Assignment 1 SPM 2022 (July-Nov)

Cryptography 101

Deadline: August 16th, 2022

Question 1) A cipher can be implemented in multiple ways depending on the underlying hardware. We have seen details about the different implementations of AES in class.
One such implementation is the AES T-Table Implementation.

This question is on a lightweight cipher called CLEFIA. The details about CLEFIA are present here along with a reference implementation.

1. The first part of the assignment is to implement a CLEFIA-128 (T-Table based) cipher (using C programming language).
2. Provide a write-up that includes the details of the cipher implementation and a Makefile.

Note: The code will be used in most of the upcoming assignments. Implementations available on google may not be a good choice. (**Marks : 50)**

Question 2) In class we saw an example of a timing side channel attack on a password checker where the password is provided by the user and the stored password is compared character by character. The password checker returns when it finds a mismatch between the two.

To prevent the attackers from obtaining the password in such a way, in practice, we compute the hash of the password provided by the user and the hash of the stored password.

Can you extract the stored password with this countermeasure in place?

Use **nc 10.21.235.179 5555** to access the binary for this question.

a) Submit the stored password. **(10 marks)**
b) Hash functions are subjected to collision attacks where multiple passwords end up having the same hash. Submit a set of 5 passwords which would also have the same hash as the stored password. **(10 marks)**
c) Submit a write up on your method used to extract the password. The write up should contain references like websites/tools used (if any) and the methods adopted should be explained in detail using code snippets. **(30 marks)**
