Do not award half marks.
In all cases give credit for appropriate alternative answers.

Question 1 (Compulsory)

(a) Computer equipments are always surrounded by many other electronic and radiation generating devices which can be potential threats and below are some of them. Give the long form of the acronym pertaining to the above context. [3]

(i) ESD
(ii) EMI
(iii) RFI

(i) ESD : Electrostatic Discharge
(ii) EMI : Electromagnetic Interference
(iii) RFI : Radio Frequency Interference

Guide : 1 mark each, overlook minor spelling error.]

(b) Computer Security is concern with threats to computer system. List the three area of threats in the context of ***computer security*** and give a clear distinct example of each in relation to ***Network.*** [6]

- **confidentiality threat, [1]**
  masquerading as the recipient and view the message. [1]

- **integrity threat, [1]**
  a hacker accessing the bank computer system compromising the integrity of the record [1]

- **availability threat. [1]**
  Spamming by either or both authorised or unauthorised causing the server to crash [1]

Guide: 1 mark each for each threat given and 1 mark each for an example.

(c) An **attack** can be as simply as spilling coffee on a keyboard, threat is when coffee can spilled onto the keyboard at any time whereas vulnerability is the ease of bring that cup of coffee. For the scenerios below state the form of ***attack*** that can happen and the ***counter-measure*** you provide for each. Do not repeat the answers.

(i) a disgruntled programmer [2]

(ii) using file sharing software in the office. [2]

(i) a disgruntled programmer,

- **Planting malicious computer program e.g logic bomb to disrupt the computer operations.**
- **Restrict the access to computer operations through access control**

Guide: 1 mark each accept other answers and the appropriate counter measures].

(ii) using file sharing software in the office,

- **Stealing computer resources e.g. computer data**
- **Forbid the use of such software in the office.**

Guide [1 mark each and accept other answers and the appropriate counter measures].

(d) Some attack cannot be prevented like natural disaster and in order to continue computer operation again a form of security measure used are cold site, warm site and hot sites.

(i) Differentiate the types of sites and [3]

(ii) Discuss the effectiveness of each site for a ***major disaster*** that is ***unpredictable***. Rank them as least, medium or highly effective and ***justify*** your answer. [3]

- **Cold site cannot guarantee server uptime, little or no fault tolerance component and the cheapest of the three. [1]**

  - **Least effective, eventhough it is low in cost because it takes longest to return to normal operations. [1]**

- **Warm site (nearline site) some duplication of components and network and data are available greater than 85% of the time and medium in terms of cost. [1]**

  - **High effective, since it is medium in cost and the uptime may be tolerable since it is a major disaster. [1]**

- **Hot site, the mot expensive as it is strictly fault-tolerant with 100% redundancy. The most expensive of the three in terms of cost. [1]**

  - **Medium, as the cost may be too prohibitive to justify a full hot site. Moreover it depends on the scale of business and the surrounding area may be effected therefore pointless to have a hot site. [1]**

Guide: 2 mark each, justification must be provided for that 1 mark.

(e) The RSA encryption method is one of the most difficult to decrypt as it uses large primes numbers.

(i) What is full name of RSA? [1]

Ronald Rivest, Adi Shamir and Len Adelman
Guide: 1 mark.

(ii) Encrypt the plaintext P = 2 using the RSA method. Assume a small prime numbers in this case used p = 3, q=5 as the prime numbers [3]

Steps:

1. n= 3x5 = 15
2. m=(3-1)(5-1)=8
3. chose e any number which has no common factor with m (8), let e = 5
4. select D such that De differs from 1 by multiple of m
De = [f x m] +1 { f is an integer }
Dx5 =[f x8] +1 { select f as 3 }
Use D =5
5. make e and n public and keep p, q, D and m secret.

RSA encrypt;
$C = P^e \bmod (n)$
$C = 2^5 \bmod (15)$
$= 32 \bmod (15)$
$= 2$

Guide: 1 mark for the steps or working, 1 mark for substitution in the formula and 1 mark for the final answer.

(f) Biometric methods of getting access to computer systems are getting common.

