University of KwaZulu-Natal | School of Engineering

Security and Encryption | ENEL4SE

10 June 2026 | Lecturer: Jonathan Parker

Total marks: 120 marks | Time: 120 minutes

Main Examination

Instructions:

You should focus on the questions you feel you can do the best in. Please pay careful attention to the mark allocation. Please answer Question 1 on the first page and answer Question 2 underneath it. Please answer every other question on a new page.

A datasheet is given on the second page of this question paper, which you may find useful.

This is a closed book exam.

Datasheet

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

P10 (permutate)

```
Input : 1 2 3 4 5 6 7 8 9 10
Output: 3 5 2 7 4 10 1 9 8 6
```

P8 (select and permutate)

```
Input : 1 2 3 4 5 6 7 8 9 10
Output: 6 3 7 4 8 5 10 9
```

P4 (permutate)

```
Input : 1 2 3 4
Output: 2 4 3 1
```

- EP (expand and permutate)

```
Input : 1 2 3 4
Output: 4 1 2 3 2 3 4 1
```

- IP (initial permutation)

```
Input : 1 2 3 4 5 6 7 8
Output: 2 6 3 1 4 8 5 7
```

- IP^{-1} (inverse of IP)
- LS-1 (left shift 1 position)
- LS-2 (left shift 2 positions)

$$S0 = \begin{bmatrix} 01 & 00 & 11 & 10 \\ 11 & 10 & 01 & 00 \\ 00 & 10 & 01 & 11 \\ 11 & 01 & 11 & 10 \end{bmatrix}$$

$$S1 = \begin{bmatrix} 00 & 01 & 10 & 11 \\ 10 & 00 & 01 & 11 \\ 11 & 00 & 01 & 00 \\ 10 & 01 & 00 & 11 \end{bmatrix}$$

Question 1 (20 marks, 2 marks for each MCQ)

Write the question number and the letter of your chosen answer in the answer book.

1.1. Which of the following statements is true?
A) It is assumed that an attacker will recognise the plaintext message once they have guessed the correct key.
B) Kerckhoff's principle states that security goals are always Confidentiality, Integrity and Availability.
C) Brute force approaches scale logarithmically with the key length.
D) Once an attacker knows a single pair of (plaintext, ciphertext), it is simple to calculate the key.

1.2. Which statement about frequency analysis attacks is true?
A) They are not effective against transposition ciphers.
B) They work better if the plaintext and ciphertext distributions are the same or at least similar.
C) They are only possible when there are only 26 choices for the key.
D) They are not effective against ciphers working on digital information.

1.3. Which statement about modes of operation for symmetric key encryption are correct?
A) With Cipherblock Chaining, if the Initilisation Vector used is incorrect, all the remaining decryptions will be incorrect.
B) With Output Feedback Chaining, identical blocks in the plaintext will be identical in the ciphertext.
C) Decryption is parallelisable for both Electronic Codebook and Cipherblock Chaining.
D) With Electronic Codebook, before the plaintext is encrypted, the plaintext must first be XORed with the ciphertext from the previous stage.

1.4. Which is a property of a cryptographic hash function?
A) Second pre-image resistance means it is computationally infeasible to find any two inputs that produce the same hash value.
B) A hash function is invertible if the trapdoor is known.
C) There is a linear relationship between the lengths of hash function inputs and outputs.
D) Given a hash value, it is computationally infeasible to find the input that produced it.

1.5. Which statement is true?
A) Salting passwords means that identical passwords will generate different deterministic hash values.
B) All authentication techniques must allow for a margin of error, to tolerate sensor noise.
C) To prevent replay attacks, transmitted passwords should be hashed.
D) Calculating the salt values is computationally expensive for the attacker.

1.6. In the context of Attribute Based Access Control, what is a policy?
A) A policy is a set of classification levels used to determine whether a subject can access an object.
B) A policy is a set of objects that a particular subject has rights over.
C) A policy is a set of sanctions (punishments) to be applied to users for accessing resources that they are not authorised to.
D) A policy is a set of rules that consider the subject, object, environment and intended action before determining whether the action is allowed.

1.7. Why might a virus compress the program it has infected?
A) To leave the file size of the infected program unaltered.
B) To alter the functionality of the program, thereby affecting integrity.
C) To slow the execution of the program, thereby reducing availability.
D) To make sure the uninfected program has the same hash as the infected program.

1.8. Which statement is true?
A) A botnet is more effective than a direct DoS attack because the command and control server can handle far more attack traffic.
B) Antispoofing filters prevent DDoS attacks by blocking all traffic from unauthorised source addresses
C) Amplification attacks are only possible if targets reply with larger packets in response to smaller packets.

D) Reducing the capacity of the command and control server's connection does not reduce the effectiveness of a DDoS attack.

1.9. Why are SQL commands vulnerable to being attacked?
A) SQL syntax does not require authorisation before data is access or modified.
B) SQL syntax allows user inputs to be mixed with SQL code.
C) SQL commands must be transmitted in plaintext over network connections.
D) SQL syntax allows names of tables and fields to be sanitised.

