УДК 621.391

Б.Ф. БАДАЛЯН, О.А. ГОМЦЯН, М.С. МАРГАРЯН

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АСИММЕТРИЧНЫХ КРИПТОСИСТЕМ RSA И ЭЛЬ-ГАМАЛЯ

Рассматриваются наиболее известные и эффективные алгоритмы асимметричного шифрования для защиты конфиденциальной информации. Представлены и описаны основные шаги алгоритма шифрования данных по схемам RSA и Эль-Гамаля. Разработана программная реализация схем асимметричного шифрования в среде MATLAB R2019a, которая позволяет оценить запас криптостойкости.

Ключевые слова: шифрование, асимметричная криптосистема, секретный ключ, алгоритм RSA, схема Эль-Гамаля, электронная цифровая подпись.

Введение. В настоящее время во всем мире особенно остро стоит проблема информационной безопасности, что обусловлено процессами стремительного расширения потоков информации, охватывающих все сферы жизни современного общества.

Информация уже не является просто необходимым для производства вспомогательным ресурсом. Она приобрела ощутимую стоимость, соразмерную реальной прибыли, получаемой при ее использовании. Появление телекоммуникационных систем и сетей сделало простым получение доступа к информации для отдельных пользователей и крупных организаций. Во всех подобных системах главной проблемой является надежное обеспечение авторизованного доступа и целостности обрабатываемой информации. В компьютерных сетях данная проблема решается применением паролей, что, однако, более пригодно для защиты доступа к вычислительным ресурсам, чем для защиты информации. Задачи, возникаемые при передаче и обработке конфиденциальной информации, решаются применением криптографических методов защиты. Криптография дает возможность преобразовать информацию таким образом, что ее прочтение или восстановление возможно только при знании секретного параметра - ключа шифрования.

Криптосистемы разделяются на бесключевые, симметричные и асимметричные (с открытым ключом). Бесключевые криптосистемы не используют каких-либо ключей в процессе криптографических преобразований. К бесключевым криптосистемам относятся хеш-функции и генераторы псевдослучайных чисел. Симметричные криптосистемы построены на основе сохранения в тайне ключа шифрования. В таких системах процессы шифрования и расшифрования основаны на использовании единого идентичного криптографического

ключа. Несмотря на высокое быстродействие симметричных криптосистем, их практическое применение ограничено сложностью генерации и распределения между пользователями секретного ключа. Наиболее перспективными представителями симметричного шифрования являются криптоалгоритмы 3-DES, AES, RC6 и Twofish [1].

В асимметричных криптосистемах для шифрования и расшифрования информации используются математически связанные, но разные ключи –открытый и секретный. Таким образом, отпадает проблема передачи секретного ключа, как в случае симметричных криптосистем.

Несмотря на все преимущества, асимметричные криптосистемы достаточно медлительны и трудоемки, а их криптостойкость базируется в основном на вычислительной сложности решения за приемлемое время некоторой математической задачи. Поэтому на практике широко применяются гибридные криптосистемы, сочетающие в себе достоинства обоих криптоалгоритмов. В подобных криптосистемах для очередного сеанса генерируется симметричный сеансовый ключ, который зашифровывается средствами асимметричной криптосистемы. После передачи секретного ключа шифрование всех последующих сообщений выполняется средствами симметричной криптосистемы.

Основная часть. Криптосистема Эль-Гамаля может быть использована в приложениях шифрования и электронной цифровой подписи. Безопасность данного шифра основана на вычислительной сложности задачи дискретного логарифмирования в конечном поле.

Для генерации пары открытый ключ - закрытый ключ выбираются большое простое число p и большое целое число g ($g < p$), которые распределяются между абонентами системы [2]. Далее каждый абонент выбирает значение секретного ключа и вычисляет значение открытого ключа $y = g^x \ mod \ p$.

Для шифрования сообщения, представленного в виде числа M, выбирается случайное число k,($1 < k < p - 1$) и вычисляются значения

$$r = g^k mod \ p; \ s = M \cdot y^k \ mod \ p. \quad (1)$$

Пара чисел (r, s) является шифротекстом, и его длина вдвое превышает длину исходного открытого сообщения M.

Уравнение расшифрования имеет вид

$$M = s \cdot r^{p-1-x} \ mod \ p. \quad (2)$$

На рис.1 представлено окно программной реализации шифра Эль-Гамаля в среде MATLAB R2019a. Как видно из рисунка, после выбора необходимой длины ключей программа генерирует ключи, и активируется поле ввода

открытого сообщения "Clear Text Message". В самой нижней части окна отображается зашифрованное сообщение.

