CMSE353 Security of Software Systems

Lab 3 Task. DES

October 1, 2019

Lab 3 aims getting understanding of DES. It supports the Term project

Tasks

1. Implement DES algorithm as a software application
2. Test it by checking correctness of the particular transformations used:
    - 2.1. Initial permutation
    - 2.2. Inverse of the initial permutation
    - 2.3. Expansion/permutation
    - 2.4. Round key generation
        - 2.4.1. Permuted choice 1
        - 2.4.2. Left circular shifts schedule
        - 2.4.3. Permuted choice 2
    - 2.5. XOR with round key
    - 2.6. S-boxes
    - 2.7. Permutation P after S-boxes
    - 2.8. XOR with left half
    - 2.9. Swap of the halves
3. Prepare and print a report on the work done. It shall have

3.1. Cover page (University, Department, Program, Course, Lab, Subject, Team members, Lecturer, Lab Assistant, Year, Semester, City, Country)

3.2. Outline

3.3. Problem definition

3.4. 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.

3.5. Conclusion

3.6. References

3.7. Appendix with source codes

3.8. CD with all the materials related to the Lab (sources, executables, test examples, report)

The report and application will be evaluated by Lab Assistant Tansel Sarihan in the lab session, 16.30, Lab 134

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