

# **BẢO MẬT CƠ SỞ DỮ LIỆU**

## **Lab03 – Mã hóa dữ liệu**

Sinh viên:

**Đỗ Trọng Nghĩa - 18120477**



Khoa Công nghệ Thông tin  
Đại học Khoa học Tự nhiên TP HCM

# I. Tạo khóa

Các đối tượng cần khởi tạo là Master key, Certificate và Symmetric key

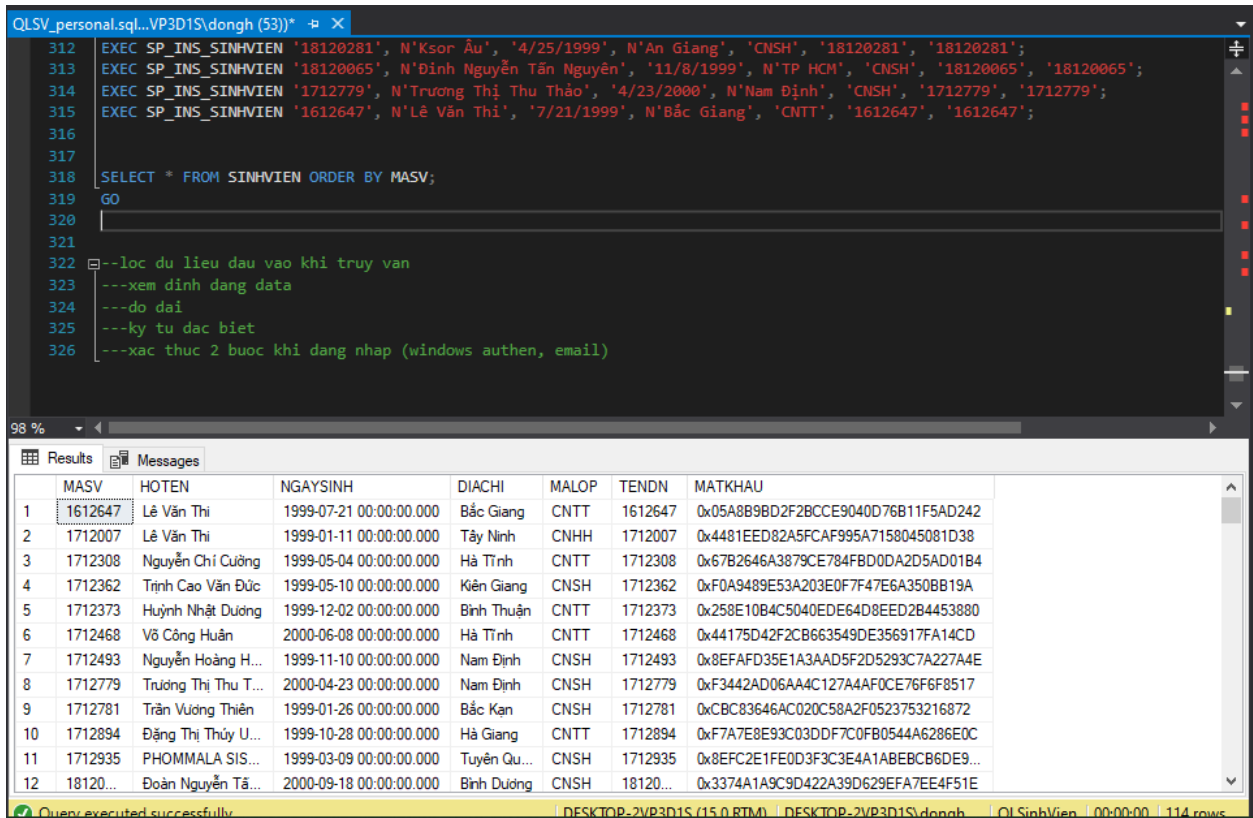
```
--_personal.sql...VP3D1S\dongh (53)) -> X
63 -----
64 -- CAU LENH TAO STORED PROCEDURE
65
66 --tao MASTERKEY
67 IF NOT EXISTS
68 (
69     SELECT*
70     from sys.symmetric_keys
71     WHERE symmetric_key_id = 101
72 )
73
74 CREATE MASTER KEY ENCRYPTION by
75     PASSWORD = '18120477'
76 GO
77
78 --tao CERTIFICATE
79 IF NOT EXISTS
80 (
81     SELECT*
82     from sys.certificates
83     WHERE name = 'myCert'
84 )
85
86 CREATE CERTIFICATE myCert
87     WITH SUBJECT = 'myCert'
88 GO
89 --drop master key
90 --drop certificate myCert
91 --tao SYMMETRIC KEY
92 CREATE SYMMETRIC KEY PriKey
93     WITH ALGORITHM = AES_256
94     ENCRYPTION BY CERTIFICATE myCert;
95
```