Рис. 1. Реализация криптосистемы Эль-Гамаля

На рис.2 показано окно программы в режиме расшифрования криптограммы.

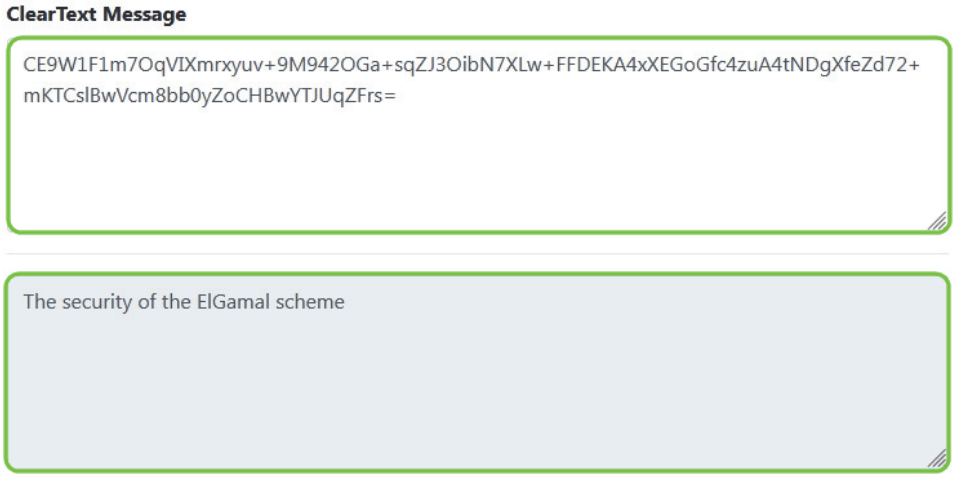

Рис. 2. Работа в режиме расшифрования

Алгоритм открытого шифрования RSA (Rivest-Shamir-Adleman) является одной из первых криптосистем, используемой для безопасной передачи данных. Основные параметры криптосистемы RSA формирует получатель сообщения.

Последовательность действий для генерации ключей шифрования алгоритма RSA выглядит следующим образом [3,4]:

1. Выбираются два произвольных больших простых числа p и q с длинами от 512 битов.
2. Вычисляется значение модуля $n = p \cdot q$.
3. Вычисляются функция Эйлера $\varphi(n) = (p-1)(q-1)$ и значение открытого ключа с учетом выполнения условий: $1 < k_o \leq \varphi(n)$, НОД $\left(k_o, \varphi(n)\right) = 1$.
4. С помощью алгоритма Евклида вычисляется значение секретного ключа $k_c \equiv k_o^{-1}(mod\ \varphi(n))$.
5. Пара чисел (n, k_o) является открытым ключом.

Криптограмма C определяется через пару открытый ключ - блок сообщения M:

$$C = M^{k_o} mod\ n. \tag{3}$$

Принятая криптограмма расшифровывается по формуле

$$M = C^{k_c}\ mod\ n. \tag{4}$$

На безопасность криптосистемы RSA влияют такие факторы, как использование абонентами одинаковых или близких значений простых чисел p и q или открытых ключей k_o, а также длины открытых и закрытых ключей [5].

С учетом вышеперечисленных формул в среде MATLAB R2019a нами разработана программная реализация криптосистемы RSA, главное окно которой в режиме генерации ключей/шифрования показано на рис.3. Программа позволяет генерировать ключи длиной от 512 до 4096 битов.

Рис. 3. Главное окно программы RSA в режиме шифрования открытого текста

Окно программы в режиме расшифрования и полученный результат показаны на рис. 4.

