Tik-79.159 Tiedon salaus ja suojaus	kevät 97
Laskuharjoitus 3, viikko 7	Tuomas Aura, Antti Huima

1. Laske (jos mahdollista):

   (a) $64303^{-1} \bmod (2^{16}+1)$

   (b) $2397^{-1} \bmod 2679$

2. Eräässä DES-algoritmin muunnelmassa käytetään joka kierroksella itsenäisesti valittua aliavainta. Algoritmin avainpituudeksi tulee silloin yhteensä 768 bittiä. Onko tällä algoritmilla jollain tavalla heikkoja avaimia?

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

4. 32 kierroksen Feistel-salauksella on sekoitusfunktion karakteristinen differenssi

   $$00\,7A\,00\,12_x \Longrightarrow 00\,00\,00\,00_x .$$

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

5. Miten kertolasku modulo $2^{16}+1$ toteutetaan tehokkaasti ohjelmassa?

6. *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?