Cryptology 1 - Homework 4

Snetkov Nikita, B88482

March 2020

1 Problem 1. Textbook RSA and hybrid encryption

Question A common variant of textbook RSA is the following: During key generation, the modulus N is chosen as usual. We chose e as $e := 3$ (instead of random). Then d is chosen with $ed = 1 \bmod \phi(N)$ (as usual). Your task is to write an adversary that, given the public key pk, and the hybrid encryption c of some message m, finds m.

Solution If e=3 and m is small, so m^e is smaller than ϕ(N), to get original m - I need just calculate $\sqrt[3]{m}$ to find original m. In case of hybrid encryption, after getting AES key like said before, original message can be just decrypted. The code is located in Github (https://github.com/Animehater/Cryptology-1)

2 Problem 2. Malleability of textbook RSA

Question The adversary get a textbook RSA encryption $c = E(pk, m)$ for some unknown message m. The adversary also knows $pk = (N, e)$. The adversary wants to compute $c^1 = E(pk, 2m)$. (This is a specific example of malleability.) How can the adversary efficiently compute c^1 from c and pk?

Solution We can present c like $c = m^e \bmod N$. In the other hand, c‘ would be c‘ $= 2m^e \bmod N$. I recombined that equation and got - c‘ $= 2^e \bmod N$ * $m^e \bmod N$, and we know that second part of product is c. So the adversary can compute $c' = 2^e mod$ N * c