FIT@HCMUS
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN, ĐHQG - HCM
KHOA CÔNG NGHỆ THÔNG TIN

LAB 3 - MÃ HÓA DỮ LIỆU SỬ DỤNG CÁC THUẬT TOÁN MÃ HÓA ĐỐI XỨNG

BỘ MÔN: BẢO MẬT CƠ SỞ DỮ LIỆU

Sinh viên thực hiện:
21120419 - Vũ Thành Công

TP. Hồ Chí Minh, tháng 4/2024

Mục lục

I. Các stored procedure (câu c)....2
1. Stored procedure SP_INS_SINHVIEN....2
a. Cài đặt....2
b. Thực thi....2
2. Stored procedure SP_INS_NHANVIEN....2
a. Cài đặt....2
b. Thực thi....3
3. Stored procedure SP_SEL_NHANVIEN....3
a. Cài đặt....3
b. Thực thi....4
II. Màn hình quản lý đăng nhập hệ thống (Câu d)....4
1. Đối với table SINHVIEN....4
2. Đối với table NHANVIEN....5
III. Sử dụng SQL Profile để theo dõi thao tác đăng nhập (câu e)....5
1. Đăng nhập....5
2. Nhận xét....7

I. Các stored procedure (câu c)

1. Stored procedure SP_INS_SINHVIEN

a. Cài đặt

```
58 CREATE PROC SP_INS_SINHVIEN
59 (
60     @MASV NVARCHAR(20),
61     @HOTEN NVARCHAR(100),
62     @NGAYSINH DATETIME,
63     @DIACHI NVARCHAR(200),
64     @MALOP VARCHAR(20),
65     @TENDN NVARCHAR(100),
66     @MATKHAU VARCHAR(32)
67 )
68 AS
69     DECLARE @ENKEY VARBINARY(MAX)
70     SET @ENKEY = CONVERT(VARBINARY, HASHBYTES('MD5', @MATKHAU));
71     INSERT INTO SINHVIEN
72     VALUES (@MASV, @HOTEN, @NGAYSINH, @DIACHI, @MALOP, @TENDN, @ENKEY)
```

b. Thực thi

```
155 EXEC SP_INS_SINHVIEN '21120419', N'VŨ THÀNH CÔNG', '1/1/2003', N'LÂM ĐỒNG', 'CNTT-K21', '21120419', 'abcd419';
156 EXEC SP_INS_SINHVIEN '35120001', N'CÔNG THÀNH VŨ', '11/11/2017', N'LONG AN', 'CNTT-K35', '35120001', 'abcd001';
157 EXEC SP_INS_SINHVIEN '46120030', N'VŨ CÔNG', '12/12/2028', N'ĐỒNG THÁP', 'CNTT-K46', '46120030', 'abcd030';
158
159 select* from sinhvien order by masv
```

132 %

Results Messages

	MASV	HOTEN	NGAYSINH	DIACHI	MALOP	TENDN	MATKHAU
1	21120419	VŨ THÀNH CÔNG	2003-01-01 00:00:00.000	LÂM ĐỒNG	CNTT-K21	21120419	0xD6FDC1A6004C3A44DC40EC97A8961FAE
2	35120001	CÔNG THÀNH VŨ	2017-11-11 00:00:00.000	LONG AN	CNTT-K35	35120001	0x192A1A8DDDC67D7CFB5EB7AA692FB143
3	46120030	VŨ CÔNG	2028-12-12 00:00:00.000	ĐỒNG THÁP	CNTT-K46	46120030	0x194A5E7DCBEE7955205C8D99C4573090

2. Stored procedure SP_INS_NHANVIEN

a. Cài đặt

Để cài đặt mã hóa cột MATKHAU trong bảng NHANVIEN, thực hiện giống như trên.