(i) Define what biometrics are. [2]

(ii) It is fallacy that biometric methods can be overcome, discuss whether an intruder can circumvent a fingerprint recognition device by making an impression of the thumb print to gain entry into an installation. [2]

(i) What is Biometric?

- **The use of characteristics(physiological, behaviourial and morphological) that can be examined and quantified to provide positive personal identification.**

(ii) Normally no, depending on the sensitivity of the installation. Thumb print alone could allow one to access a low security area but in addition to thumb print other verification technique may be used [1]. The impression made must be of high quality [1].

Guide: 2 mark for discussion with reasons given.

(g) Explain Secure Socket layer (SSL) in relation to network. [3]

- **a protocol layer in between the session and transport layer for added protection [1]**
- **which allows applications to exchange data over public network, [1]**
- **it is important for secure electronic transaction over the web. [1]**

Guide: 1 mark each accept other relevant answers.

Question 2

(a) What is the purpose of a digital certificate, and of what does it consist? [2]

- **purpose is to verify the authenticity of an individual or a party**
- **digital certificate consist of three parts i) a public key, ii) a certificate to identify the individual and iii) a digital signature to verify the authenticity of the holder.**

Guide: 1 mark each; accept other relevant description

(b) There are some similarities between digital signature and handwritten ones. Identify and briefly and describe *the five properties* pertaining to handwritten signature that are imitated by a digital signatures. [5]

- **signed documents is not alterable**
  the signature is a function of the document and content cannot be changed.t

- **signature is unforgettable**
  the person only knows how the signature is to written and remembers each time.

- **signature is authentic**
  recipient do not need the signer to verify and recognise the signature as genuine

- **signature cannot be repudiated**
  the signer cannot deny its signature

- **signature is not reusable**
  signature cannot be transferred from one document to another.

Guide: 1 mark for each identification and description following it.

(c) Explain what is meant by *timestamping* a digitally signed document. What problem does this technique solve? [2]

***Timestamping* involves appending the date and time to the document before signing it [1]. This foils a *resent message* attack [1], as it becomes obvious that a message has been copied.**

(d) Explain what is meant by signing a *one-way hash* of a document rather than the document itself. Which of the properties from part (b) fails to hold if the hash is not one-way? [2]

A predetermined hash function is applied to the document, and the resulting hash value signed instead of the document itself [1]. It is important that the hash is one way: if it is feasible to construct a document with a given hash, then the signature can be reused [1]. [One could argue that this is a matter of reusing the signature, or of altering the document, or of allowing the purported signer to repudiate the signature; the mark should be awarded for any one of these answers.]

(e) Suppose a given document requires the signatures of two people rather than one. Explain *two* different approaches by which this may be achieved, and identify one disadvantage of each approach. [4]

In the parallel approach, two separate copies of the document are made, one to be signed by each party [1]; this has the disadvantage that the resulting signed data is twice as long as it would otherwise have been [1]. In the serial approach, a single copy of the document is signed first by one party and then the other [1]; this has the disadvantage that the first party's signature cannot be verified without first verifying the second party's [1].

Question 3

(a) If the ciphertext below uses the monoalphabetic substitution cipher Ci=Pi + 3 (Caesar Cipher), what is the *plaintext*? Where Ci is ciphertext and Pi is plaintext. [2]

Cipher text: ndvlvnl phwkrg

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

ndvlvnl **phwkrg**
KASISKI ***METHOD***
[1] **[1]**

[1 mark for each term]

(b) Assume that another variation uses a **key** "VIRUS" what is the plaintext for the ciphertext below. [2]

Cipher text: hsnfgs csgghvj

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
v	i	r	u	s	a	b	c	d	e	f	g	h	j	k	l	m	n	o	p	q	t	w	x	y	z

hsnfgs **csgghvj**
MERKLE **HELLMAN**
[1] **[1]**

Guide: 1 mark for each term]

(c) How do polyalphabetic substitution cipher technique differ from monoalphabetic substitution ciphering technique? What advantage does a polyalphabetic technique have over a monoalphabetic one, and why? [3]

- **Polyalphabetic use two or more substitution / replacement for the same alphabet depending on its position in the message e.g. whether the position is odd or even position. [1]**
- **This makes it more secure [1], by smoothing out the frequency distribution [1].**

(d) Another type of encryption technique is the *transposition* ciphering method.

