Homework 9 in Cryptography I

Prof. Dr. Rudolf Mathar, Paul de Kerret, Georg Bocherer

15.07.2010

Exercise 25. Alice plays with the ElGamal encryption system and encrypts the messages m_1 and m_2 using her own public key. The generated cryptograms are

$$\mathbf{C}_1 = (1537, 2192) \text{ and } \mathbf{C}_2 = (1537, 1393).$$

The public key of Alice is $(p, a, y) = (3571, 2, 2905)$.

a) What did Alice do wrong?

b) The first message is given as $m_1 = 567$. Determine the message m_2.

Exercise 26. Consider the finite field $\mathbb{F}_{2^3}$ with 8 elements. This field can be constructed as the residue ring of the polynomial ring $\mathbb{F}_2[u]$ modulo an ideal generated by an irreducible polynomial of degree 3.

a) Determine all irreducible polynomials of degree 3 in $\mathbb{F}_2[u]$.

Consider the cyclic group $G = \mathbb{F}_{2^3}^*$, where the multiplication is taken modulo the polynomial $f(u) = u^3 + u + 1$.

b) Show that u is a generator for G.

Exercise 27. Consider the group G of the last exercise and choose as the primitive element $a = u$. Execute the generalized ElGamal encryption with public key $y = (110)$, which is the binary representation of the polynom $u^2 + u$, message $m = (111)$ and $k = 3$. What is the private key x of Alice?