Tik-79.159 Tiedon salaus ja suojaus	kevät 98
Laskuharjoitus 1, viikko 5	Tuomas Aura, Antti Huima

1. Muunna binääriluvuksi:
   (a) 777777
   (b) 1023
   (c) 1024

   Muunna desimaaliluvuksi:
   (d) 1010001101_2
   (e) $6AFF_{16}$
   (f) 4567_8

2. Ratkaise x (jos ratkaisuja on monia, anna pienin ei-negatiivinen ratkaisu):
   (a) $x \equiv 11 + 14 \pmod{2^4}$
   (b) $x = (321 \cdot 123) \bmod 456$
   (c) $x + 5 \equiv 4 \pmod{2^4}$
   (d) $x \oplus 11100011_2 = 00100101_2$
   (e) $114 \oplus 211$
   (f) 114 AND 211.

3. Oletetaan, että tehokas nykyaikainen tietokone pystyy kokeilemaan 100 000 avainta sekunnissa ja että suurella organisaatiolla on 1000 000 tietokonetta käytössään. Kauanko keskimäärin kestää 40-, 56-, 72 ja 128-bittisen avaimen löytäminen kokeilemalla nykyteknologiaa käyttäen? Tietokoneiden laskentatehon on arvioitu kasvan noin 100-kertaiseksi 10 vuodessa. Kuinka kauan avainten löytämiseen tämän arvion mukaan menee 30 vuoden kuluttua?

   Onko mielekästä valita tämän hetken teknologian mukaan lyhin kelvollinen avainpituus? Montako vuotta on virhemarginaali vastustajan teknologian tasoa arvioitaessa?

4. Laske kielen absoluuttinen ja todellinen informaatiosisältö (R ja r) sekä redundanssi (D) kielelle, jonka aakkosto on $M = \{A, B, C, D\}$ (kunkin merkin esittämiseen käytetään 2 bittiä) ja merkkien todennäköisyydet

   (a) ovat $P(A) = 0.5$, $P(B) = 0.25$, $P(C) = 0.125$, $P(D) = 0.125$
   (b) riippuvat aina edellisestä merkistä:

$$\begin{array}{llll}
P(A|A) = 0.5, & P(B|A) = 0.25, & P(C|A) = 0.125, & P(D|A) = 0.125 \\
P(A|B) = 0.25, & P(B|B) = 0.25, & P(C|B) = 0.25, & P(D|B) = 0.25 \\
P(A|C) = 0.25, & P(B|C) = 0.25, & P(C|C) = 0.25, & P(D|C) = 0.25 \\
P(A|D) = 0, & P(B|D) = 0.5, & P(C|D) = 0.5, & P(D|D) = 0.
\end{array}$$

5. Montako erilaista salausfunktiota on olemassa 64 bitin lohkoilta toisille? Kuinka suuri niistä on käytössä salausmenetelmässä, joka käyttää 128-bittisiä avaimia?

6. Millä todennäköisyydellä saadaan kaksi samaa alkiota, kun n alkion joukosta tehdään k satunnaista valintaa? Mikä tämä todennäköisyys on, kun
   (a) $n = 10$, $k = 5$,
   (b) $n = 10^6, k = 1000$.

   Vihje: käytä Stirlingin kaavaa ja muokkaa tulos numeerisen laskennan kannalta sopivaan muotoon.