بسم الله الرحمن الرحیم

آموزشگاه تحلیل داده

تخصصی ترین مرکز برنامه نویسی و دیتابیس در ایران

رمزگذاری اطلاعات در SQL Server

مدرس : مهندس افشین رفوآ

دوره آموزش SQL Server Administration

رمزگذاری اطلاعات در SQL Server

SQL Server توابعی را ارائه می دهد که با بهره گیری از certificate (گواهینامه)، کلید نامتقارن و یا کلید متقارن، اطلاعات را رمزگذاری/رمزگشایی نماید. SQL Server تمامی این کارها را در یک certificate store داخلی مدیریت می کند. certificate store از یک سلسله مراتب رمزگذاری بهره می گیرد که کلیدها و certificate ها را در یک سطح با لایه ی بالایی خود در سلسله مراتب secure می کند. این بخش از SQL Server، Secret Storage خوانده می شود.

سریع ترین روش رمزگذاری که توسط توابع encryption پشتیبانی می شود، رمزگذاری با استفاده از کلید متقارن (symmetric key encryption) می باشد. این روش بهترین گزینه برای مدیریت حجم بزرگی از داده ها تلقی می شود. کلیدهای متقارن را می توان با بهره گیری از certificate ها، گذورواژه ها یا دیگر کلیدهای متقارن رمزگذاری نمود.

کلیدها و الگوریتم ها

SQL Server از چندین الگوریتم رمزگذاری پشتیبانی می کند که از جمله ی آن ها می توان به DES، Triple DES، RC2، RC4، 128-bit RC4، DESX، 128-bit AES، 192-bit AES و 256-bit AES اشاره کرد. الگوریتم های مربوطه توسط رابط برنامه سازی کاربردی (API) Windows Crypto پیاده سازی می شوند.

SQL Server می تواند به طور همزمان چندین کلید متقارن باز را در محدوده (scope) یک اتصال پایگاه داده حفظ کند. یک کلید باز از محل ذخیره سازی (store) بازیابی شده و برای رمزگشایی داده ها در دسترس قرار می گیرد. زمانی که یک بخشی از اطلاعات رمزگشایی می شود، دیگر نیازی به مشخص کردن یک کلید متقارن (برای استفاده) نیست. هر مقدار رمز گذاری شده ای دربردارنده ی key identifier/GUID(شناسه ی منحصر بفرد سراسری کلید) کلیدی است که برای رمزگذاری آن بکار می رود. چنانچه کلید مورد نظر و صحیح رمزگشایی شده و باز باشد، موتور جریان بایت های رمزگذاری شده (encrypted byte stream) را با کلید متقارن باز match می کند. کلید نام برده سپس به منظور اجرای پروسه ی رمزگشایی و بازیابی اطلاعات مورد بهره وری قرار می گیرد. در صورت باز نبودن کلید صحیح ، NULL بازگردانی می شود.