Show your working in all calculations.

1. Alice and Bob communicate using a public key infrastructure (**PKI**).

   a) Alice wants to send a short private message to Bob. Alice encrypts the message to Bob using Bob's **public key**.
      i. Which goal of a secure system does this achieve?
      ii. What action is taken by Bob on receipt of the message in order to read it?

      (2 marks)

   b) Why does Alice not encrypt the message using:
      i. Bob's private key?
      ii. Her own public key?
      iii. Her own private key?

      (3 marks)

   c) Alice applies a **cryptographic hash function** to the message. She sends the resulting checksum to Bob along with the encrypted message and tells him which cryptographic hash function she used.
      i. Which goal of a secure system does this help achieve?
      ii. What action is taken by Bob in order to verify that this goal has been achieved?

      (2 marks)

   d) Alice does not encrypt the checksum. Why not?

      (1 mark)

   e) Bob's public key is contained within an **X.509 digital certificate** issued by a Certification Authority (**CA**) that Alice trusts. Give an example of two checks Alice should carry out using information in the certificate to assure herself that that it is safe to trust Bob's public key.

      (2 marks)

   f) The plaintext of Bob's X.509 certificate has a cryptographic checksum generated and it, and the certificate, are signed by the issuing CA.
      i. What does this mean?
      ii Why do these two actions increase Alice's confidence in Bob?

      (2 marks)

   g) One month after the successful transmission of Alice's message to Bob, Alice and Bob have an argument and Alice denies ever having sent Bob the message. The next time Alice tries to send Bob a message, Bob insists that Alice carries out an additional step to prevent her repudiating the message. What is this extra step and what is it called?

      (2 marks)

   h) One year before his digital certificate is due to expire, Bob accidentally leaves a pen drive containing his private key on the Bus. What actions should the CA take?

      (1 marks)

   i) With the help of a diagram, explain what you understand by the terms **chain of trust**, **closed domain PKI** and ***open PKI***. Use the diagram to illustrate how two business organisations might use both types of PKI to collaborate on a project.

      (10 marks)

2. In a **general election** in the UK, voters cast their vote for the candidate whom they wish to represent their constituency in parliament. Only registered voters may vote. A voter may cast one vote only. The number of votes cast for each candidate must remain secret until after the close of voting. No person or organization should be able to induce a voter to vote a particular way using bribery or intimidation. It should not be possible to connect a vote to the person who cast the vote.

   A constituency will have a number of polling stations, which are physical locations where voters go to vote. No photography is permitted inside a polling station. On election day, voters go to the polling station at which they are registered, which is staffed by election officials. A voter queues to have their identity checked by an official against the electoral roll; a list of voters registered at that polling station. When their identity has been checked, a tick is placed against the voter's entry in the electoral roll and the voter is given a voting slip containing the names of the candidates. The voter takes the slip to a private booth and puts a cross next to the name of the candidate for whom they wish to cast their vote. They must then post the voting slip through a slot in a ballot box. When the polls close, the polling station's ballot box is sealed and taken to a counting station staffed by more election officials. At the counting station, each polling station's ballot box is unsealed and the voting slips taken out. From the voting slips, the number of votes cast for each candidate is counted. When all the votes have been counted, the number of votes cast for each candidate is announced and the winning candidate is declared. (NB. we have ignored postal votes in this description)

   a) From the above description of a general election identify:

      i. What are the **assets** that need to be protected?
      ii. What are the **vulnerabilities**?
      iii. What are the **threats**?
      iv. What are the **controls** used?

      (8 marks)

   b) Now consider replacing the above voting system with an **e-voting** system in which, instead of requiring voters to attend a polling station and vote on a paper voting slip, a voter can cast their vote from a browser running on any device with an Internet connection.

      i. Are the assets, vulnerabilities and threats the same? If not, how are they different?

      (6 marks)

      ii. Identify any new controls needed to counter the threats and assess how effective they are likely to be.

      (4 marks)

   c) There is an on-going debate about whether e-voting software should be **proprietary** to the developer or **open source**. From a security viewpoint, summarise what you believe to be the key arguments for and against both of these positions.

      (2 marks)

   d) To maintain trust in a voting system, there needs to be a means to verify the integrity of the votes. Ideally, it should be possible to check that a voter's vote is added to the tally of votes for their chosen candidate. However, if designed poorly, this check for integrity may conflict with confidentiality. Explain why.

      (5 marks)

3. a) Outline the difference between **cryptography** and **cryptanalysis**.

(4 marks)

b) i. Explain the difference between **substitution** and **transposition** cyphers;
ii. Give an example of a substitution cypher;
iii. Give an example a cypher that combines both substitution and transposition.

(4 marks)

c) The following cyphertext has been encrypted using the **Vigenère cypher** with the key "LUKE".

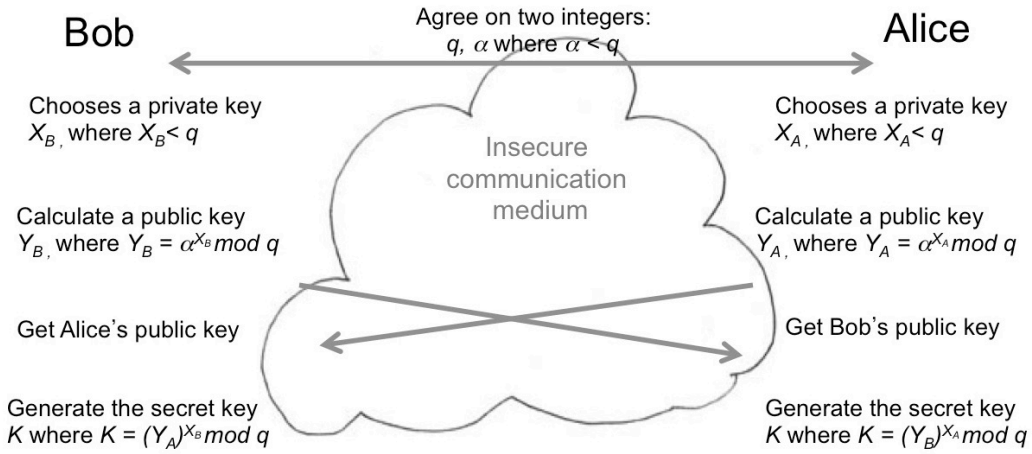
"EBOPLMDNPXS"

