Topics in Algebra: Cryptography - Blatt 7

11.30-12:15, Seminarraum 9, Oskar-Morgenstern-Platz 1, 2.Stock

http://www.mat.univie.ac.at/~gagt/crypto2018

Goulnara Arzhantseva
goulnara.arzhantseva@univie.ac.at

Martin Finn-Sell
martin.finn-sell@univie.ac.at

1 Test questions from the lecture to refresh:

Question 1. Is the k given in the example of the LFSR the period?

Question 2. Show that the matrix obtained from the linear equations of the Linear Feedback Shift register is invertible mod 2.

Question 3. Consider the LFSR as a bit generator. What are, in this case, the values of k and l for the definition of a bit generator?

2 Exercises

Question 4. Suppose that Alice is using the ElGamal signature scheme. In order to save time in generating random numbers k such that are used to sign messages, Alice choses an initial random value k_0 and then signs the i^{th} message using the value $k_i = k_0 + 2i \mathrm{mod}(p-1)$ (note that this means $k_i = k_{i-1} + 2\mathrm{mod}(p-1)$).

i) Suppose that Bob observes two consecutive signed messages $(x_i, sig(x_i, k_i))$ and $(x_{i+1}, sig(x_{i+1}, k_{i+1}))$. Describe how Bob can easily compute Alice's secret key a given this information without solving an instance of the discrete logarithm problem. Is this method independent of i?

ii) (Practical) Suppose that the parameters of the scheme are $p = 28703$ and $\alpha = 5, \beta = 11339$, and the two messages observed by Bob are:

$$x_i = 12000, sig(x_i, k_i) = (26530, 19862)$$
$$x_{i+1} = 24567, sig(x_{i+1}, k_{i+1}) = (3081, 7604).$$

Find the value of a using the attack from part i).

Question 5. Let f be a bit generator that only produces sequences in which exactly $l/2$ bits have value 0 and $l/2$ bits have value 1. Define the function **dst** by:

$$\mathbf{dst}(z_1, \ldots, z_l) = \begin{cases} 1 \text{ if } (z_1, \ldots, z_l) \text{ has exactly } l/2 \text{ bits equal to } 0 \\ 0 \text{ otherwise.} \end{cases}$$

i) Show that $E_{\mathbf{dst}}(p_u) = \frac{\binom{l}{l/2}}{2^l}$.

ii) Show also that $E_{\mathbf{dst}}(p_f) = 1$.

iii) Finally, show that for any fixed $\epsilon > 0$, that p_u and p_f are ϵ-distinguishable if l is sufficiently large.