GLASGOW COLLEGE UESTC

Mock Exam

Information Security (UESTC 4036)

Date:
Time:

Attempt all PARTS. Total 100 marks

Use one answer sheet for each of the questions in this exam.
Show all work on the answer sheet.

Make sure that your University of Glasgow and UESTC Student Identification Numbers are on all answer sheets.

An electronic calculator may be used provided that it does not allow text storage or display, or graphical display.

All graphs should be clearly labelled and sufficiently large so that all elements are easy to read.

The numbers in square brackets in the right-hand margin indicate the marks allotted to the part of the question against which the mark is shown. These marks are for guidance only.

Q1 (a) Briefly explain 'threat vector' with an example. How a threat vector can be identified? [7]

(b) What is the difference between a virus and a worm? [4]

(c) Explain active attack with the aid of a diagram. Give some examples of active attacks. [7]

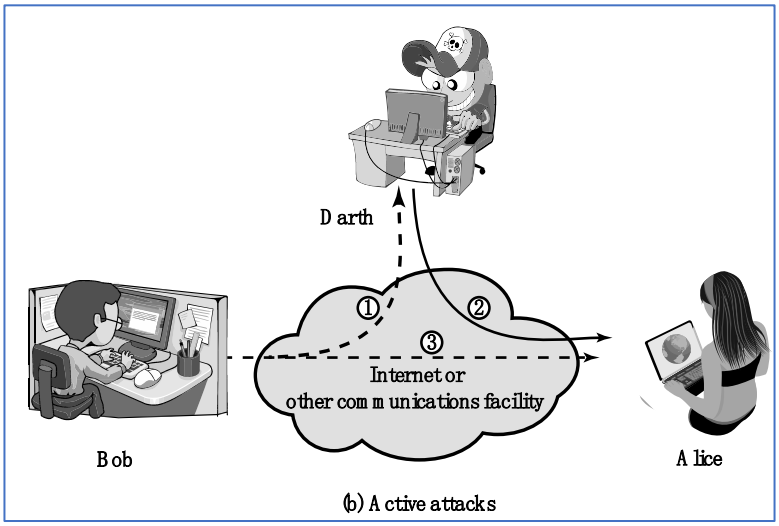
(d) Design a playfair cipher matrix for a given keyword 'Chengdu'. Encrypt the following plaintext using this playfair cipher matrix: 'My place is secure' [7]

Q1 Solution:

a) A threat vector is a term used to describe where a threat originates and the path it takes to reach a target.
An example of a threat vector is an e-mail message sent from outside the organization to an inside employee, containing an irresistible subject line along with an executable attachment that happens to be a Trojan program, which will compromise the recipient's computer if opened.
A good way to identify potential threat vectors is to create a table containing a list of threats you are concerned about, along with sources and targets

b) A virus is a self-replicating program that uses other host files or code to replicate. Most viruses infect files so that every time the host file is executed, the virus is executed too. A computer worm uses its own coding to replicate, although it may rely on the existence of other related code to do so. The key to a worm is that it does not directly modify other host code to replicate.

c) An **active attack** may change the data or harm the system. Attacks that threaten the integrity and availability are active attacks.
As shown in the figure 1 below, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorised entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.
Examples of active attacks are modification, masquerading, replaying, repudiation, and denial of service.



(b) Active attacks

d) The playfair matrix is shown below

C	H	E	N	G
D	U	A	B	F
I/J	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

First, we have to make alphabets in in pair: my pl ac ei sx se cu re

So, the encrypted text will be: SN RI DE CL RY RN HD XA

Q2 (a) Explain the AddRoundKey transformation function for AES method. [4]

(b) What is avalanche effect of an encryption algorithm? [4]

(b) Explain the process of **ShiftRows** and perform the **ShiftRows** operation on the following state matrix. [7]

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

(d) What are the essential steps for proper functioning of public key decryption algorithm? Explain with the aid of a diagram. [10]

Solution Q2:

