Державний торговельно-економічний університет  
Кафедра інженерії програмного забезпечення та кібербезпеки

**ЛАБОРАТОРНА РОБОТА №6**

**З ДИСЦИПЛІНИ «БАЗИ ДАНИХ»**

**НА ТЕМУ: «УПРАВЛІННЯ ДОСТУПОМ ДО СИСТЕМ БД»**

**Виконала**: студентка факультету

інформаційних технологій

групи\_курсу 3-4

Авєріна Наталія Ігорівна

**Перевірила**: Рзаєва Світлана Леонідівна

Київ 2024

**Лабораторна робота №6**

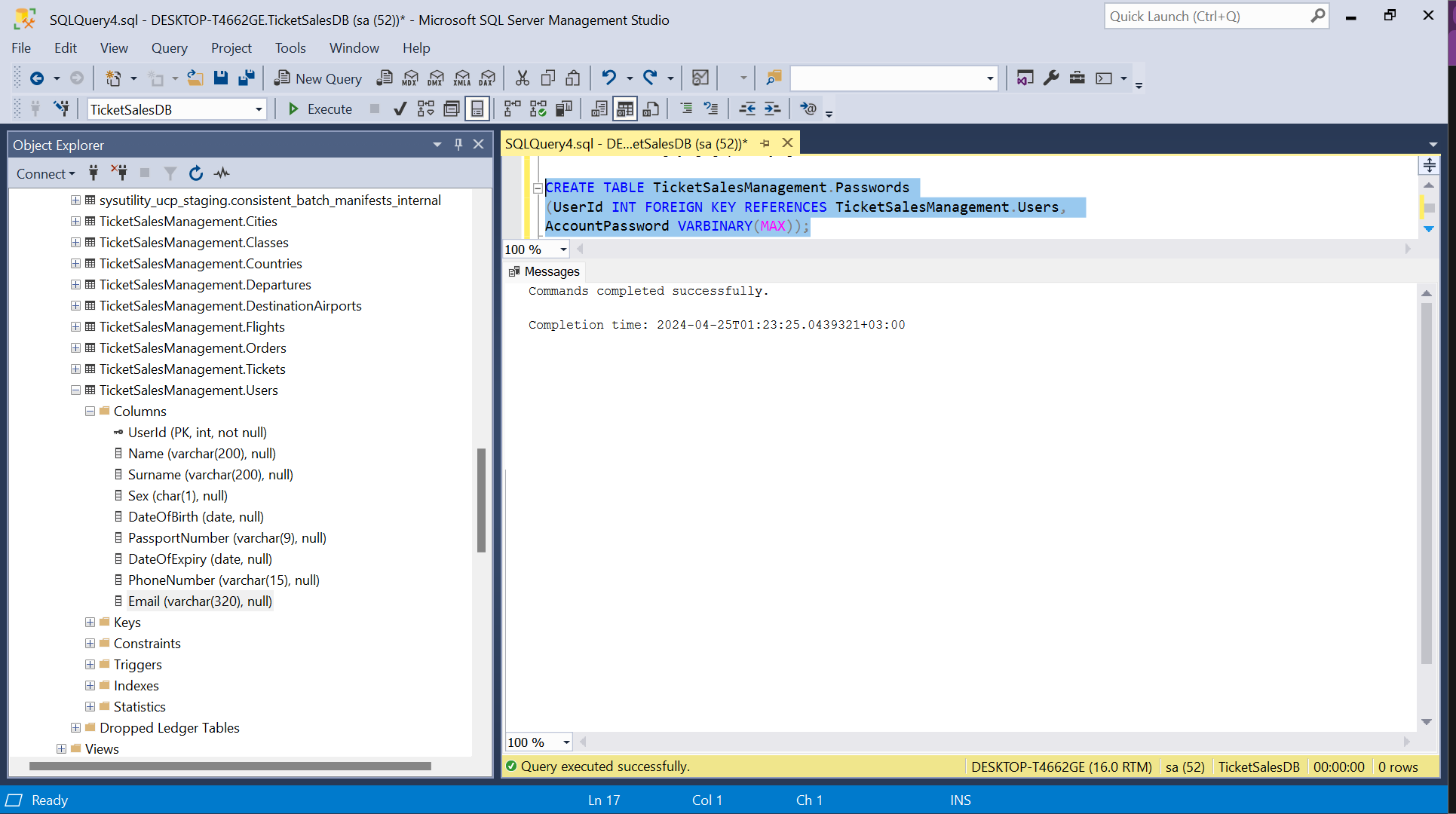
**Тема: «Управління доступом до систем БД»**

**Мета:** набути практичних навичок щодо встановлення режимів аутентифікації користувачів і об'єктів баз даних, особливостей авторизації користувачів, надання їм привілеїв.

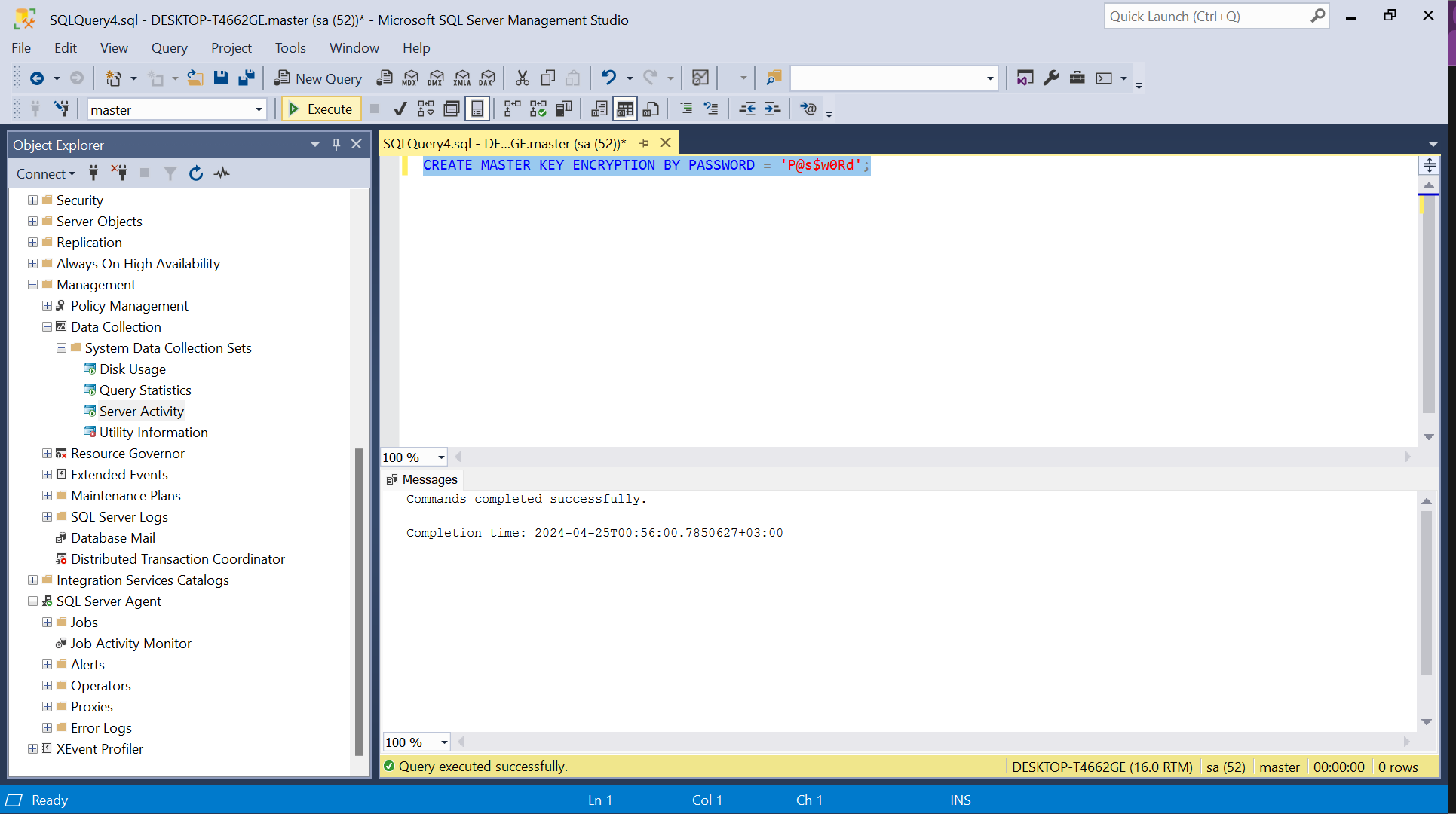
**Хід роботи:**

Створення асиметричного ключа для БД TicketSalesDB.

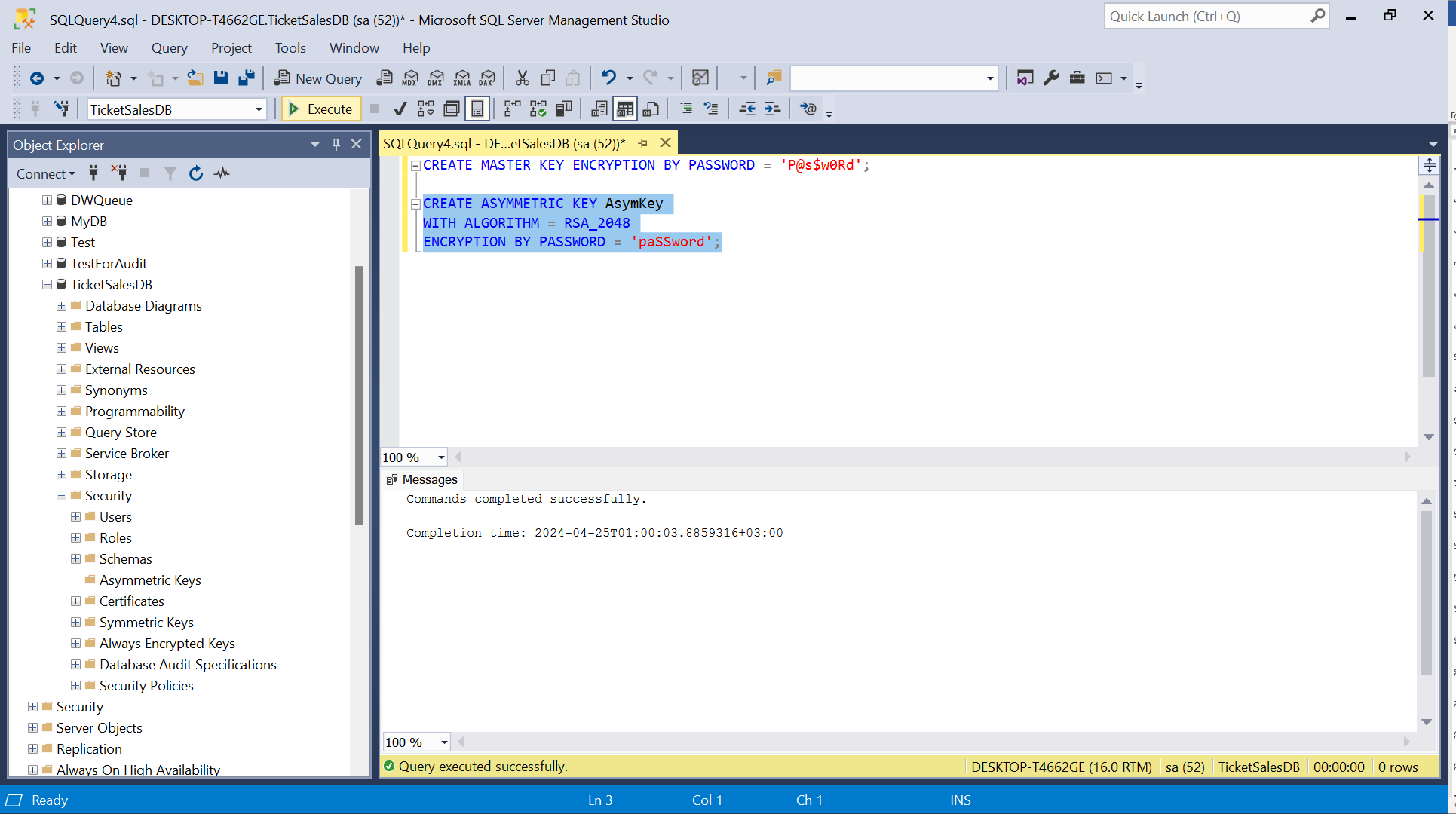
1. Створюємо таблицю в базі даних, в якій будуть міститися зашифровані дані – паролі користувачів.



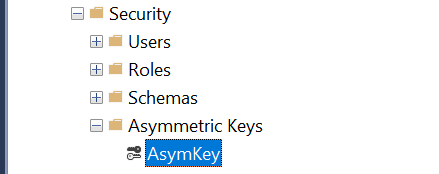
1. Створюємо головний ключ БД.



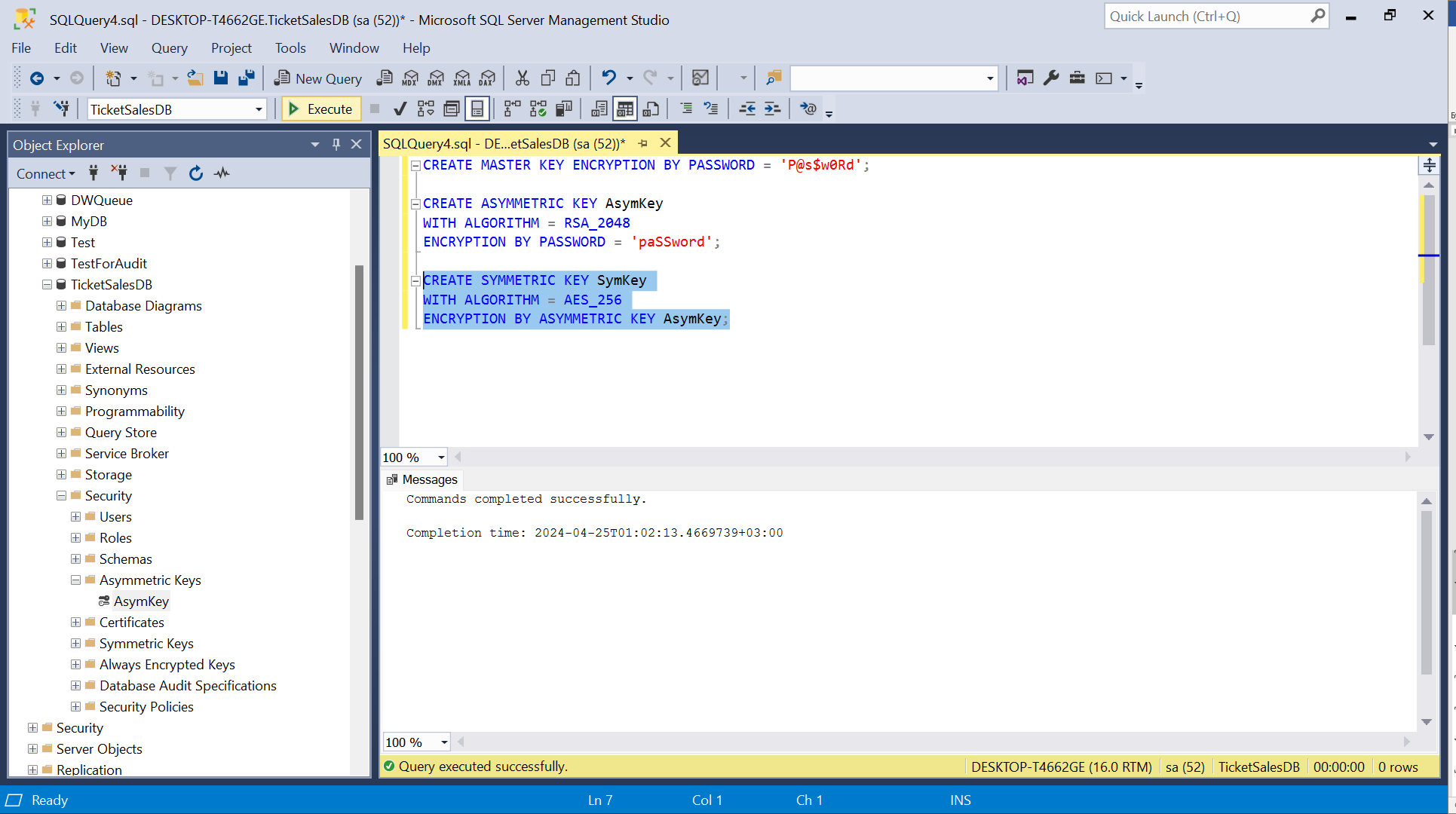
1. Створюємо асиметричний ключ, який зашифрований парольною фразою, за допомогою команди CREATE ASYMMETRIC KEY з алгоритмом шифрування RSA\_2048.



