National University of Computer and Emerging Sciences

MID-1 SOLUTION

Q1. Answer questions using AGREE or DISAGREE and adding one sentence ONLY for explanation/reason in case of DISAGREE. Giving NO explanation/reason or irrelevant details will get you ZERO credit. Each question carries 0.5 point. [0.5 x 10 = 05 marks]

i. If Alice has a message to send to Bob and she wants to encrypt the message using asymmetric cryptography so that no one other than Bob can read it, she does so by using Bob's private key.
DISAGREE: She uses Bob's public key

ii. A certificate authority is trusted third party which provides a way for one party to learn the public and private keys of another party. Web browsers have a list of these trusted third parties, to support communication using HTTPS.
DISAGREE: only the public keys of another party

iii. Public-key certificate is a signed document by a trusted authority that a given public key indeed belongs to a given party.
AGREE

iv. Hash functions used in cryptography are always reversible, meaning you can retrieve the original input from the hash output.
DISAGREE: one-way functions

v. The Data Encryption Standard (DES) is a symmetric-key block cipher that uses a 128-bit key.
DISAGREE: uses 64-bit key

vi. Cryptographic algorithms that are considered secure today may become vulnerable in the future due to advances in computing power or new mathematical discoveries.
AGREE

vii. The Diffie-Hellman key exchange algorithm allows two parties to establish a shared secret key over a secure communication channel.
DISAGREE: insecure communication channel

viii. Advanced Encryption Standard (AES) operates on variable-sized blocks of data.
DISAGREE: fixed-sized block

ix. Privacy assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
AGREE:

x. In encryption, computationally secure means that no matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there.
DISAGREE: this is the meaning of unconditionally secure

Q.2 You have implemented RSA algorithm for encryption in your security course project. In your viva, the teacher asked you to use an example to show its key-pair generation, message encryption and decryption process. Show the steps using an example scenario. **[2 marks]**

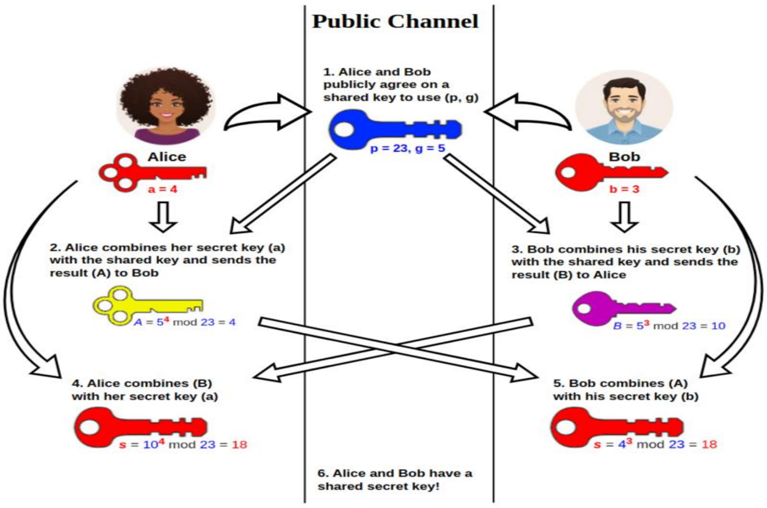
RSA Algorithm Example

- Choose p = 3 and q = 11.
- Compute n = p * q = 3 * 11 = 33.
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20.
- Choose e such that 1 < e < φ(n) and e and φ (n) are coprime. ...

- Compute a value for d such that (d * e) % φ(n) = 1. ...
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

Q.3 What is the importance of Diffie-Hellman algorithm? Illustrate (use block diagram) the output/result using an example scenario. **[2 marks]**

Importance: It is used to exchange symmetric key over an insecure channel without disclosing the key.


Public Channel
1. Alice and Bob publicly agree on a shared key to use (p, g)
p = 23, g = 5
Alice
a = 4
Bob
b = 3
2. Alice combines her secret key (a) with the shared key and sends the result (A) to Bob
A = 5⁴ mod 23 = 4
3. Bob combines his secret key (b) with the shared key and sends the result (B) to Alice
B = 5³ mod 23 = 10
4. Alice combines (B) with her secret key (a)
s = 10⁴ mod 23 = 18
5. Bob combines (A) with his secret key (b)
s = 4³ mod 23 = 18
6. Alice and Bob have a shared secret key!