(a) In the forward add round key transformation, called AddRoundKey, the 128 bits of State are bitwise XORed with the 128 bits of the round key. The operation is viewed as

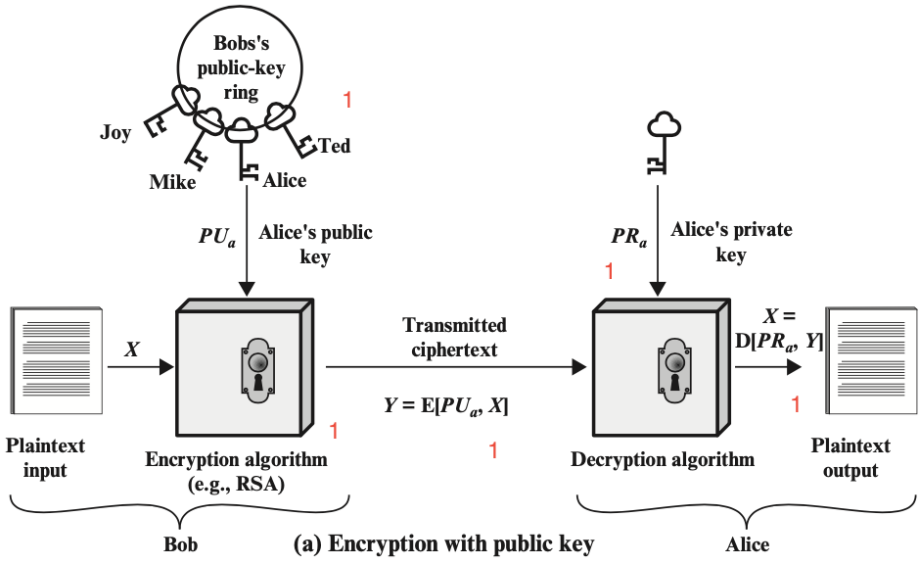
a columnwise operation between the 4 bytes of a state column and one word of the round key; it can also be viewed as a byte-level operation.

(b) A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext. In particular, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the avalanche effect.

(c) ShiftRows: The first row of State is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the fourth row, a 3-byte circular left shift is performed.

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

(d) This public key cryptography algorithm accepts the ciphertext and the matching key and produces the original plaintext.



The essential steps are the following:

(1) Each user generates a pair of keys to be used for the encryption and decryption of messages.

(2) Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private. As Figure A2 suggests, each user maintains a collection of public keys obtained from others.

(3) If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.

(4) When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

Q3

(a) Blockchain is an emerging distributed ledger technology to record data/transactions. Please answer the below questions about the basics of this technology.

(i) List **three** different nodes in blockchain system, and indicates which node can generate new transactions. [**4 marks**]

Answer: full node, lightweight node and miner node. Full node and lightweight node can generate new transactions.

(ii) Blockchain has some unique features that distinguish it from traditional database systems. List **any three** features of blockchain system.

[**3 marks**]

Answer: **Accept any three of the below**.

Decentralization
Transparency
Immutability
Availability
Security
Data tampering
Pseudonymity
Non-repudiation
Auditability

(iii) Explain the access permission respectively for public chain, private chain and consortium chain. [**3 marks**]

Answer: Public Blockchain Network — Permissionless
Private Blockchain Network — Permissioned
Consortium Blockchain Network — Permissioned

(b) To resist attacks, blockchain has unique working principles for data/transactions management.

(i) List and explain two typical failures occurred in a blockchain system. [**4 marks**]

Answer: Crash-failures [1 mark]. The node cannot work properly (either receiving data or transmitting data) [1 mark].

Byzantine attacks/failures [1 mark]. The node can arbitrarily send any fault information. [1 mark]

(ii) List **any three** consensus mechanisms used in blockchain systems. **[3 marks]**

Answer: PoW, PoS, RAFT, Paxos, PBFT, etc.

