ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 002.56

О МОДЕЛИРОВАНИИ ПРОЦЕССОВ ШИФРОВАНИЯ ДАННЫХ В ТЕХНОЛОГИИ ДОСТУПА WiMAX

А.А. ВОЙТЕНКО
А.Д. БУХАНЦОВ
И.В. ГУРЬЯНОВА

Белгородский государственный Национальный исследовательский университет

e-mail:
503563@bsu.edu.ru
bukhantsov@bsu.edu.ru
gurjanova@bsu.edu.ru

В статье представлена программная модель процессов шифрования данных в технологии доступа WiMAX. Разработанное программное обеспечение позволяет не только изучать процессы защиты информации в комплексном виде, но и проводить анализ возможных неучтенных разработчиком угроз с целью дальнейшего совершенствования механизмов защиты в соответствующих технологиях доступа.

Ключевые слова: система моделирования, технология доступа WiMAX, криптографическая защита.

Современные технологии беспроводного доступа имеют существенные преимущества и удобства в использовании по сравнению с системами фиксированной связи. Однако обмен данными по радиоканалу требует достаточно высокого уровня криптозащиты, в связи с чем механизмы защиты существующих технологий доступа постоянно совершенствуются. При подготовке специалистов в данной области, как правило, используются программные продукты, реализующие отдельные криптоалгоритмы. Системный подход к моделированию систем защиты реализуется на основе абстрактного представления и анализа угроз информационной системе [1]. Модели, реализующие комплексное изучение и исследование процессов шифрования в составе системы защиты информации технологий беспроводного доступа, практически отсутствуют [2].

Актуальность работы обусловлена необходимостью применения объективных и универсальных моделей систем защиты информации в различных технологиях передачи данных, позволяющих в доступной форме получить знания об алгоритмах, участвующих в шифровании данных, описание криптографического анализа каждого из алгоритмов. При этом возможность исследовать их эффективность, выявить достоинства и недостатки может позволить выработать соответствующие предложения по дальнейшему совершенствованию таких систем.

Разработанный программный продукт представляет собой совокупность окон, каждое из которых выполняет определённые функции. Программа делится на информационную часть (обучающую) и практическую. Программное окно с начальным интерфейсом представлено на рис. 1.

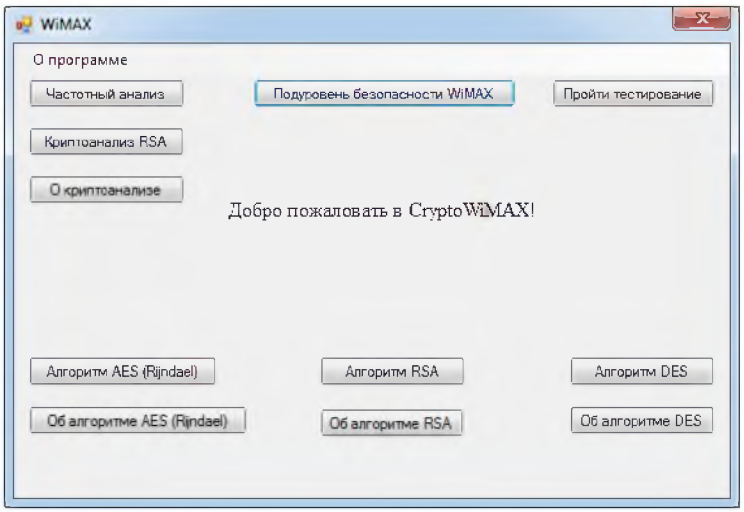


Рис. 1. Окно начального интерфейса программы

Обучающая часть программы предоставляет теоретическую информацию о подуровне безопасности технологии доступа WiMAX, об алгоритмах шифрования, представленных в модели, и подробное описание методов криптоанализа каждого из рассмотренных алгоритмов.

В программной модели реализована работа алгоритмов DES, участвующего в шифровании ключей, AES, используемого для шифрования трафика, а также RSA для шифрования ключа авторизации AK в процессе аутентификации абонентской и базовой станций.