Q4:

i. Your friend explained you how Caesar cipher works. He/she then sent you an encrypted message "**pumvythapvu zljbypaf tpkalyt ylzbsaz**" to share some confidential information, however, forgot to share the key. Identify the plaintext and the key. **[1 mark]**

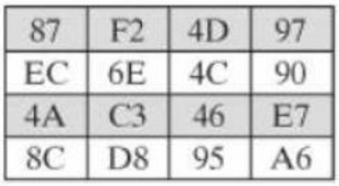
Information security midterm results **Key = 7**

ii. Is Data Encryption Standard (DES), a good and cryptographically strong algorithm to use? Why or why not? Explain. **[1 mark]**

Not a good algorithm as it is weak because of several reasons including weak keys and processes such as S-boxes etc.

Q5:

i. Apply AES shift rows operation on the following state matrix and show the result. **[1 mark]**



87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

87	**F2**	**4D**	**97**
6E	**4C**	**90**	**EC**
46	**E7**	**4A**	**C3**
A6	**8C**	**D8**	**95**

ii. Discuss the key sizes supported by AES and their respective security levels. How do larger key sizes contribute to stronger encryption? **[1 mark]**

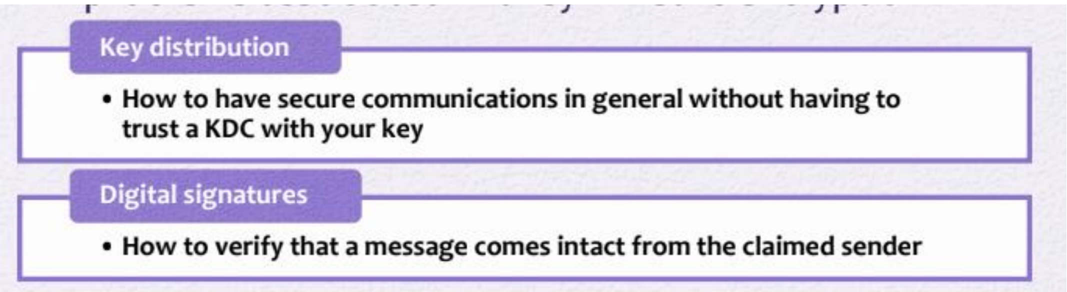
AES-128 uses a 128-bit key length to encrypt and decrypt message blocks.
AES-192 uses a 192-bit key length to encrypt and decrypt message blocks.
AES-256 uses a 256-bit key length to encrypt and decrypt message blocks.

A larger key size indicates greater cryptographic strength and increases the difficulty of cracking it through brute force or other attacks.

Q6:

i. You are insisting your friend to use public-key cryptography for confidentiality. Highlight and explain him/her with two major reasons for your preference over using symmetric key. **[1 mark]**

The concept of public-key cryptography evolved from an attempt to attack two of the most difficult problems associated with symmetric encryption:



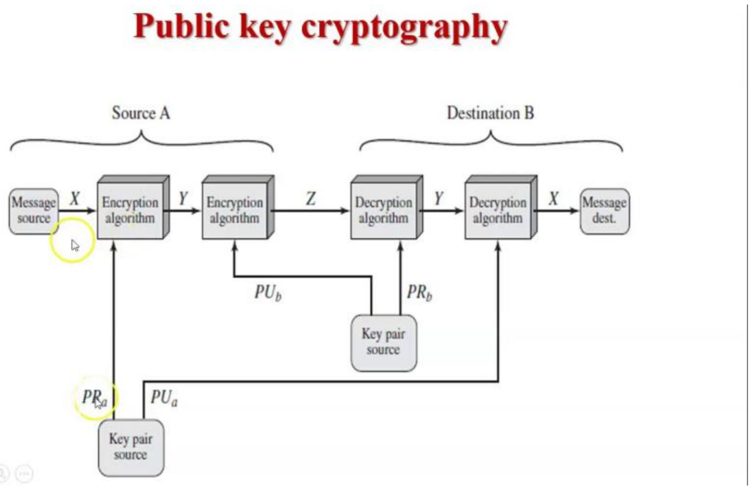
Key distribution

- How to have secure communications in general without having to trust a KDC with your key

Digital signatures

- How to verify that a message comes intact from the claimed sender

ii. Ali and Bilal are given a project to develop a secure chatting application. Draw a suitable diagram showing how can they apply message authentication, integrity, and confidentiality? **[1 mark]**



Add hash-based authentication for integrity with digital signature in this diagram.