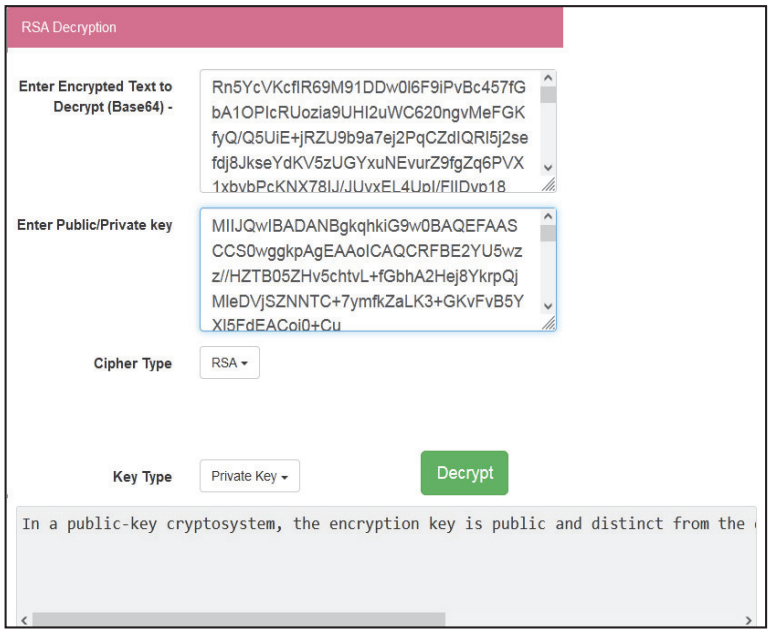

Рис. 4. Главное окно программы RSA в режиме расшифрования криптограммы

Заключение. Схему Эль-Гамаля можно применить не только для шифрования данных, но и в стандартах электронной цифровой подписи. Проведенные исследования показывают, что данная криптосистема решает задачу передачи зашифрованного сообщения за одну пересылку, однако объем криптограммы увеличивается в два раза по сравнению с объемом открытого текста. Криптосистема RSA лишена подобного недостатка, однако ее безопасность во многом определяется корректным выбором параметров. Данная криптосистема подвержена таким атакам, как метод бесключевого чтения, криптоанализ на основе китайской теоремы об остатках и атака методом Ферма. Проанализировав полученные результаты, можно сделать вывод, что криптосистемы RSA с размером модуля менее 2048 битов находятся на грани потери надежности. На практике большим потенциалом безопасности обладает 4096-битовая RSA, однако подобная длина ключа отрицательно сказывается на производительности.

СПИСОК ЛИТЕРАТУРЫ

1. **Панасенко С.П.** Алгоритмы шифрования: Специальный справочник. — СПб.: БХВ-Петербург, 2009. - 576 с.
2. **Баранова Е.К., Бабаш А.В.** Основы информационной безопасности: Учебник.- М.: РИОР:ИНФРА-М, 2019.-202 с**.**

3. **Смарт Н.** Криптография.- М.: Техносфера, 2005.-528 с.
4. **Rivest R.L., Shamir A., Adleman L.M.A.** A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // CACM.-1978.-V.21, №2.-P.120-126.
5. **Васильева И.Н.** Криптографические методы защиты информации: Учебник и практикум для академического бакалавриата.-М.: Издательство “Юрайт”, 2017.-349 с.

Բ.Ֆ. ԲԱԴԱԼՅԱՆ, Հ.Ա. ԳՈՄՑՅԱՆ, Մ.Ս. ՄԱՐԳԱՐՅԱՆ

RSA և ԷԼ-ԳԱՄԱԼԻ ԱՍԻՄԵՏՐԻԿ ԿՐԻՊՏԱՀԱՄԱԿԱՐԳԵՐԻ ԾՐԱԳՐԱՅԻՆ ԻՐԱԿԱՆԱՑՈՒՄԸ

Դիտարկված են գաղտնի ինֆորմացիայի պաշտպանության համար ասիմետրիկ գաղտնագրման առավել հայտնի և հեռանկարային ալգորիթմները: Ներկայացված և մանրամասն նկարագրված են RSA և Էլ-Գամալի սխեմայով տվյալների գաղտնագրման ալգորիթմների հիմնական քայլերը: MATLAB 2019a միջավայրում մշակվել է ասիմետրիկ գատնագրման սխեմաների ծրագրային իրականացումը, որը թույլ է տալիս գնահատել կրիպտակայունության պաշարը:

Առանցքային բառեր. գաղտնագրում, ասիմետրիկ կրիպտահամակարգ, գաղտնի բանալի, RSA ալգորիթմ, Էլ-Գամալի սխեմա, էլեկտրոնային թվային ստորագրություն:

B.F. BADALYAN, H.A. GOMTSYAN, M.S. MARGARYAN

SOFTWARE IMPLEMENTATION OF RSA AND ELGAMAL ASYMMETRIC CRYPTOSYSTEMS

The most well-known and effective asymmetric encryption algorithms for protecting confidential information are considered. The main steps of the data encryption algorithm according to the RSA and ElGamal scheme are presented and described. A software implementation of asymmetric encryption schemes in the MATLAB R2019a environment has been developed, which allows estimating the cryptographic strength margin.

Keywords: encryption, asymmetric cryptosystem, private key, RSA algorithm, ElGamal scheme, electronic digital signature.