Алгоритм DES является симметричным алгоритмом блочного шифрования, состоящим из 16 раундов схемы Фейстеля. В программе моделируется работа алгоритма DES с объёмом ключа 56 бит. В ранних версиях технологии WiMAX данный алгоритм используется для шифрования данных (трафика). Новый стандарт IEEE 802.16e использует тройной DES на двух ключах для шифрования ключей шифрования трафика TEK, которые базовая станция отправляет абонентской станции после процедуры авторизации.

В настоящее время DES считается небезопасным, поэтому в новом стандарте IEEE 802.16e для шифрования данных используется алгоритм AES. Алгоритм AES также является блочным симметричным шифром с определенным числом раундов преобразований. В технологии доступа WiMAX алгоритм AES использует объём ключа 128 бит и размер блока 128 бит. Однако использование тройного, но все же устаревшего DES как указано выше для шифрования такого ключа с дальнейшей его передачей по радиоканалу может быть небезопасным. Кроме того, небольшое время жизни ключа TEK и ограниченное число его идентификаторов может привести к повторному использованию ключей TEK, чей срок жизни уже истек.

Алгоритм RSA является ассиметричным алгоритмом с открытым ключом, стойкость которого основана на вычислительной сложности задачи факторизации больших целых чисел. Данный алгоритм используется в процессе авторизации и аутентификации абонентских станций в технологии доступа WiMAX. Открытый ключ, извлекаемый из сертификата авторизованной абонентской станции, используется для шифрования по протоколу RSA ключа авторизации AK, передаваемого по радиоканалу от базовой станции к абонентской. В свою очередь, ключ AK участвует в генерации ключей шифрования ключей KEK (ключей, используемых в тройном DES для шифрования ключей TEK). Таким образом, стойкость используемого в WiMAX алгоритма RSA существенно влияет не только на процесс аутентификации абонентской станции, но и на безопасный обмен данными по радиоканалу в целом.

В соответствии с вышеизложенным, помимо моделирования алгоритма RSA в программе предусмотрена возможность провести его криптоанализ на основе так называемого метода бесключевого чтения [3]. Данный метод заключаться в том, что при условии доступа к открытому ключу (K, N) и зашифрованному тексту C, злоумышленник подбирает число j такое, для которого должно выполняться соотношение: $C^{Kj} = C \bmod N$. То есть, злоумышленнику необходимо провести j раз шифрование с помощью открытого ключа перехваченного закрытого текста. Это выглядит следующим образом:

$$((C^K)^K\ldots)^K \bmod N = M, \quad (1)$$

где M – открытый текст.

На первый взгляд может показаться, что при случайном формировании секретного и открытого ключей значение j может быть настолько велико, что атака будет вычислительно нереализуемой. Однако, в отдельных случаях, если в разложении

$$F(N) = (P-1)(Q-1), \quad (2)$$

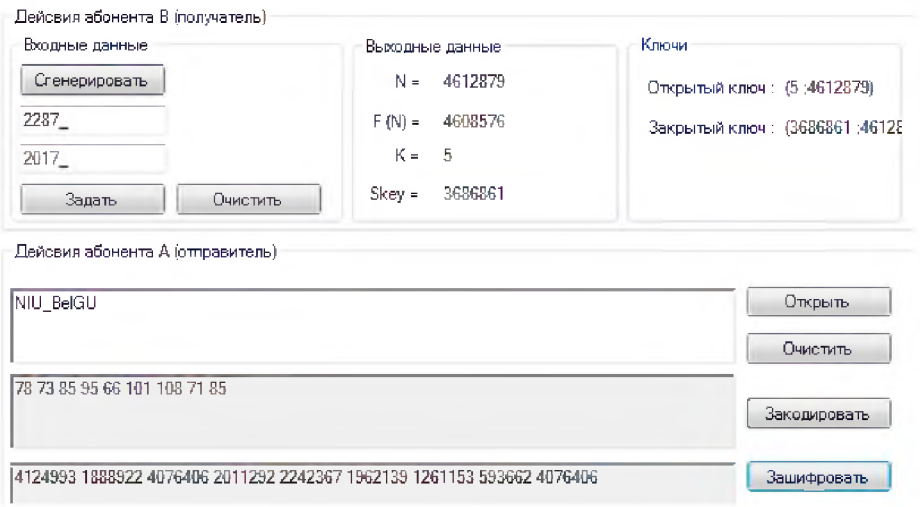
где P и Q – большие простые числа, причем $N=PQ$,
имеются множители небольшой длины, то возможна вероятность случайного выбора «плохого» открытого ключа K. Фактически при бесключевом чтении рассматривается возможность реализации сравнения

