T-79.503 Kryptologian perusteet
Tentti
10.12.2004

1. (6p.) Olkoon m positiivinen kokonaisluku. Tarkastellaan salaamismenetelmää, jossa $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0,1\}^m$ ja avaimet valitaan yhtä suurin todennäköisyyksin. Tällä menetelmällä salaataan kieltä, joka koostuu keskenään riippumattomista ja yhtä todennäköisistä m bitin lohkoista, joissa on vain yksi nollasta eroava bitti. Arvioi ratkaisukynnystä n_0 kaavalla

$$n_0 \approx \frac{\log_2 |\mathcal{K}|}{R_L \log_2 |\mathcal{P}|},$$

ja osoita että se on korkeintaan 2 kaikilla m, paitsi kun $m = 3$.

2. (6p.) Olkoon e_K lohkosalaamismenetelmän salaamismuunnos, missä avaimen K pituus on 64 bittiä. Avaimenpituus kasvatetaan kaksinkertaiseksi seuraavalla tavalla. Kun on annettu kaksi 64 bitin avainta K_1 ja K_2 niin 64-bittinen selväkieliteksti x muunnetaan salakielitekstiksi y kaavalla

$$y = e_{K_2}(x \oplus K_1).$$

Oletetaan että hyökkääjällä on kaksi selväkieli-salakieliparia x_1, y_1 ja x_2, y_2 tällä tavalla salattuna 128-bittisellä avaimella (K_1, K_2). Esitä miten hyökkääjä voi löytää koko oikean avaimen suurella todennäköisyydellä käymällä läpi vain toisen 64-bittisen osa-avaimen kaikki mahdolliset arvot. Anna arvio onnistumistodennäköisyydelle.

3. (6p.) Tarkastellaan äärellistä kuntaa $\mathbb{F} = \mathbb{Z}_2[x]/(x^4+x+1)$, ja jonosalaamismenetelmää, jossa $\mathcal{P} = \mathcal{C} = \mathbb{F}$ and $\mathcal{K} = \mathbb{F}^* = \mathbb{F} - \{0\}$. Tällä menetelmällä salataan kieltä, joka koostuu neljän bitin lohkoista, joissa on vain yksi nollasta eroava bitti. Kun on annettu avain $K = \beta \in \mathbb{F}^*$ ja jono selväkielilohkoja $x_i,\ i = 1, 2, ...$, salaamisjono ja salaamissääntö määritellään seuraavasti

$$z_i = \beta^i, \text{ and } y_i = e_{z_i}(x_i) = z_i + x_i,\ i = 1, 2, ...$$

Salakielijonon kolmas lohko on

$$y_3 = 0111 = x^2 + x + 1.$$

Kun tämä tiedetään, on tasan kolme mahdollista avainta. Mitkä ne ovat?

4. (6p.) Tiedetään että

$$12^{2004} \equiv 4815 \,(\mathrm{mod}\, 50101),$$

missä 50101 on alkuluku. Osoita että alkion $\alpha = 4815$ kertaluku on 25 multiplikatiivisessa ryhmässä $\mathbb{Z}^*_{50101}$.

5. (6p.) Yritä ratkaista diskreetti logaritmi x yhtälöstä

$$4815^x \equiv 48794 \,(\mathrm{mod}\, 50101).$$

Shanksin menetelmällä. Vihje: Katso Tehtävä 4.

(Jos sinulla ei ole mukana taskulaskinta, riittää kun esität kuinka suorittaisit laskut, jos sinulla olisi laskin.)