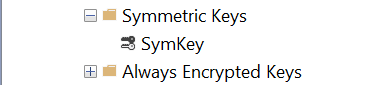
Створений ключ можна переглянути у вкладці бази даних Security => Asymmetric Keys.



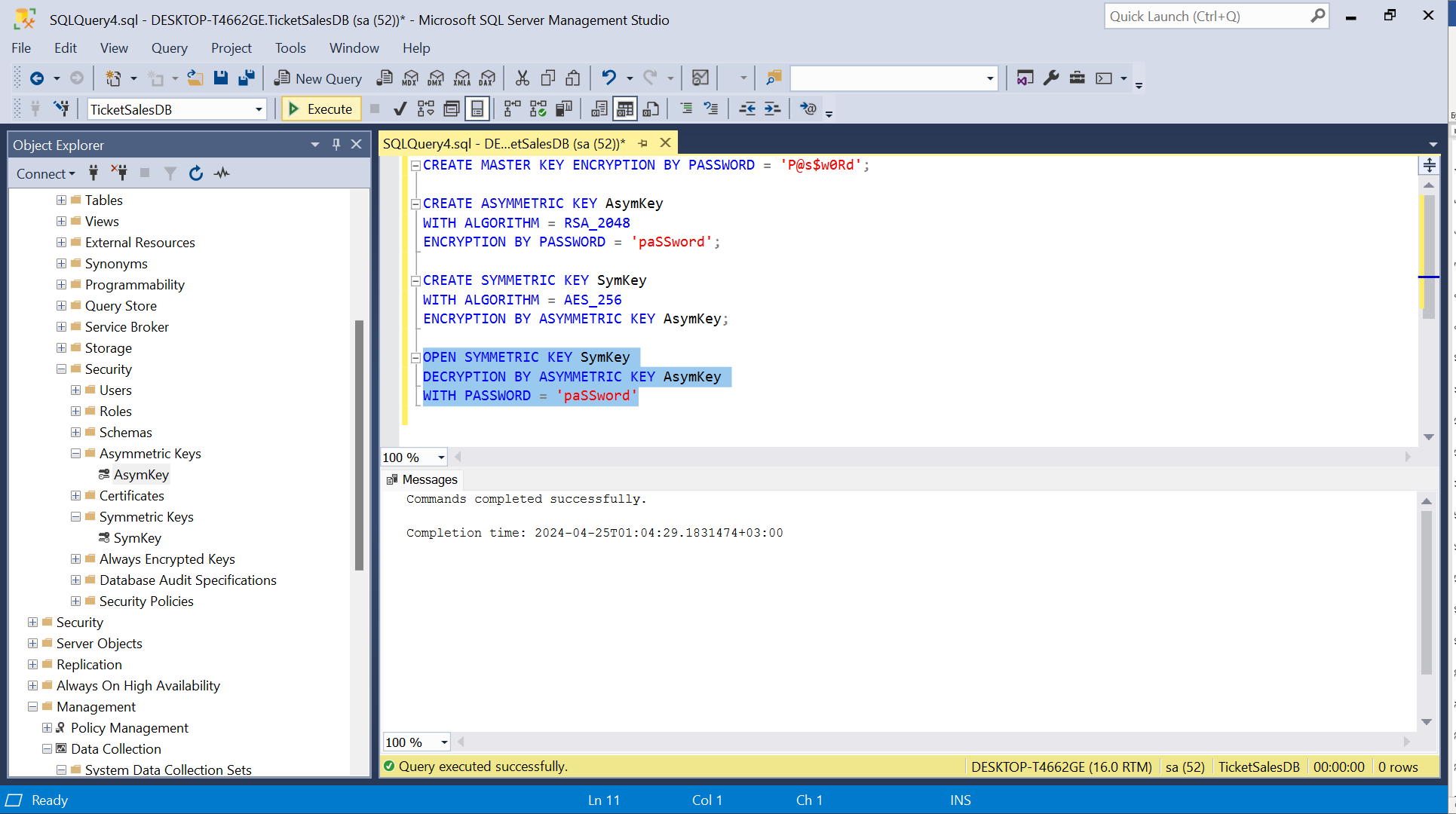
1. Створюємо симетричний ключ, який зашифрований асиметричним, за допомогою команди CREATE SYMMETRIC KEY з алгоритмом шифрування AES\_256.



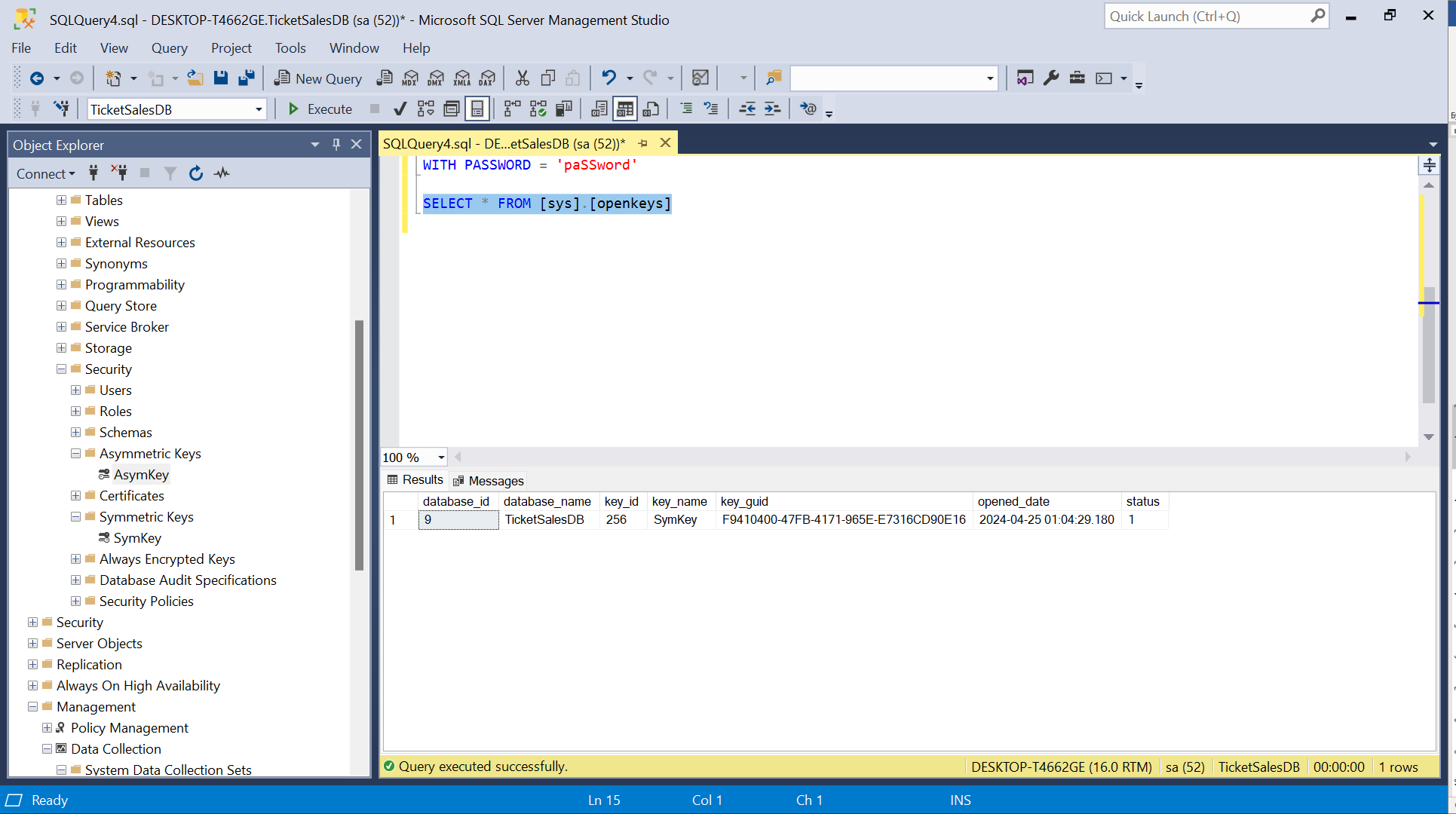
Переглянути його можна у вкладці бази даних Security => Symmetric Keys



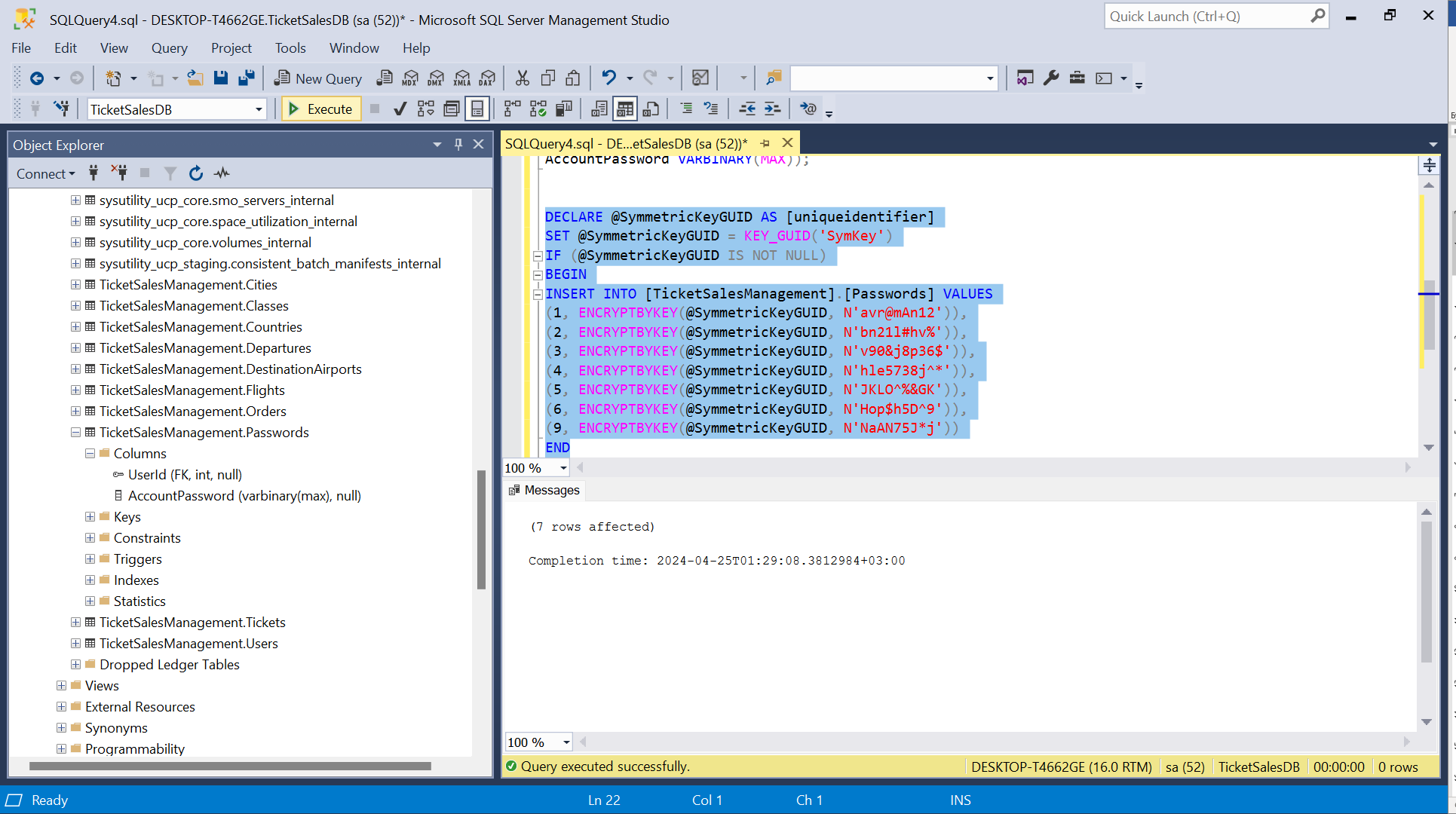
1. Відкриваємо симетричний ключ за допомогою команди Open Symmetric.