## II. Tạo Stored Procedure có mã hóa dữ liệu

### a. SP\_INS\_SINHVIEN

```
97  --SP_INS_SINHVIEN
98  create proc SP_INS_SINHVIEN
99  (
100     @MASV nvarchar(20),
101     @HOTEN nvarchar(100),
102     @NGAYSINH datetime,
103     @DIACHI nvarchar(200),
104     @MALOP varchar(20),
105     @TENDN nvarchar(100),
106     @MATKHAU varchar(32)
107 )
108 As
109 Begin
110     DECLARE @EnKey VARBINARY(max);
111     SET @EnKey = CONVERT(VARBINARY, HASHBYTES('MD5', @MATKHAU));
112     INSERT INTO SINHVIEN
113     VALUES (@MASV, @HOTEN, @NGAYSINH, @DIACHI, @MALOP, @TENDN, @EnKey)
114 End
115 --drop procedure SP_INS_SINHVIEN
116 go
```

- Kết quả chạy test:



The screenshot shows a SQL Server Enterprise Manager interface. The top pane displays a query window with the following SQL code:

```

312 EXEC SP_INS_SINHVIEN '18120281', N'Kson Âu', '4/25/1999', N'An Giang', 'CNSH', '18120281', '18120281';
313 EXEC SP_INS_SINHVIEN '18120065', N'Đinh Nguyễn Tấn Nguyên', '11/8/1999', N'TP HCM', 'CNSH', '18120065', '18120065';
314 EXEC SP_INS_SINHVIEN '1712779', N'Trương Thị Thu Thảo', '4/23/2000', N'Nam Định', 'CNSH', '1712779', '1712779';
315 EXEC SP_INS_SINHVIEN '1612647', N'Lê Văn Thi', '7/21/1999', N'Bắc Giang', 'CNTT', '1612647', '1612647';
316
317
318 SELECT * FROM SINHVIEN ORDER BY MASV;
319 GO
320
321
322 --loc du lieu dau vao khi truy van
323 ---xem dinh dang data
324 ---do dai
325 ---ky tu dac biet
326 ---xac thuc 2 buoc khi dang nhap (windows authen, email)

```

The bottom pane shows the results of the query execution. The results are displayed in a table with 12 rows and 7 columns: MASV, HOTEN, NGAYSINH, DIACHI, MALOP, TENDN, and MATKHAU. The status bar at the bottom indicates that the query was executed successfully and returned 114 rows.

MASV	HOTEN	NGAYSINH	DIACHI	MALOP	TENDN	MATKHAU
1	1612647	Lê Văn Thi	1999-07-21 00:00:00.000	Bắc Giang	CNTT	1612647
2	1712007	Lê Văn Thi	1999-01-11 00:00:00.000	Tây Ninh	CNHH	1712007
3	1712308	Nguyễn Chí Cường	1999-05-04 00:00:00.000	Hà Tĩnh	CNTT	1712308
4	1712362	Trịnh Cao Văn Đức	1999-05-10 00:00:00.000	Kiên Giang	CNSH	1712362
5	1712373	Huỳnh Nhật Dương	1999-12-02 00:00:00.000	Bình Thuận	CNTT	1712373
6	1712468	Võ Công Huân	2000-06-08 00:00:00.000	Hà Tĩnh	CNTT	1712468
7	1712493	Nguyễn Hoàng H...	1999-11-10 00:00:00.000	Nam Định	CNSH	1712493
8	1712779	Trương Thị Thu T...	2000-04-23 00:00:00.000	Nam Định	CNSH	1712779
9	1712781	Trần Vương Thiên	1999-01-26 00:00:00.000	Bắc Kạn	CNSH	1712781
10	1712894	Đặng Thị Thúy U...	1999-10-28 00:00:00.000	Hà Giang	CNTT	1712894
11	1712935	PHOMMALA SIS...	1999-03-09 00:00:00.000	Tuyên Qu...	CNSH	1712935
12	18120...	Đoàn Nguyễn Tã...	2000-09-18 00:00:00.000	Bình Dương	CNSH	18120...