(i) Explain how transposition enciphering and deciphering are done. [2]

Enciphering a message involves writing it in rows of a fixed length but reading it in columns [1]; deciphering is the same process, but the correct row length must be determined somehow [1].

(ii) Is this a stream or a block cipher method? What consequences does that difference have for efficiency? [2]

It's a block method [1], so less efficient in time and space because a whole block must be read before any output can be written [1].

(iii) What is the other main difference between this method and a method like the Caesar cipher? [1]

It permutes letters rather than substituting them. [1]

(iv) The cipher text below has undergone columnar transposition once; find the plaintext. [3]

apsor otsty tefoe osbgt fcgte aheur ebref
ramrd afepc olmoc hakeo rrine sutyc nnsn#

Table:

a	**s**	**e**	**c**	**u**	**r**	**e**	**c**	**r**	**y**
p	**t**	**o**	**g**	**r**	**a**	**p**	**h**	**l**	**c**
s	**y**	**s**	**t**	**e**	**m**	**c**	**a**	**n**	**n**
o	**t**	**b**	**e**	**b**	**r**	**o**	**k**	**e**	**n**
r	**e**	**g**	**a**	**r**	**d**	**l**	**e**	**s**	**s**
o	**f**	**t**	**h**	**e**	**a**	**m**	**o**	**u**	**n**
t	**o**	**f**	**e**	**f**	**f**	**o**	**r**	**t**	**#**

Plaintext:

"a secure cryptographic system cannot be broken regardless of the amount of effort# "

1 mark for having the right approach (laying out in a tabular form); 1 mark for guessing the table size; 1 mark for the correct plaintext.

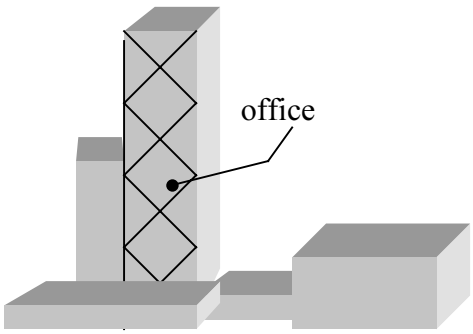
Question 4

A company XYZ International is a stock exchange company and have many branches overseas. The company deals in trading of shares and communicates all its transactions electronically through email, telephones and other methods.

The company operates 24 hrs a day and throughout the whole year.

The brief specification of the company are given below

Location: The office is in a 25th storey of 50 storey building occupying the whole floor.
Work force: 100 employees total
Hardware: associated mixed of computers about 100 and peripherals
Software: customised and off-the-shelf software.



Site Layout

(a) There are many risks and threats associated with the above company because of the many diverse mixed of components. One potential threat is the electrical power problem. Distinguish the following terms in relation to power supply. [3]

(i) Sag

(ii) Brownout

(iii) Blackout

(i) Sag
An <u>inverted spike</u> when power drops below the normal and rise back to the normal in a about a second e.g. light flicker or even a reboot.

(ii) Brownout
An <u>inverted surge</u> when power drops and return to the normal after a few seconds e.g. the light dims and return to normal.

(iii) Blackout
<u>Total lost</u> of power for several seconds , minutes or hours.

Guide: 1 mark each and answers must clearly distinguish between them. Key words are important but students can use their own words. A clear diagram to illustrate is also awarded 1 mark in lieu of explanation.

(b) List the issues that should be addressed by a security plan to protect the above company. [3]

- **Policy**
- **Current state**
- **Recommendations and requirements**
- **Time frame / time table**
- **Continuing attention**

Guide: Give the full 3 marks if the candidates gave as above deduct 1 mark for each mistake. If candidates gave their own answers then their answers must correspond with the answers above.

(c) (i) Assume the company is located in the Earthquake prone area, give **one** collateral threats that might result. [1]

Collateral threat
- **Fire, power outages building collapse etc. [1]**

Guide: 1 mark

(ii) Give the **two** objective of good Design a Disaster Recovery Plan. [2]

Two objectives
- **To minimise impact of a disaster on the ability to recover and continue**
- **Speedy and accurate recovery to normal operations**

Guide: 2 marks for the above two and other relevant answers acceptable.