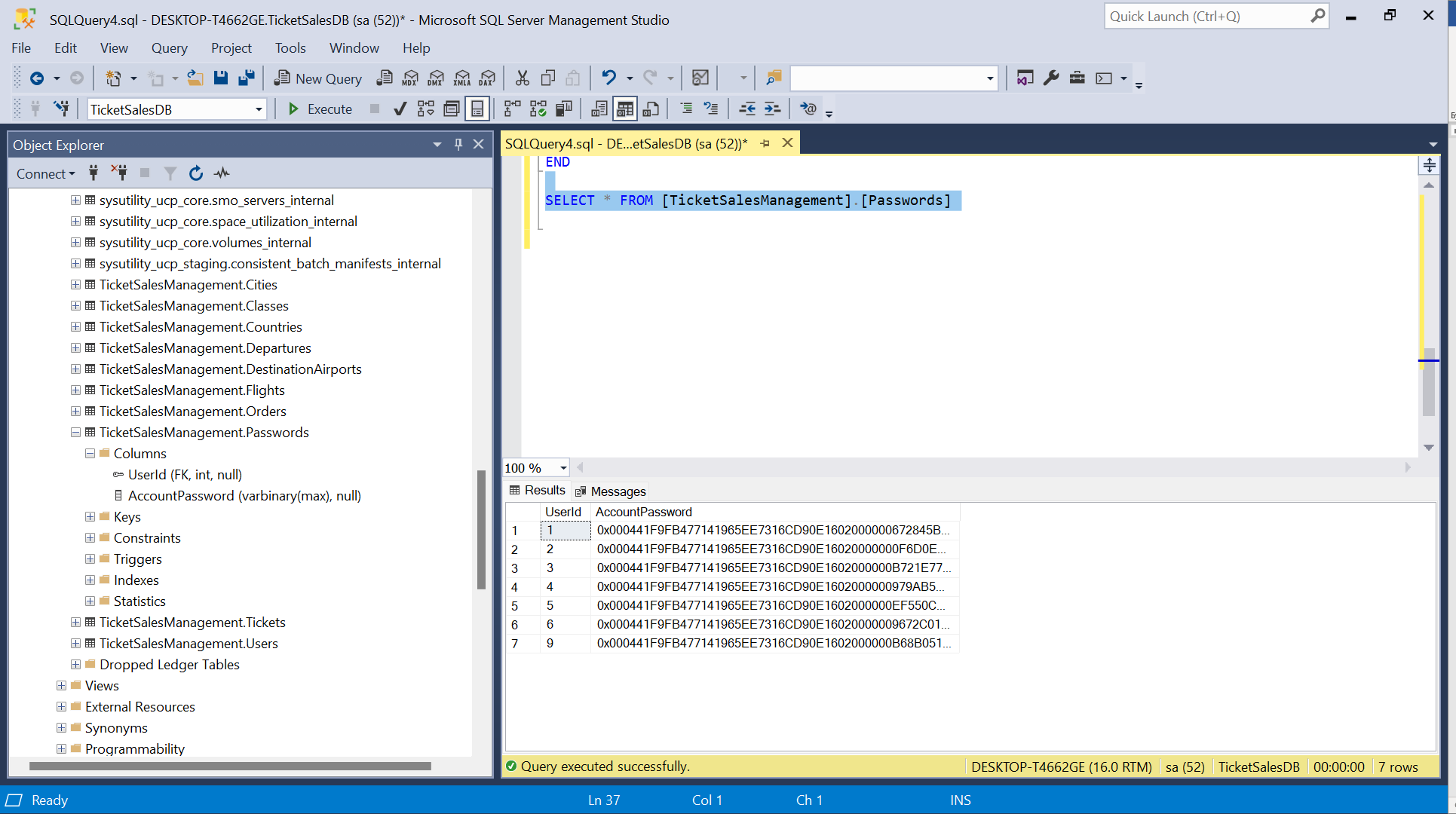
1. Перевіряємо відкриті ключі.



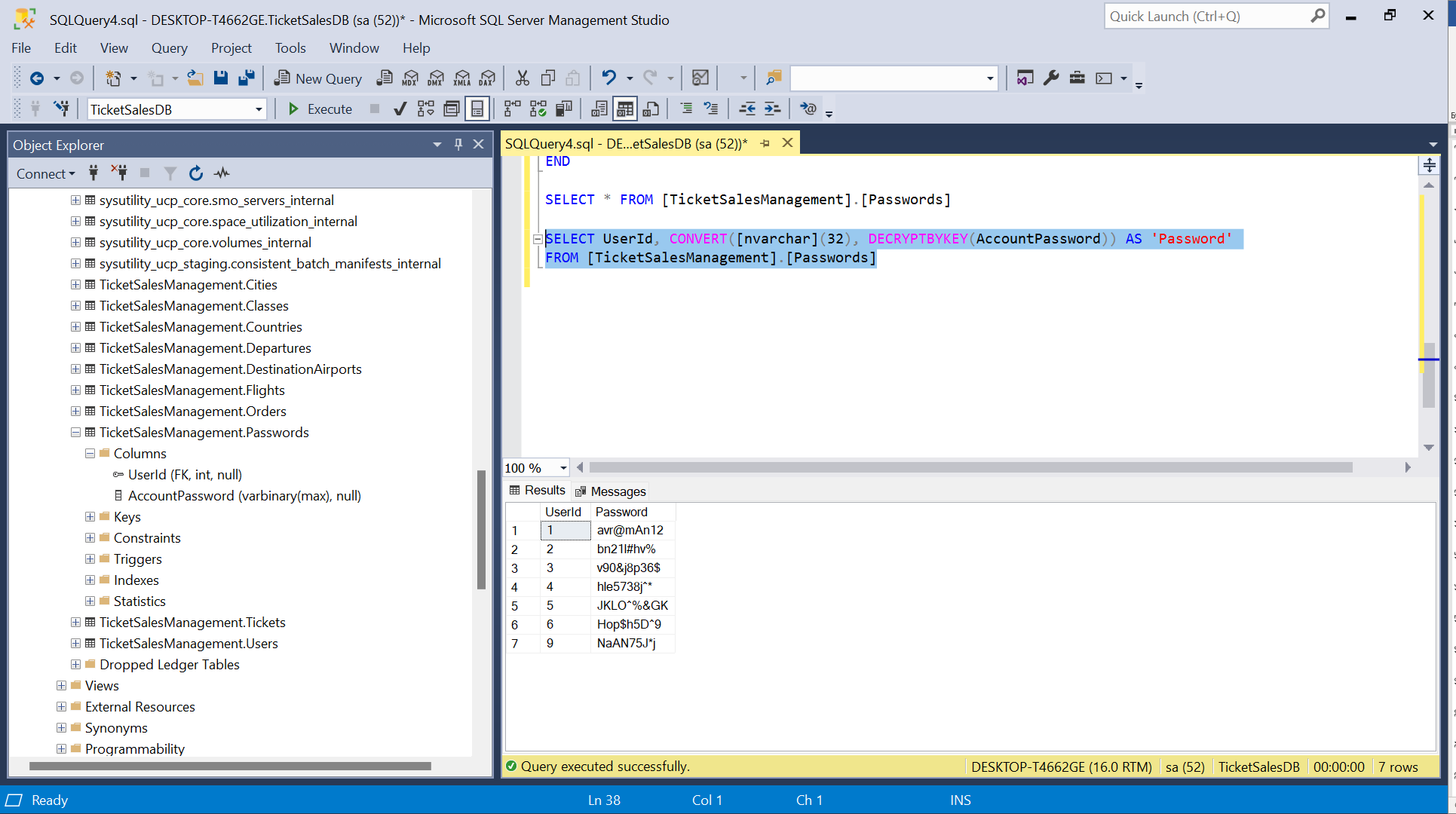
1. Вносимо дані в створену таблицю, зашифровуючи паролі.



1. Якщо ми виведем дані за допомогою команди SELECT \* FROM, то побачимо паролі в бінарному вигляді.

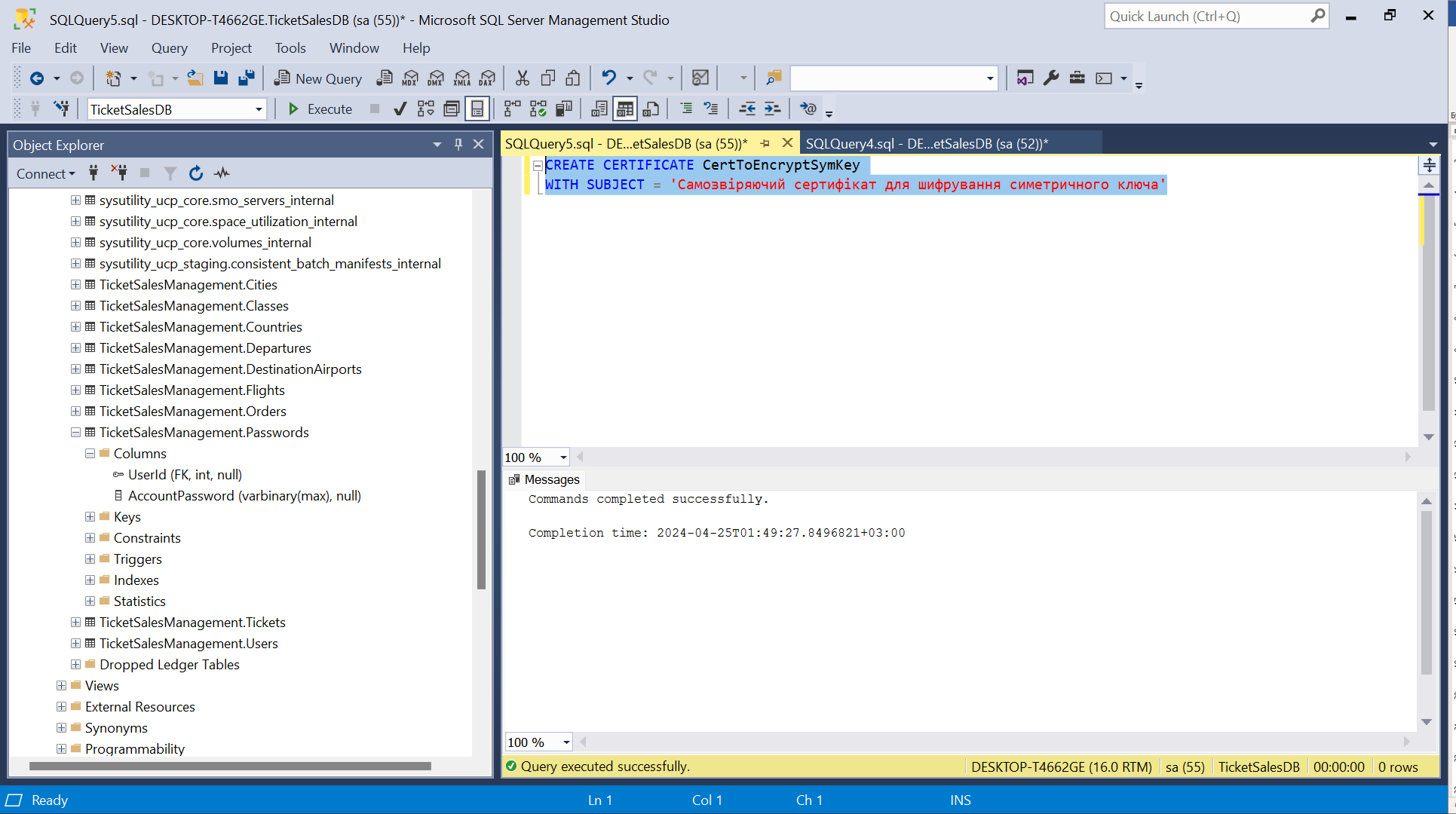


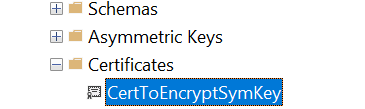
1. Для того, щоб вивести розшифровані дані, потрібно скористатися командою DecryptByKey.



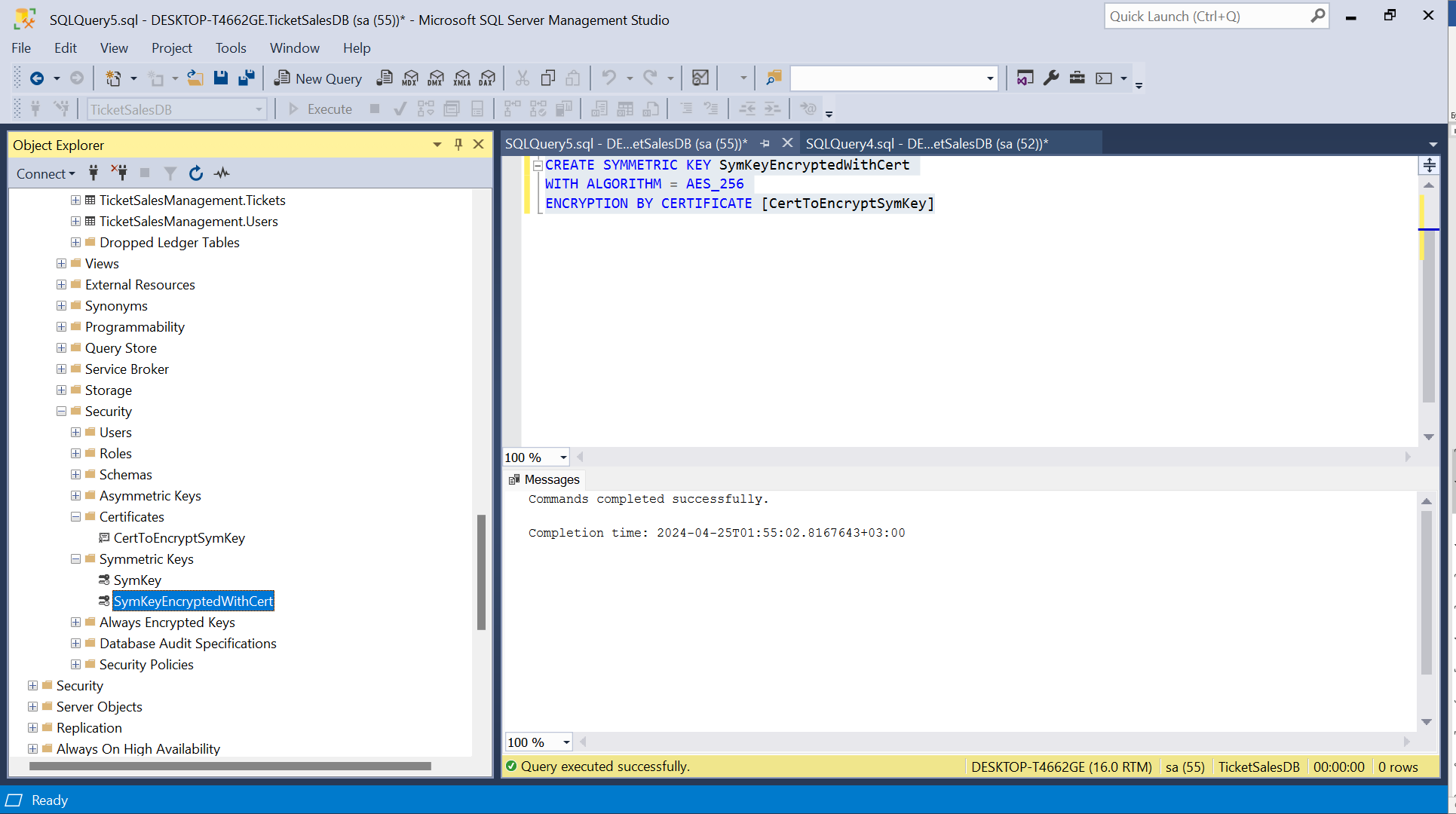
Створення сертифікату для БД

1. Створюємо сертифікат за допомогою команди Create Certificate.

