Asymmetrical Cryptography Handout

Qcamp 2018, Experimental Session 01/06/2018

1 Introduction

In Mission 1, you construct a basic communication channel which uses infrared light as the communication medium. However, as we have learned over the weeks, this communication channel is not secure. Not even the channel that you usually use to access the internet!

In Mission 2 and 3, we will explore a QKD method to help secure the channel. However, what we have today is not QKD. The security of our internet connection nowadays relies upon some sort of an implementation of asymmetrical cryptography.

This exercise will only explore the basic of the basic, pedagogical implementation of kid-RSA [1], which hopefully will get you to appreciate the big picture of this internet cryptography business. If you are interested to go much more deeper and geeky into this subject, this article [2] is a good place to start.

1.1 Main Idea

Asymmetrical cryptography (also known as public key cryptography) works “somewhat" like this:

1. From some “random" numbers, Alice generates a pair of keys, known as the public key and the private key. Alice then sends the public key to Bob, and keeps the private key for herself.

2. Bob “locks" his message with the public key, rendering it unreadable to any eavesdroppers. Bob then sends the encrypted message to Alice.

3. Alice can then “open" the message with the private key.

The key idea in this scheme is that, the key to “lock" and “open" the message are two different keys, hence the name asymmetrical cryptography. The main assumption is that from the public key, it is “extremely hard" to obtain the private key.

One can quantify the “(extreme) hardness" of obtaining the private key from the public key by estimating the number of years it takes. The highest number of RSA-bits cracked was 768, and it took them an equivalent of almost 2000 years of computing on a single-core 2.2 GHz AMD Opteron-based computer [3]. The internet nowadays uses 1024 or even 2048 RSA-bits, and the time it takes to crack them with today technology is probably much more than the age of the universe. So far no one has successfully crack beyond 768 bits, but if you want to try your luck, you can try [4].

[1] Neal Koblitz., Cryptography As A Teaching Tool, https://sites.math.washington.edu/ koblitz/crlogia.html
[2] How RSA Works: TLS Foundations, https://fly.io/articles/how-rsa-works-tls-foundations/
[3] In case you are wondering, they used a lot of computers in parallel. https://eprint.iacr.org/2010/006.pdf
[4] RSA numbers, https://en.wikipedia.org/wiki/RSA_numbers

1.2 Kid-RSA

Kid-RSA is very similar to RSA, as it has most of the properties of RSA encryption algorithm. However, it is not secure as it can be broken by mathematicians who have studied number theory [5].

Follow these steps to implement kid-RSA:

1. Choose four “random" numbers a, b, a', and b'.
2. Evaluate the following numbers:
   - $M = a \times b - 1$
   - $e = a' \times M + a$
   - $d = b' \times M + b$
   - $n = (e \times d - 1)/M$
3. From these numbers, e and n are the public keys, and d is the private key.
4. To encrypt the message P, use the operation $C = (e \times P) \mod n$.
   Note that the message P is an integer and can only have values between 0 and $n - 1$.
5. To decrypt the ciphertext C, use the operation $P' = (d \times C) \mod n$.

2 Assignment

Task 1 [2 pts] Show that n is always an integer, i.e. $e \times d - 1$ is divisible by M.

[5] If you are interested, you can read about Extended Euclidean Algorithm. There is even an online calculator version in https://planetcalc.com/3298/

Task 2 [2 pts] Show that $P' = P$, i.e. by performing decryption on the encrypted message, you will obtain the original message.

Task 3 [2 pts] Try to encrypt the message $(\mathrm{QC})_{26} = 17 \times 26 + 3 = 445$. Show your working steps.

Task 4 [2 pts] Try to decrypt the encrypted message obtained in Task 3, and show that you obtained $445 = (\mathrm{QC})_{26}$. Show your working steps.

Task 5 [2 pts] You overheard an encrypted message 78025 with the public keys $(e, n) = (12413, 323279)$. Try to crack the message, and express your answers in the form of $(???)_{26}$.
Hint: Show that you can find the private key d from public keys (e, n) with $d \times e + k \times n = 1$. Also, you might want to consult some mathematician afterwards.