T-79.5501 Kryptologia
2008 / Tentti
15.5.2008

1. (6 pst) Oletetaan, että salausmenetelmällä on seuraava ominaisuus: jokaisella selväkieli-salakieli parilla (x, y), $x \in \mathcal{P}$ ja $y \in \mathcal{C}$ on yksi ja vain yksi avain $K \in \mathcal{K}$ siten että $e_K(x) = y$, eli $H(\mathbf{K}|\mathbf{PC}) = 0$. Osoita että tällöin salausmenetelmä on täydellisesti salaava jos ja vain jos $H(\mathbf{K}) = H(\mathbf{C})$.

2. (6 pst) Kun $f(x)$ on binaarisen LFSR:n takaisinkytkentäpolynomi, niin $(f^*)^* = f$ ja $\Omega(f)$ on tämän LFSR:n generoimien jonojen joukko. Olkoon nyt $f(x)$ ja $g(x)$ kahden binaarisen LFSR:n takaisinkytkentäpolynomit. Todista seuraava väite: Jos $\Omega(f) \subset \Omega(g)$, niin polynomi $f(x)$ jakaa polynomin $g(x)$.

3. (6 pst) Oletetaan että $\mathbf{X}_1$ ja $\mathbf{X}_2$ ovat riippumattomia satunnaismuuttujia jotka saavat arvoja joukossa $\{0, 1\}$. Olkoon ϵ_i muuttujan $\mathbf{X}_i$ bias, jolloin $\epsilon_i = \Pr[\mathbf{X}_i = 0] - \frac{1}{2}$, kun $i = 1, 2$. Todista että satunnaismuuttujat $\mathbf{X}_1$ ja $\mathbf{X}_1 \oplus \mathbf{X}_2$ ovat riippumattomia jos ja vain jos $\epsilon_2 = 0$ ja $\epsilon_1 = \pm\frac{1}{2}$.

4. (6 pst) Kokonaisluvun $n = 89855713$ tiedetään olevan kahden alkuluvun tulo. Lisäksi tiedetään että $\phi(n) = 89836740$. Määritä luvun n tekijät.

5. (6 pst) Alkion $\alpha = 14$ kertaluku on 13 multiplikatiivisessa ryhmässä $\mathbb{Z}_{157}^*$. Tiedetään että alkio $\beta = 93$ kuluu alkion α generoimaan aliryhmään. Laske alkion $\beta = 93$ diskreetti logaritmi x kantaluvun $\alpha = 14$ suhteen, eli ratkaise yhtälö

$$14^x \equiv 93 \,(\mathrm{mod}\, 157).$$

T-79.5501 Cryptology
2008 / EXAM
Thursday, May 15, 2008

1. (6 pts) Suppose that in a cryptosystem the following holds: for each pair (x, y), $x \in \mathcal{P}$ and $y \in \mathcal{C}$, there is exactly one key $K \in \mathcal{K}$ such that $e_K(x) = y$, that is, $H(\mathbf{K}|\mathbf{PC}) = 0$. Prove that then the cryptosystem achieves perfect secrecy if and only if $H(\mathbf{K}) = H(\mathbf{C})$.

2. (6 pts) Let $f(x)$ be a feedback polynomial of a binary LFSR. Then $(f^*)^* = f$ and $\Omega(f)$ is the set of binary sequences generated using this LFSR. Now, let $f(x)$ and $g(x)$ be feedback polynomials of binary LFSRs. Prove the following result: If $\Omega(f) \subset \Omega(g)$, then $f(x)$ divides $g(x)$.

3. (6 pts) Suppose that $\mathbf{X}_1$ and $\mathbf{X}_2$ are independent random variables which take on values from the set $\{0, 1\}$. We use ϵ_i to denote the bias of $\mathbf{X}_i$, $\epsilon_i = \Pr[\mathbf{X}_i = 0] - \frac{1}{2}$, for $i = 1, 2$. Prove that the random variables $\mathbf{X}_1$ and $\mathbf{X}_1 \oplus \mathbf{X}_2$ are independent if and only if $\epsilon_2 = 0$ or $\epsilon_1 = \pm\frac{1}{2}$.

4. (6 pts) The integer $n = 89855713$ is known to be a product of two primes. Further, it is given that $\phi(n) = 89836740$. Determine the factors of n.

5. (6 pts) Element $\alpha = 14$ is of order 13 in the multiplicative group $\mathbb{Z}^*_{157}$. It is given that element $\beta = 93$ is in the subgroup generated by α. Using Shanks' algorithm compute the discrete logarithm x of $\beta = 93$ to the base $\alpha = 14$, that is, solve the equation

$$14^x \equiv 93 \,(\mathrm{mod}\, 157).$$