Tik-79.159 Tiedon salaus ja suojaus	kevät 98
Laskuharjoitus 3, viikko 8	Tuomas Aura, Antti Huima

1. *Meet-in-the-middle*-hyökkäys kaksinkertaista DES:iä vastaan etsii avainpareja K_1, K_2, joille $E_{K_1}(P_0) = D_{K_2}(C_0)$, missä P_0, C_0 on tunnettu selväkieli-salakielipari. Arvioi montako tällaista paria keskimäärin löytyy ennen oikeaa ratkaisua?

2. Kuinka *meet-in-the-middle*-hyökkäystä voidaan soveltaa **kolmen** avaimen EDE-moodiin? (Vihje: salataan suuri määrä valittuja selväkielisiä lohkoja.)

3. Erään Feistel-salauksen on sekoitusfunktiolla on karakteristinen differenssi

$$00\,7A\,00\,12_{16} \Longrightarrow 00\,00\,00\,00_{16}.$$

   Sen todennäköisyys on 0.034. Kuinka monta kierrosta algoritmissa on tämän perusteella vähintään syytä käyttää, kun avaimen pituus on 128 bittiä?

4. Miten voidaan estää (symmetrisessä salauksessa) seuraavien tietojen paljastuminen:

   (a) sanoman uudelleenlähetys

   (b) sanoman sisällä toistuvat lohkot

   (c) sanoman pituus

   (d) liikenteen vilkkauden vaihtelu

   (e) liikennöivät osapuolet

   (f) avain, jos lähettäjä tai vastaanottaja joutuu vihollisen hallintaan

   (g) aiempien sanomien sisältö, jos lähettäjä tai vastaanottaja joutuu vihollisen hallintaan.

5. Miten kertolasku modulo $2^{16} + 1$ toteutetaan tehokkaasti ohjelmassa? (tarvitaan IDEA-salauksessa)

6. Osoita, että kun n alkion joukosta valitaan noin $\sqrt{n}$ satunnaista alkioita (palauttaen valitut joukkoon ennen seuraavaa valintaa) on todennäköisyys, että jokin alkio tulee valittua kahdesti, suuruusluokkaa 50 %. (liittyy kryptografisiin hajautusfunktioihin)