УДК 004.056.55

ИМИТАЦИОННАЯ МОДЕЛЬ ДЛЯ ОЦЕНКИ ВЛИЯНИЯ МЕТОДА ШИФРОВАНИЯ ДАННЫХ НА ПРОИЗВОДИТЕЛЬНОСТЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ

К. т. н. С. Л. Зиноватная, Р. А. Андриевский

Одесский национальный политехнический университет
Украина, г. Одесса
svzino@rambler.ru

Рассмотрены достоинства и недостатки применения различных способов преобразования информации, хранящейся в базе данных, с точки зрения их влияния на возможность несанкционированного доступа к особо конфиденциальным данным и времени доступа к информации санкционированным пользователем. Предложены средства количественной оценки для сравнения использования различных методов шифрования данных.

Ключевые слова: конфиденциальные данные, производительность информационной системы, шифрование, имитационная модель.

При разработке информационных систем (ИС), которые сохраняют конфиденциальные данные, например, результаты медицинских исследований, очевидной задачей является защита таких данных от несанкционированного доступа. Традиционным решением является шифрование данных в базе данных (БД). При выборе метода шифрования необходимо учесть следующее: надежность кодирования, возможность обратного преобразования, скорость получения результирующего набора данных, ограниченные возможности программно-аппаратных средств, представление данных в удобном пользователю виде. При использовании асимметричного метода RSA-шифрования [1], предполагающего, что открытый ключ, с помощью которого шифруется текст, отличается от закрытого ключа, используемого для дешифровки [2], и использующего 512-битовый ключ, трудности могут возникнуть при шифровании текста, содержащего смешанные символы (кириллица, латиница и любые другие символы). Проблема также состоит в частом воспроизведении алгоритма дешифрования, что значительно замедляет работу ИС. Метод шифрования с помощью встроенной функции md5 не дает возможности выполнить обратимое шифрование [3]. Метод перестановок прост и быстр в процессе шифрования и дешифрования, затраты на хранение шифрованной информации минимальны, но его криптостойкость недостаточно высокая. Шифрование методом перестановки по таблице имеет такой же недостаток, что и предыдущий метод, хотя все выражение либо текст укладывается в матрицу, однако возможна расшифровка просто с использованием логики [4]. Алгоритмы с использованием метода замены (шифр Виженера, алгоритм Цезаря) не сложны в реализации, а также в самом понимании процесса. При большом выборе методов и алгоритмов шифрования, однако, существует проблема не только надежной защиты данных, но и в приемлемости времени расшифровки и удобстве представления данных пользователю (сортировка). Целью работы является повышение производительности ИС благодаря использованию имитационной модели для оценки влияния применения различных методов шифрования на время выполнения запроса к БД и, следовательно, время отклика ИС на запрос пользователя.

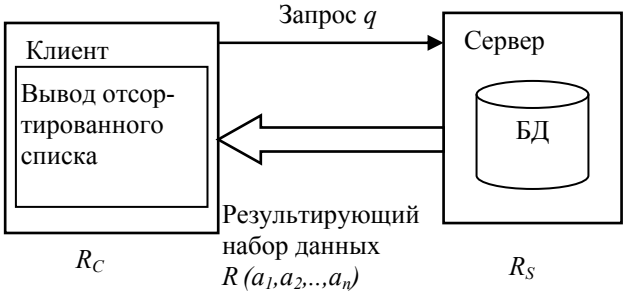

Рис.1. Схема взаимодействия «Клиент—Сервер» с использованием БД

Взаимодействие между рабочим местом пользователя и БД можно пред-

ставить в виде схемы (рис. 1), где R_C – набор данных, представленный клиенту на экране или при печати; R_S – набор данных, сформированный сервером.

Пусть R_q – результат выборки необходимых данных из БД; *fDcd* – функция, выполняющая дешифрование данных из R_q; *fOrd* – функция, выполняющая сортировку набора данных по заданному критерию.

Рассмотрим следующие случаи:

1) $R_C=R_S$, $R_S=fOrd\ (fDcd\ (R_q))$ $R_C= R_S$, – дешифрование данных и их сортировка выполняется сервером;

2) $R_C\neq R_S$, $R_S= fOrd\ (R_q)$, $Rc= fDcd\ (R_S)$ – дешифрование данных выполняется клиентом, сортировка выполняется сервером;

3) $R_C\neq R_S$, $R_S= R_q$, $R_C=fOrd\ (fDcd\ (R_S))$ – дешифрование данных и их сортировка выполняется клиентом.

В качестве *fOrd* для сервера используется конструкция ORDER BY оператора SELECT SQL, для клиента – программный код. В первом случае возникает проблема создания на стороне сервера функции, удовлетворяющей критериям надежной защиты данных; во втором случае может возникнуть проблема утери сортировки после дешифровки данных; третий случай решает названные проблемы, но требует написания дополнительного кода и дополнительных ресурсов на стороне клиента.

Предложенная имитационная модель позволяет задать запрос q, метод шифрования-дешифрования данных и оценить время отклика на запрос τ_q с учетом сортировки или без нее (рис. 2). Модель учитывает сортировку по отдельным полям из набора $(a_1,a_2,..,a_n)$ или по их комбинации.

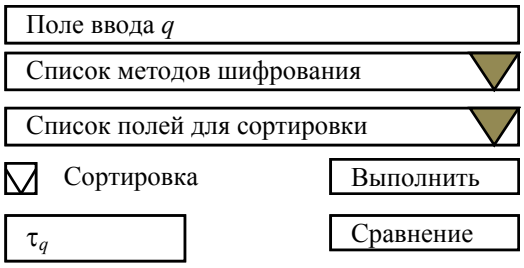

Рис. 2. Интерфейс имитационной модели

Был проведен эксперимент для запросов к БД медицинского учреждения, например, в случае запроса q, требующего объединения результирующих таблиц двух подзапросов, каждый из которых в свою очередь выполняет соединение четырех базовых таблиц, время вывода на экран при использовании различных методов шифрования изменялось от 10 до 12 с (2377 кортежей в результирующем наборе) и от 21 до 28 с (6094 кортежей).

Таким образом, в случае большого количества кортежей в результирующем наборе данных сортировка этого набора по требованию пользователя может потребовать значительного времени, что приведет к тому, что время отклика на запрос пользователя станет неприемлемым. Предложенная имитационная модель позволяет проводить поиск приемлемого варианта шифрования данных с точки зрения компромисса между степенью надежности защиты данных и временем получения отклика на запрос пользователя.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. RSA шифрование в PHP [Электронный ресурс].— Режим доступа: https://habrahabr.ru/post/255799/.

2. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии.— Москва: Мир, 2007.

3. Руководство по PHP — Справочник функций-Обработка текста-Строки-Обработка строк-md5 [Электронный ресурс].— Режим доступа: http://php.net/manual/ru/function.md5.php.

4. Аграновский А. В., Хади Р. А. Практическая криптография: алгоритмы и их программирование.— Москва: Солон-Пресс, 2009.

S. L. Zinovatnaya, R. A. Andrievskiy

A simulation model for evaluation of the impact of a data encryption method on information system performance

Advantages and disadvantages of applying different methods for transformation of information stored in the database are considered from the point of view of their impact on possibility of unauthorized access to particularly confidential data and time of access to information by an authorized user. Means of quantitative evaluation for comparison of application of different methods for data encryption are proposed.

Keywords: *confidential data, performance of information system, encryption, simulation model.*