Prof. Christian Cachin
Luca Zanolini

Exercise 11

11.1 Computing with encrypted messages (2 pts)

Consider the ElGamal encryption scheme for messages in a cyclic group $\mathbb{G}$ and the RSA encryption scheme with public key N for messages in $\mathbb{Z}_N^*$. Both schemes allow for computation on ciphertexts. This means that anyone can take two messages m_1 and m_2 encrypted under the same key and create a proper encryption of another message m_3, using only the public key and the public parameters. Formally, there are operations $\otimes$ and $\oplus$ such that

$$\mathsf{Enc}(pk, m_1) \otimes \mathsf{Enc}(pk, m_2) \; = \; \mathsf{Enc}(pk, m_3),$$

where $m_3 = m_1 \oplus m_2$. For each of ElGamal and RSA, describe the operations $\otimes$ and $\oplus$.

If such operations exist, an encryption scheme is called *malleable*, in the sense than an attacker can change an encrypted message in a controlled way. Malleable cryptosystems are *insecure* against *chosen-ciphertext attacks* and, hence, not suitable for practical use.

11.2 RSA parameters (3 pts)

a) Explain why the RSA encryption exponent e must always be an odd number.

b) Show that given an RSA modulus N and $\phi(N)$, it is possible to factor N easily. *Hint:* Formulate two equations in two unknowns.

11.3 Bad choice of prime factors (3 pts)

This problem explores the importance of properly choosing the two prime factors p and q of an RSA modulus. In particular, let N be an RSA modulus with $|N| = \lambda$, where λ is the security parameter,

a) Suppose that p is "small," i.e., that $|p| = O(\log \lambda)$. Devise an efficient (in λ) algorithm, which factors N under this asumption, and state it in pseudo-code notation.

b) Suppose that $|p - q| = O(\log \lambda)$, i.e., the two primes are "close" to each other. Devise an efficient (in λ) algorithm, which factors N under this asumption, and state it in pseudo-code notation.

11.4 RSA oracle (2 pts)

Consider the textbook RSA encryption as presented in class, where Alice's public key is (N, e), her private key is d, the encryption $\mathsf{Enc}((N, e), m)$ returns ciphertext $m^e \,\mathbf{mod}\, N$ and decryption proceeds accordingly. Suppose Eve knows a ciphertext c and can ask Alice to decrypt *any* ciphertext *except* c itself. How can Eve decrypt c nevertheless?