UNIVERSITY OF NEW BRUNSWICK
Faculty of Computer Science
Network Security (CS4415-CS6415) – Winter 2022
Handout (3) – Data Protection
Dr. Hassan Mahdikhani

CIC

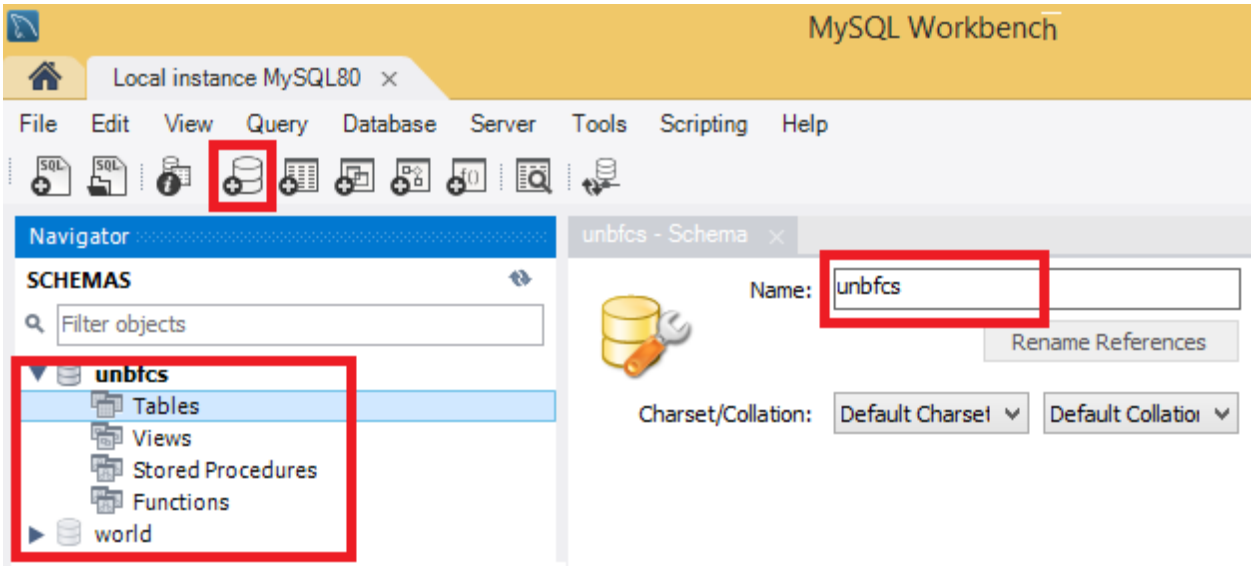
This handout will help you understand the data protection techniques in database management systems to protect data from unauthorized insiders/outsiders and curios DBAs as well as during data exchange process over network.

A. Data Integrity

1. Connect to your local MySQL DBMS and create UNBFCS (or lowercase unbfcs) database by choosing Create new scheme icon from toolbar.

```
CREATE SCHEMA `unbfcs` ;
```