Nhưng đối với cột LUONG cần mã hóa sử dụng AES 256, cần tiến hành khởi tạo các đối tượng lần lượt là Master Key, Certificate và cuối cùng là Symmetric key.

```
75 --TAO MASTERKEY
76 IF NOT EXISTS
77 (
78     SELECT*
79     FROM SYS.symmetric_keys
80     WHERE symmetric_key_id = 101
81 )
82 CREATE MASTER KEY ENCRYPTION BY PASSWORD = '21120419'
```

```
--TAO CERTIFICATE
IF NOT EXISTS
(
    SELECT*
    FROM sys.certificates
    WHERE NAME = 'MYCERT'
)
CREATE CERTIFICATE MYCERT WITH SUBJECT = 'MYCERT'
```

```
--TAO SYMMETRIC KEY
IF NOT EXISTS
(
    SELECT*
    FROM sys.symmetric_keys
    WHERE NAME = 'PRIVKEY'
)
CREATE SYMMETRIC KEY PRIVKEY WITH ALGORITHM = AES_256
    ENCRYPTION BY CERTIFICATE MYCERT;
```

Sau đó, mới tiến hành cài đặt SP_INS_NHANVIEN

```
CREATE PROC SP_INS_NHANVIEN
(
    @MANV VARCHAR(20),
    @HOTEN NVARCHAR(100),
    @EMAIL VARCHAR(20),
    @LUONG INT,
    @TENDN NVARCHAR(100),
    @MATKHAU VARCHAR(32)
)
AS
    DECLARE @ENPASS VARBINARY(MAX);
    DECLARE @ENSALARY VARBINARY(MAX)
    SET @ENPASS = CONVERT(VARBINARY, HASHBYTES('SHA1', @MATKHAU))
    SET @ENSALARY = ENCRYPTBYKEY(KEY_GUID('PRIVKEY'), CONVERT(VARBINARY(MAX), @LUONG))
    INSERT INTO NHANVIEN(MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU)
    VALUES (@MANV, @HOTEN, @EMAIL, @ENSALARY, @TENDN, @ENPASS);
```

b. Thực thi

```
EXEC SP_INS_NHANVIEN 'NV01', N'NGUYEN DINH THUC', 'NGTHUC@MAIL.COM', 3000, N'NDT', 'NDT@1'
EXEC SP_INS_NHANVIEN 'NV02', N'NGUYEN THI HUONG', 'NTHUONG@MAIL.COM', 2000, N'NTH', 'NTT@2'
EXEC SP_INS_NHANVIEN 'NV03', N'TRAN NGOC BAO', 'TNBAO@MAIL.COM', 2000, N'TNB', N'TNB@3'

select*from NHANVIEN
```

132 %

Results Messages

	MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU
1	NV01	NGUYEN DINH THUC	NGTHUC@MAIL.COM	0x00D241F4534B6841B2066E385E78014B02000000A62F704...	NDT	0xA16CE247A0D39EBA64E1254E7C0AAFB9FC0C8773
2	NV02	NGUYEN THI HUONG	NTHUONG@MAIL.COM	0x00D241F4534B6841B2066E385E78014B0200000015A42E6...	NTH	0xA964B1EFA10A8B49DC47FACA9CBE665674C1368F
3	NV03	TRAN NGOC BAO	TNBAO@MAIL.COM	0x00D241F4534B6841B2066E385E78014B02000000F43E43...	TNB	0x8E08DC0FF8B464A3722AC594F1D4009C2D1DF0F4

3. Stored procedure SP_SEL_NHANVIEN

a. Cài đặt

```
125 CREATE PROC SP_SEL_NHANVIEN
126 AS
127     OPEN SYMMETRIC KEY PRIVKEY
128     DECRYPTION BY CERTIFICATE MYCERT
129     SELECT MANV, HOTEN, EMAIL, CONVERT(INT, DECRYPTBYKEY(LUONG)) AS LUONGCB
130     FROM NHANVIEN
```

b. Thực thi

```
147
148 exec SP_SEL_NHANVIEN
149
```

145 %

Results | Messages

	MANV	HOTEN	EMAIL	LUONGCB
1	NV01	NGUYEN DINH THUC	NGTHUC@MAIL.COM	3000
2	NV02	NGUYEN THI HUONG	NTHUONG@MAIL.COM	2000
3	NV03	TRAN NGOC BAO	TNBAO@MAIL.COM	2000

