**German University in Cairo**
**Faculty of Media Engineering and Technology**
**Mervat Abu-Elkheir**
**Ahmad Helmy**
**Mohamed Abdelrazik**

# CSEN1001: Computer and Network Security

Spring Term 2019

**Tutorial 6**

## Problem 1 - Asymmetric keys

Alice and Bob both have a Public key and a private key. Given the following scenarios, how would Alice and Bob make use of the keys?

a) Alice wants to send a message M to Bob. She wants to make sure only Bob can read this message.
b) Alice wants to send a message to Bob. Alice is not concerned if someone other than Bob reads her email message, but she is mostly concerned that Bob is sure that she is the one who sent the message.
c) Alice wants to send Bob an encrypted email and she also wants to assure Bob that she's the one who wrote the message.

## Answer

a) Alice can encrypt the message with Bob's public key. In this case only Bob can decrypt it using his private key.
b) Alice can sign the message with her private key. When Bob gets the message, he can decrypt the signature using Alice's public key to make sure that Alice is the one who wrote that message.
c) Alice can sign the message using her private key to assure Bob that she's the one who wrote the message. Then, she can encrypt the message and the encrypted signature with Bob's public key to make sure only Bob can decrypt it.
When Bob receives the message, he will first decrypt it using his private key. Then, he can decrypt the signature again using Alice's public key to make sure that she's the one who sent the message.

## Problem 2 - RSA Key generation

Describe the key generation procedure in RSA algorithm.

## Answer

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

- Choose two distinct prime numbers **p** and **q**.
- Compute **n = p*q**.

    - **n** is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
- Compute **φ(n) = φ(p)*φ(q) = (p − 1)(q − 1)**, where **φ** is Euler's totient function.
- Choose an integer e such that **1 < e < φ(n)** and **gcd(e, φ(n)) = 1**; i.e. **e** and **φ(n)** are co-prime.
- Determine **d = e-1 mod (φ(n))**. In other words: **d*e = 1 + k * φ(n)** where **k** is any integer number.
    - The public key consists of the modulus **n** and the public (or encryption) exponent **e**.
    - The private key consists of the modulus **n** and the private (or decryption) exponent **d**, which must be kept secret.
    - **p**, **q**, and **φ(n)** must also be kept secret because they can be used to calculate **d**.
- Publish **e** and **n** and keep **d**, **p**, and **q** secret

$$p, q$$
$$n = pq \qquad \phi(n) = (p-1)(q-1)$$
$$e, \qquad 1 < e < \phi(n) \qquad \gcd(e, \phi(n)) = 1$$
$$d = e^{-1} \bmod \phi(n)$$

## Problem 3 - RSA Ciphering

Explain how the message is ciphered and deciphered using RSA.

## Answer

**Encryption**

- Let the plaintext be **M**. We assume **0 < M < n**. The sender obtains the public key of the recipient **PU = {e, n}**.
- Computes **C = $M^e$ mod n**
- Anybody who knows e and n can perform the encryption.

**Decryption**

- The recipient uses his private key **PR = {d, n}**
- computes **M = $C^d$ mod n**

## Problem 4 - RSA Encryption

Perform encryption using the RSA algorithm for the following:
**p** = 11, **q** = 23, **M** = 26.

## Answer

Generate the key pair:

1. Since **p** = 11 and **q** = 23. Thus, **n** = 253
2. **φ(n) = (p-1) × (q-1)** = 10 × 22 = 220
3. Select e with **1 < e < φ(n)** and **gcd(e, φ(n)) = 1**. For example **e** = 3.
4. Compute **de = 1+ k × φ(n)** ➔ **d = (1+ k × 220)/3**
    - Trying **k** = {1, 2 …} and choose first **k** that makes **d** integer, which we get when **k** = 2, so **d = (1+ 2 × 220)/3** = 147.
5. We have now **e** = 3, **n** = 253, and **d** = 147.
6. The message **M** is 26. Encrypt **C = $M^e$ mod n** = 263 mod 253 = 119.

## Problem 5 - RSA Encryption/Decryption

Perform encryption using the RSA algorithm for the following:
**p** = 3, **q** = 11, **e** = 7, **M** = 5.

## Answer

Generate the private key:

1. Since **p** = 3 and **q** = 11. Thus, **n** = 33
2. **φ(n) = (p-1) × (q-1)** = 2 × 10 = 20
3. Compute **de = 1+ k × φ(n)** ➔ **d = (1+ k ×20)/7**
    - Trying **k** = {1, 2 …} and choose first **k** that makes **d** integer, which we get when **k** = 1, so **d = (1+ 1 × 20)/3** = 3.
4. We have now **e** = 7, **n** = 33, and **d** = 3.

- The message **M** is 5. Encrypt **C = $M^e$ mod n** = $5^7$ mod 33 = 14.
- The cipher **C** is 14. Decrypt **M = $C^d$ mod n** = $14^3$ mod 33 = 5.

## References


- http://en.wikipedia.org/wiki/Extended_Euclidean_algorithm
- http://pajhome.org.uk/crypt/rsa/rsa.html
- Some questions & answers are from Chapter 9 in the book.