МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ   
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА №34

ОТЧЕТ ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| доцент, к.т.н. |  |  |  | В.А. Мыльников |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №7  **Методы шифрования объектов базы данных** |
|  |
| по курсу: БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ |

РАБОТУ ВЫПОЛНИЛ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТ ГР. № | 3843 |  |  |  | А.П.Конева |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2021

**Цель работы**

Ознакомление с методами шифрования объектов базы данных.

**Задача**

Разработать и продемонстрировать модель защиты объектов базы данных с использованием симметричных, асимметричных ключей и сертификатов.

**Шифрование на уровне ячеек**

Пример таблицы «CreditCard» с подготовленным атрибутом с типом данных «varbinary» для хранения зашифрованных данных.

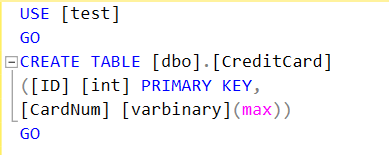


Рисунок 1 - Создание таблицы «CreditCard»

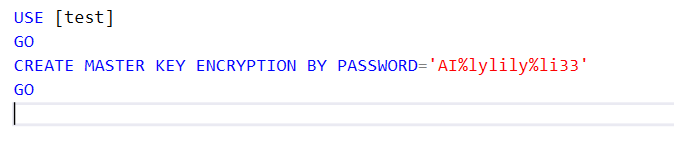
На Рис. 2 продемонстрирован скрипт для создания главного ключа базы данных DMK для базы данных «Test».

Рисунок 2 - Создание главного ключа базы данных DMK для базы данных «Test»

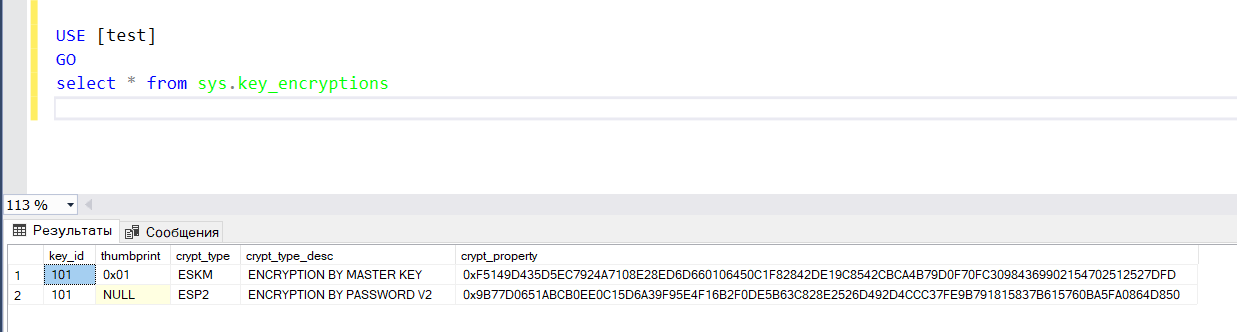
Далее произведем проверку существования главного ключа (Рис. 3):

Рисунок 3 - Проверка существования главного ключа

Создадим асимметричный ключ данных (Рис. 4):

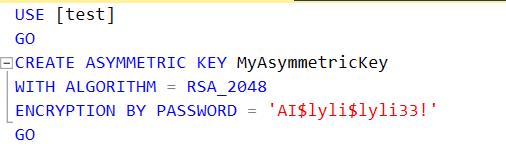


Рисунок 4 - Создание асимметричного ключа данных

Создадим симметричный ключ данных, зашифрованный асимметричным ключом (Рис. 5):

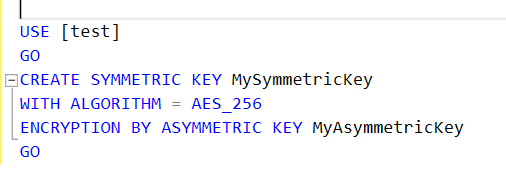


Рисунок 5 - Создание симметричного ключа данных, зашифрованного асимметричным ключом

На Рис. 6 показано открытие симметричного ключа для шифрования в сеансе пользователя.

