PROJECT: Introduction to cybersecurity

Subject : Password Storage

The goal is to propose a solution for password storage.

The solution will use the MD5 hashing function.

PART 1 : Implementation MD5 (IETF RFC 1321).

PART 2 : Using the Implementation of MD5 you should propose a solution for password storage. This solution is defined without salt.

Different steps:

- Generation of 100 passwords of different size. Each password is associated to an identity (e.g. Id1, … id100)
- Compute the hash of the passwords and store the value associated to the identity.

PART 3 : Implement a solution with salt. In order to improve the security, we use the solution with salt.

This solution also use the MD5 implementation.

- Use the password generated at the question 2.
- Generated some random (“salt”) associated to each password and identity.
- Compute the hash of the password concatenate with the salt, for each identity, and store the value.

PART 4 : H-MAC are designed with cryptographic hashing function. They are used for the definition proptocls like SSL.

Implement an H-MAC using the MD5 function (reference for the H-MAC specifications IETF RFC 2104). In order to test your implementation you can use (IETF RFC 2202).

IFM, BI, IRV, IL: project part 1, 2, 3 and 4

ISCE :

- **Security of a PA8 project. A report is due.**
- **Part 1 of this project.**

Project to realise

- Written report : the report must be well written and structured.
- Clean Code-source

- the code must answer to the following requirements :

1. produces a clean and understandable display
2. easy to test with any input value for the message and the key
3. compilation with no warnings will be greatly appreciated
4. must be an original production - **ANY SIMILAR PROGRAMS will be awarded 0** regardless of their producer(s)

Project due date: 12/01/2018