

### 

### Assignment Cover Sheet

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Student name:** | **Danish Ali** | | | | | |
| **Student number:** | **2875170** | | |  | | |
| **Faculty:** | **Computing Science** | | |  | | |
| **Course:** | **BSc (Hon.)** | | | **Stage/year:** | **4** | |
| **Subject:** | **Advance Network Theory** | | | | | |
| **Study Mode:** | Full time | **Yes** |  | Part-time |  |  |
| **Lecturer Name:** | **Faheem Bukhatwa** | | | | | |
| **Assignment Title:** | **Worksheet 08** | | | | | |
| **No. of pages:** | **5** | | |  | | |
| **Disk included?** | Yes / **No** |  |  |  |  |  |
| **Uploaded to Moodle?**  **Additional Information:** | Yes / **No**  (ie. number of pieces submitted, size of assignment, A2, A3 etc) | | | | | |
|  | | | | | |
|  | | | | | |
| **Date due:** | **13/12/2018** | | |  | | |
| **Date submitted:** | **13/12/2018** | | |  | | |
|  | | | | | | |
| **Plagiarism disclaimer:**  *I understand that plagiarism is a serious offence and have read and understood the college policy on plagiarism. I also understand that I may receive a mark of zero if I have not identified and properly attributed sources which have been used, referred to, or have in any way influenced the preparation of this assignment, or if I have knowingly allowed others to plagiarise my work in this way.*  *I hereby certify that this assignment is my own work, based on my personal study and/or research, and that I have acknowledged all material and sources used in its preparation. I also certify that the assignment has not previously been submitted for assessment and that I have not copied in part or whole or otherwise plagiarised the work of anyone else, including other students.*  **Signed: Danish Ali Date: 13/12/2018** | | | | | | |

## 

Please note: Students MUST retain a hard / soft copy of ALL assignments

# Q1

# What is a session key?

In single communication session, single-use symmetric key is used for encrypting all messages of in process communication and then destroyed.

# Q2

# Recommend five ways through which a conventional encryption system can be made more difficult to break?

A conventional encryption system uses a ciphertext to encrypt the original message. It can only be deciphered using the key. It is fast but to make it more secure:

1. Use maximum key length available
2. Using latest encryption standard such as AES 128 or AES 512 to encrypt the key
3. Encrypt in layers
4. Store encryption keys securely
5. Using a secure cipher such that the cost of breaking the cipher exceeds the useful lifetime of the information
6. Destroy key carefully after job is done.
7. Use complex encryption algorithms.

# Q3

# Write the definition of each of the following:

# (i) Data Integrity, (ii) Authenticity, (iii) Non-Repudiation. (iv) Data confidentiality (v) Denial of Service Attack (DoS)?

i) Data Integrity refers to assurance of data received is as sent by authorized entity.

ii) Authenticity is assurance that a message or other information is from the source it claims to be from.

iii) Non-repudiation is an assurance that a party to a contract cannot deny the authenticity of their signature on a message or a piece of information that they originate from. Its protection against denial by one of the parties in a communication.

iv) Data confidentiality in security allows authorized users to access protected data. Its protection of data from unauthorized disclosure.

v) DoS is a cyber-attack that occurs when systems flood the bandwidth of a target system with infinite requests to disturb the services of the target. Target is unable to serve such many requests and crashes.