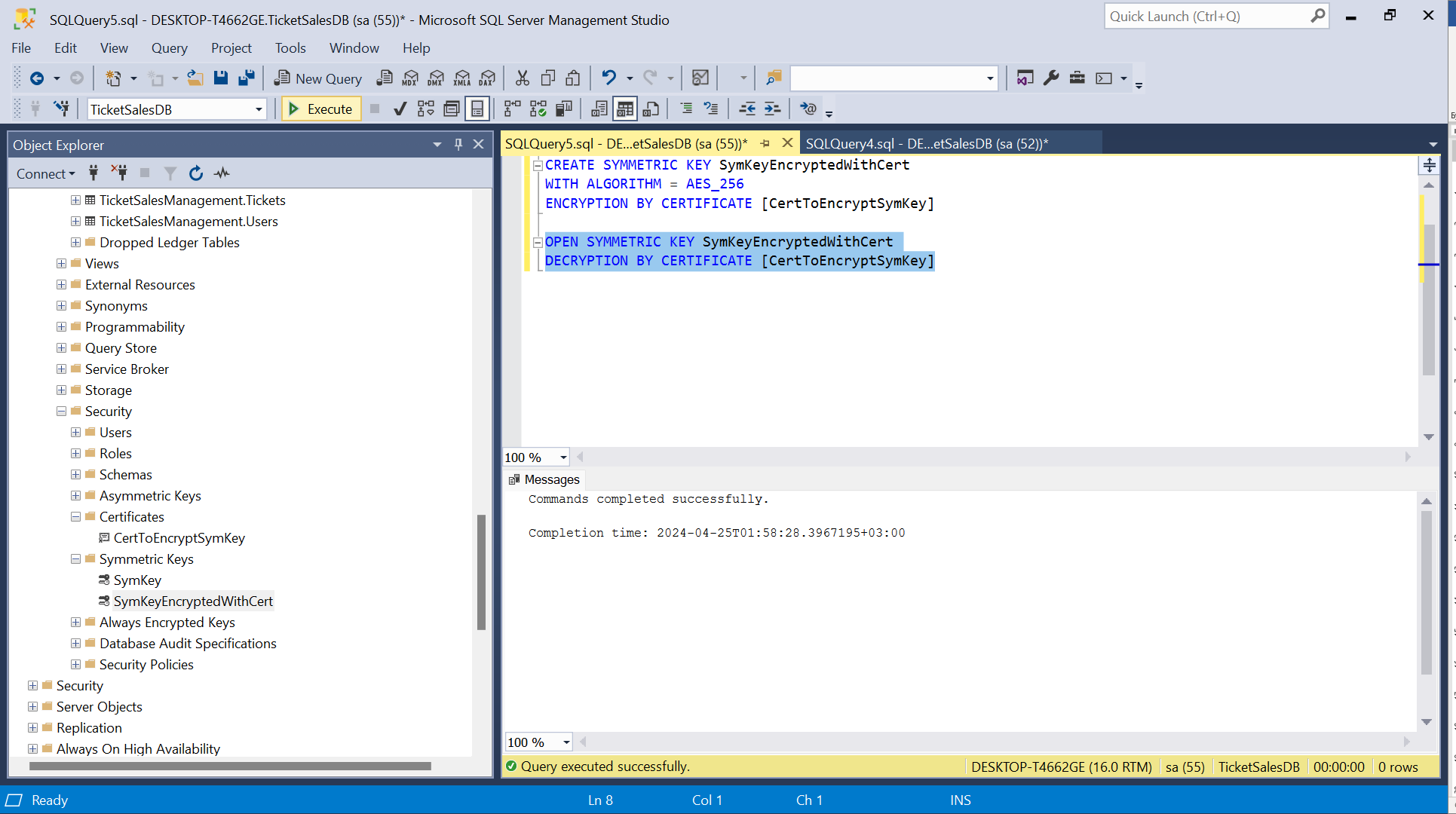




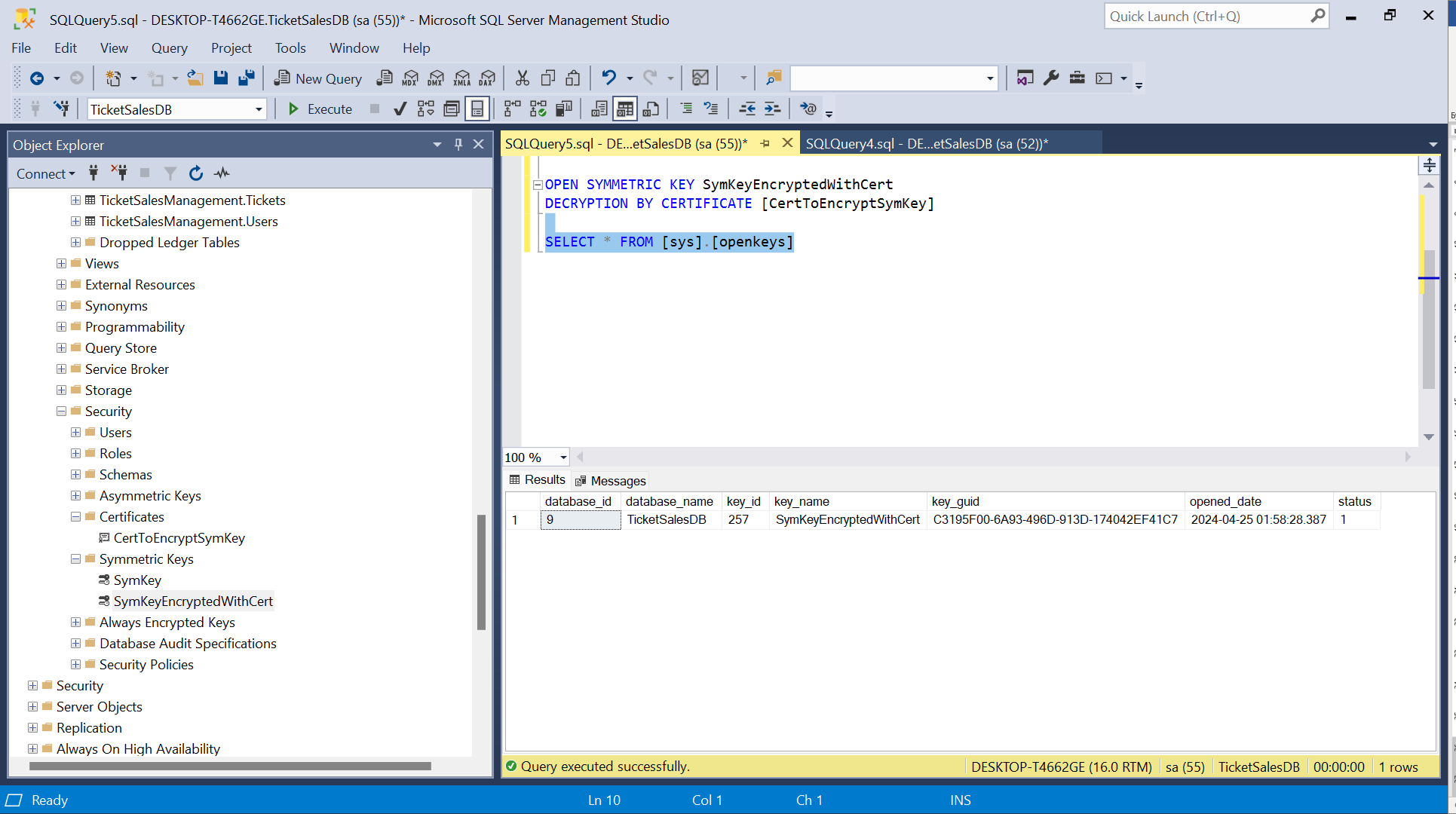
1. Створюємо симетричний ключ, який буде зашифрований сертифікатом



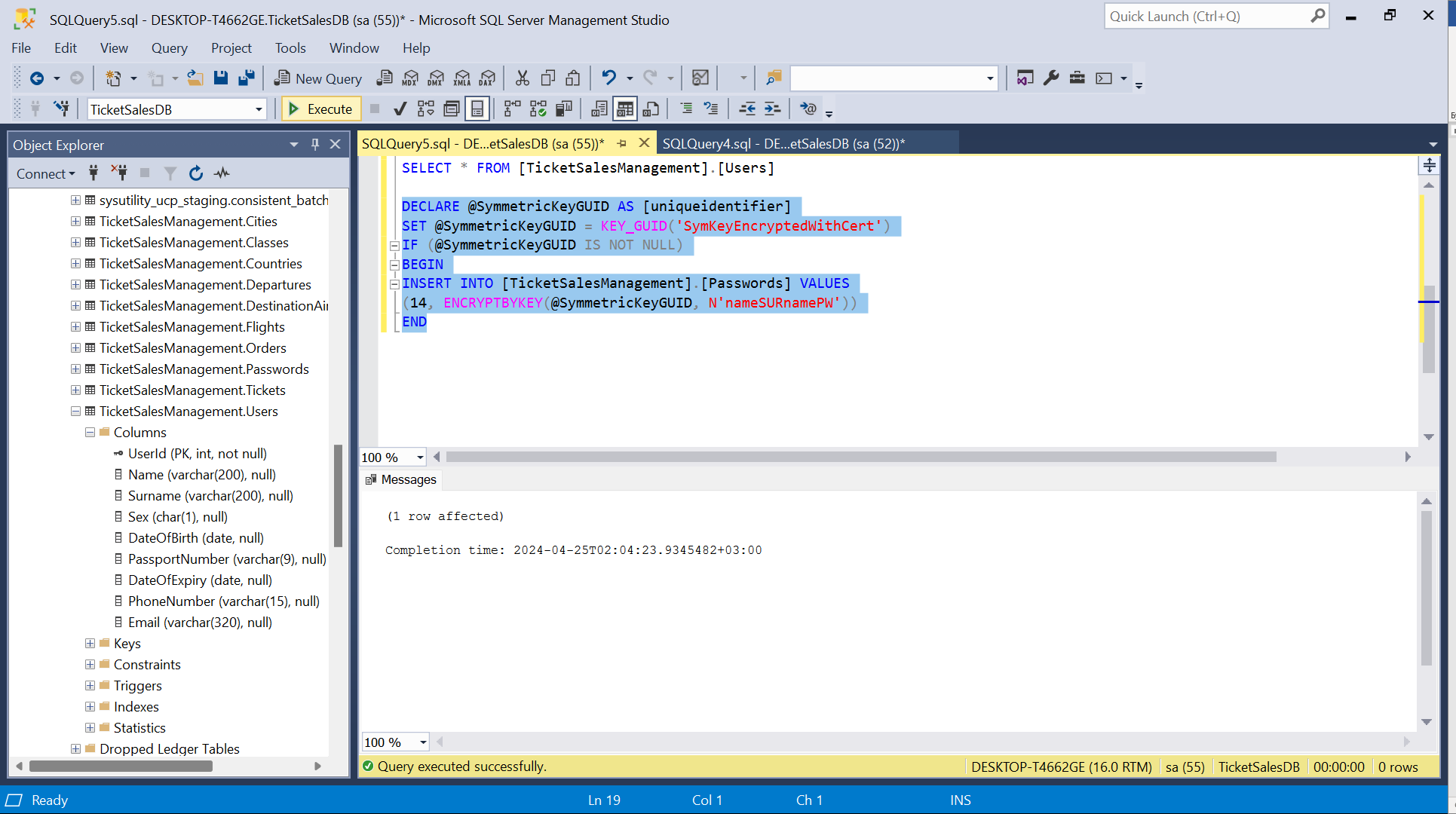
1. Відкриваємо створений ключ та дешифруємо його



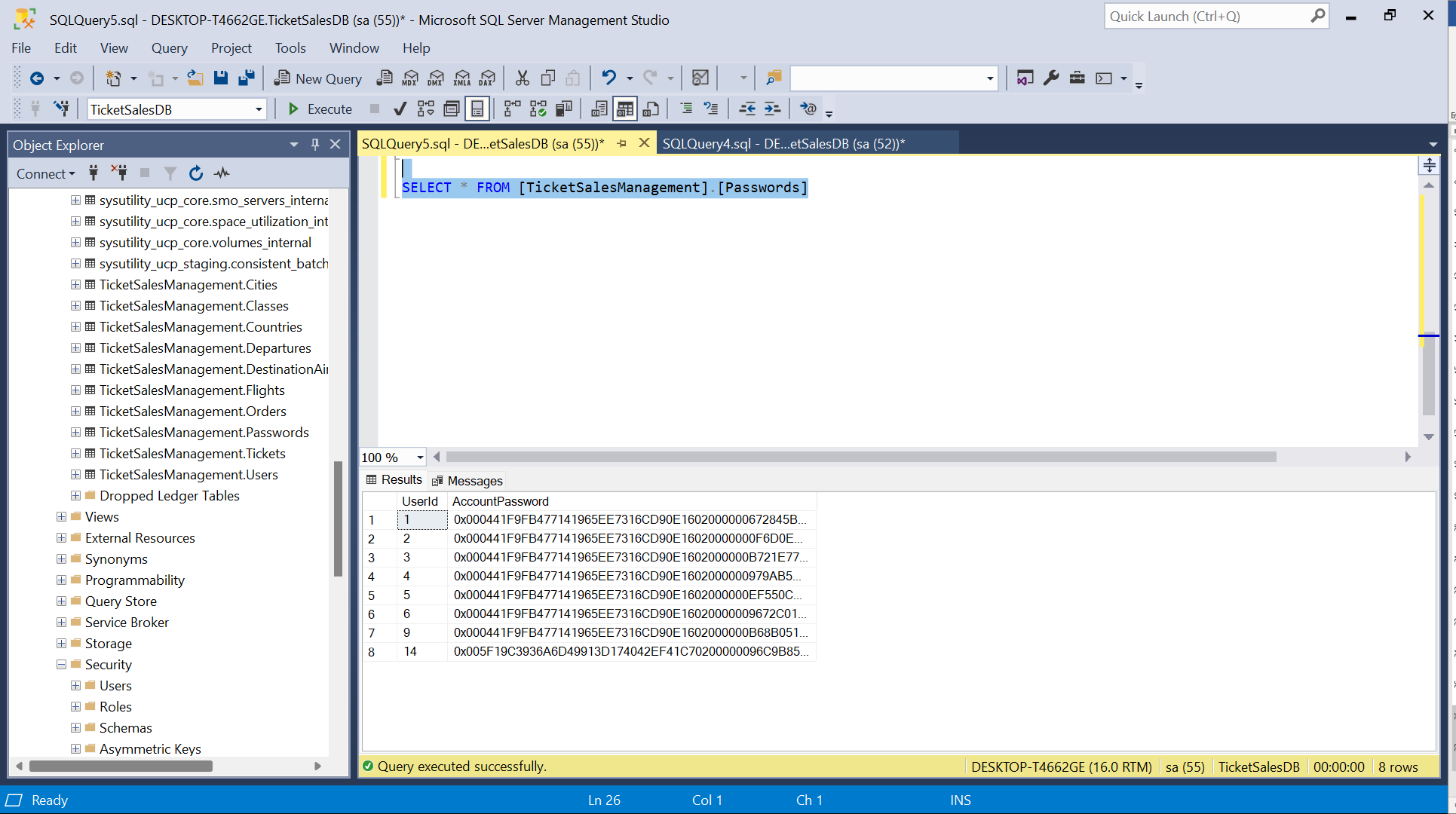
1. Переконуємося, що ключ відкритий.

