А. Н. Светляк, А. С. Печеренко, В. В. Шумигай

АНАЛИЗ ШИФРОВАНИЙ БАЗ ДАННЫХ

Рассматриваются современные методы шифрования баз данных, а также рассматриваются сферы их применения.

Введение

В современном мире обработка и передача данных играют важную роль в различных областях жизни, начиная от банковских транзакций и заканчивая передачей личных данных в сети. Шифрование данных представляет собой процесс преобразования информации в нечитаемый формат с целью защиты ее от несанкционированного доступа. Для этого используются криптографические алгоритмы.

I. Анализ современных шифрований баз данных

Существует несколько методов и технологий, доступных для шифрования базы данных.

Прозрачное шифрование. Метод шифрования защищает информацию в базе данных (БД) путем шифрования базовых файлов БД, а не самих данных. Для безопасности TDE хранит ключи шифрования во внешнем (по отношению к базе данных) модуле безопасности (хранилище ключей).

Шифрование на уровне столбцов. Для каждого столбца (отдельно) в базе данных можно использовать совершенно уникальные ключи шифрования.

Симметричное шифрование. Происходит через метод закрытого ключа. Этот закрытый ключ изменяет информацию таким образом, что ее невозможно прочитать без предварительной расшифровки. (рис. 1)

Рис. 1 – Симметричное шифрование.

Асимметричное шифрование. Расширяет симметричное шифрование путем включения в метод шифрования двух разных типов ключей: закрытых (приватных) и открытых (публичных) ключей. В большинстве сценариев открытый ключ – это ключ шифрования, тогда как закрытый ключ – это ключ дешифрования.(рис. 2)

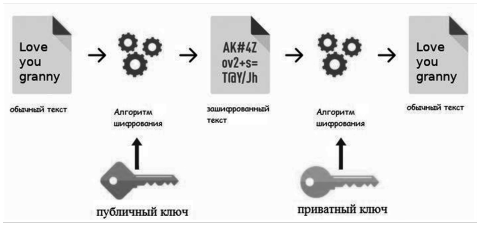

Рис. 2 – Асимметричное шифрование.

II. Применение криптографии

Финансовые транзакции: онлайн-платежи, банковские переводы, электронные денеги и т.д. Компьютерная безопасность: защита данных на компьютерах, включая защиту паролей, файлов и дисков. Коммуникации: конфиденциальность персональных сообщений и данных в электронной почте, мессенджерах, социальных сетях и т.д. Здравоохранение: защита медицинских данных пациентов и обмен электронными медицинскими данными. Кроме того, криптография также применяется в различных технических областях, таких как электроника, автоматизация, производство и т.д.

III. Выводы

Криптография имеет широкое применение, где важно обеспечить конфиденциальность и безопасность информации. Рассмотренные методы шифрования баз данных помогают глубже понять суть криптографии и ее важность в разработке приложений. Анализирование методов шифрования баз данных позволяет выбирать наиболее подходящие методы шифрования для конкретных направлений разработки.

1. Мао В. Современная криптография : теория и практика / В. Мао ; пер. с англ. - Москва : Вильямс, 2005. – 768 с.
2. Katz, J., Lindell, Y. Introduction to modern cryptography // 2-ое издание. – 2016.– 336 с.

Светляк Ангелина Николаевна, студент кафедры ИТАС БГУИР, angelinasvetlyak@mail.ru,
Шумигай Владислав Викторович, студент кафедры ИТАС БГУИР, vlad.shumihai@gmail.com
Печеренко Александра Сергеевна, студент кафедры ИТАС БГУИР, alex.pech841@gmail.com
Научный руководитель: Трофимович Алексей Фёдорович, старший преподаватель кафедры ИТАС, заместитель декана ФИТУ trofimaf@bsuir.by.