II. Màn hình quản lý đăng nhập hệ thống (Câu d)

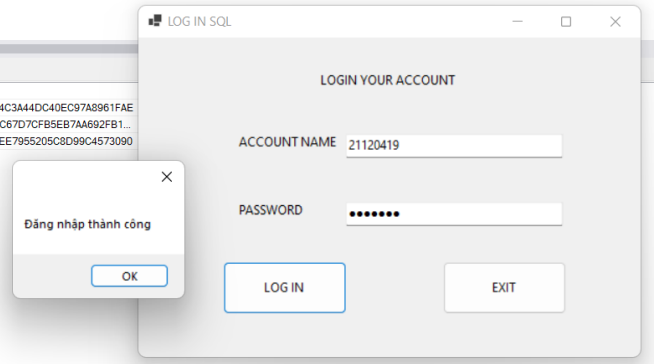
1. Đối với table SINHVIEN

```
140 EXEC SP_INS_SINHVIEN '21120419', N'VŨ THÀNH CÔNG', '1/1/2003', N'LÂM ĐỒNG', 'CNTT-K21', '21120419', 'abcd419';
141 EXEC SP_INS_SINHVIEN '35120001', N'CÔNG THÀNH VŨ', '11/11/2017', N'LONG AN', 'CNTT-K35', '35120001', 'abcd001';
142 EXEC SP_INS_SINHVIEN '46120030', N'VŨ CÔNG', '12/12/2028', N'ĐỒNG THÁP', 'CNTT-K46', '46120030', 'abcd030';
143
144 select* from sinhvien order by masv
145
```

132 %

Results | Messages

	MASV	HOTEN	NGAYSINH	DIACHI	MALOP	TENDN	MATKHAU
1	21120419	VŨ THÀNH CÔNG	2003-01-01 00:00:00.000	LÂM ĐỒNG	CNTT-K21	21120419	0xD6FDC1A6004C3A44DC40EC97A8961FAE
2	35120001	CÔNG THÀNH VŨ	2017-11-11 00:00:00.000	LONG AN	CNTT-K35	35120001	0x192A1A8DDDC67D7CFB5EB7AA692FB1...
3	46120030	VŨ CÔNG	2028-12-12 00:00:00.000	ĐỒNG TH...	CNTT-K46	46120030	0x194A5E7DCBEE7955205C8D99C4573090

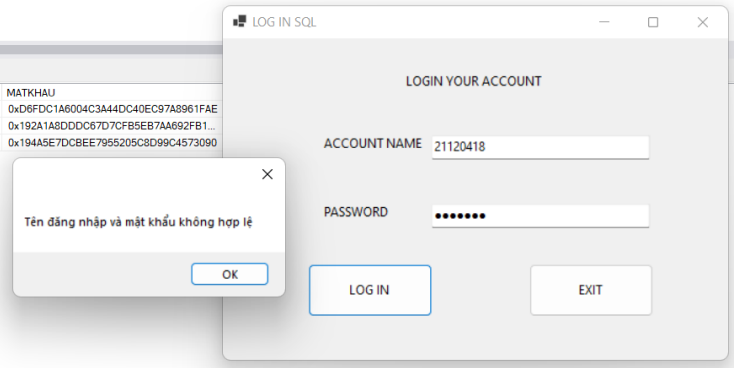



```
139
140 EXEC SP_INS_SINHVIEN '21120419', N'VŨ THÀNH CÔNG', '1/1/2003', N'LÂM ĐỒNG', 'CNTT-K21', '21120419', 'abcd419';
141 EXEC SP_INS_SINHVIEN '35120001', N'CÔNG THÀNH VŨ', '11/11/2017', N'LONG AN', 'CNTT-K35', '35120001', 'abcd001';
142 EXEC SP_INS_SINHVIEN '46120030', N'VŨ CÔNG', '12/12/2028', N'ĐỒNG THÁP', 'CNTT-K46', '46120030', 'abcd030';
143
144 select* from sinhvien order by masv
145
```