2. Expand the UNBFCS database and select tables



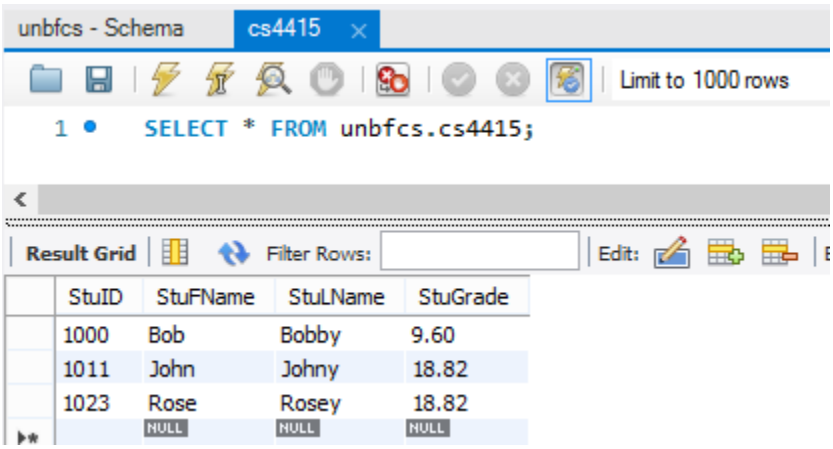
3. Create the CS4415 table with following fields and add three listed records.

```
CREATE TABLE `unbfcs`.`cs4415` (
  `StuID` INT NOT NULL,
  `StuFName` VARCHAR(45) NULL,
  `StuLName` VARCHAR(45) NULL,
  `StuGrade` FLOAT NULL,
  PRIMARY KEY (`StuID`));


INSERT INTO `unbfcs`.`cs4415`
(`StuID`,`StuFName`,`StuLName`,`StuGrade`) VALUES (1000, 'Bob', 'Bobby', 9.6);

INSERT INTO `unbfcs`.`cs4415`
(`StuID`,`StuFName`,`StuLName`,`StuGrade`)  VALUES  (1011,  'John',  'Johny',
18.82);

INSERT INTO `unbfcs`.`cs4415`
(`StuID`,`StuFName`,`StuLName`,`StuGrade`)  VALUES  (1023,  'Rose',  'Rosey',
18.82);
```



4. Create new table (CS4415Hashed) with one additional column, i.e., StuHashValue, with VarChar(32). Now read from original cs4415 table and insert into CS4415Hashed. You can use INSERT statement with extra computational field along with SELECT query.

- → ***MD5 algorithm generates a 128-bit digest that is represented by 32 hexadecimal characters.***
- → ***Use MD5() embedded method that is implemented in MySQL to generate MD5 digest.***
- → ***Concat() built-in method concatenates the values.***

Question 1. Insert your student ID, student first/last name, and your grade along with MD5 value into CS4415Hashed. (3 marks)

Question 2. Modify your grade and provide an SQL statement that present your record has been modified. (5 marks)

Question 3. Consider the case that an insider/outsider or and curious DBA opens the table and modify the field value and generate the new MD5 digest and update the StuHashValue. What is your solution to protect the table against this type of attack? (4 marks)

B. Data Confidentiality

1. Create the corresponding encrypted grade table (CS4415Enc).

- → ***To store encrypted value generated by AES(str, key_str) method, use a column with a VARBINARY or BLOB binary data type.***
- → ***The MySQL AES_ENCRYPT/AES_DECRYPT function is used for encrypting/decrypting a plaintext/ciphertext using Advanced Encryption Standard (AES) algorithm. The MySQL AES_ENCRYPT/AES_DECRYPT function encodes/decodes the data with 128 bits key length but it can be extended up to 256 bits key length.***
- → ***To cast BLOB data into characters and directly view BLOBs in MySQL Workbench, use the CAST method as follows:***

```
SELECT CAST(<BLOB Data> AS CHAR)
```

```
CREATE TABLE `cs4415enc` (
  `StuID` blob NOT NULL,
  `StuFName` blob,
  `StuLName` blob,
  `StuGrade` blob
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
```

2. Read original plaintext data from CS4415 and encrypt the field values and insert them into the CS4415Enc table. You can use INSERT statement with aes_encrypt method along with SELECT query.

```
INSERT INTO cs4415enc (StuID, StuFName, StuLName, StuGrade)
SELECT aes_encrypt(StuID,'qazWSX123!@#'), aes_encrypt(StuFName,
'qazWSX123!@#'), aes_encrypt(StuLName, 'qazWSX123!@#'), aes_encrypt(StuGrade,
'qazWSX123!@#')  FROM cs4415;
```

→ ***qazWSX123!@# is my secret key to encrypt the plaintext data and to decrypt the cipher text data. You can choose your own secret key. Note that, AES is a symmetric encryption algorithm because it uses same key to encrypt and decrypt data.***

Question 4. Insert your encrypted information into the CS4415Enc table. (3 marks)
Question 5. Update your grade with Rose's/John's grade, i.e., encrypted value of 18.82. (2 marks)
Question 6. Do you have any solution to prevent the above attack? (4 marks)
Question 7. Decrypt the entire data stored in the table and preset it in the clear form. (4 marks)