Indian Institute of Technology Delhi

COL 759 - Cryptography

Assignment 4

Garv Nagori, Naman Agarwal
2021CS10549, 2021CS10555

Contents

§1 Question 1

In this question we attempt to factorise the value of N by exploiting the fact that one of its factors is sampled from a low entropy system.

1. We sample values of N and store them in a list.
2. For each value of N sampled we check if the GCD with previous values of N sampled is not equal to 1.
3. If the GCD is not 1, we have successfully found a factor of N.
4. We can find $\phi(N)$ and using it find d = e^{-1} and then decrypt required ciphertext.

§2 Question 2

In this question, we had to create a forgery for a given message using the RSA Digital Signature. The verification works as follows:

1. The signature is of appropriate length (2024).
2. The first two bytes are $'0x00'$ and $'0x01'$.
3. No $'0x00'$ in the middle part of the padded message.
4. The bytes after the second $'0x00'$ is the message.

We exploit the fact that the verification key $e = 3$. The attack works as follows:

1. We ensured that the suffix is 0x00 [M] using the method shown in the assignment.
2. We then ensured the correct length and first 2 bytes being $'0x00'$ and $'0x01'$ by placing the 676^{th} and 677^{th} of the signature as 1. Cubing this satisfies the requirements.
3. For ensuring no middle bytes of the cubed ciphertext to be 0 we randomise the middle part of the ciphertext and cube to check if any bit is 0. We do this till all requirements are satisfied and then return the final ciphertext.

§3 Question 3

In this question, we had to implement the CCA attack given by Bleichenbacher for PKCS#1 v1.5. The attack works as follows:

1. Create an interval in which the message can lie
2. Find a s_i such that $(s_i)^e c$ passes the Padding Oracle check
3. Based on the value of s_i, update the interval in which the message lies.
4. If the number of intervals is 1, we start a heuristic optimised search in a specific interval as specified in the paper.
5. If not, then we search by increasing s one by one.
6. If there is only one interval of the form (a, a), then we know that the padded message is a. We remove the padding and recover the original message.

§4 Acknowledgements

We have used the style file from here[1] to typeset and the style file from here[2] for cryptographic games and protocols to produce this document.

[1] https://github.com/vEnhance/dotfiles/blob/main/texmf/tex/latex/evan/evan.sty

[2] https://github.com/arnomi/cryptocode