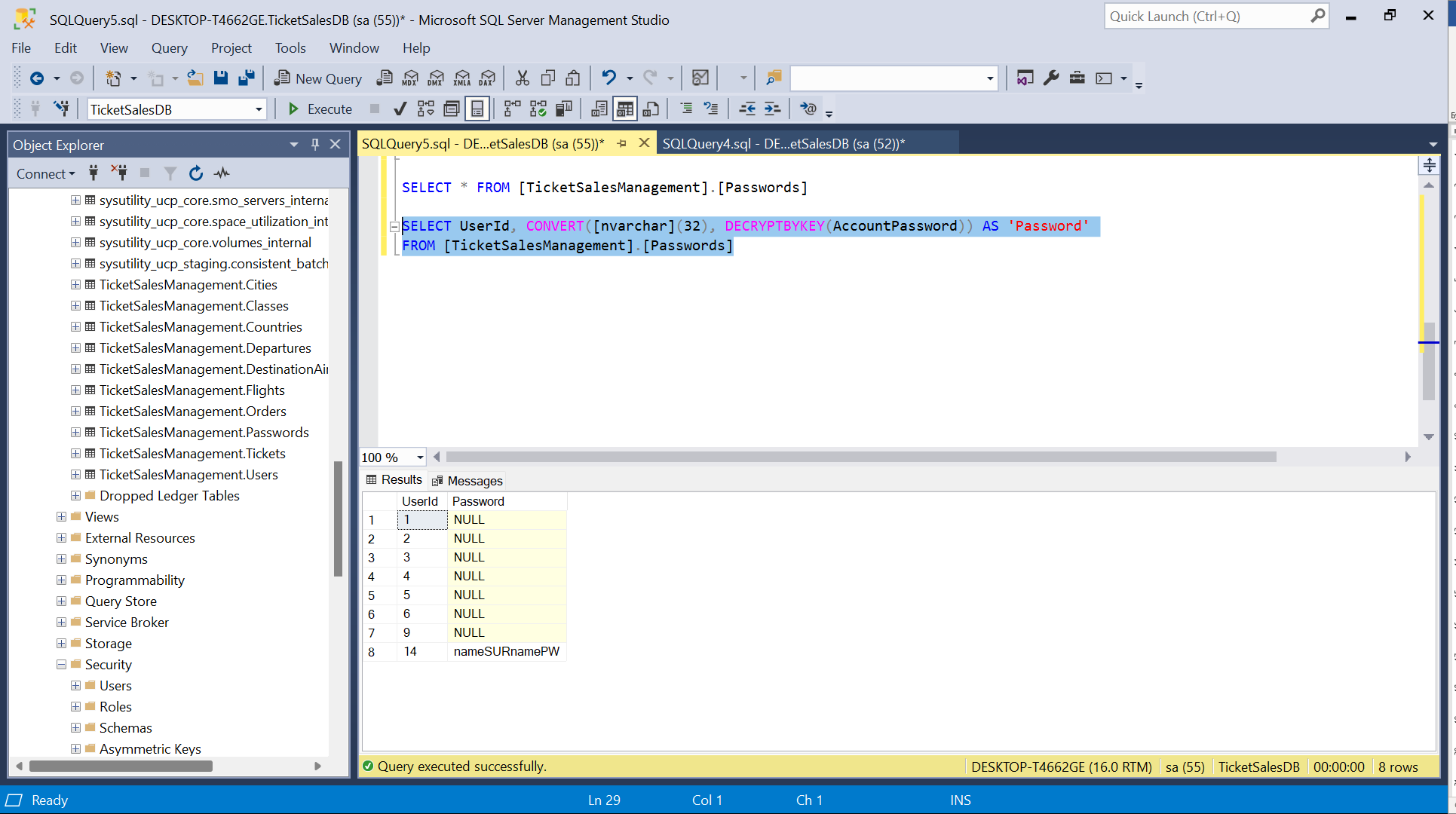


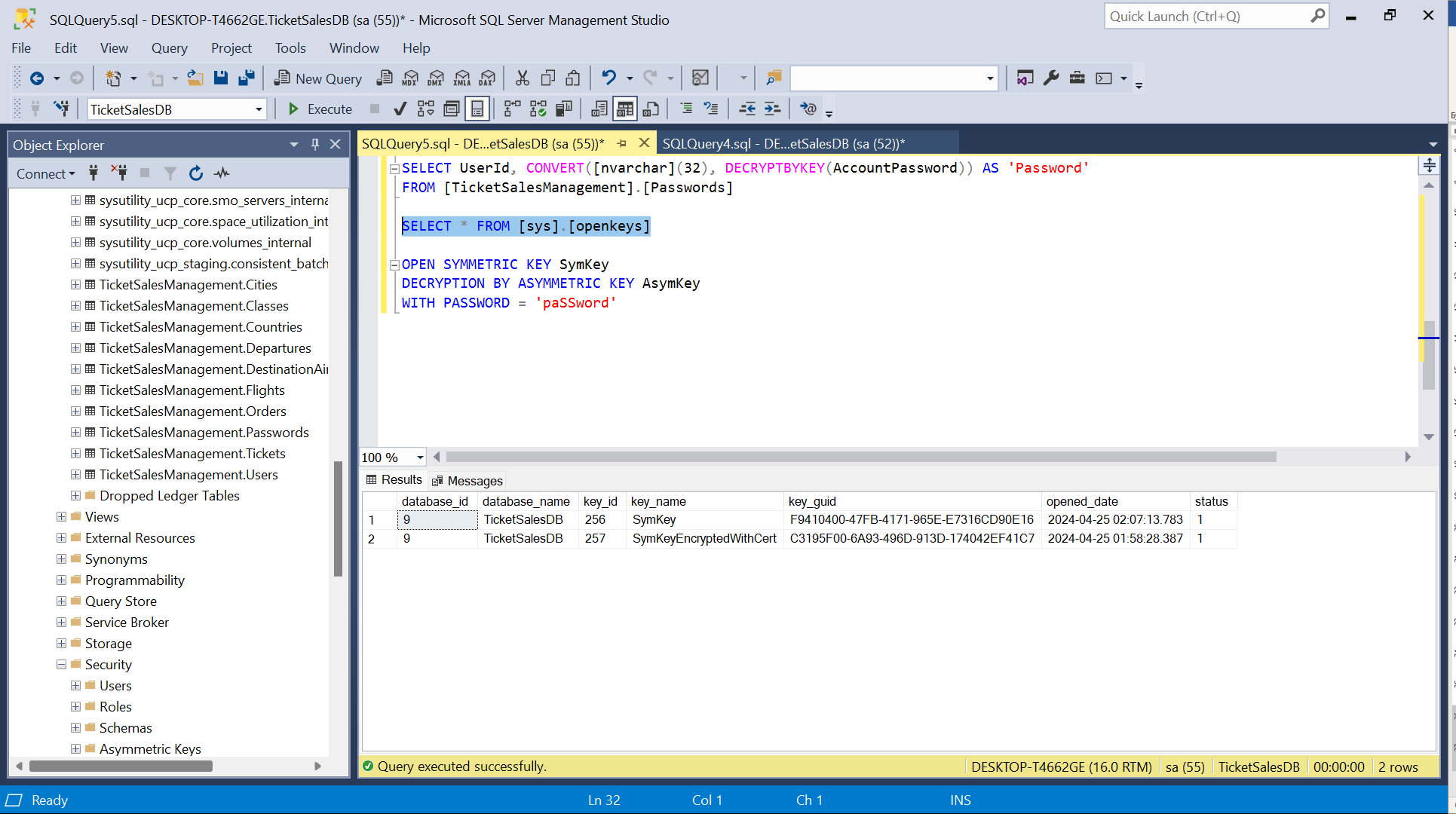
1. Заповнюємо таблицю зашифрованими паролями.



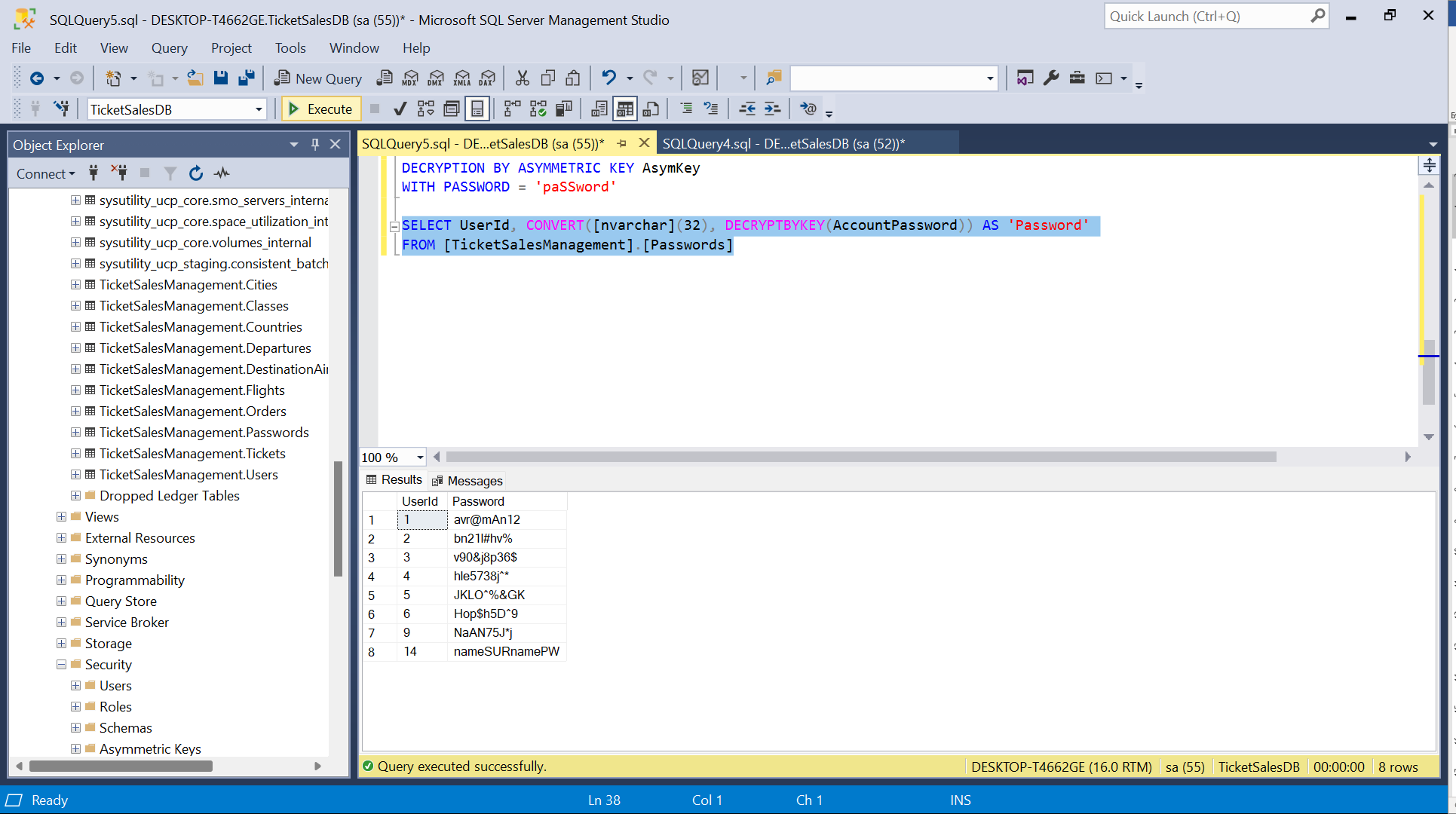
1. Виводимо дані таблиці на екран. Бачимо, що всі паролі зашифровані.



1. Розшифровуємо дані і бачимо, що лише за останнім створеним ключем дані вивелися коректно. 
2. Це означає, що ключ SymKey потрібно відкрити, для того щоб всі дані можна було розшифрувати.

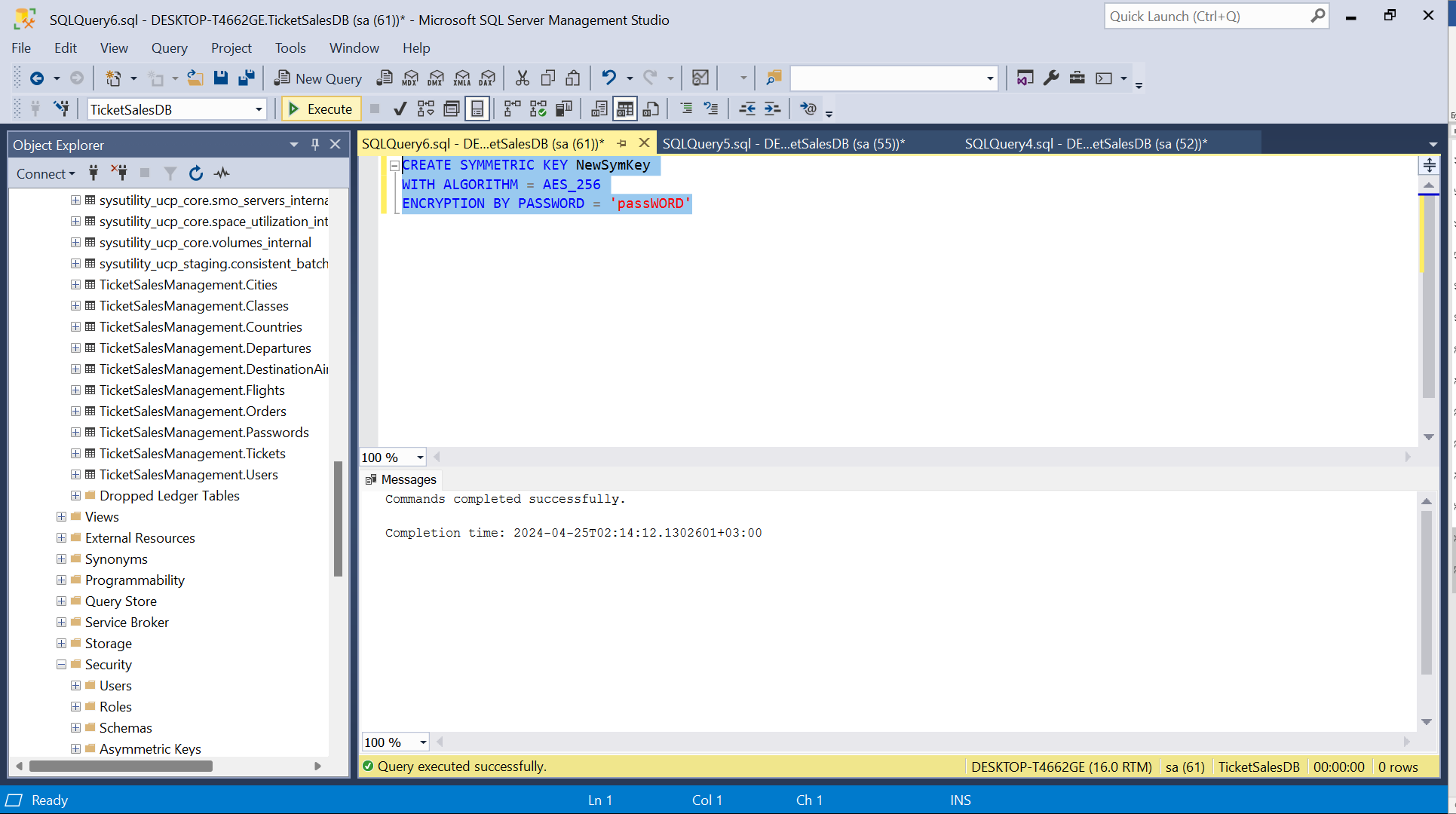


1. Після виконаних дій можемо побачити, що обидва ключі відкриті та розшифровують дані в зрозумілий для користувача вигляд.

