TIK-110.503 Kryptologian perusteet
Loppukoe
16.12.2000

1. (6 pist.) Tarkastellaan jonosalaajaa joka on määritelty seuraavasti:

$$\begin{aligned} \mathcal{P} &= \mathcal{C} = \mathbb{Z}_7,\ \mathcal{K} = \{(a,b) \mid \gcd(a,7) = 1\} \\ z_i &= (a \times i + b) \bmod 7,\ i = 1, 2, \ldots, \text{ where } (a,b) \text{ is the key.} \\ e_z(x) &= (x + z) \bmod 7 \end{aligned}$$

   a) Tulkitse salakieliteksti 25542531 käyttäen avainta (5,3).

   b) Tiedetään että selväkielen osaa 110503 vastaava salakieli on 501153. Määritä tuntemattomasta avaimesta (a,b) niin paljon kuin mahdollista. Mitä lisätietoa tarvitset koko avaimen määrittämiseksi?

2. (6 pist.) Olkoon annettu positiiviset kokonaisluvut n ja r sekä funktio $f : \mathbb{Z}_2^n \times \mathcal{K} \to \mathbb{Z}_2^n$. Määritellään *Feistel salaaja* seuraavasti: $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$, missä $K_i \in \mathbb{Z}_2^n$, $i = 1, 2, \ldots, r$, ja L_j, $R_j \in \mathbb{Z}_2^n$, $j = 0, 1, 2, \ldots, r$. Selväkieli on $X = (L_0, R_0)$ ja salakieli on $Y = (R_r, L_r)$.

   Tarkastellaan nyt seuraavaa Feistel salaajaa, missä puolilohkon koko on $n = 3$ ja kierrosten lukumäärä on $r = 2$, ja käytetään kahta riippumatonta 3 bitin kierrosavainta K_1 ja K_2. Määritellään funktio f asettamalla $f(A, K) = F(A \oplus K)$, missä $F(x) = x^3$ Galois kunnassa $GF(2^3)$ polynomilla $x^3 + x + 1$.

   a) Kuvaa tunnetun selväkielen ratkaisumenetelmä jota käyttäen tämän salausmenetelmän salainen avain voidaan ratkaista.

   b) Ratkaise salainen avain kun on annettu selväkieli/salakieli pari

$$X = 000000 \ / \ Y = 111111.$$

3. (6 pist.) SHA-1 hashfunktion määrittelyssä käytetään funktiota T joka on annettu seuraavasti. Olkoon X_0, X_1 ja X_2 kolme 32 bitin jonoa. Silloin $T(X_0, X_1, X_2) = (X_0 \wedge X_1) \vee (X_0 \wedge X_2) \vee (X_1 \wedge X_2)$, missä $\wedge$ on biteittäin suoritettu "and" kertolasku, ja $\vee$ on biteittäin suoritettu "or" yhteenlasku.

   Olkoon $t(x_0, x_1, x_2)$ Boolen funktio, joka on funktion T yhden ulostulobitin muodostama komponentti. Olkoon $L_w(x_0, x_1, x_2) = w_0 x_0 \oplus w_1 x_1 \oplus w_2 x_2$, missä $w = (w_0, w_1, w_2) \in \mathbb{Z}_2{}^3$. Osoita että funktiolla t on lineaaristen funktioiden L_w kanssa seuraavat korrelaatiot:

$$c(t, L_w) = \begin{cases} 0, & \text{if } H_W(w) = 0 \text{ or } 2 \\ \frac{1}{2}, & \text{if } H_W(w) = 1 \\ -\frac{1}{2}, & \text{if } H_W(w) = 3 \end{cases}$$

4. (6 pist.) Bob käyttää Rabinin julkisen avaimen menetelmää, missä $n = 1999 \times 499$ ja $B = 0$. Määritä salakielen $y = 2000$ kaikki neljä mahdollista tulkintaa.

5. (6 pist.) Oletetaan että Bob käyttää El Gamal allekirjoitusmenetelmää kunnassa $\mathbb{Z}_p$, ja että Bobin allekirjoitukset viesteille x_1 ja x_2 ovat (γ_1, δ_1) ja (γ_2, δ_2), vastaavasti. Alice näkee viestit ja niiden allekirjoitukset ja huomaa että $\gamma_1 = \gamma_2$.

   a) Kuvaa miten Alice voi nyt johtaa tietoa Bobin salaisesta avaimesta.

   b) Olkoon $p = 13$, $x_1 = 1$, $x_2 = 4$, $\delta_1 = 11$, ja $\delta_2 = 2$, ja $\gamma_1 = \gamma_2 = 7$. Mitä Alice voi tässä tapauksessa sanoa Bobin salaisesta avaimesta?

   (Avuksesi kaavat: $\gamma = \alpha^k \bmod p$ and $\delta = (x - a\gamma)k^{-1} \bmod (p-1)$.)