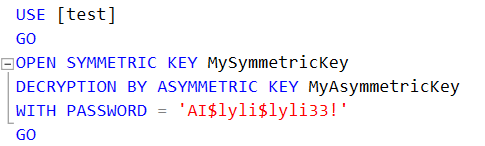


Рисунок 6 - Открытие симметричного ключа для шифрования в сеансе пользователя

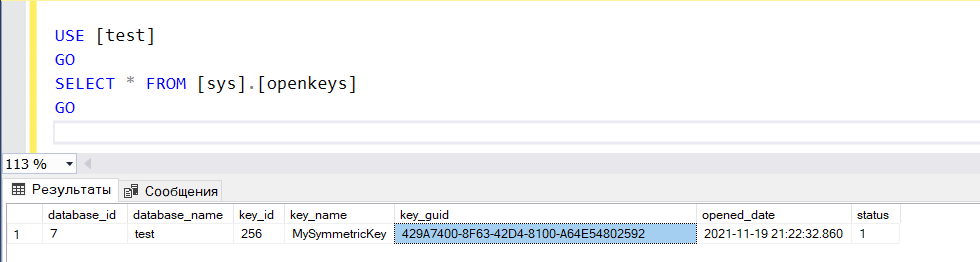
Просмотрим открытые сертификаты (Рис. 7):

Рисунок 7 - Просмотр открытых сертификатов

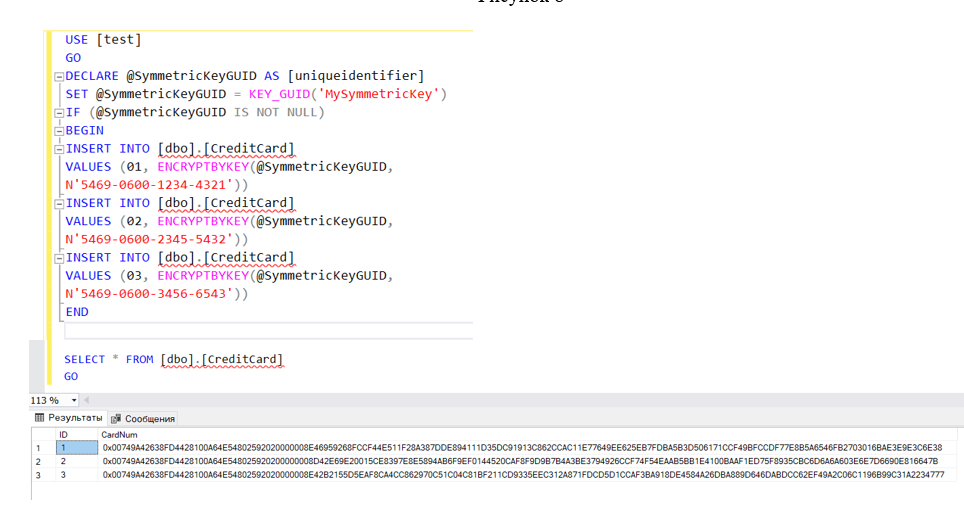
На Рис. 8 изображен пример заполнения значений с использованием симметричного ключа.

Рисунок 8 - Пример заполнения значений с использованием симметричного ключа

Создадим сертификат для симметричного ключа данных (Рис. 9):

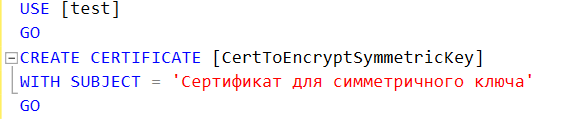


Рисунок 9 - Создание сертификата для симметричного ключа данных

Создадим симметричный ключ данных на базе сертификата (Рис. 10):