1.10. What role do certificates play in establishing encrypted channels?
A) They allow the ownership of a public key to be verified by a third party.
B) They provide sender authentication for all packets.
C) They allow a Certification Authority to check for malicious packets to prevent attacks.
D) They generate public and private keys on behalf of clients and servers requesting encrypted channels.

Question 2 (14 marks)

2.1. (2 marks) State Kerckhoff's principle and explain what it means in practice.
2.2. (4 marks) What is the relationship between a one-time pad and the Vigenère cipher. Explain why a one-time pad is unbreakable but impractical.
2.3. (8 marks) You receive "XCDMEOFXBF" as a ciphertext, and you know the key is "BOMB". You don't know whether it was encrypted using a Vigenère cipher or a Playfair cipher. Decrypt using both ciphers. Determine which cipher (if any) was used and determine the plaintext. **Show all working.**

Question 3 (18 marks)

3.1. (8 marks) Given an input of $X = \{1, 0, 0, 1, 1, 1, 0, 0\}$ and key $K = \{1, 1, 1, 0, 0, 1, 0, 1, 1, 0\}$, and round keys $K_1 = \{1, 0, 1, 0, 1, 1, 0, 1\}$ and $K_2 = \{1, 1, 1, 0, 0, 1, 1, 1\}$ generate the output after one round of sDES (including the SWOP operation). Show all steps of working.
3.2. (10 marks) Assuming an encryption using a single DES stage is vulnerable, show that an encryption using two cascaded DES stages (ie Double DES) is also vulnerable. State the name for this attack.

Question 4 (8 marks)

Encrypt message $m = 5$ using an RSA encryption scheme $n = 46$, $e = 17$, $d = 13$. Without performing decryption, using the underlying prime numbers $p = 2$ and $q = 23$, show that e and d are multiplicative inverses.

Question 5 (17 marks)

Consider the following rules for forming passwords:

- Rule 1: A string of 5 lowercase characters (repetition is allowed), but all of the "i"'s might have been replaced by "1" and "o"'s might have been replaced by 0.
- Rule 2: A string of up to 4 lowercase characters and digits (repetition is not allowed), where the first character must be a digit.

5.1. (4 marks) How many passwords can be formed according to Rule 1?
5.2. (4 marks) How many passwords can be formed according to Rule 2?
5.3. (2 marks) What is the difference between identification and verification in the context of biometric authentication?

Consider the following MAC system:

Alice requires READ access to File Y to complete a new task.

Entity	Type	Classification	Category
Alice	Subject	Confidential	Finance
File X	Object	Top Secret	HR

File Y	Object	Top Secret	Finance
File Z	Object	Secret	Finance

5.4. (2 marks) Explain why Alice currently cannot read File Y.
5.5. (2 marks) State the minimum change to Alice's attributes that would grant her READ access to File Y.
5.6. (3 marks) What inadvertent READ access does Alice gain as a result of this change? For each file, justify your answer with reference to Alice's updated attributes.

Question 6 (10 marks)

A user receives a targeted email appearing to come from their bank, referencing their recent transactions by name. The email contains a link to a convincing login page. The user enters their credentials. Shortly after, the attacker uses those credentials to access the user's account.

6.1. (3 marks) What specific type of phishing attack is this and what distinguishes it from a standard phishing attack?
6.2. (2 mark) What category of payload does this attack deliver and what propagation mechanism was used?
6.3. (3 marks) A keylogger was also installed on the user's machine. Why might a keylogger be more effective than simply sniffing network traffic for capturing credentials?
6.4. (2 marks) Suggest one defence for the initial phishing attempt.

Question 7 (15 marks)

An attacker launches a ping flood attack against a target. Initially the attacker sends all packets from their own IP address. They then switch to using a different spoofed source address for every packet.

7.1. (2 marks) Why is the initial attack (no spoofing) problematic for the attacker themselves?
7.2. (2 marks) What specific problem does using a different spoofed address for every packet solve, compared to using a single fixed spoofed address?
7.3. (3 marks) An ISP blocks all ICMP traffic leaving its network. Is this an effective countermeasure? What is the drawback?

A router is configured to drop packets addressed to a broadcast address if they originate from outside the subnet.
7.4. (4 marks) Explain how a directed broadcast address amplification attack works
7.5. (4 marks) Why would the above countermeasure be effective against this amplification attack but would not be effective against a basic reflection attack.

Question 8 (10 marks)

A web application allows users to search for products. The following PHP code is used:

```
SELECT * FROM stock WHERE item = '$_GET["item"]'
```

The stock table contains the following data:

item	quantity
Pens	100
Paper	54
Pencils	19

8.1. (2 marks) What is a piggyback query in the context of SQL injection?
8.2. (2 marks) Explain the use of end-of-line comments in the context of SQL injection – what happens if it is not used?
8.3. (6 marks) Write a search input to delete the stock table. Show the resulting SQL command that is executed. State explicitly the assumptions that are made in forming this attack.

Question 9 (8 marks)

9.1. (2 marks) What is the difference between signature detection and anomaly detection in the context of intrusion detection systems?

9.2. (2 marks) What is the key disadvantage of signature detection that anomaly detection does not share?

9.3. (4 marks) Explain why threshold detection is considered too simple to be effective in practice and explain the key advantage of profile-based statistical anomaly detection over threshold detection?