Public Key Cryptography

by Ergun Erdogmus

“Anna has a box.”

CMPE 220, 08.11.2016

What will you learn at the end of this presentation

1 - What is “Symmetric Cryptography” and “Asymmetric Cryptography”

2 - Why prime numbers are imporant in Asymmetric Cryptography

3 - An example algorithm : RSA

Symmetric Cryptography

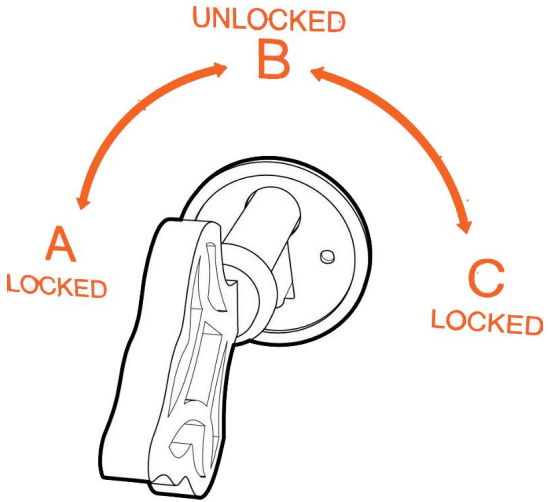
Let’s assume Anna has a box with an ordinary lock

If Anna wants to protect something, she puts it in the box and locks it.

Only he or someone else who has the key can open the box.

Asymmetric Cryptography

This time, let's assume Anna has a box with a lock like this :



The lock has 2 locked states (A, C) and 1 unlocked state (B)

This lock has two separate keys.

The **first one** only turns **clockwise** and the **second one** only turns **counter clockwise**.

Anna picks the first key and keeps it to herself. (**Private Key**)

She makes hundred of copies of the another key. (**Public Key**)

Then, she gives the copied keys to everyone else she knows.

What can we do with these keys?

First of all, we can send Anna a private document easily.

Put the document in the box and use a copy of the public key to lock it.

Since, only Anna’s private key turns lock counter clockwise, only she can open it.

Secondly, we can see if a document has come from Anna.

Let’s say someone delivers me a box and says this box is from Anna. I don’t believe it but I try to open the box with Anna’s public key and it works!

This is called “**digital signature.**”

Prime numbers in cryptography.

If you multiply to prime numbers, you get a huge non-prime number with only two prime factors.

However, factoring that number is not an easy task.

We can use the huge non-prime number as the **public key**. That public key is used to encrypt the message.

We can use the **secret key** consisting of those two prime numbers to decrypt the message.

RSA Algorithm

1 - Choose two large prime numbers p and q

2 - Calculate $n = pq$

3 - Calculate the totient $\phi(n) = (p-1)(d-1)$

4 - Choose an integer e such that $1 < e < \phi(n)$ and e is coprime to $\phi(n)$

5 - Compute d such that $de \equiv 1 \mod n$

Keys

The **public key** is made of the modulus ***n*** and the public exponent ***e***.

The **private key** is made of the modulus ***n*** and the private exponent ***d*** which must be kept secret.

Encrypting messages

Let’s say Anna is using RSA for her box.

Anna gives her public key (***n*** & ***e***) to me and keeps her private key (***n*** & ***d***) secret.

When I want to send message **M** to Anna, I turn **M** into ***m*** smaller than ***n*** by using an agreed-upon reversible protocol **padding scheme**.[1]

1 : More information on **https://simple.wikipedia.org/wiki/RSA_(algorithm)#Padding_schemes**

Then, I compute $c \equiv m^e \mod n$

This is easy.

Afterwards, I send ***c*** to Anna.

Decrypting messages

Anna can recover ***m*** from ***c*** by using her private key ***d*** with the following procedure :

$$m = c^d \mod n$$

Given ***m*** she can recover the message **M**.

Signing Messages

When Anna wants to send me a signed message,

she produces a **hash value**[2] of the message, raises it to the power of **d** and take mod **n** (just like decrypting a message).

$$s \equiv h^d(M) \mod n$$

2 : More information on **https://simple.wikipedia.org/wiki/Cryptographic_hash_function**

When I receive the message, I raise the signature to the power of ***e*** and take mod ***n*** (just like encrpyting a message)

$$h_2(M) = s^e \mod n$$

and compare the resulting hash value with the message's actual hash value.

if $h_2(M) = h(M)$ then I know that message is sent by Anna.

References and further reading

References

- Public Key Cryptography for Non Geeks
  https://blog.vrypan.net/2013/08/28/public-key-cryptography-for-non-geeks/
- Photo By Koppas (Own Work), CC-BY-SA-3.0
  http://commons.wikimedia.org/wiki/File%3ADetail_of_lock_on_antique_wooden_lap_desk.JPG
- Answers of “Why are primes important in crpytography?” from StackOverflow
  http://stackoverflow.com/questions/439870/why-are-primes-important-in-cryptography

- Simple Wikipeadia Page RSA
  https://simple.wikipedia.org/wiki/RSA_(algorithm)
- Latex online equation editor
  http://www.codecogs.com/latex/eqneditor.php

Further Reading

- RSA Proof of Correctness
  http://crypto.stackexchange.com/questions/2884/rsa-proof-of-correctness

Thank you!