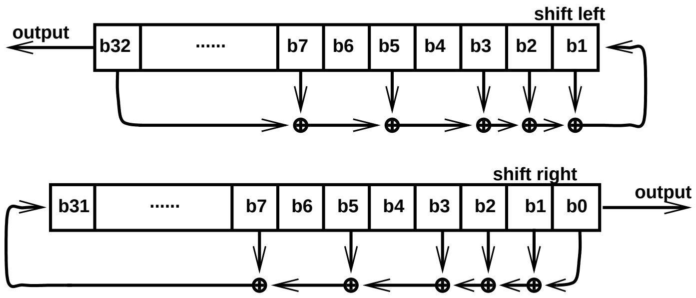
Tik-79.159 Tiedon salaus ja suojaus	kevät 98
Laskuharjoitus 4, viikko 9	Tuomas Aura, Antti Huima

1. Generoi alkua lineaarisen siirtorekisterin bittivirrasta, kun karakteristinen polynomi on $(8, 4, 3, 2, 0)$. Polynomi on primitiivinen; mikä on bittivirran jaksonpituus? Voiko bittivirtaa käyttää salaukseen?

   Huom! Schneier numeroi siirtorekisterin bitit vallan oudosti ja laittaa inputin ja outputin väriin päihin. Ainakin kuva 16.4 on väärin ja samoin teksti samalla sivulla. Polynomia $(32, 7, 5, 3, 2, 1, 0)$ vastaavat seuraavat siirtorekisterit:



   Alempi rekisteri generoi samaa bittivirtaa kuin ylempi, mutta päinvastaiseen suuntaan. (Käytetään mieluummin ylempää.)

2. Anna A5-bittivirran jaksonpituudelle yläraja. GSM-järjestelmässä A5:n tuottamaa bittivirtaa käytetään 112 bitin lohkojen salaamiseen. Arvioi, onko jaksonpituus riittävä tähän nähden?

   Kunkin 112 bitin lohkon jälkeen salaus alustetaan avaimen ja lohkonumeron perusteella. Avain vaihdetaan yleensä yhteyden alussa ja lohkonumerot toistuvat noin 3 tunnin 29 minuutin välein. Millaisen liikenteen turvallisuudelle tästä voi olla haittaa?

3. Tiedetään vastustajan käyttävän 8-bittistä ASCII-koodia sanomien lähettämiseen. Lisäksi on saatu selville, että sanomat salataan lineaarisella siirtorekisterillä, jonka karakteristisen polynomin aste on 5.

   Kaapataan salakielinen sanoma:

   10111000 11100110 01101111 11100100 10111111

   Epäillään, että sanoma alkaa merkeillä "AB". Mikä tallöin on koko sanoman selväkielinen sisältö?

   Opetus: lineaarisella siirtorekisterillä salatun sanoman murtamiseen riittää 2 kertaa rekisterin pituuden verran tunnettua selväkieltä.

4. LaGrange-kynnysrakenne:

   (a) Laadi $(3, 5)$-kynnysrakenne, jossa salaisuus on 4321.

   (b) $(3, 5)$-kynnysrakenteesta (mod $2^{16}+1$) tunnetaan varjot (2,19535), (4,1583), (5,44146). Laske salainen sanoma.

5. Kiinalaiseen jäännöslauseeseen perustuva kynnysrakenne:

   (a) $p = 983$. Tunnetaan varjot $(1013, 64)$, $(1019, 421)$ ja $(1021, 840)$. Laske salainen sanoma.

   (b) Lisää kynnysrakenteeseen uusi varjo.

6. Kiinalaiseen jäännöslauseeseen perustuvassa (m, n)-kynnysrakenteessa valitaan alkuluku p ($p >$ suurin mahdollinen salainen sanoma) ja modulit $d_1 < d_2 < \ldots < d_n$, joilla ei ole yhteisiä alkutekijöitä. Moduleille on lisäksi vaatimus

$$d_1 \cdot d_2 \cdots d_m > p \cdot d_{n-m+2} \cdot d_{n-m+3} \cdots d_n.$$

   Alkuperäinen sanoma s sekoitetaan $s' = s + rp$, missä r on satunnaisluku. Varjot saadaan laskemalla $k_i = s' \bmod d_i$.

   (a) Mitä tapahtuu, jos modulit valitaan väärin ja

$$d_1 \cdot d_2 \cdots d_m < d_{n-m+2} \cdot d_{n-m+3} \cdots d_n?$$

   (b) Entä, jos

$$d_1 \cdot d_2 \cdots d_m < p \cdot d_{n-m+2} \cdot d_{n-m+3} \cdots d_n?$$

   (c) Miltä väliltä sekoituskerroin r pitää valita?