## b. SP\_INS\_NHANVIEN

```

118 --SP_INS_NHANVIEN
119 create proc SP_INS_NHANVIEN
120 (
121     @MANV varchar(20),
122     @HOTEN nvarchar(100),
123     @EMAIL varchar(20),
124     @LUONG int,
125     @TENDN nvarchar(100),
126     @MATKHAU varchar(32)
127 )
128 As
129 Begin
130     DECLARE @EnPass varbinary(max);
131     DECLARE @EnWage varbinary(max);
132     SET @EnPass=CONVERT(varbinary, HashBytes('SHA1',@MATKHAU));
133     SET @EnWage = ENCRYPTBYKEY(KEY_GUID('PriKey'), CONVERT(varbinary(MAX), @LUONG))
134     insert into NHANVIEN(MANV,HOTEN,EMAIL,LUONG,TENDN,MATKHAU)
135     values (@MANV, @HOTEN, @EMAIL, @EnWage, @TENDN,@EnPass);
136 END
137
138 --drop procedure SP_INS_NHANVIEN
139 go

```

Kết quả chạy test:

189  
190 select \* from NHANVIEN  
191

98 %

	MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU
1	NV01	NGUYEN DINH THUC	NDT@mail.com	0x00E82820C2489A47B520F8C327ECE54B020000004548553...	NDT	0xF54DDE4FADCC9F06E5175B79F3812222EFC281A
2	NV02	HUYNH THANH TAM	HTT@mail.com	0x00E82820C2489A47B520F8C327ECE54B0200000043DE641...	HTT	0xD6716285FABC939C4902F2908CDDC7FF70D29F9
3	NV03	NGO DINH HY	NDH@mail.com	0x00E82820C2489A47B520F8C327ECE54B02000000F3F042F...	NDH	0x89490E19B5FAFF3A4AAD632AC5C855D471845C3

## c. SP\_SEL\_NHANVIEN

```
143 create procedure SP_SEL_NHANVIEN
144 As
145 Begin
146     OPEN SYMMETRIC KEY PriKey
147     DECRYPTION BY CERTIFICATE myCert
148     SELECT MANV,HOTEN,EMAIL,CONVERT(int, DECRYPTBYKEY(LUONG)) as LUONGCB
149     FROM NHANVIEN
150 END
151
152 --drop procedure SP_SEL_NHANVIEN
153
154 go
155
```

- Kết quả chạy test:

```
143 create procedure SP_SEL_NHANVIEN
144 As
145 Begin
146     OPEN SYMMETRIC KEY PriKey
147     DECRYPTION BY CERTIFICATE myCert
148     SELECT MANV,HOTEN,EMAIL,CONVERT(int, DECRYPTBYKEY(LUONG)) as LUONGCB
149     FROM NHANVIEN
150 END
151
152 --drop procedure SP_SEL_NHANVIEN
153
154 go
155
```

## d. SP\_LOG\_IN hỗ trợ đăng nhập (hỗ trợ tác vụ Authentication)

```
157 create proc SP_LOG_IN
158 (
159     @TENDN nvarchar(100),
160     @MATKHAU varchar(32)
161 )
162 As
163 Begin
164     DECLARE @EnPassSHA1 varbinary(max);
165     DECLARE @EnPassMD5 varbinary(max);
166     DECLARE @COUNT INT;
167     SET @EnPassSHA1=CONVERT(varbinary, HashBytes('SHA1',@MATKHAU));
168     SET @EnPassMD5=CONVERT(varbinary, HashBytes('MD5',@MATKHAU));
169     SET @COUNT = (SELECT COUNT(*) FROM NHANVIEN WHERE TENDN = @TENDN and MATKHAU = @EnPassSHA1)
170     if @COUNT = 1
171         BEGIN SELECT COUNT(*) FROM NHANVIEN WHERE TENDN = @TENDN and MATKHAU = @EnPassSHA1 RETURN END
172     ELSE
173         BEGIN SELECT COUNT(*) FROM SINHVIEN WHERE TENDN = @TENDN and MATKHAU = @EnPassMD5 END
174     END
175
176
177 go
```

### III. Xây dựng màn hình đăng nhập

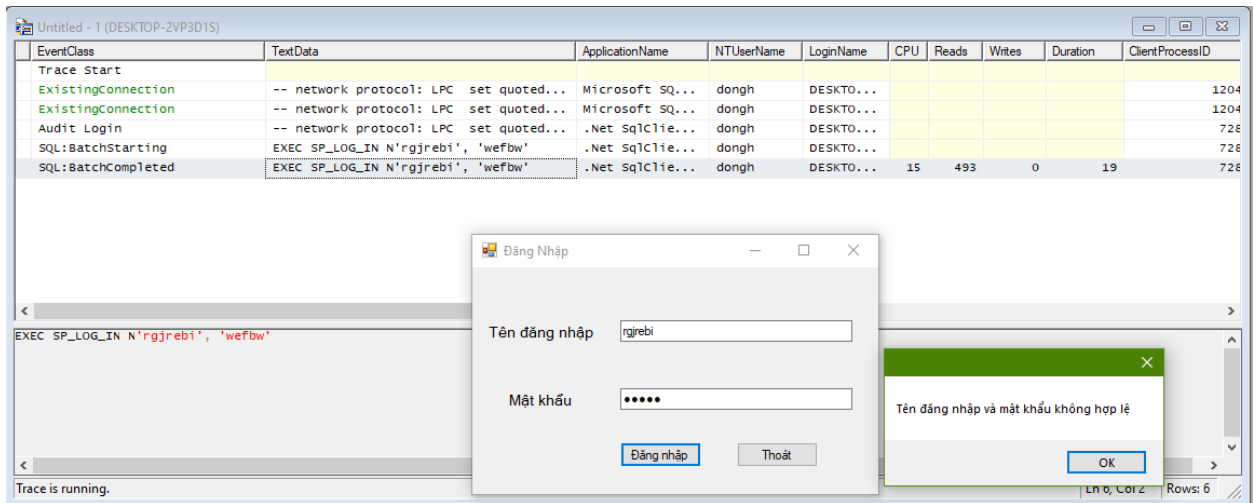
The screenshot shows a standard login window titled "Đăng Nhập". It contains two input fields: "Tên đăng nhập" (Username) and "Mật khẩu" (Password). Below the fields are two buttons: "Đăng nhập" (Login) and "Thoát" (Exit).

