CSI2108–Cryptographic Concepts

Module 6 vignette videos, slides, reading

**Video 1**: Overview of asymmetric encryption (12:08)

How do symmetric and asymmetric encryption compare?

Generally speaking, neither one is better than the other it all depends on what they are used for. For example, in part one Alice and bob needed to find a way to securely exchange the key for the message encryption. As they performed the encryption with the symmetric method, exposing the key that could have been intercepted by Oscar during the exchange as While encryption and decryption in the symmetric cipher are made using the same key(y=x + s & x=y + s). the asymmetric cipher uses different keys for both encryption and decryption. For example, the RSA cryptosystem uses a public key and a private key for each user.

**Intro**

In portfolio 1 we used a symmetric block cipher with a key block to encrypt the message to secure the plaintext. However, the key exchange was a problem as the symmetric cryptosystem does not guarantee the integrity of the plaintext such as oscar could have easily manipulate or decrypt the message by intercepting the key.

In this second part I will demonstrate how we can take an advantage of RSA cryptosystem

The following steps outlines the actions taken to generate the RSA public/private key pair for Alice

**Define RSA modulus (n)**

* Choose two prime number (p) and (q)
* Calculate n = p \* q for solid encryption is best to choose large primes

**Define (phi)**

* Phi is the result of (p - 1) \* (q - 1)

**Find RSA public exponent (e)**

* (e) can be any number coprime of (phi) between 1 and (phi)

**Make the public key (n, e)**

* The public key is form by the pair of the public exponent (e) and the public modulus (n)

**Make the private key (d)**

* The private key (d) is formed with (e) and (phi)
* (d) Is the number that multiplied by (e) is the equivalent of 1 modular (phi)
* (d) = (de) ≡ 1 mod (phi)
* to define (d) we multiply the public exponent (e) to each number on the left column all modular (phi) until we find 1 on the right column. once we find 1, we pick the number on the left column as (d) = (de) ≡ 1 mod (phi) as per look up table in the excel implementation

now we can use Alice’s RSA public key to encrypt the key.

**RSA encryption formula**

* y = xe mod n
* the RSA strength is based on the difficulty of calculating the root of modular arithmetic.
* Even if (n) and (e) are publicly available is difficult for Oscar to decrypt the message
* Is considered one-way function

**RSA decryption formula**

* x = yd mod n

**5. (Week 8) Design a simple hash function to create a message digest for X (the message from Portfolio Part 1). (6 MARKS)**

**Hash function design**

* each word within the plain corresponds to a number on the Ascii table
* all number are summed together
* the result of the sum is modularized to a fixed size

**Hash function**

* the hash method is a function that accepts an input of any chosen size and returns a fixed-size value.

**Hash function desirable property security**

* the hash function can accept an input of any length
* the output should be short and fixed length
* computably easy
* the hash function should be one way function
* the function should be sensible to all bits in a way that if an input is swapped with another the output should be different

the hash function design can be improved as if Oscar attempting to interchange values within the message the hash output will remain the same.

Add security to the hash function

* multiplication raw implementation

the multiplication raw multiply each single number within the ascii raw with the next number. then, the sum of multiplication values will ensure the integrity of the message. This way, if Oscar attempt to interchange the values within the ascii raw the output will be completely different.

* The encryption of the key K using Alice’s RSA public key
* The dencryption for the key K using Alice’s RSA public key.

First of all, we are going to find the RSA modulus (n).

in order to generate a pair of both private and public key for Alice

* Encrypt the key K using Alice’s RSA public key
* And decrypt the key K using her private key

for N value, I have multiplied two prime numbers P and Q

P = 13 and Q = 17 N = 221. Then, I have calculated PHI which is = (P-1) \* (Q-1). After that, I get to choose the public exponent E which is a coprime factor between 1 and the value of PHI - 1 .then d which is equal to d \* e equivalent to 1 mod phi. To find d I have use the look-up table that display the results of E multiplied by the numbers on the left and picked the number on the left side which corresponds 1 on the right column. As d = d \* e = 1 mod phi

p = large prime number

q = large prime number

n = p \* q

phi = (p - 1) \* (q - 1)

e = coprime factor between 1 and the value of phi

d = d \* e = 1 mod phi

the encryption is cipher text = plain text at the power of the value of e modular n. While the decryption is plaintext = cipher text at the power of d modular n

presentation I am going to demonstrate how we can generate both public and private key to encrypt the key used in the block cipher for portfolio one.

**RSA public key:** kpub = (n, e)

**RSA Private Key**: kpr = d

d = private exponent

Encryption: y = xe mod n

Decryption: x = yd mod n

Encryption: y = xe mod n and Decryption: x = yd mod n

n = is the result of a multiplication between to prime numbers greater than 13

n has to be greater than x and y. This way, even if Oscar can see the public key will be computationally difficult for him to find the plaintext.

To generate a pair of public and private keys I chosen two large prime numbers. P and Q. computed n which is p multiplied by q and computed PHI which is p minus 1 multiplied by q - 1 than I get to choose a coprime of phi between 1 and the value of phi – 1 for E value and finally compute d which is

Additionally, RSA cryptosystem provides key distribution, message authentication and digital signature

Why are they so important??????????????

Cryptology of our cipher :

It used an asymmetric cipher (block cipher) to encrypt a message as it is efficient, then the sender encrypt the block cipher key using the receiver RSA public key

Encryption and Decryption RSA :

Find a way to make excel perform big exponential calculation

RSA encryption for the key

Key block: CAVANI

RSA C A V A N I

RSA Encryption Formula

**5. (Week 8) Design a simple hash function to create a message digest for X (the message from Portfolio Part 1). (6 MARKS)**

What is asymmetric encryption useful for?

What is a one-way function?

What are the main families of public-key encryption algorithms?

4. (Week 6) Write an algorithm which encrypts the block cipher key K using RSA.   
(6 MARKS)   
State the key K that you will using for your block cipher. (This would normally be the   
same as the key you used for Portfolio Part 1 Task 2.)   
   
- Choose two prime numbers p and q which are both greater than 13 and generate an   
RSA public/private key pair for Alice, explaining the steps you took to do so. (2 marks)   
- Encrypt the key K using Alice’s RSA public key. (If your key is a sequence of   
alphabetic characters, you will need to think about how to convert these to numeric   
values and hence how to apply the RSA encryption algorithm. There are many ways   
you could choose to do this!) (2 marks)   
- Explain how Alice will decrypt the key K using her private key. (2 marks)   
   
[Your explanations in Task 4 should include a demonstration of your code performing   
the RSA encryption and decryption, with the algorithms clearly explained. You will lose   
marks if your code cannot perform the encryption or decryption.]