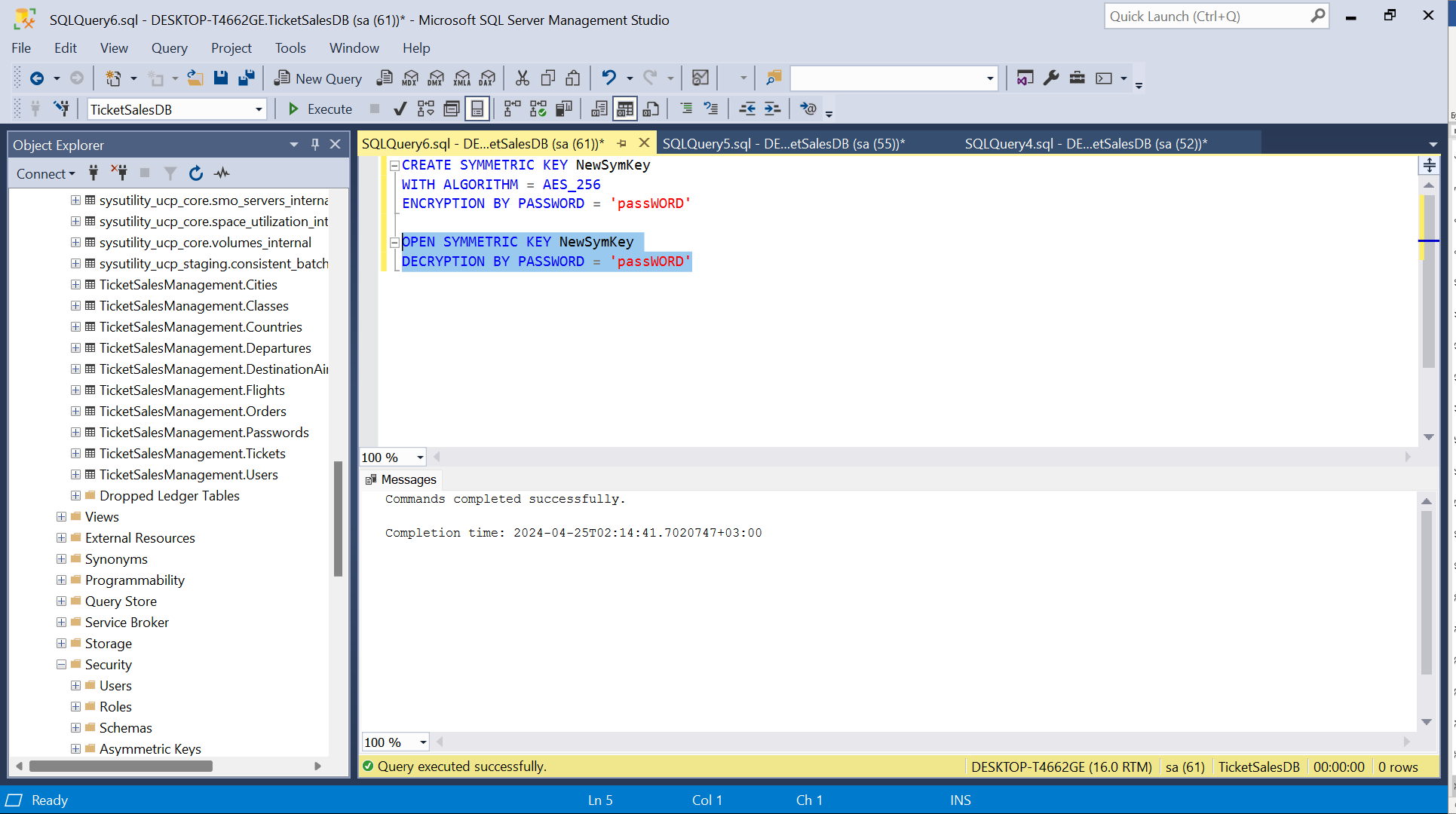


Створення симетричного ключа розробленої БД

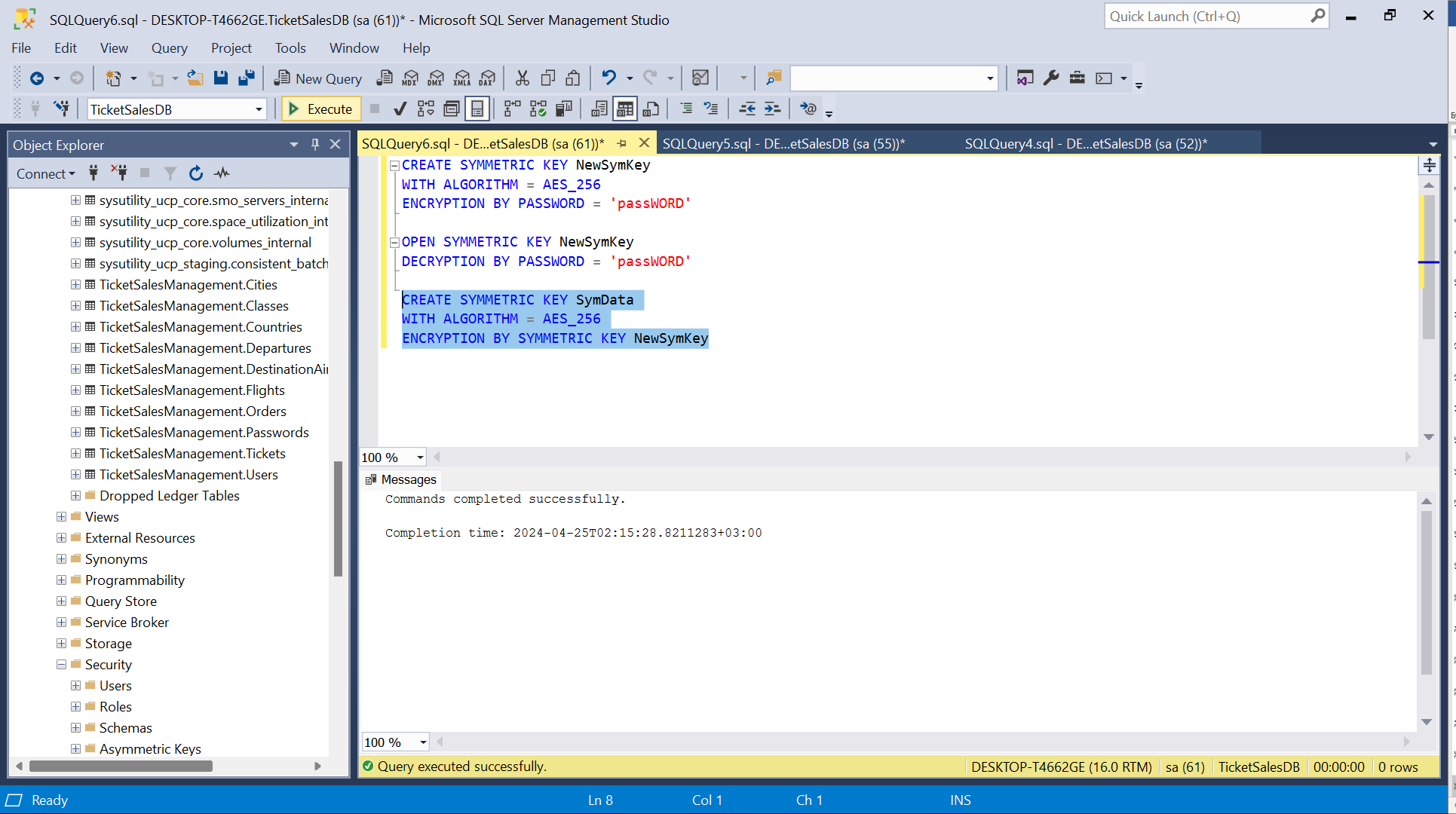
1. Створимо новий симетричний ключ з розшифруванням за допомогою паролю.



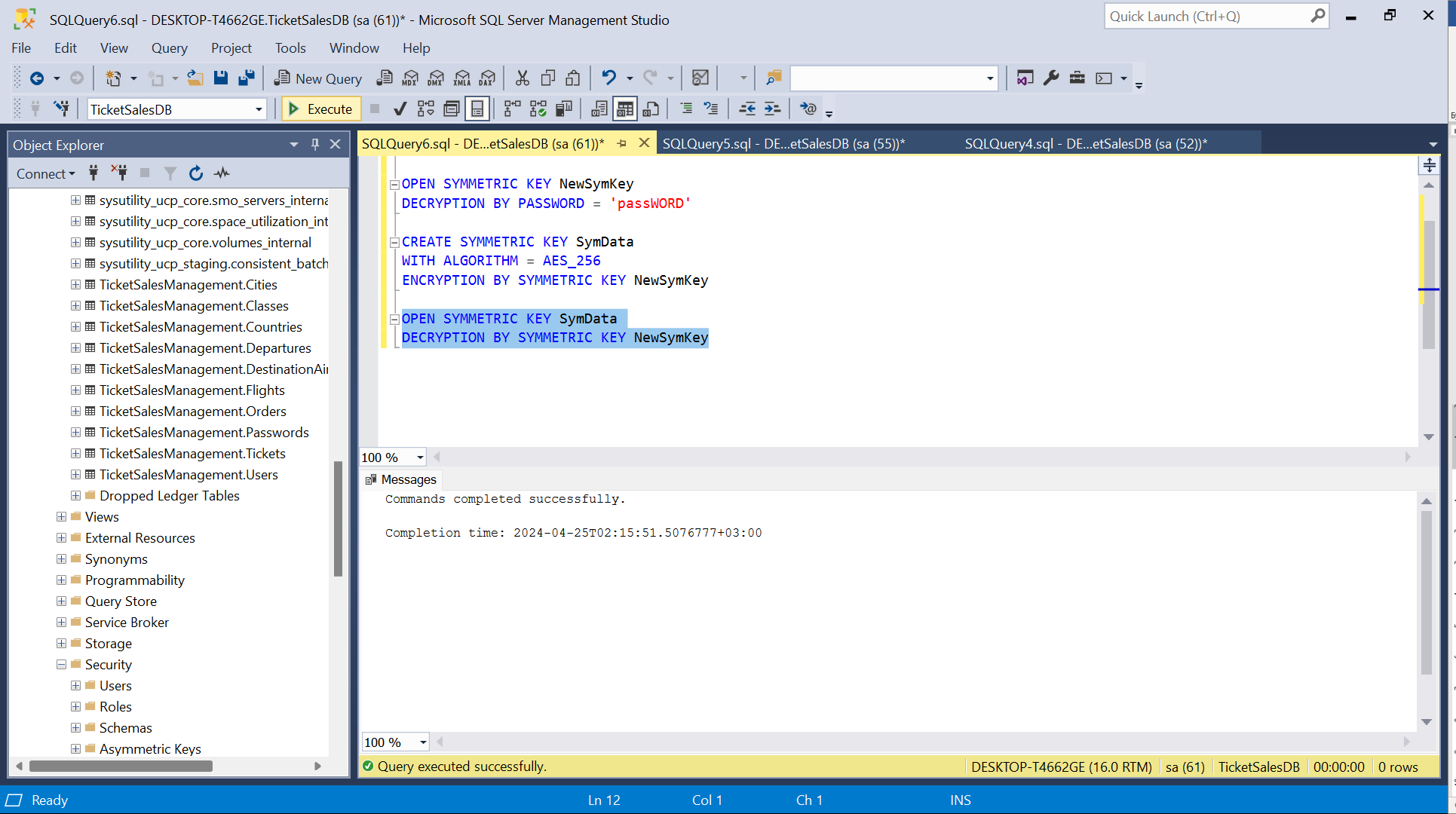
1. Відкриваємо створений ключ.



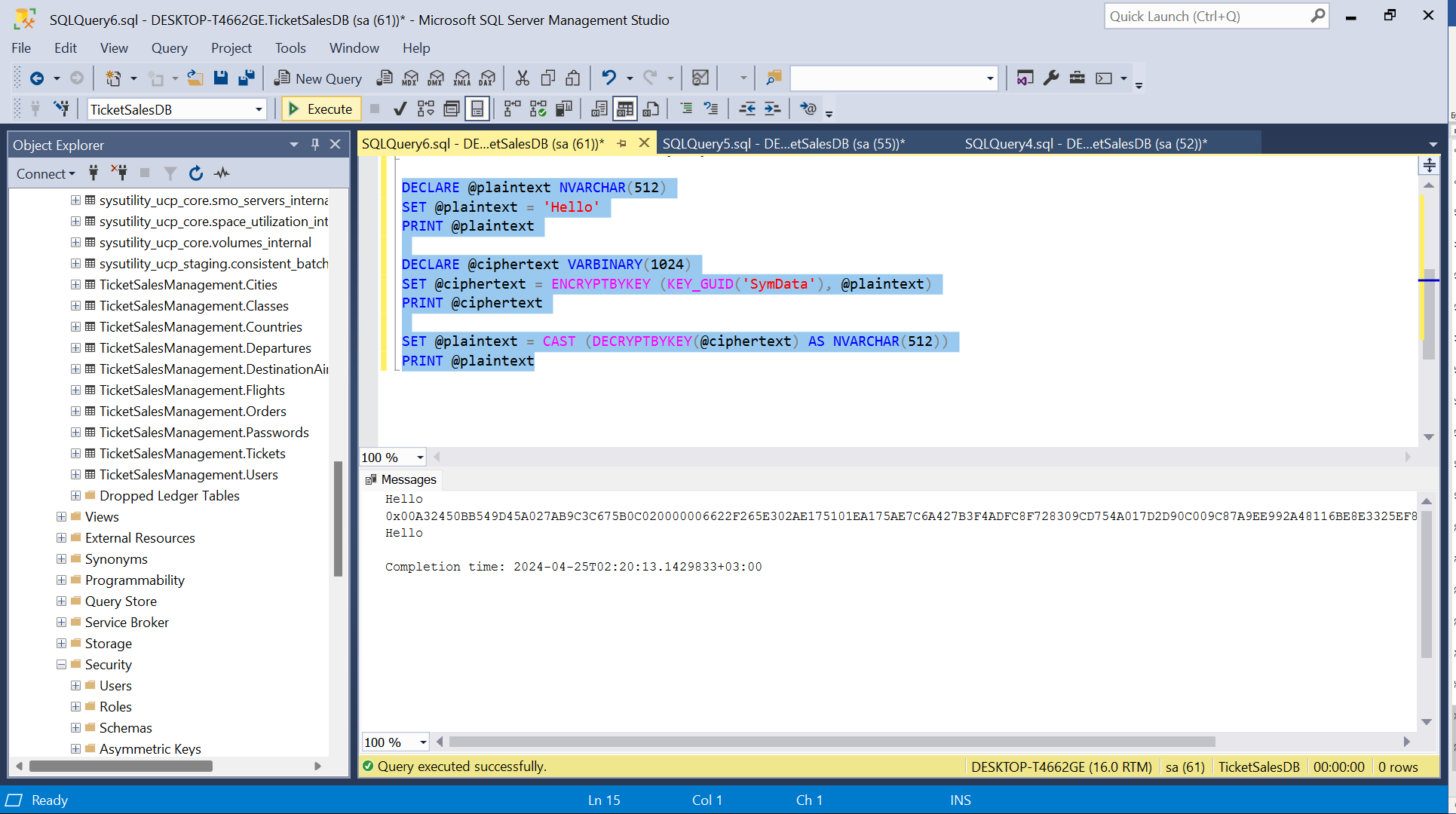
1. Створюємо симетричний ключ, який буде зашифрований іншим симетричним ключем.



