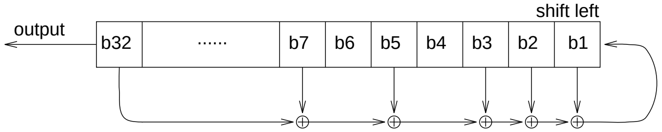
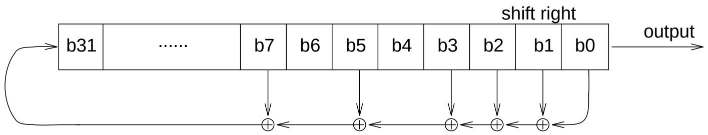
Tik-79.159 Tiedon salaus ja suojaus	kevät 97
Laskuharjoitus 4, viikko 8	Tuomas Aura, Antti Huima

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 vaihtuu 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. Mitä kryptografisen hajautusfunktion funktion ominaisuuksia tarvitaan seuraavissa käyttötarkoituksissa:

   (a) pseudosatunnaislukujen generointi $(x, H(x), H(H(x)), \ldots)$

   (b) haaste-vastemenettely salaisen avaimen tuntemisen osoittamiseksi avainta ulkopuolisille paljastamatta

   (c) istuntoavaimen generointi yhteisestä salaisuudesta (pääavaimesta) ja muusta datasta (nonsseista)

   (d) digitaalinen allekirjoitus

   (e) ohjelmakoodin muuttumattomuuden osoittava (allekirjoittamaton) sormenjälki

   (f) dokumentin aikaleimaus julkaisemalla funktion arvo sanomalehdessä.

   MD5-hajautusfunktiosta arvellaan lähivuosina löytyvän siinä määrin törmäyksiä, että funktio tulee epäluotettavaksi. Mihin edellä mainitusta tarkoituksista se ei sopisi?

5. 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, lähes 50 %.

6. Allekirjoituksissa käytettävän kryptografisen hajautusfunktion tuottaman arvon bittien määrä (esim. 128 bittiä) on yleensä noin noin kaksinkertainen lohkosalauksen salauslohkon pituuteen nähden (esim. 64 bittiä). Selitä, miten sopivat pituudet määräytyvät?