**Class Activity: Database Hashing and Encryption**

**Introduction**

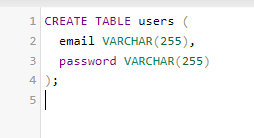
This report documents the steps and results of a class activity focused on database hashing and encryption. The objective was to create a secure database to store user credentials and card details, hash the passwords, and encrypt the card details. Additionally, we attempted to crack the hashed passwords using online tools.

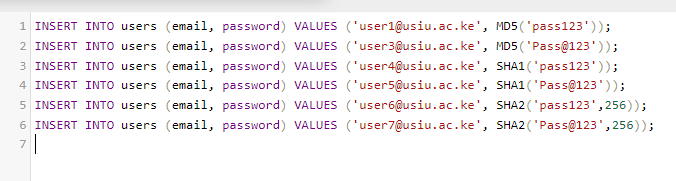
**Tools and Software**

* **XAMPP**: A local server environment used for testing and development.
* **phpMyAdmin**: A web-based database management tool for MySQL.
* **CrackStation**: An online hash cracking tool.

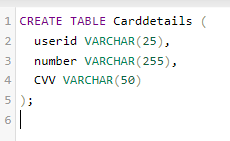
**We created 2 tables and inserted values into the tables**

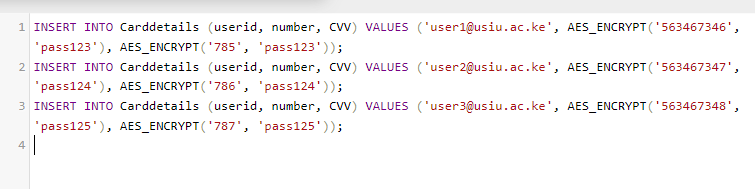
1. **User**



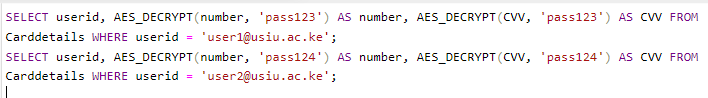


1. **Carddetails**



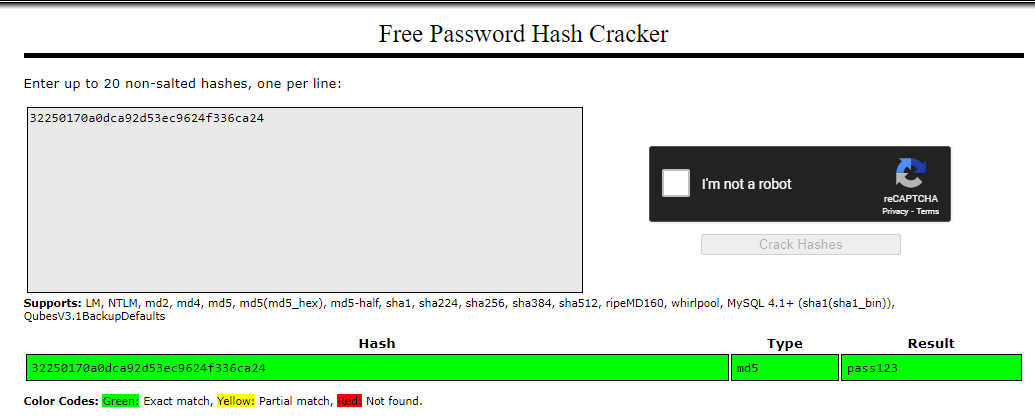


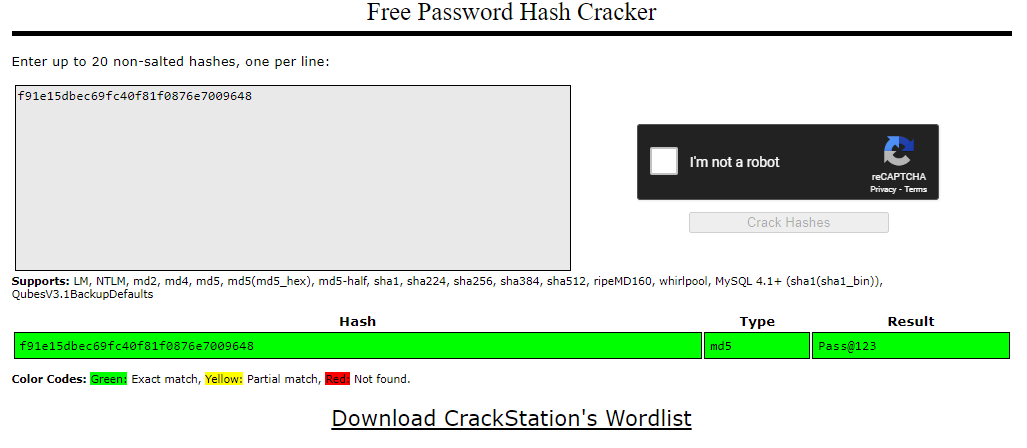
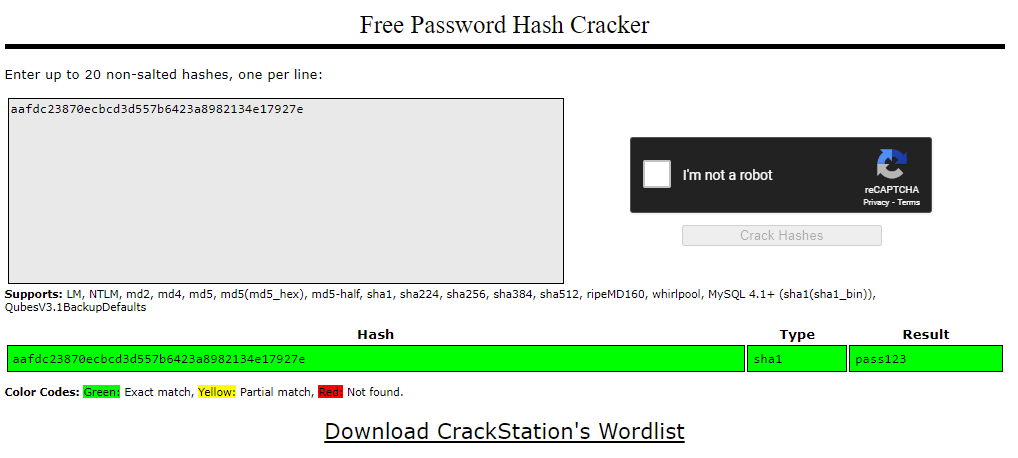
Retrieve and decrypt values from the Carddetails table:

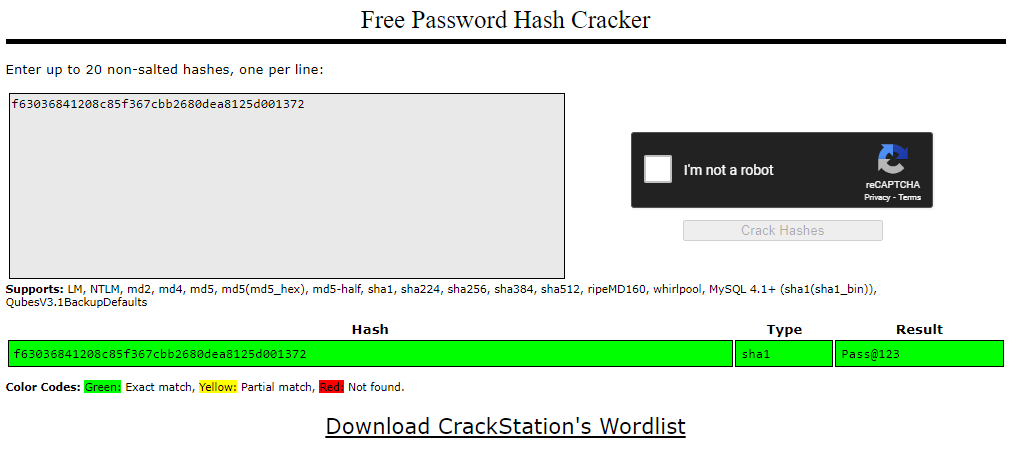


**Crack hash values**: Using CrackStation, the following passwords were successfully cracked as shown in the screenshots below

* 32250170a0dca92d53ec9624f336ca24 (MD5) -> pass123
* f91e15dbec69fc40f81f0876e7009648 (MD5) -> Pass@123
* aafdc23870ecbcd3d557b6423a8982134e17927e (SHA1) -> pass123
* f63036841208c85f367cbb2680dea8125d001372 (SHA1) -> Pass@123
* 9b8769a4a742959a2d0298c36fb70623f2dfacda8436237df08d8dfd5b37374c (SHA256) -> pass123
* b6bc7b58510319a151d168ba3d5aecb3ac0a9708d06dd930f37fbc89b6cdc697 (SHA256) -> Pass@123











**Observations and Conclusion**

* **Security Insight**: Hashing algorithms like MD5 and SHA1 are relatively easy to crack with modern tools. Stronger algorithms like SHA256 offer better security but are still vulnerable to dictionary attacks if weak passwords are used.
* **Encryption**: AES encryption for card details ensures data confidentiality. Proper management of encryption keys is crucial for maintaining security.
* **Password Security**: Users should employ strong, unique passwords to enhance security. Systems should implement measures like salting and iterative hashing to protect passwords further.