# Q4

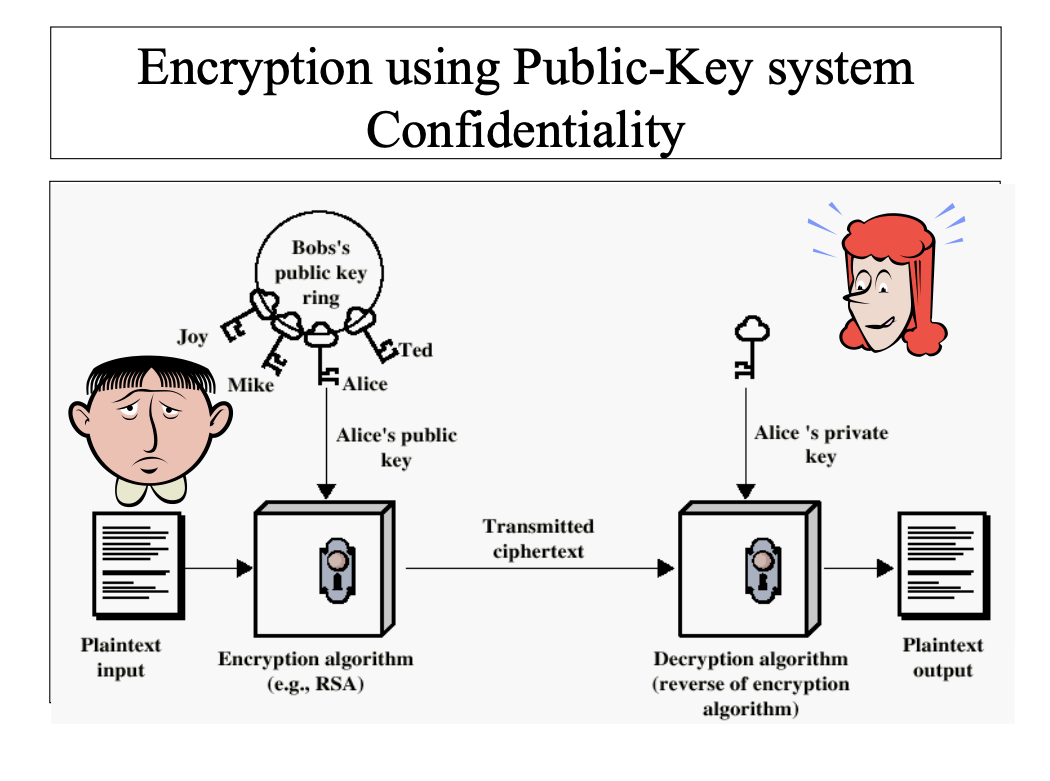
# What is the difference between substitution encryption and transposition encryption?

Substitution encryption is a method by which letters of plaintexts are replaced with a cipher text (letters or by numbers or symbols) according to a fixed system.

Transposition encryption is a method of encrypting information in which plaintexts are rearranged. The cipher text is now permutation of the plaintext.

# Q5

# With the help of a diagram explain the basic operation of a Conventional encryption system.



# Q6

# Briefly, what is the difference between passive and active attacks?

A passive attack is an attack on a network in which a system is monitored, eavesdropping on open ports and other vulnerabilities to obtain message contents. No data is modified on the target and it just monito of traffic flows.

Active attack is an attack on a network in which intruder may masquerade an entity and modification of data stream of. Denial of service, replay previous messages and modify messages in transit.