$$K^j \equiv 1 \bmod F(N), \quad (3)$$

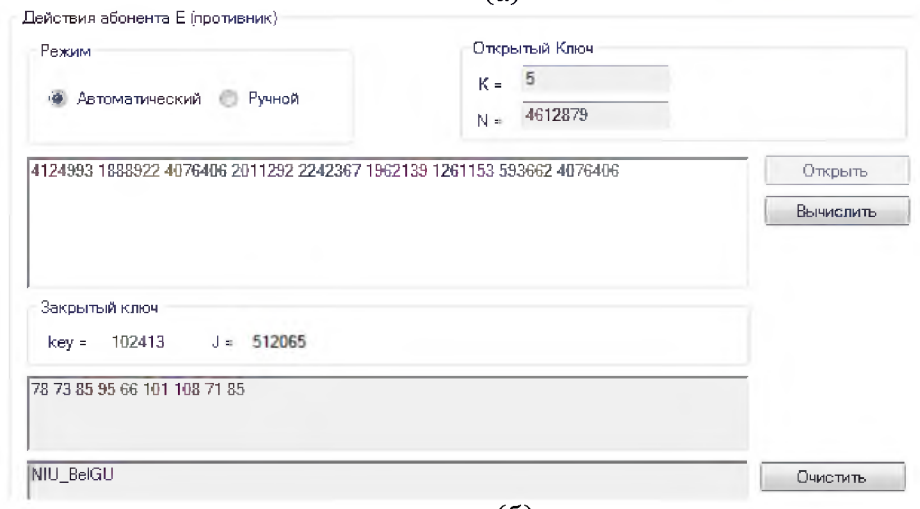
в котором j является минимальным показателем числа K по модулю $F(F(N))$.

Следовательно, при генерации ключей RSA в абонентском устройстве целесообразно учитывать возможность появления «плохой» пары ключей и предлагать пути дальнейшего совершенствования подуровня безопасности в технологии WiMAX.

Фрагменты работы алгоритма, реализующего метод бесключевого чтения RSA в программной модели, представлены на рис. 2.



(а)



(б)

Рис. 2. Фрагменты работы алгоритма, реализующего метод бесключевого чтения RSA:
а – действия абонентов; б – действия злоумышленника

Таким образом, разработанный программный продукт позволяет получить целостное представление о механизмах защиты информации подуровня безопасности

технологии WiMAX в процессе моделирования их работы. Рассмотренный подход к изучению и анализу системы защиты информации делает не только более эффективным процесс изучения таких систем, но и облегчает поиск и анализ неучтенных и новых угроз с целью дальнейшего совершенствования технологий защиты для систем беспроводного доступа.

Список литературы

1. Ищейнов В.Я., Чудинов С.М. Модель безопасности конфиденциальной информации в информационной системе // Научные ведомости БелГУ. Сер. История. По-литология. Экономика. Информатика. – 2012. – № 13 (132). – Вып. 23/1. – С. 205-209.

2. Рашич А. В. Сети беспроводного доступа WiMAX [Текст] : учебное пособие / А. В. Рашич. – СПб. : Изд-во Политехн. ун-та, 2011. – 179 с.

3. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. – СПб.: БХВ-Петербург, 2005. – 288 с.

ABOUT MODELING DATA ENCRYPTION, ACCESS TECHNOLOGY WiMAX

A.A. VOITENKO
A.D. BUKHANTSOV
I.V. GURJANOVA

Belgorod National Research University

e-mail:
503563@bsu.edu.ru
bukhantsov@bsu.edu.ru
gurjanova@bsu.edu.ru

This article describes the operation of the system modeling data encryption technology to access WiMAX. Dan-tion software allows you to fully explore the process of data encryption and solve problems related to cryptographic protection of information.

Key words: modeling, technology dos dumb WiMAX, cryptographic protection.