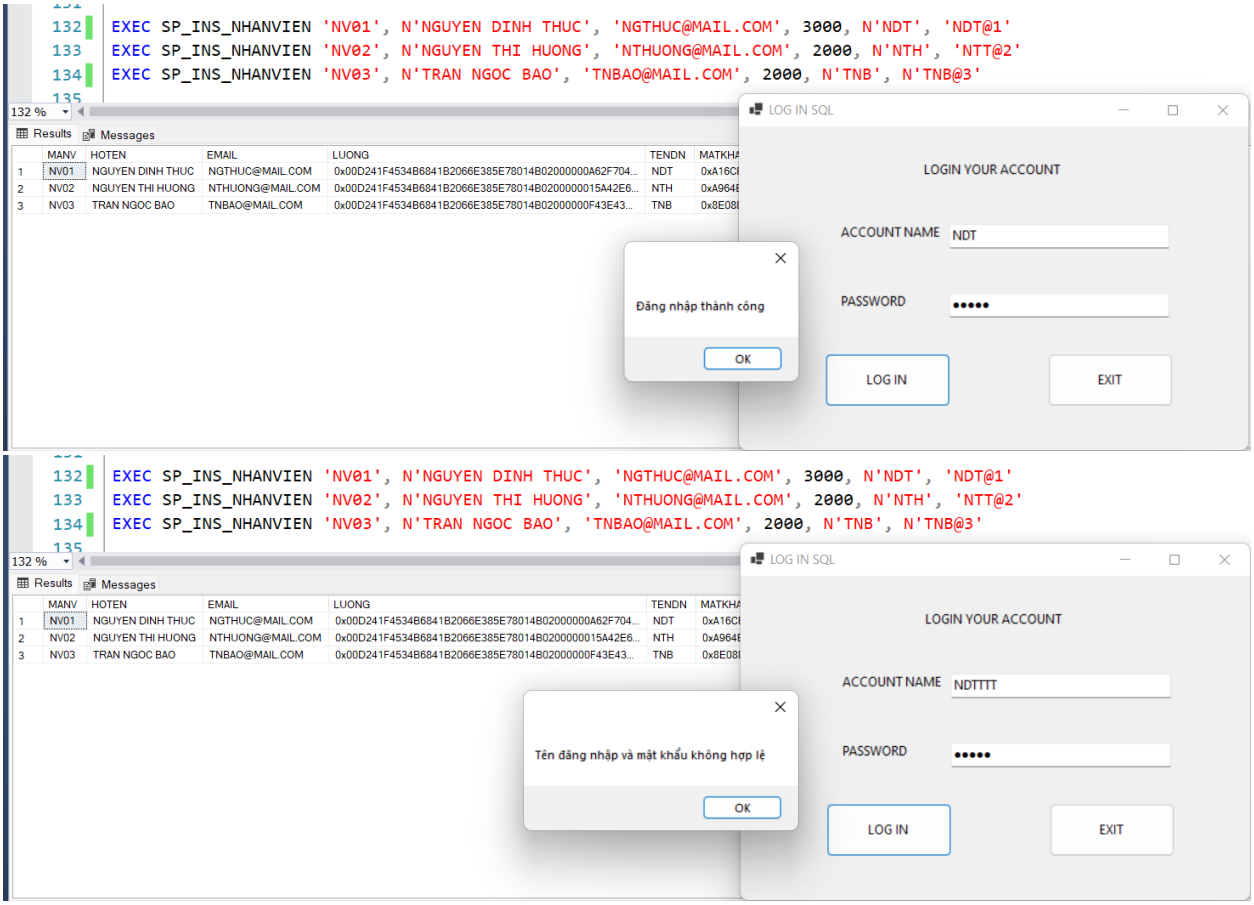
132 %

Results | Messages

	MASV	HOTEN	NGAYSINH	DIACHI	MALOP	TENDN	MATKHAU
1	21120419	VŨ THÀNH CÔNG	2003-01-01 00:00:00.000	LÂM ĐỒNG	CNTT-K21	21120419	0xD6FDC1A6004C3A44DC40EC97A8961FAE
2	35120001	CÔNG THÀNH VŨ	2017-11-11 00:00:00.000	LONG AN	CNTT-K35	35120001	0x192A1A8DDDC67D7CFB5EB7AA692FB1...
3	46120030	VŨ CÔNG	2028-12-12 00:00:00.000	ĐỒNG TH...	CNTT-K46	46120030	0x194A5E7DCBEE7955205C8D99C4573090