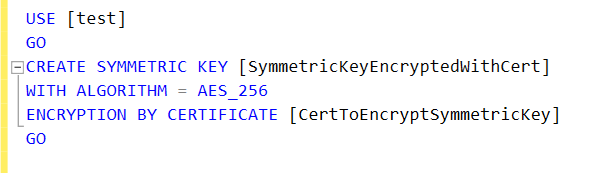


Рисунок 10 - Создание симметричного ключа данных на базе сертификата

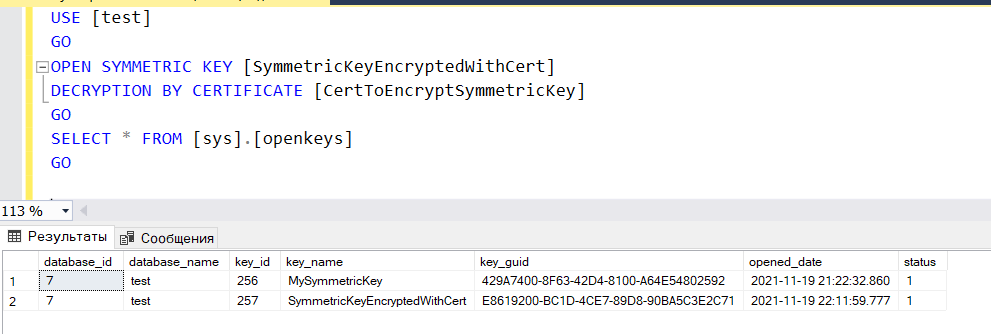
Откроем симметричный ключ в сеансе и проверим его статус (Рис. 11):

Рисунок 11 - Открытие симметричного ключа в сеансе и проверка его статуса

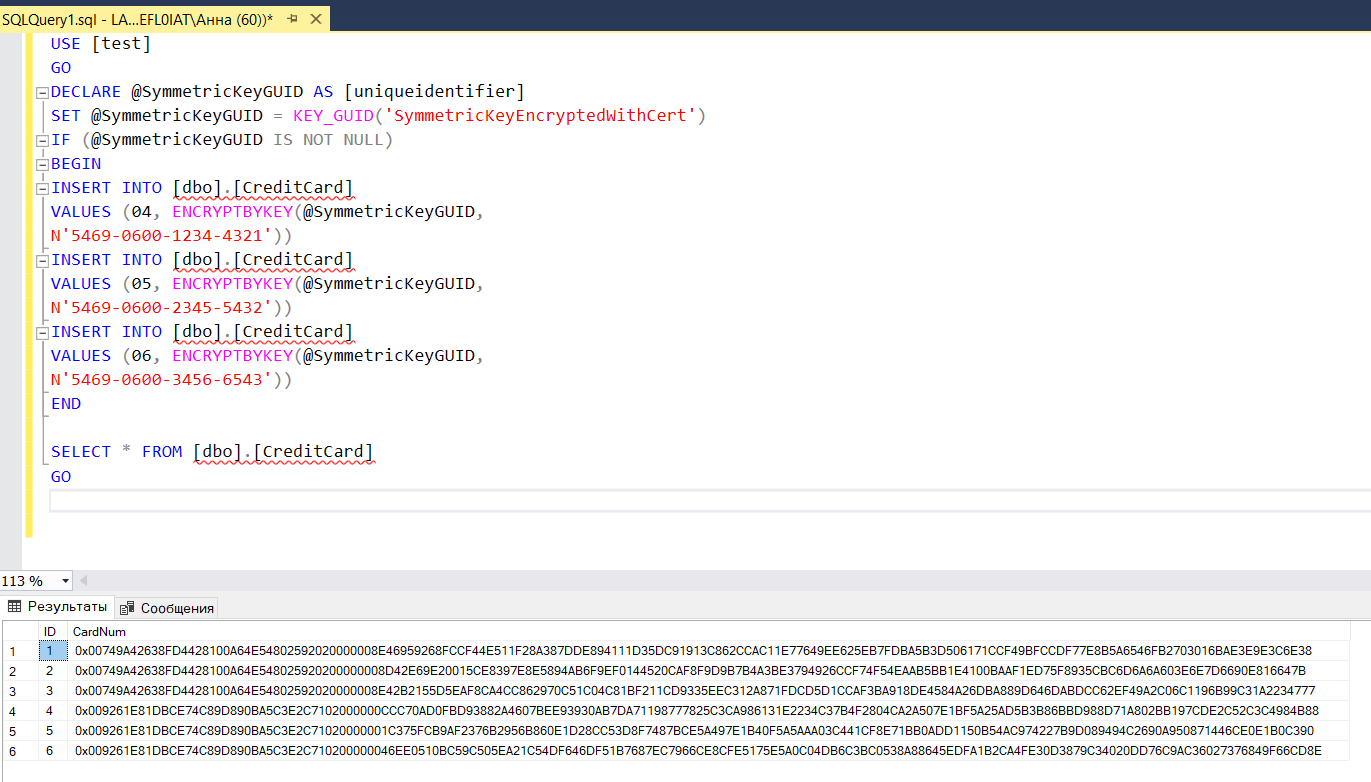
Далее выполним шифрование данных с использованием симметричного ключа на базе сертификата (Рис. 12):

