eksponentti $b = 4$. Selvitä A:n ja B:n julkiset avaimet k_A, k_B sekä yhteinen avain $k_{A,B}$.