TIK-110.503 Kryptologian perusteet
Loppukoe
29.4.2000

1. (6 pist.) DES avainten pituus on 64 bittiä ja joka kahdeksas bitti on pariteettibitti, joka lasketaan seitsemän sitä edeltävän bitin modulo 2 summana. Avaintenhallintakeskus käyttää DES algoritmia ja kiinteätä "master"-avainta loppukäyttäjien DES-avainten salaamiseen. Jokaisessa salakielilohkossa on salattuna yksi DES avain. Arvioi tämän järjestelmän ratkaisukunnystä, eli kuinka monta salakielilohkoa tarvitaan master-avaimen määrittämiseksi yksikäsitteisesti.

2. (6 pist.)"Piling-up lemma": Olkoon X_1, X_2, ...,X_n riippumattomia {0,1}-arvoisia satunnaismuuttujia ja olkoon $X = X_1 \oplus X_2 \oplus \ldots \oplus X_n$. Osoita että tällöin

$$2p - 1 = \prod_{i=1}^{n} (2p_i - 1),$$

missä p_i on todennäköisyys sille, että $X_i = 0$, $i = 1, 2, \ldots, n$, ja p on todennäköisyys sille, että $X = 0$.

3. (6 pist.) Kokonaisluvun $n = 89855713$ tiedetään olevan kahden alkuluvun tulo. Lisäksi tiedetään, että $\phi(n) = 89836740$. Jaa luku n tekijöihin.

4. Olkoon p pariton alkuluku ja olkoon d, $d > 1$, luvun $p - 1$ tekijä. Tarkstellaan kongruenssiyhtälöä

$$x^d \equiv a \,(\mathrm{mod} p),$$

missä a ja x ovat kokonaislukuja.

   a) (3 points) Kun a on annettu osoita, että ratkaisu x on olemassa silloin ja vain silloin kun

$$a^{\frac{p-1}{d}} \equiv 1 \,(\mathrm{mod} p).$$

   b) (3 points) Osoita, että kongruenssilla

$$x^4 \equiv 2000 \,(\mathrm{mod} 29)$$

   ei ole ratkaisua.

5. (6 pist.) Tarkastellaan seuraavaa ElGamal allekirjoitusmenetelmän muunnosta jossa allekirjoitettu viesti "tulkitaan" allekirjoituksesta. Menetelmän julkiset parametrit ovat parittomat alkuluvut p ja q, missä q jakaa luvun $p - 1$, sekä kunnan $\mathbb{Z}_p$ alkio α, jonka multiplikatiivinen kertaluku on q. Käyttäjän salainen avain on kokonaisluku a, missä $1 < a < q$, ja käyttäjän julkinen avain β on laskettu seuraavasti, $\beta = \alpha^a \bmod p$. Sanoman $x \in \mathbb{Z}_q$ allekirjoitus on pari (γ, δ), $\gamma \in \mathbb{Z}_q$ ja $\delta \in \mathbb{Z}_q$, ja ne lasketaan seuraavasti: Käyttäjä muodostaa salaisen satunnaisluvun k, missä $1 < k < q$ ja laskee

$$\begin{aligned} \gamma &= x - (\alpha^k \bmod p) \bmod q \\ \delta &= k - a\gamma \bmod q. \end{aligned}$$

Näytä kuinka viesti x voidaan laskea allekirjoituksesta (γ, δ) kun on annettu julkiset parametrit p, q, α ja β.