HOMEWORK

COURSE NAME : CRYPTOGRAPHY AND COMPUTER SECURITY
COURSE CODE : CSE 470
COURSE HOURS AND CREDITS: (3+0=3)
DELIVERY DATE : 27.12.2024 17:30)

Programming project1: As you know, prime numbers have an important place in cryptography. In this homework, the large prime number test is a procedure that must be done in applications. In this assignment, prime number testing algorithms will be researched and explained in the report. Then, the design, coding and running of the program that produces comparative results for the same number by implementing the Miller-Rabin, Eratosthenes and Atkin algorithms in C/C++ or Python and selecting them from an interface will be provided.

ASCON GIFT-COFB

The source codes and compiled versions of the programs will be uploaded to Teams.

Research: • Explain the analysis and comparison of lightweight symmetric encryption algorithms and newly proposed algorithms. Also explain analysis of the finalist algorithm of Ascon in detailed. (BIL470-list-topic, For two cryptography algorithms mentioned in the given list). https://csrc.nist.gov/Projects/lightweight-cryptography/email-list and Lightweight Cryptography | CSRC (nist.gov) information from this link will be used

.

Programming project2: In this tool, which will be implemented in C/C++ or Python, encryption/ decryption, extraction, file integrity control methods will be implemented personally, and archive/API will not be used. Source codes of the implemented programs will be given with explanations;

a) Implementation of the two lightweight encryption algorithms examined and their use in encryption/decryption (with test data).
b) Perform the work in CBC and OFB modes using the implemented Symmetric encryption algorithm and prepare it for tests.
c) In order to understand whether any changes have been made to any document (.doc/.docx, .pdf, ppt, xls, etc.) and the identity of the person who made it, a tool that will extract it and encrypt it with a key known only to the person who made the transaction and add it to the end of the file (as in option b). use implementation as extract function)
d) To check whether the integrity of the file has changed, show sample tests by performing the verification tool that compares it with the first generated extract value by performing the operations in

.

Research: Post quantum cryptography: In future, quantum computing will reach sufficient computing power to break cryptographic algorithms. Therefore new quantum resistant cryptographic algorithms should be developed. In this work please explain all of proposed quantum resistant cryptographic algorithms. Also compare them in your report. Ref: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization information from this link will be used

The results of the work done on the homework problems will be uploaded to the course group in teams before the completion time in the form of a written report as .doc/docx.

Good luck.