T-110.503 Kryptologian perusteet
Tentti
17.12.2002

1. (6 pist.) Salaamismenetelmän avaimen pituus on 100 bittiä. Avaimen generointi suoritetaan pseudosatunnaisgeneraattorilla, joka tuottaa viiden bitin lohkoja. Generaattorissa on vika, josta johtuen sen tuottamissa viiden bitin lohkoissa on `1`-bittejä aina vähemmän kuin `0`-bittejä. Jokaisen tällaisen lohkon esiintymistodennäköisyys on yhtä suuri. Kuinka vahvoja tuotetut avaimet ovat, eli mikä on tällä generaattorilla tuotetun avaimen entropia?

2. (6 pist.) Tarkastellaan S-boxia, jolla on kolme syöte-bittiä ja kolme tuotos-bittiä, ja joka on määritelty funktiolla $\pi_S(z) = z^3$, missä $z \in \mathbb{Z}_2[x]/(x^3 + x + 1)$. Esimerkiksi $\pi_S(\texttt{011}) = \pi_S(x+1) = (x+1)^3 = x^3 + x^2 + x + 1 = x^2 = (\texttt{100})$. Laske S-boxin π_S differenssijakaumataulun (*Difference Distribution Table*) rivi syöte-erotuksella $a' = \texttt{100}$.

3. (6 pist.) Oletetaan että AES lohkosalaamismenetelmää käytetään CBC käyttötavalla.

   a) Kuinka monta salakielilohkoa arviolta tarvitaan jotta todennäköisyys sille että löytyy kaksi samaa salakielilohkoa on suurempi kuin 0.5?

   b) Oletetaan että löytyy kaksi samanlaista salakielilohkoa, jotka on muodostettu samalla avaimella (ja CBC käyttätavalla). Mitä voidaan sanoa näitä salakielilohkoja vastaavista selväkielilohkoista?

4. (6 pist.) Tarkastellaan alkulukua $p = 2003$. Muodosta joku kertalukua $q = 13$ oleva alkio multiplikatiivisessa ryhmässä $\mathbb{Z}^*_{2003}$.

5. (6 pist.) Olkoon RSA menetelmän julkinen avain (n, b), missä $n = 84773093$ ja $b = 37869107$. Yritä jakaa n tekijöihin Wienerin Algoritmilla. Jos onnistut, määritä myös salainen eksponentti a sekä $\phi(n)$.