# **CMSE353 Security of Software Systems**

# Lab 2. DES in ECB Mode of Operation

October 28, 2023

Lab 2 aims supporting the Term project by getting understanding of DES in electronic-code book (ECB) mode of operation. In ECB mode of DES operation, any size plaintext message is split into 64-bit size blocks, and each plaintext block is encrypted independent from other ones (as pages in a book) producing respective 64-bit ciphertext block.

**Task**

1. Implement DES algorithm in ECB mode of operation as a network application with sender (encryptor) and receiver (decryptor) residing on two separate computers
2. Test it by checking correctness of the particular transformations used:
	1. Initial permutation
	2. Inverse of the initial permutation
	3. Expansion/permutation
	4. Round key generation
		1. Permuted choice 1
		2. Left circular shifts schedule
		3. Permuted choice 2
	5. XOR with round key
	6. S-boxes
	7. Permutation P after S-boxes
	8. XOR with left half
	9. Swap of the halves
3. Test correctness of the block cipher in ECB mode
4. Prepare and print a report on the work done. It shall have
	1. Cover page (University, Department, Program, Course, Lab, Subject, Team members, Lecturer, Lab Assistant, Year, Semester, City, Country)
	2. Outline
	3. Problem definition
	4. Work done. For each problem 1-4 considered, show your work done by explaining your code developed and presenting screenshots of the running in step mode of the debugger DES cipher with the tested variables watched.
	5. Conclusion
	6. References
	7. Appendix with source codes

Printed report (one per team) shall be handed to Lab Coordinator [**NADA IBRAHIM S. M. S. KOLLAH**](https://cmpe.emu.edu.tr/tr/hakkimizda/personel/personel-detayi?sid=268&n=nada-ibrahim-s-m-s-kollah)**, CMPE-135,** and Zip-file with all the materials related to the Lab (sources, executables, test examples, report) shall be uploaded to Teams assignment (to be defined later) by December 12, Tuesday, 2023, 10.30 (Group 1), and December 11, Monday, 2023, Monday, 8.30 (Group 2). Zip-file shall be named as follows: “CMSE353 Fall2023 DES Lab Stid1 Stid2 Stid3 Stid4.zip”, where Stid1-4 are the student IDs of the team members.

The report and application will be evaluated by Lab Assistants.

Grading policy: report – 40%, explanations – 60%