German University in Cairo
Faculty of MET (CSEN 1001 Computer and Network Security Course)
Dr. Amr El Mougy
Reham Ayman
Abdelrahman Osama

Hacking Assignment 2.4 : Hash-SHA and CFB-AES

Discussion 04/03/2020 **Task Grade** 5%

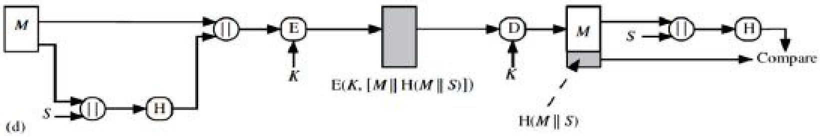
1 Introduction

In this task you're required to implement SHA Hashing and CFB encryption and decryption schemes using PyCrypto library here: `https://pypi.org/project/pycrypto/`

2 Details

You are given a starter code for this assignment containing the base implementation of the task in Python. You will find the starter code for this assignment uploaded on the MET website named **In-class 2.4 StarterCode.py**.

You are required to implement the Hashing using SHA256 and the encryption and decryption functions for CFB using AES according to the following figure:



You are given the values; **plain and key**. Use the IV generated for CFB as the S for the hashing. **The size of the hash is 64 bytes.**. In the encryption return (v||cipher) as you will use the same IV for decryption. In the decryption return the plain text and if it is corrupted or not.

3 Submission

You will be required to submit your source code file by maximum one week from the tutorial slot (e.g. if your tutorial slot is on Sunday, your deadline is the following Saturday at 23:59) . Upload the source code file to the MET website in the corespondent submission link for your tutorial group. The source code file should be named as $[ID]\_[TutoiralNumber]\_[Task\_Number]$ (e.g. $[37-1111]\_[T01]\_[Task2]$).

In case there was a problem in the submission through the MET website, then send an email to your TA with the title same as the name of the .py file.