Рисунок 12 - Шифрование данных с использованием симметричного ключа на базе сертификата

Просмотр данных, зашифрованных различными способами через представление. При условии открытия всех необходимых симметричных ключей (Рис. 13).

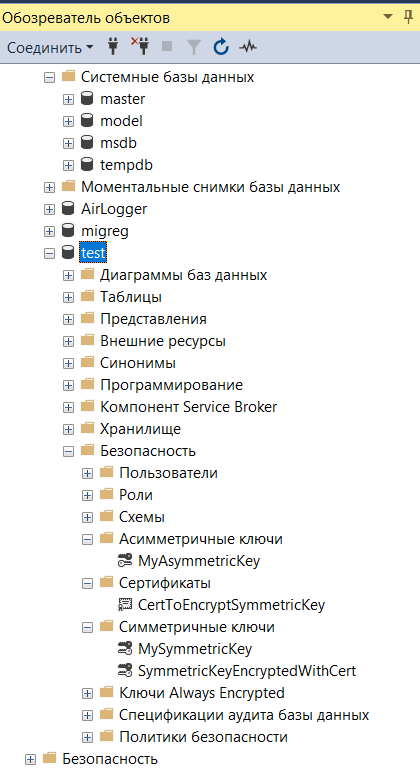
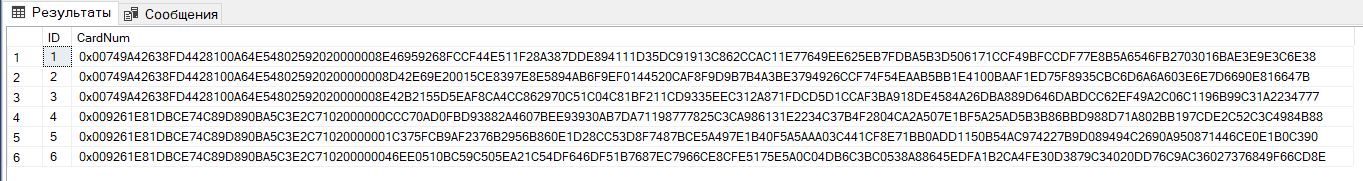


Рисунок 13 - Список ключей базы данных

Результаты запроса без расшифровки (Рис.14, а) и с расшифровкой (Рис.14, б) представлены на соответствующих рисунках.