This screenshot shows the login window with a modal dialog box displayed in the center. The dialog box has the title "Đăng Nhập thành công" (Login successful) and an "OK" button. The "Đăng nhập" button on the login form is highlighted with a blue border.

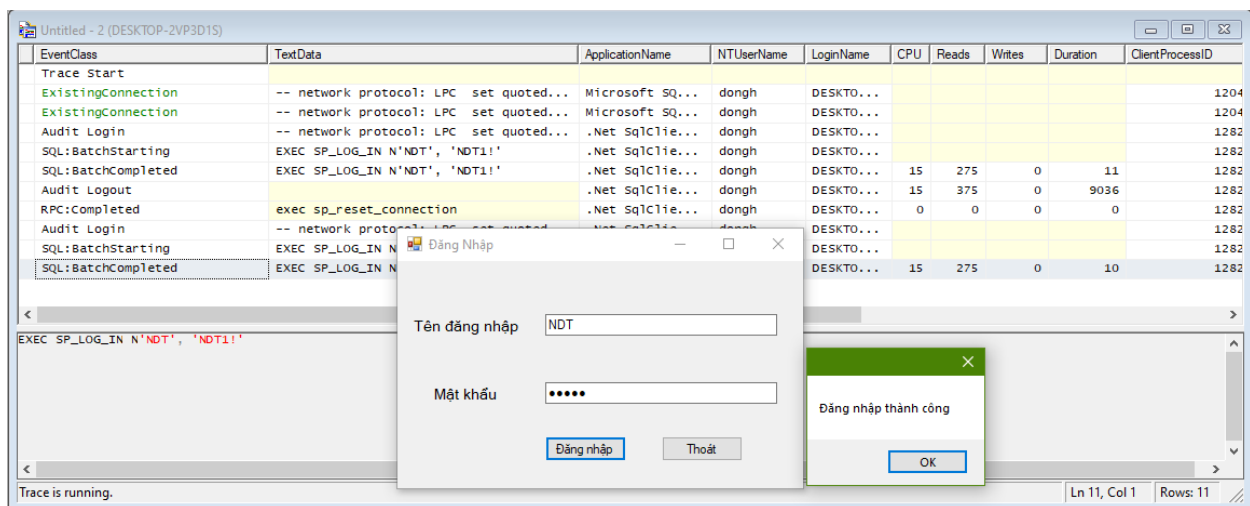
This screenshot shows the login window with a modal dialog box displaying an error message: "Tên đăng nhập hoặc mật khẩu sai" (Username or password is incorrect). The dialog box has an "OK" button. The "Đăng nhập" button on the login form is highlighted with a blue border.



- Sử dụng SQL Profile khi đăng nhập
  - Tài khoản và mật khẩu sai



- Đăng nhập với mật khẩu và tài khoản đúng  
Với giáo viên



## Với sinh viên

The screenshot displays the SQL Server Profiler interface with a trace running. The main window shows a table of events with columns: EventClass, TextData, ApplicationName, NTUserName, LoginName, CPU, Reads, Writes, Duration, and ClientProcessID. The trace includes several SQL:BatchStarting and SQL:BatchCompleted events, as well as Audit Logout and RPC:Completed events. A 'Đăng Nhập' (Login) dialog box is open in the foreground, showing the username '18120650' and a masked password. A small 'Đăng nhập thành công' (Login successful) message box is also visible.

Trong database phân mật khẩu có ký tự đặc biệt nên khó dùng Regular Expression để các ký tự đó ra khỏi truy vấn đăng nhập

- Nhận xét:
  - Người có quyền truy cập tới Tool SQL Server Profiler hoặc nghe trộm có thể thấy dữ liệu rõ giữa client và server gửi với nhau
  - Cần phải mã hóa dữ liệu ở cả hai chiều client và server