Tik-79.159 Tiedon salaus ja suojaus	kevät 98
Laskuharjoitus 2, viikko 7	Tuomas Aura, Antti Huima

1. 2 kierroksen Feistel-salaus ei ole turvallinen. Miksi? (Vihje: oleta, että selväkielisen tekstin toinen puolisko osataan arvata ja että valitun selväkielen hyökkäys on mahdollinen.)

2. Suunnittele Feistel-salakirjoitus, jossa käytettään XOR-operaattorin $\oplus$ sijasta jotain muuta operaattoria, joka muodostaa algebrallisen ryhmän 32-bittisten kokonaislukujen kanssa. Mitä vaatimuksia sekoitusfunktion pitää täyttää?

3. Arvioi, monenko kierroksen jälkeen jokainen salakielen bitti riippuu jokaisesta selväkielen bitistä DES-algoritmissä. (S-boxin tuloksen kaikkien bittien katsotaan riippuvan kaikista sen syötteen biteistä.)

4. Salakirjoitus on *pure*, jos salaaminen peräkkäin kolmella mielivaltaisella avaimella K_1, K_2, K_3 vastaa aina salaamista jollain yhdellä avaimella K_4,

$$E_{K_3}(E_{K_2}(E_{K_1}(P))) = E_{K_4}(P).$$

   Mitä seurauksia tällä on algoritmin käytön kannalta? Jos salakirjoitus on *pure*, onko se ryhmä tai kääntäen? (todistus)

5. Salataan sanoma DES-algoritmilla ensin 64 bitin CFB-moodissa (Cipher FeedBack mode) ja sitten uudelleen ECB-moodissa (Electronic Code Book mode) käyttäen samaa avainta. Millainen moodi saadaan?

6. Laske:

   (a) $6^{-1} \pmod{19}$

   (b) $100^{-1} \pmod{2^{16}+1}$