The alphabet used by the cypher is the set of 26 letters 'A' to 'Z', which can be mapped onto ordinal numbers 0 to 25 respectively.

Find the plaintext. Be sure to show all your working including the decryption formula.

(4 marks)

d) The figure below illustrates (in simplified form) the **Diffie-Hellman** algorithm.



What long-standing problem with crypto systems was Diffie-Hellman developed to solve?

(2 marks)

e) Which innovation did Diffie-Hellman introduce in order to solve (d)?

(2 marks)

f) Diffie-Hellman is vulnerable to **man-in-the-middle** attacks. Redraw the figure to illustrate how a man-in-the-middle could dupe Bob and Alice to reveal their secret key. To save time, you do not need to reproduce all the detail in the figure above but you do need to show the steps taken by the man-in-the-middle and their interactions with Bob and Alice.

(6 marks)

g) The most efficient **integer factorization** algorithm currently known, that can be implemented to run on a conventional computer, works in sub-exponential time. Thus, the calculation of the prime factors of a large integer is currently impractical. However, when powerful quantum computers become a reality, they will be able to run algorithms capable

of finding integers' prime factors in polynomial time. What do you think the effect of this will be on information security as currently used in (e.g.) banking, government communications, social networking and so on?

(3 marks)

4. a) What is the principal difference between a computer **virus** and a computer **worm**? Give an example of each.

(4 marks)

b) Anti-virus programs scan computer disks looking for the signatures of known viruses.

i. Explain what this means.

(2 marks)

ii. Explain how a **polymorphic** virus would make is harder to achieve (3 marks).

(3 marks)

c) The following pseudo-code specifies a program to prompt a user for their password and log them in if the password they enter is correct. Password correctness is evaluated by hashing it and comparing the resultant checksum against the checksum of the correct password (`PWDCHKSUM`).

```
String: pwd /* a string */
Boolean: isValid

isValid = FALSE

while NOT isValid do
     get pwd
     if hash(pwd) == PWDCHKSUM
         isValid = TRUE

log user in
/* end of program */
```

A programmer implements the pseudo code in C. They declare a 16-`char` array to store the string `pwd`; and an `int` to represent `isValid`. `isValid` is initialized to `0` and assigned the value 1 if `pwd` contains the valid password.

When the compiled program is loaded, the run-time system allocates `pwd` a contiguous sequence of 16 bytes at addresses `0000` to `000F` (Hex), and allocates `isValid` the 2 bytes at addresses `0010` and `0011`.

i. Explain the key vulnerability of this implementation of the program.

(4 marks)

ii. What should the programmer do to control the vulnerability?

(2 marks)

d) Malicious code may be both data and instructions. Explain why this is true and illustrate your explanation with reference to how a **buffer overflow** in a subroutine may be exploited to both install code and execute it on exiting the subroutine.

(10 marks)

5. a) The diagram below shows the **access control matrix** for several components of an IT system:

	File-1	File-2	File-3	File-4
User-1	r	orw	orw	–
User-2	–	–	–	–
User-3	–	r	r	orwx
User-4	orw	r	r	rx

Outline how examining the access control matrix of an information system can help identify potential **covert channels**.

i. With reference to the access control matrix, identify two potential covert channels for this information.

(2 marks)

ii. For both of these potential covert channels, explain what confidential information may be disclosed, who is the sender of this information and who is the attacker.

(4 marks)

b) Consider the table of subjects, objects and integrity levels below.

Integrity level	Subject	Object
3 (highest)	Alice	Personnel files
2	Bob	System log files
1 (lowest)	Dan	Blog files

Alice, Bob and Dan work for a company whose information systems adopt the **Biba security model**.

i. Which security goal does the Biba model prioritise?

(1 mark)

ii. Dan and Bob have a fierce argument about office stationery and afterwards, Dan decides to try to damage Bob's career. The worst he is able to do is make a false statement about the validity of Bob's qualifications in his blog. With reference to Alice, Bob and Dan explain the value of the Biba model's principles of **no read down** and **no write up**.

(4 marks)

c) Suppose that a 20-server web site is subjected to a SYN **distributed denial of service (DDOS) attack** carried out by a hacker who uses 4 zombie PCs to send 25-byte SYN packets to the attacked network.

Suppose that each web-site server maintains a table for 256 TCP connection requests, and that in response to a fake SYN, these servers send a SYN-ACK packet four times, at $t = 32$s time intervals, then purge the request from the table.

i. What is the minimum per-zombie rate of SYN packets that should raise the suspicion of an Internet Service Provider (ISP) so that the participation of a PC in the attack is detected immediately by the ISP?

(8 marks)

ii. How much bandwidth does each zombie use to perpetrate this attack?

(4 marks)

iii. Is it possible for an ISP to detect this DDOS attack by monitoring sudden increases in the bandwidth used by individual computers? Explain your reason.

(2 marks)

END OF EXAMINATION PAPER