Topics in Algebra: Cryptography - Blatt 4

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. i) Why does ElGamal produce **two** components of ciphertext?

ii) Why are the exponents used for decryption smaller for ElGamal compared to RSA?

iii) Why is ECC more popular than the original ElGamal?

Question 2. Which of the following statements is true:

i) Breaking ElGamal is equivalent to solving "Asymmetry of ElGamal";

ii) ElGamal is less efficient for encryption than RSA;

iii) ElGamal is more efficient for decryption than RSA;

iv) There is no message expansion in the RSA-OAEP cryptosystem.

Question 3. Prove the Cayley–Bacharach theorem.

2 Exercises

Question 4. In this question, Alice and Bob are experimenting with the ElGamal cryptosystem. Let G be a finite group of order 43, with generator g and suppose Alice's private key is 10.

1. What is Alice's public key, and what is her decryption function?
2. If Bob wants to send Alice the message $m \in G$, and picks exponent $t = 7$, what ciphertext does Alice receive?

3. Check that Alice's decryption function correctly recovers m.

Question 5. We will do a more complicated implementation of the ElGamal cryptosystem, this time implemented in $\mathbb{F}_{3^3}$. The Polynomial $x^3 + 2x^2 + 1$ is irreducible over $\mathbb{Z}_3[x]$, and hence $\mathbb{Z}_3[x]/(x^3 + 2x^2 + 1)$ is the finite field $\mathbb{F}_{3^3}$. We can associate the 26 letters of the alphabet with the 26 non-zero field elements, and thus encrypt ordinary text in a convenient way. We will use lexicographic ordering on the (non-zero) polynomials to set up the correspondence. This gives:

$$\begin{array}{ccc}
A \leftrightarrow 1 & B \leftrightarrow 2 & C \leftrightarrow x \\
D \leftrightarrow x+1 & E \leftrightarrow x+2 & F \leftrightarrow 2x \\
G \leftrightarrow 2x+1 & H \leftrightarrow 2x+2 & I \leftrightarrow x^2 \\
J \leftrightarrow x^2+1 & K \leftrightarrow x^2+2 & L \leftrightarrow x^2+x \\
M \leftrightarrow x^2+x+1 & N \leftrightarrow x^2+x+2 & O \leftrightarrow x^2+2x \\
P \leftrightarrow x^2+2x+1 & Q \leftrightarrow x^2+2x+2 & R \leftrightarrow 2x^2 \\
S \leftrightarrow 2x^2+1 & T \leftrightarrow 2x^2+2 & U \leftrightarrow 2x^2+x \\
V \leftrightarrow 2x^2+x+1 & W \leftrightarrow 2x^2+x+2 & X \leftrightarrow 2x^2+2x \\
Y \leftrightarrow 2x^2+2x+1 & Z \leftrightarrow 2x^2+2x+2 &
\end{array}$$

Suppose Alice uses $g = x$ and $d =$ private key $= 11$, then $y = x + 2$. How would Alice decrypt the following string of ciphertext (and what does it say)?

$$(K, H)(P, X)(N, K)(H, R)(T, F)(V, Y)(E, H)(F, A)(T, W)(J, D)(U, J)$$

3 Hasse's bound

In this section we add some notes for proving Hasse's bound. It requires two facts, and we will discuss them in detail in the next exercise class. Let E be an elliptic curve and let $K(E)$ be the field we obtain doing algebraic geometry to E - that is the field extension of K obtained by taking $K[x, y]$ and dividing it by the ideal generated by the polynomial $y^2 - ax^3 - b^x - c$, and then passing to the maximal field quotient.

1. The degree of a map of elliptic curves $\phi : E_1 \to E_2$ is determined by the corresponding type of *field extension* we get in duality to ϕ - that is we define:

$$deg(\phi) = [K(E_1) : \phi_* K(E_2)]$$

   This will then be related to the size of the corresponding Galois group, etc. We'll discuss this.

2. The degree of a composition of endomorphisms of E satisfies:

$$|deg(f \circ g) - deg(f) - deg(g)| \leq 2\sqrt(deg(f)deg(g))$$

   The proof of this uses bilinear forms - and then we can get to the proof of Hasses theorem from here - one has to understand degree correctly in this case, however.