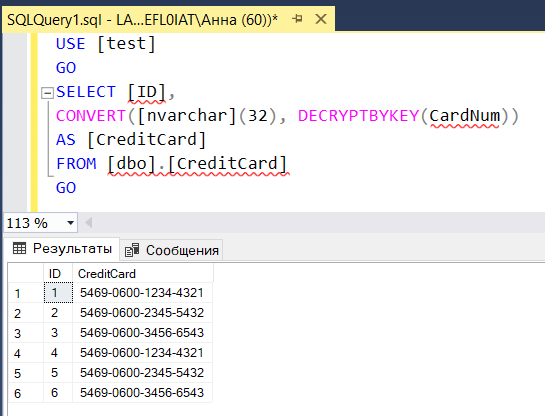
Рисунок 14, а - Результат запроса без расшифровки

Рисунок 14, б - Результат запроса с расшифровкой

**Использование прозрачного шифрования**

Создадим главный ключ и сертификат для сервера следующим сценарием (Рис. 15):

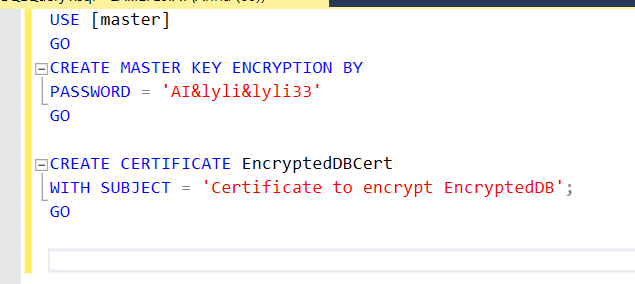


Рисунок 15 - Создание главного ключа и сертификата для сервера

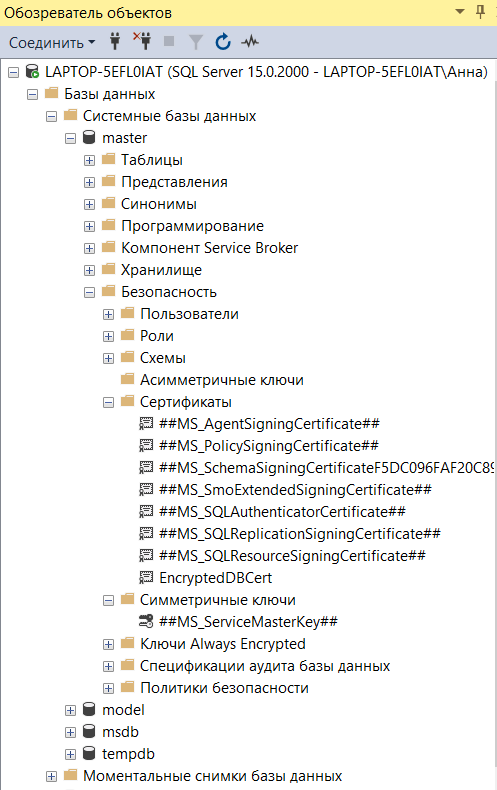
Далее необходимо убедиться в его наличии для продолжения работы (Рис. 16).

Рисунок 16 - Проверка создания ключа и сертификата

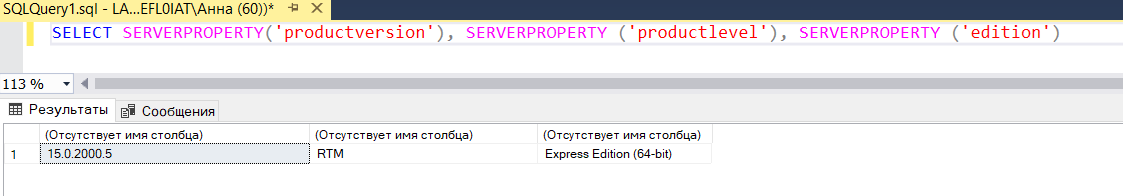
При проверке версии СУБД выяснили, что она не удовлетворяет требованиям для активации прозрачного шифрования всей базы данных (Рис. 17), поскольку используемая версия MS SQL Server не является Enterprise или Developer версиями.

Рисунок 17 - Проверка

**Вывод**

Подготовили модель базы данных для использования метода шифрования на уровне ячеек. Создали необходимые ключи и сертификаты (Рис. 2, 4,5,9,10,15). Подготовили SQL - сценарии для шифрования (Рис. 8, 12) и расшифровки данных на уровне ячеек (Рис. 14, б). Активировать прозрачное шифрование всей базы данных не удалось, поскольку используется MS SQL Server Express.