(iii) Hence design your Disaster Recovery Plan change by giving the three steps in which you would go about doing it. [3]

- **Step 1**
  Cost benefit Analysis; determine the value of each resources and compare with the cost of protecting the resource.

- **Step 2**
  Decide which activities and resources are vital to the operations

- **Step3**
  Protecting the most vulnerable resources and those that are vital to the operations

Guide: 3 marks for the above and other relevant answers acceptable.

(iv) Assume an earthquake has occurs give the six steps in which you would go through to restore normal operations. [3]

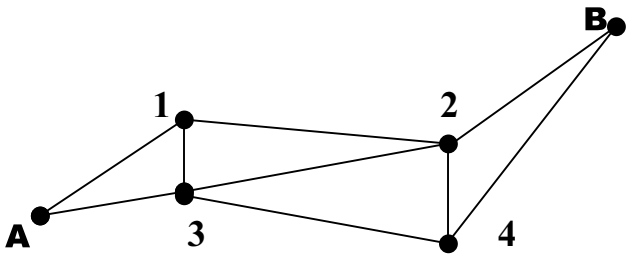
- **Securing the sites. Restoring records and overseeing salvage work.**
- **Communication and information, including notifiying the public and heading of rumours.**
- **Negotiating with the insurance carriers**
- **Locating a new facility**
- **Acquiring new equipment etc**
- **Restoring normal operations**

Guide: 3 marks for the above and other relevant answers acceptable.

Question 5

Networks are getting more and more important as individual and companies can easily make connections into existing ones either for personal use or for business activities.

The design and construction of a network can be complex as it involves computer hardware, communication hardware, software(s) and communication media.



Network

(a) List four *different types* of Network Access Control that can be implemented at point A. [4]

- **Port control**
- **Automatic call-back**
- **Differential access right**
- **Node authentication**

Guide: 1 mark for each listing of network access control, accept other relevant answers.

(b) Describe Link Encryption and End- to-End Encryption with respect to point A and point B in the network. [4]

- **Link encryption provides encryption between two computers through a line (normally a secure leased line) between two parties that need frequent secure communications for example between point A and point B. [1]**
- **End-to-End Encryption applied on the user end though software and is more flexible compared to hardware link encryption for point A and B [1]**
- **The intermediate nodes 1,2,3 and 4 normally would have the same encryption method throughout the network. [1]**
- **Mixing of the link Encryption and End –to-End encryption may result in the flaw of the network and subject to exploitation. [1]**

Guide: 1 mark each and if student gave the description for each type only maximum is 2 marks accept other relevant answersbv. This is a simple application question on Link and End-to-End encryption and students must refer to the network diagram.

(c) Explain what a firewall is, and how it can be used to prevent unauthorised access. Why would a firewall not be effective in preventing a virus attack in the network at point A, and what alternative technique might be more effective? [4]

- **A "device" (hardware/software) that controls traffic between two networks to monitor the content of the message to ensure they follow proper protocol. [1]**
- **Illegal traffic can be filtered before it enters the point A yet allowing organisation to do business over the network and act as a corporate ambassador and thus protect sensitive and propriety data [1]**
- **Virus can still come as an attachment to legal traffic and once entered can be activated. [1]**
- **Therefore virus scanning software and firewall are normally treated separately each with a different and distinct function. [1]**

(d) Discuss whether the network at point A is still vulnerable to attacks after considering the implementation of *Network Access Controls*, *Link and End-to-End encryption* and *firewall* (with any additional support as answered above) give **three good distinct** reasons to support **why no!** [3]

- **Password spoofing at any node e.g B, allow one to by-pass network access control and enter into point A.**
- **Network is still subject to natural disaster or spamming which result in the Distributed Denial of Access attack at A.**
- **New viruses in which the virus scanning software may not be effective. Need to update the virus scanning software every now and then by the network administrator.**
- **Other relevant points**

Guide: 1 mark each for good clear reasons.

- END OF PAPER -