

COMP3028 Computer Security 2025/26 – Coursework 1

Due on: 27th Feb 2026, 4pm

(Based on Crypto Lab of SEED Lab 2.0 – Secret-Key Encryption)

This coursework will contribute 10% towards the final marks. The actual duration of this task is 4 hours; however, the submission deadline will be by 4pm on 27th Feb 2026. This should cover the 25% extra time needed by students with learning disability, therefore there will be strictly NO EXTENSION granted under any circumstances.

The standard University penalty for late submission should be 5% per day, until the mark reaches zero. A deduction of 5% of the actual mark achieved shall be imposed upon expiry of the deadline, and an additional 5% per subsequent 24 - hour period (weekends and University closure days do not count as days where a 5% is to be imposed).

You need to submit a detailed report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits.

The report must be converted to PDF format and submitted through the submission link in Moodle.

Task 1: Frequency Analysis (20 marks)

Decipher the ciphertext given in MOODLE. The ciphertext was created using a substitution cipher. Explain how you discovered the encryption key. Write the encryption key in the following format in your report:

Plaintext	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
Ciphertext																										

Was your approach in discovering the encryption key be same as the one in lab exercise? Explain why.

Task 4: Padding (10 marks)

Use the three files provided in MOODLE, which contain 5 bytes, 10 bytes, and 16 bytes, respectively. Use ECB, CBC, CFB, and OFB modes to encrypt each file. Please report which modes have paddings and which ones do not. For those that do not need paddings, please explain why. (Instruction given in the lab manual will be useful)

Task 5: Error Propagation – Corrupted Cipher Text (20 marks)

Use the Task 5 plaintext provided in Moodle. Encrypt the file using AES-128 cipher in ECB, CBC, CFB, and OFB modes using the key and IV provided in Moodle. Corrupt a single bit (you choose your own bit) of the 55th byte in the encrypted file. As explained during the lab session, you can achieve this corruption using a hex editor (I used ghex during the lab demo, you may use whichever you feel comfortable using). Decrypt the corrupted ciphertext file using the same key and IV.

How much information can you recover by decrypting the corrupted file in each of the modes of operation? Please provide justification.