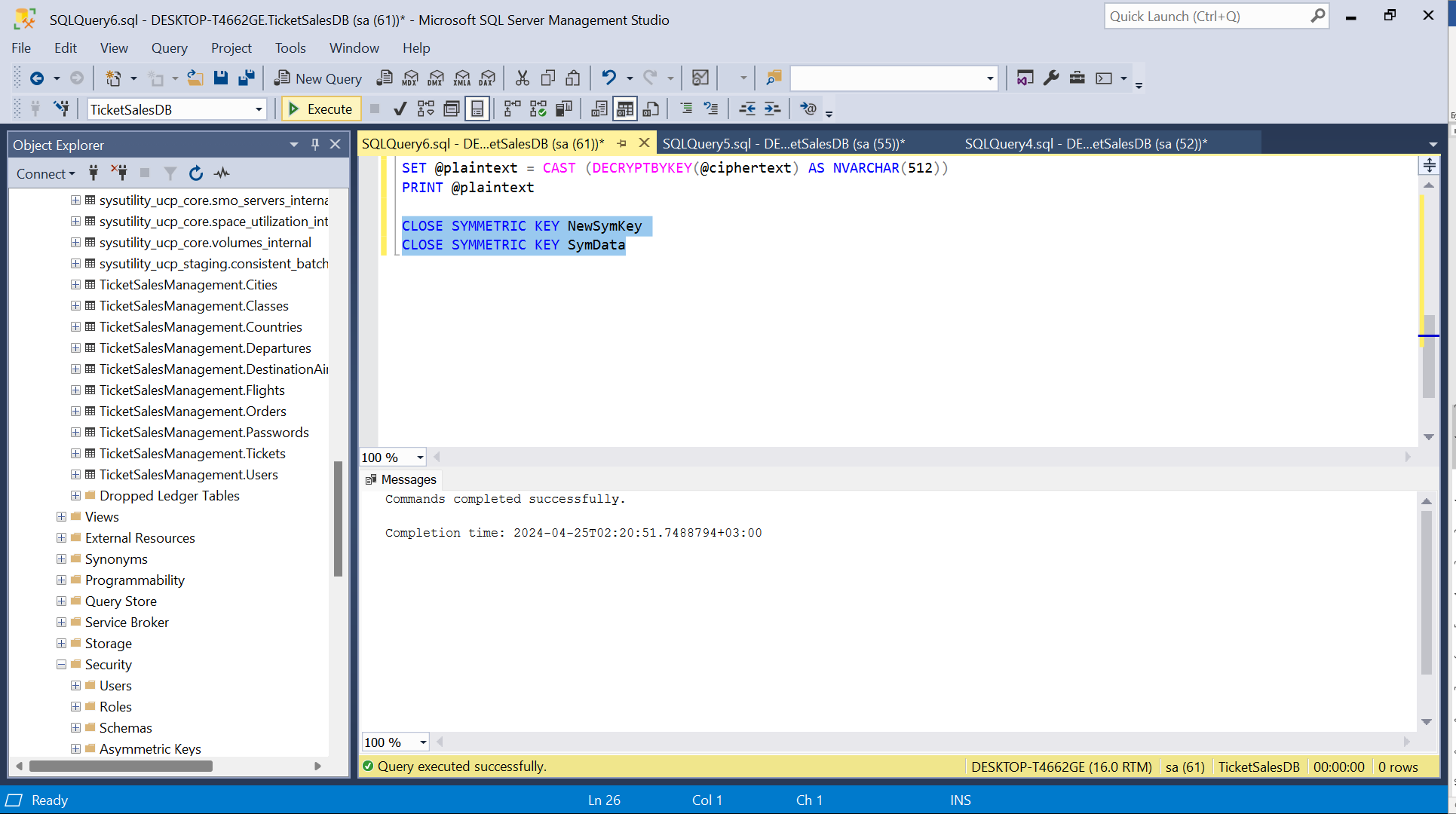
1. Відкриваємо ключ.

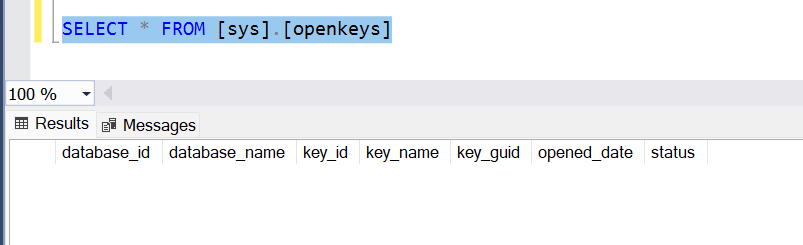
****

1. Створюємо запит на шифрування та дешифрування тексту.



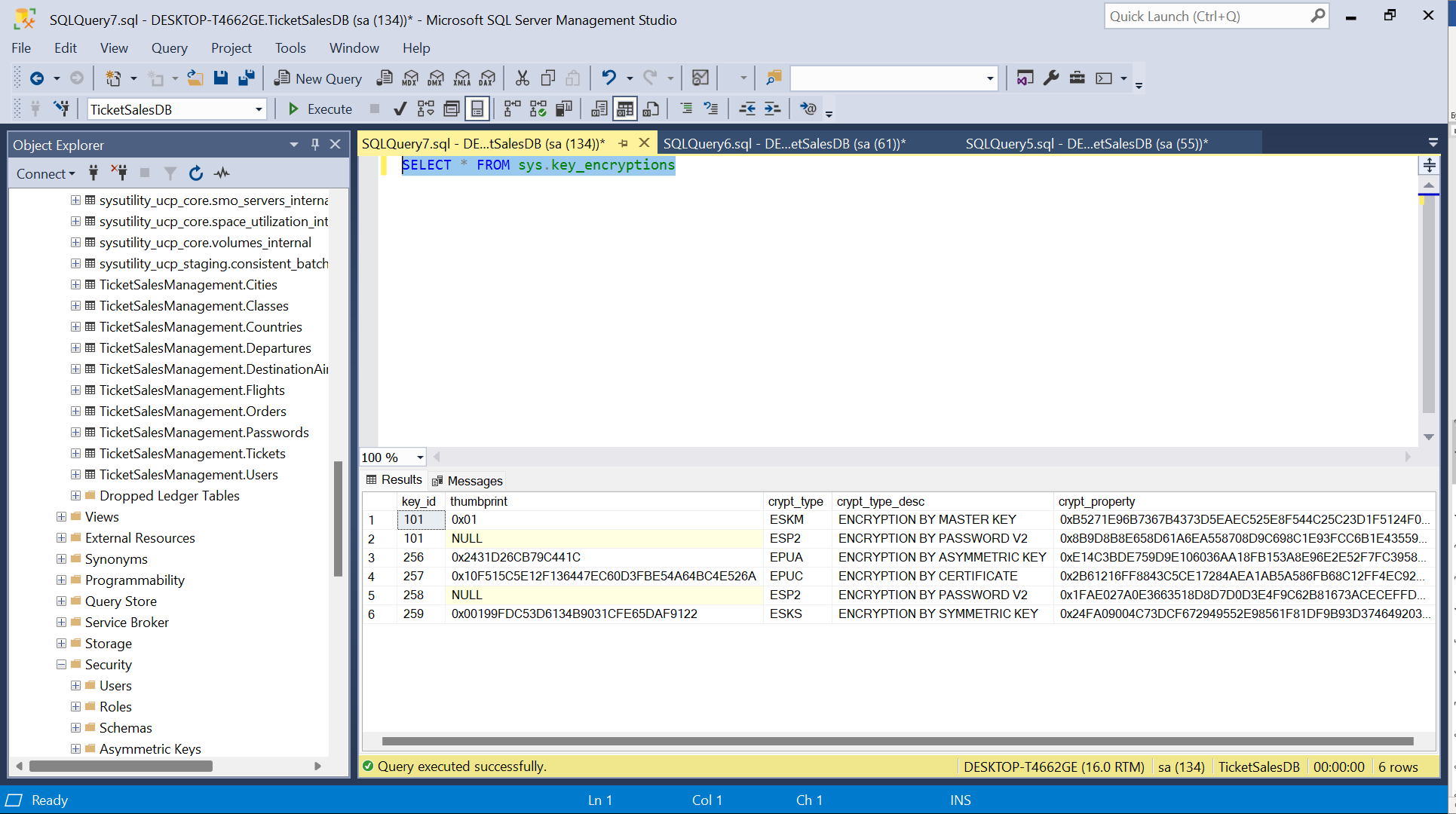
1. Закриваємо ключі.



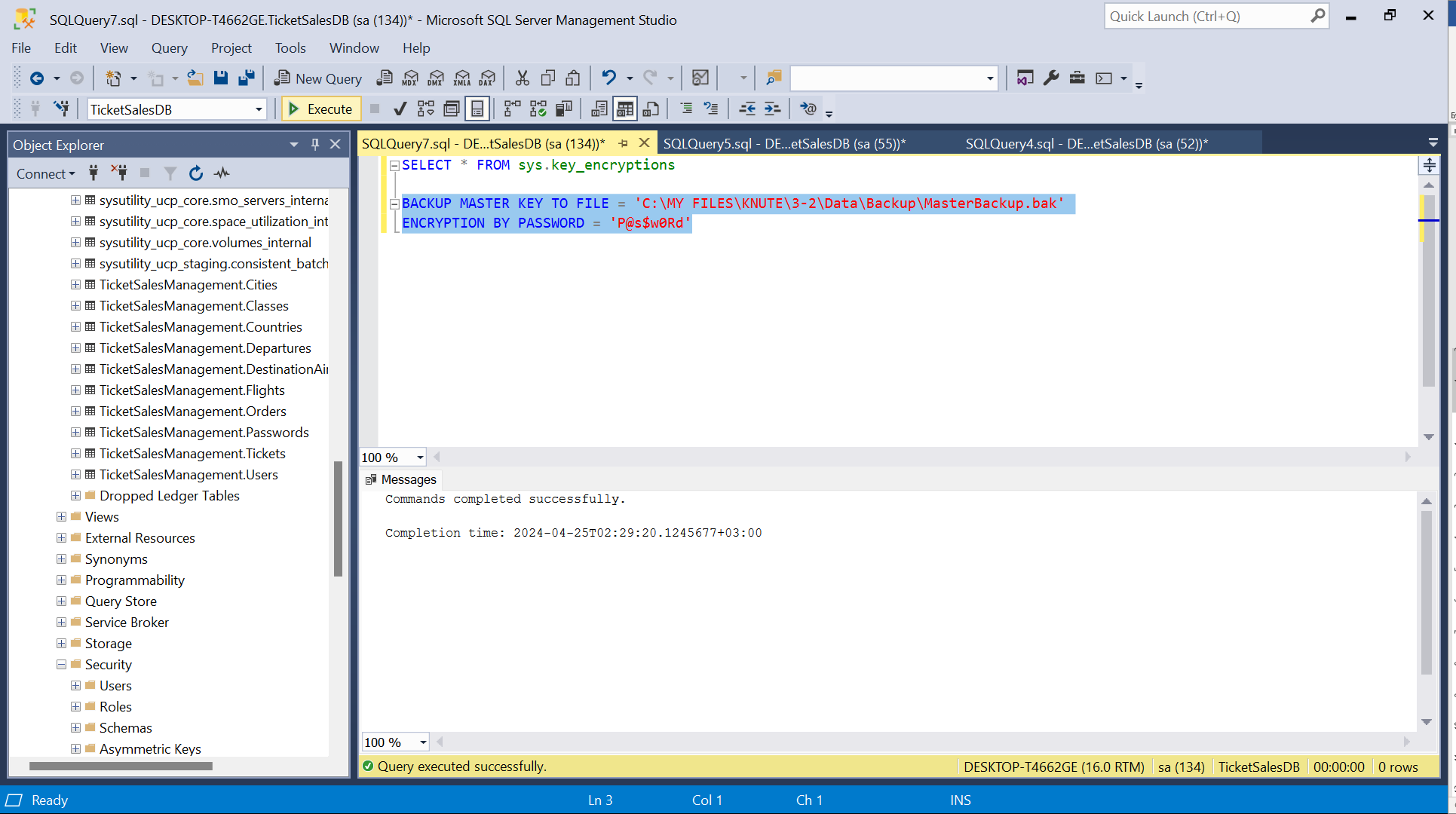


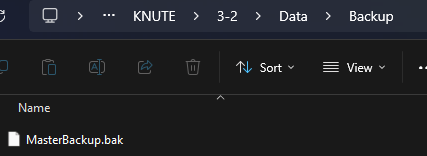
Шифрування БД шляхом прозорого шифрування

1. Переглянемо створені ключі.