(iii) Suppose a blockchain network has a block size of 6 MBytes, transaction size of 80 Bytes, Block time is 200 seconds and it requires to wait for 20 blocks to confirm any new block. Calculate the average block confirmation time and transaction per second (throughput) of this blockchain network. [**3 marks**]

Answer:
$\text{Transaction Throughput} = \frac{6\ (\text{M Bytes})}{80\ (\text{Bytes}) \times 200\ (\text{seconds})}$ [1 mark]
$= 37.5\ Tx/second$ [1 mark]

Average Confirmation Time = 20 × 200 seconds = 4000 seconds [1 mark]

(iv) If there are 3 crash-failure nodes participating in a distributed consensus process, calculate the minimum number of legitimate nodes to achieve crash-failure tolerance (the derivation should be provided). **[3 marks]**
Answer: the total number of nodes N participated in this consensus should satisfy

$N \geq 2 * 3 + 1 = 7$ [2 marks]

Hence, the minimum number of legitimate nodes should be 7-3=**4** [1 mark].

(v) Explain the advantages of sharing. **[2 marks]**

Advantages: **Accept any two of the below, and 1 mark each**.

High scalability [1 mark]

Great transaction capacity [1 mark]

Low cost [1 mark]

Q4

(a) Consensus is the key component of a blockchain system.

(i) Consider a PoW-based blockchain system with five participating nodes (N1, N2, N3, N4), with computing power (hash rate) values $\phi 1$=3, $\phi 2$=5, $\phi 3$=4, and $\phi 4$=x. If the probability of winning the puzzle by N1 is 20%, calculate the value of x. [**3 marks**]

Answer: $\frac{\phi 1}{\phi 1+\phi 2+\phi 3+\phi 4} = 20\%$ [1 mark]

$\phi 1 + \phi 2 + \phi 3 + \phi 4 = 15$ [1 mark]

$x = \phi 4 = 3$ [1 mark]

(ii) Discuss the advantages of PoS over PoW. [**2 marks**]

Answer: less energy consumption, less computing resource required.

(iii) Paxos is a fundamental consensus mechanism in distributed systems to reach an agreement by using a broadcast way. Explain the main process of Paxos, including the nodes and phases. [**5 marks**]

Answer: refer to the slides in lecture 16.

(iv) If there are 3 Byzantine attackers participating in a distributed consensus process, calculate the minimum number of **legitimate nodes** to achieve

Byzantine attack tolerance (**derivations** should be provided).

[**3 marks**]

Answer: the total number of nodes N participated in this consensus should satisfy

$N \geq 3 * 3 + 1 = 10$ [2 marks]

Hence, the minimum number of legitimate nodes should be 10-3=**7** [1 mark].

(v) List the three roles that the nodes can take in the RAFT consensus mechanism and indicate if the RAFT can resist Byzantine attacks/failures. [**4 marks**]

Answer: Leader [1 mark], Follower [1 mark] and Candidate [1 mark]. RAFT **cannot** resist Byzantine attacks/failures. [1 mark]

(c) Applying blockchain to wireless cognitive radio is promising to establish a trusted spectrum sharing scheme.

(i) List the **any two** benefits of avoiding user access collisions happening in a wireless communication network. [**2 marks**]

Answer: **Accept any three of the below, and 1 mark each**

Improve system throughout

Improve spectrum utilization

Reduce latency

Reduce energy consumption

Improve the connectivity of the system

(ii) Explain licensed spectrum and unlicensed spectrum in a wireless radio system. [**2 marks**]

Answer: licensed spectrum can only be used by licensed users [1 mark], unlicensed spectrum can be used by everyone in the system [1 mark].

(iii) List **any two** challenges of using blockchain technology into cognitive radio networks. [**2 marks**]

Answer: Accept any two of the below, and 1 mark of each.

High communication overhead

High memory overhead

High computing resource consumed

How nodes join and leave the blockchain network?

The ownership of the ledger.

(iv) List **any other two** potential blockchain-enabled applications. [**2 marks**]

Answer: any distributed systems requiring trusted data exchange should be accepted, such as smart grid, autonomous driving, cryptocurrency, food supply chain system, etc.