# **CMSE353 Security of Software Systems**

# Lab 3 Task. DES

December 18, 2020 - January, 6, 2021

Lab 3 aims getting understanding of DES.

**Task**

1. Implement DES algorithm as a software application
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. 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 the problems 1, 2 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
	8. Archived (rar, zip, etc.) with all the materials related to the Lab (sources, executables, test examples, report)

The report and application will be evaluated by Lab Assistants in the lab session, 12.30

Grading policy: report – 50%, explanations – 50%