Cryptography and Security — Deferred Final Exam

Solution

Serge Vaudenay

2.3.2022

- duration: 1h
- no documents allowed, except one 2-sided sheet of handwritten notes
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will **not** answer any technical question during the exam
- readability and style of writing will be part of the grade
- answers should not be written with a pencil

The exam grade follows a linear scale in which each question has the same weight.

1 ElGamal over another Group

Let n be a positive integer. We consider the set of real angles $A = \{\frac{2k\pi}{n}; k \in \mathbf{Z}\}$ and the set of 2×2-matrices

$$G = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}; \theta \in A \right\}$$

Q.1 Together with the matrix multiplication, prove that G is a cyclic group and give its order and a generator.

The lazy solution to this question can invoke smart algebra theorems. $A = \frac{2\pi}{n}\mathbf{Z}$ is a group for the addition. The function $f : A \to G$ mapping $\theta \in A$ to $f(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is actually homomorphic. This comes from that $f(\theta)$ is the matrix of a rotation by an angle θ. Hence, G inherint from the group structure of A. The group G is isomorphic to the quotient of A by the kernel of A. The kernel is clearly the set of multiples of 2π. Hence, G is actually isomorphic to $\mathbf{Z}_n$, which is cyclic. The rotation by $\frac{2\pi}{n}$ generates all others so $f(\frac{2\pi}{n})$ is a genarator of G.
The standard solution would prove the group properties one after the other. We have

$$\begin{aligned} &\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \\ = &\begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{pmatrix} \\ = &\begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} \end{aligned}$$

(This proves the homomorphic property $f(\alpha)f(\beta) = f(\alpha+\beta)$.) So, G is closed under the multiplication. Associativity is obtained by

$$(f(\alpha)f(\beta))f(\gamma) = f(\alpha+\beta)f(\gamma) = f(\alpha+\beta+\gamma) = f(\alpha)f(\beta+\gamma) = f(\alpha)(f(\beta)f(\gamma))$$

We have commutativity due to $f(\alpha)f(\beta) = f(\alpha+\beta) = f(\beta+\alpha) = f(\beta)f(\alpha)$. We have a neutral element $f(0)$ which is the identity matrix. The inverse of $f(\theta)$ is $f(-\theta)$ due to $f(\theta)f(-\theta) = f(\theta-\theta) = f(0)$. We easily see that $k \mapsto f(\frac{2k\pi}{n})$ is periodic of period n. So, G is an Abelian group of order n. We can see that $f(\frac{2k\pi}{n}) = f(\frac{2\pi}{n})^k$ so $f(\frac{2\pi}{n})$ is a genarator of G.

Q.2 Fully specify the adaptation of the ElGamal cryptosystem over the group G. Carefully specify domains and algorithms, and carefully verify correctness.

A secret key is an element $x \in \mathbf{Z}_n$.
A public key is an element of G obtained by $y = f(\frac{2\pi}{n})^x = f(x\frac{2\pi}{n})$.
A message is an element $\mathsf{pt} \in G$.
To encrypt pt *with public key y, we pick a random $r \in \mathbf{Z}_n$ and produce $(f(\frac{2\pi}{n})^r, y^r) \in G^2$.*
To decrypt (u, v) with secret key x, we compute v/u^x.
If encryption was honestly done, then decryption gives $v/u^x = y^r/f(\frac{2\pi}{n})^{xr} = 1$ so the cryptosystem is correct.

Q.3 Make a complete analysis of the security of the proposed cryptosystem.

Given $y \in G$ we can find $\theta \in A$ such that $y = f(\theta)$ then find $k \in \mathbf{Z}$ such that $\theta = \frac{2k\pi}{n}$. We have $y = f(\frac{2k\pi}{n}) = f(\frac{2\pi}{n})^k$. So, the discrete logarithm problem in G is easy to solve. Hence, we can compute the secret key from the public key and solve the key recovery problem. This is a key recovery attack with no more priviledge than the access to the public key. The cryptosystem is badly insecure.