School of Digital Media and Infocomm Technology

### ST2504 Applied Cryptography

1. The development of public-key cryptography is the greatest and perhaps the only true revolution in the entire history of cryptography. The purpose is to complement rather than to replace the private key cryptography.

a) State two (2) issues that the public-key cryptography attempts to address.

**Key Distribution – how to have secure communications in general without having to trust a KDC with your key**

**Digital Signatures – how to verify a message comes intact from the claimed sender**

b) Explain the problems with key management and how it affects symmetric cryptography?

**The primary weakness of symmetric encryption algorithm is keeping the secret key secure.**

**If bob wants to send an encrypted message to Alice using symmetric encryption, he must be sure that she has the secret key to decrypt the message. He would not want to send it to the internet – as it is insecure. Issue of sharing of key.**

**He cannot encrypt and send the secret key over internet, as the recipient first need to know the key to decrypt.**

**Even Alice received the key securely, how can she be certain that the attacker has not seen the secret key on Bob’s computer? – Authenticity of key**

**In addition, how can bob know that the secret key has not been tampered? – Degree of trust**

**As such, key management is a significant impediment to using symmetric encryption.**

2. Perform encryption and decryption using the RSA algorithm for the following:-

1. p=3; q=5; e=7; d=3; M=7

Where: **p**, **q** are two prime numbers used to generate modulus ***n***,

**e** is the public key,

**d** is the private key and

**M** is the message.

**Given p=3; q=5; e=7; d=3; M=7**

**C = M^e mod n**

**M = C^d mod n**

**N = (p \* q) = 3 \* 5 = 15**

**Encryption**

**Given e(P)**

**e = 7, M = 7**

**= 7^7 mod 15**

**= 13**

**Decryption**

**Given d = 3**

**d(P) = 13^3 mod 15**

**= 17**

1. Explain why one would never use both the given public keys in parts (i) and (ii) for real encryption? What needs to be done to make it really secure?

**The keys are too short for real security. The security of RSA relies on the difficulty of factorization of large prime numbers.**

**To secure the above, one has to increase the key size.**

3. Tom wants to send a highly confidential message to Jerry using public key cryptosystem. Tom encrypts his message using his own private key and sends the encrypted message to Jerry. When Jerry receives the message, he uses Tom’s public key to read the message. However, the highly confidential message was also known to some other people even though Jerry did not reveal the message to anyone else. Tom was upset and concerned how other people managed to read the message.

a) Explain how some other people managed to read the confidential message that was meant for Jerry.

**Interceptors who know the message originated from Tom could obtain Tom’s public key, which is known, and decrypt the message that Tom sends.**

1. If Tom persists in using public key cryptosystem, describe what he should do to prevent the loss of confidentiality of the message.

**Tom should encrypt the message using Jerry’s public key. In the event that the message is intercepted, it could not be read because the interceptor does not have Jerry’s private key that is needed to decrypt the message.**

4. Contrast the two classes of algorithms – Symmetric and Asymmetric.

|  |  |  |
| --- | --- | --- |
| **Characteristics** | **Symmetric Algorithm** | **Asymmetric Algorithm** |
| **Key used for encryption/decryption** | Same key is used for encryption and decryption | One key for encryption and another, different key is used for decryption |
| **Speed of encryption/decryption** | Very fast | Slower |
| **Size of resulting encrypted text** | Usually same as or less than the original plain text size | More than the original plain text size |
| **Key agreement/exchange** | A big problem | No problem at all |
| **Number of keys required as compared to the number of participants in the message exchange** | n (n-1) / 2 | Key pairs same as the number of the participants |
| **Usage** | Mainly for encryption and decryption (confidentiality), cannot be used for digital signature (integrity and non-repudiation checks) | Can be used for encryption and decryption (confidentiality), as well as for digital signature (integrity and non-repudiation checks) |

5. List and explain four (4) possible approaches to attacking the RSA algorithm.

**Brute force. This involves trying all possible private keys.**

**Mathematical attacks based on factoring. There are several approaches, all equivalent in effort to factoring the product of two primes. (i.e. factor 262417 to 397 \* 661)**

**Timing attacks. These depend on the running time of the decryption algorithm. (*Every logical operation in a computer takes time to execute, and the time can differ based on the input; with precise measurements of the time for each operation, an attacker can work backwards to the input*)**

**Chosen ciphertext attacks. This type of attack exploits properties of the RSA algorithm. (Try to deduce the secret key)**