Cryptography and Security — Deferred Final Exam

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

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.

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

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