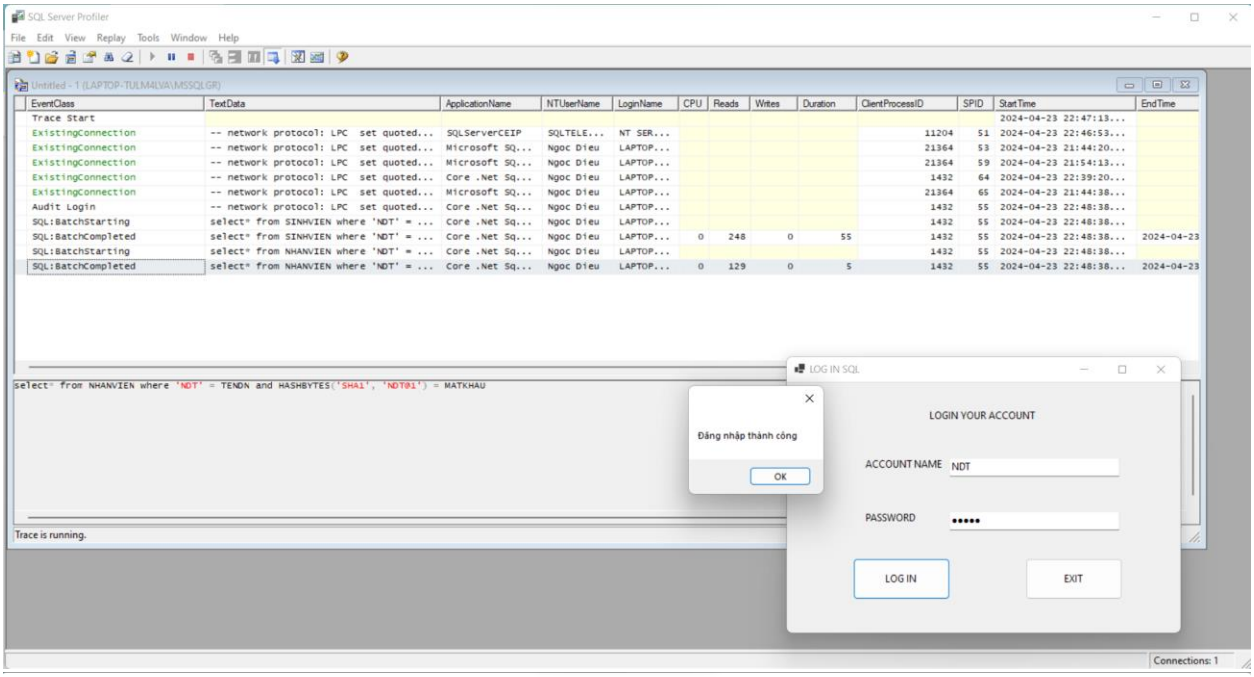
2. Đối với table NHANVIEN

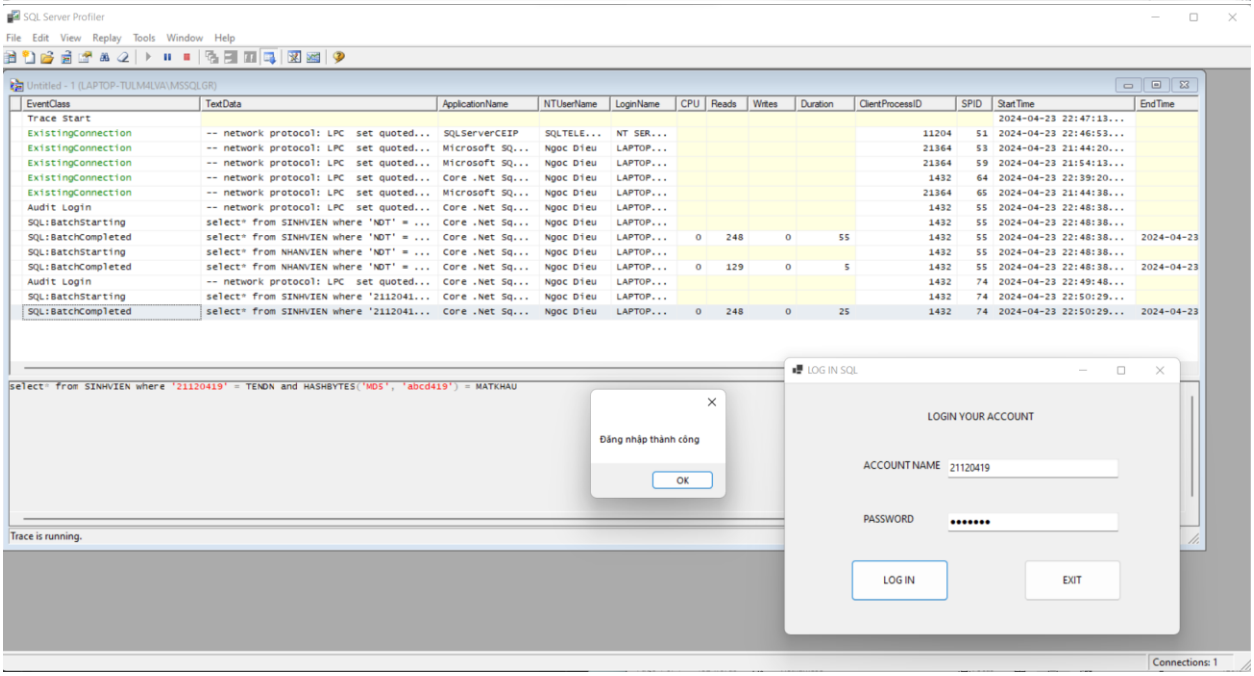


III. Sử dụng SQL Profile để theo dõi thao tác đăng nhập (câu e)

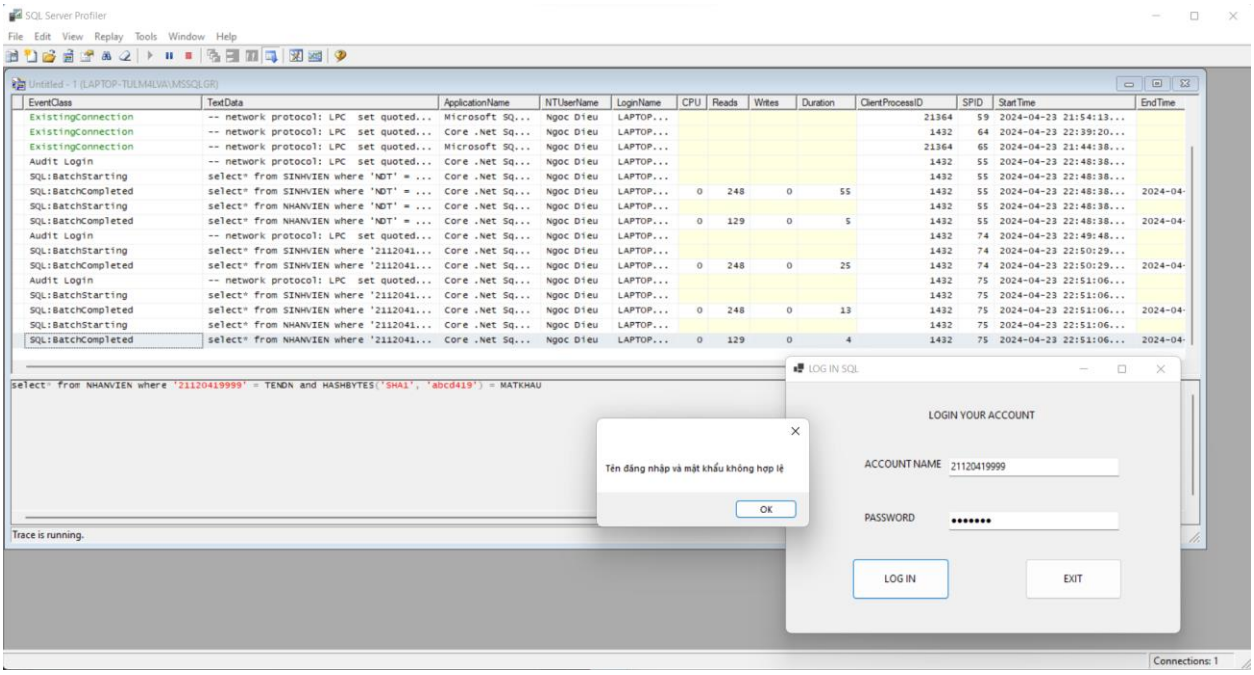
1. Đăng nhập

- Đối với tài khoản và mật khẩu đúng





- Đối với tài khoản và mật khẩu sai



2. Nhận xét

- Đoạn code SQL được đưa vào từ C# được SQL Profile bắt lấy và hiển thị ở dạng bản rõ.
- Người có quyền truy cập tới Tool SQL Server Profiler hoặc nghe trộm có thể thấy rõ dữ liệu giữa client và server gửi cho nhau.
- Cần phải mã hóa dữ liệu ở cả 2 chiều client và server