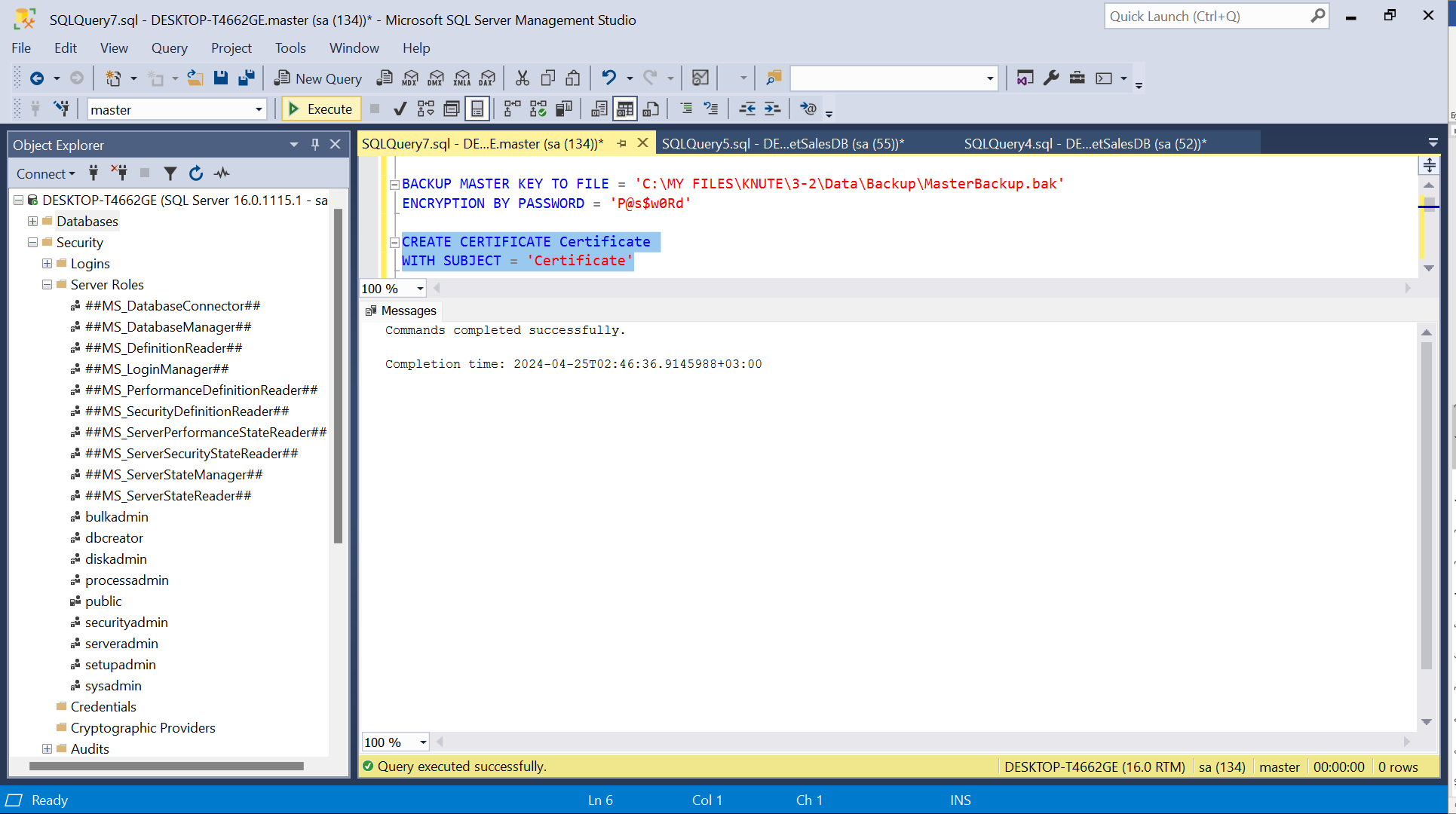


1. Робимо резервне копіювання головного ключа.



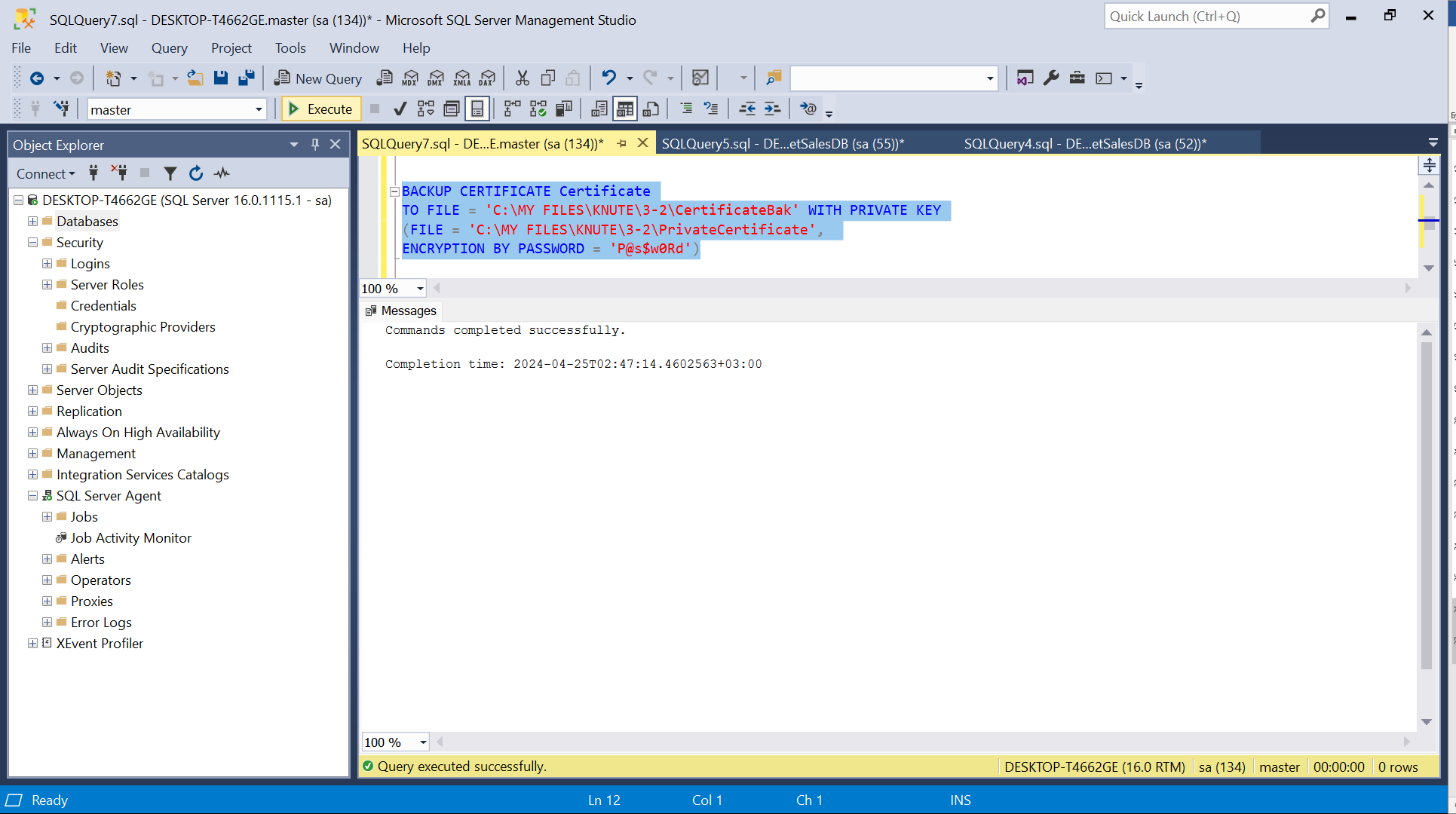


1. Створюємо серверний сертифікат

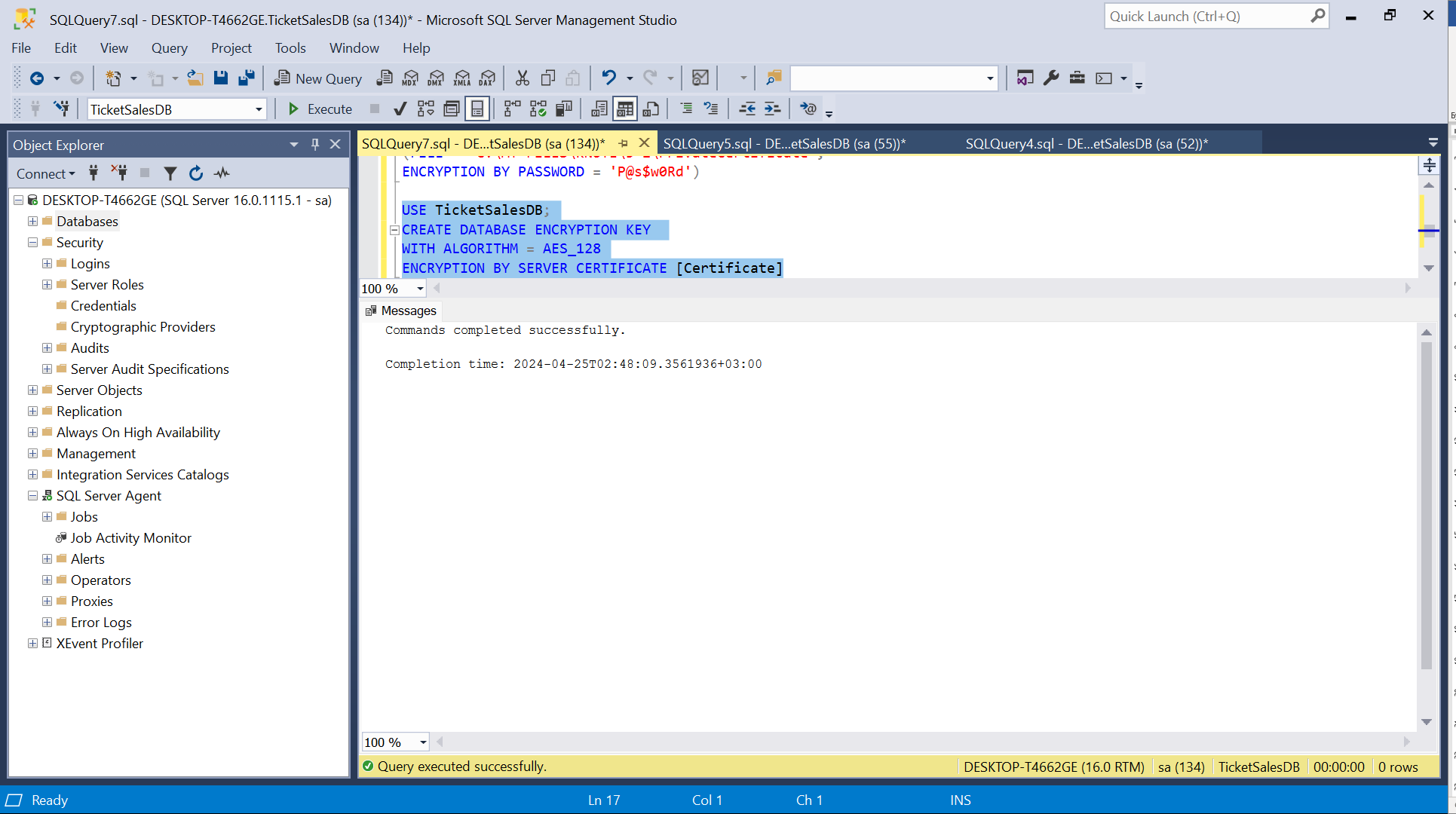


****

1. Робимо резервне копіювання сертифіката із закритим ключем.



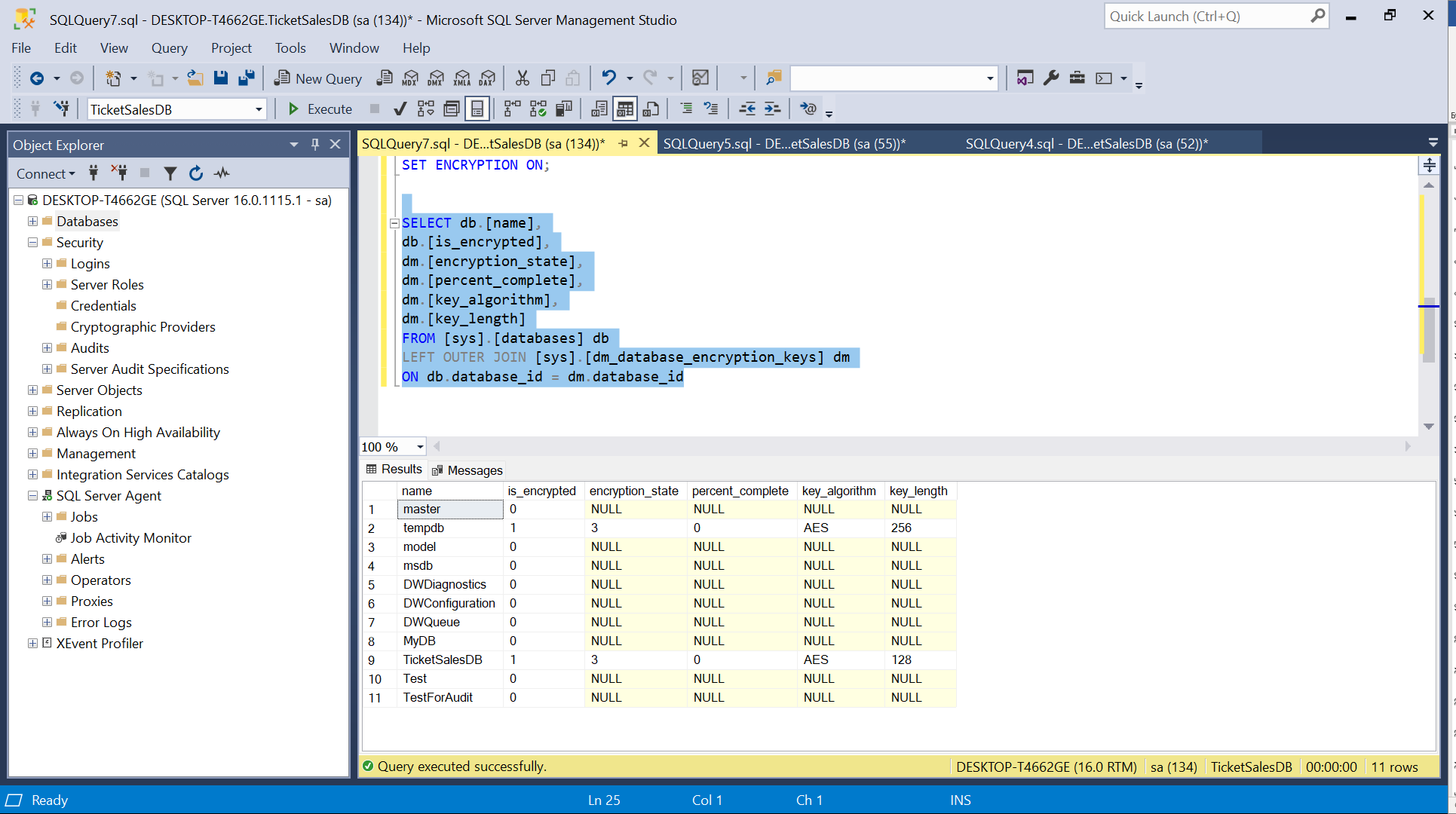
1. Створюємо ключ шифрування в базі даних.



1. Вмикаємо шифрування за допомогою команди SET ENCRYPTION ON



1. Виводимо на екран зашифровані бази даних.



**Висновок**: в ході виконання лабораторної роботи було набуто практичних навичок з шифрування бази даних, а саме створення асиметричних та симетричних ключів, сертифікатів шифрування. А також було зашифровано власну базу даних шляхом прозорого шифрування.