Homework 2 for Cryptology 1

Christian Majenz & Carsten Baum, DTU

March 13, 2023

Exercise 1. (**1. Attack RSA! - 5 points**)

In this exercise, you will attack a small instance of RSA. You are given a modulus $N = 4294967317$, ciphertext $c = 17$, and encryption exponent $e = 2^{16} + 1$.

1. Write a simple script (e.g. in Python) to factor N using trial division.
2. Implement the Extended Euclidean Algorithm from the lecture to compute d.
3. Show that you obtained the correct plaintext m by re-encrypting it.

The solution consists of your code as well as the correct plaintext m and decryption key d.

Exercise 2. (**2. IND-CCA security - 5 points**)

In the lecture, we have seen the security notion of IND-CPA security. We will now consider an even stronger security notion, called IND-CCA which stands for Indistinguishability under Chosen Ciphertext Attacks. It is defined as a game between an attacker A and a challenger C as follows:

1. The challenger runs $(pk, sk) \leftarrow KG$ and gives pk to A.
2. A sends two messages m_0, m_1 to C.
3. C flips a bit b, computes $c^* \leftarrow Enc(m_b, pk)$ and sends c^* to A.
4. A may now send arbitrary ciphertexts c to C. C will respond with $m = Dec(c, sk)$ if $c \neq c^*$ and with $\perp$ if $c = c^*$.
5. A outputs a guess b' to C.
6. We say A wins if $b = b'$.

Show that there exists a simple algorithm A which wins the IND-CCA security game for RSA with probability 1 with one ciphertext query to C. To show this, consider what happens if you multiply two messages $m_1 \cdot m_2 \bmod N$ or two ciphertexts $c_1 \cdot c_2 \bmod N$.