# Q7

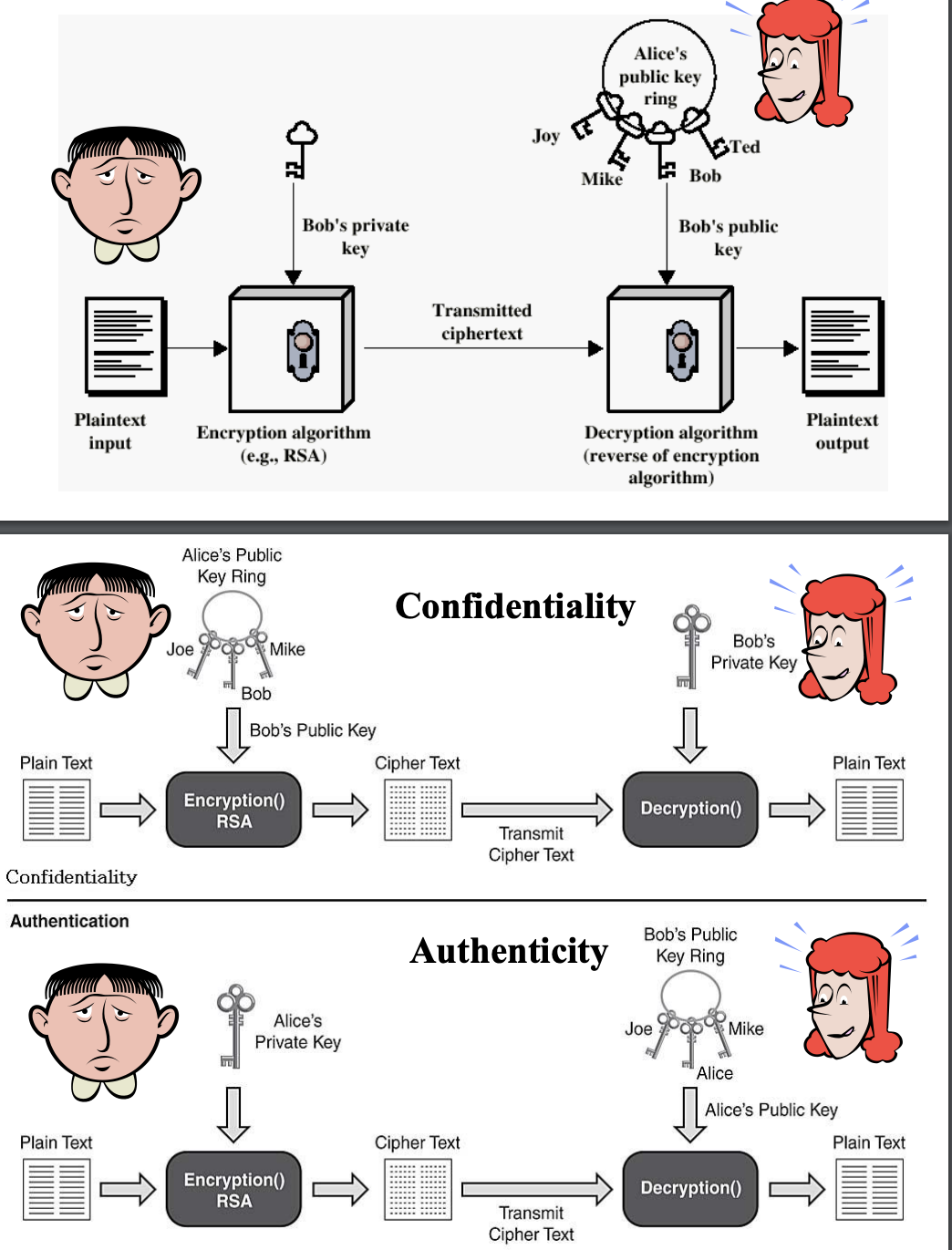
# How can symmetric encryption systems be attacked? and how could such attacks be resisted?

(Brute Force Attacks) BFA in which intruder uses every possible key to decrypt message, proportional to key size.

Long key can prevent Brute force attack. There is no way to defend against BFA because containing intruder from trying key searcher method is impossible. However, if key is long enough, key searcher is not feasible enough to decrypt it in given reasonable time. For instance, with 128 bit key [ 5.9 \* 1030 years] are required to decrypt it.

# Q8

# Regarding asymmetric (public key) encryption systems: Draw a diagram and describe how the public key encryption and decryption system works, showing the six elements of the system.



# Q9

# Give two characteristics of the keys used in public key encryption systems.

1. Two parties do not need to trust each other.
2. Two separate keys: a public and a private key.
3. Typically, slow

Example: RSA, ElGamal Encryption, ECC.

# Q10

# Name three methods of how keys are distributed.

There are different key distribution methods for different encryption types:

1. In symmetric key encryption, trusted key distribution center (KDC) is acting as intermediary between n parties.
2. In public key encryption, public key servers are used for both uploading and downloading public keys.
3. Public key infrastructure (PKI) is used to share SSL certificate, Certificate Authority (CA) provides public keys and validation of SSL.

# Q11

# Explain the difference between using public key encryption system for confidentiality or authentication?

Confidentiality is reached when message is encrypted with receiver’s public key. In this case, decryption of message is only possible using a matching private key by sender. It ensures proprietorship of key and association with the public key.

Authentication is reached when the public key verifies that a holder of the paired private key has sent the message. In short, it verifies message coming from authorized sender

# Q12

# State three functions (or services) that asymmetric encryption systems provide.

Asymmetric encryption systems perform an encryption function that encrypts a message using a public key and a decryption function that uses a private key to decrypt a message that is encrypted with paired public key. It provides authenticity and confidentiality.