УДК 004.032

СОВРЕМЕННЫЕ МЕТОДЫ РЕШЕНИЯ КРИПТОАНАЛИТИЧЕСКИХ ЗАДАЧ

Тимошенко Л.Н.[1)], Вербик К.В.[2)]
Одесский национальный политехнический университет
[1)] к.э.н., доцент; [2)] магистрант

I. Постановка проблемы

Компьютерные системы активно внедряются в финансовые, промышленные, торговые и социальные сферы. Вследствие этого резко возрос интерес широкого круга пользователей к проблемам защиты информации. Среди всего спектра методов защиты данных от нежелательного доступа особое место занимают криптографические методы. В зависимости от ключевой системы различают симметричные и асимметричные системы.

Большинство часто используемых алгоритмов ассиметричного шифрования, например, RSA, используют вычислительную сложность факторизации в качестве основы своей криптостойкости. Для гипотетического квантового компьютера алгоритм, осуществляющий разложение числа на простые множители за полиномиальное время, уже разработан, но вопрос существования такового для классического компьютера остаётся открытым. А значит, ускорение существующих методов факторизации является одной из наиболее актуальных задач.

II. Цель работы

Целью работы является анализ современных методов решения криптоаналитических задач и исследование особенностей метода Ферма.

III. Анализ методов решения криптоаналитических задач

Криптографическая защита информации - вид защиты информации, реализуется путем преобразования информации с использованием специальных (ключевых) данных с целью сокрытия/восстановления содержания информации, подтверждения ее подлинности, целостности, авторства и т.п.

Криптография – с греческого означает тайнопись, предназначение криптографии защитить или сохранить в тайне необходимую информацию [1] . Для современной криптографии характерно использование открытых алгоритмов шифрования, предполагающих использование вычислительных средств.

Асимметричное шифрование (или криптографическая система с открытым ключом) - система шифрования и / или электронной цифровой подписи (ЭЦП), при которой открытый ключ передается по открытому (то есть незащищенному, доступном для наблюдения) каналу, и используется для проверки ЭЦП и для шифрования сообщения. Для генерации ЭЦП и для расшифрования сообщения используется секретный ключ.

Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH.

Что касается криптоанализа, сфера его интересов противоположная - разработка и исследование методов дешифрования (раскрытия) шифрограммы даже без знания секретного ключа.

Криптоанализ - наука занимающаяся оценкой сильных и слабых сторон методов шифрования, а также разработкой методов, позволяющих взламывать криптосистемы. Задача криптоанализа состоит в том, чтобы определить вероятность взлома шифра и, таким образом, оценить его применимость в той или иной области.

На рисунке 1 методы криптоанализа систематизированы по хронологии их появления и применимости для взлома различных категорий криптосистем. Горизонтальная ось разделена на временные промежутки: в область "вчера" попали атаки, которые успешно применялись для взлома шифров в прошлом; "сегодня" - методы криптоанализа, представляющие угрозу для широко используемых в настоящее время криптосистем; "завтра" - эффективно применяемые уже сегодня методы, значение которых в будущем может возрасти, а также методы, которые пока не оказали серьезного влияния на криптологию, однако со временем могут привести к прорывам во взломе шифров. На вертикальной оси обозначены области применения методов криптоанализа: для взлома криптосистем с секретным ключом, открытым ключом или хеш-функций.

Как видим, на сегодняшний день для взлома криптосистем с открытым ключом успешно применяются методы полного перебора ключом, анализ ключевого генератора, факторизация/дискретное логарифмирование и анализ по побочным каналам.

Практически все используемые алгоритмы асимметричной криптографии основаны на задачах факторизации (например, известная криптосистема RSA) и дискретного логарифмирования в различных алгебраических структурах (схема электронно-цифровой подписи Эль-Гамаля) [2] .

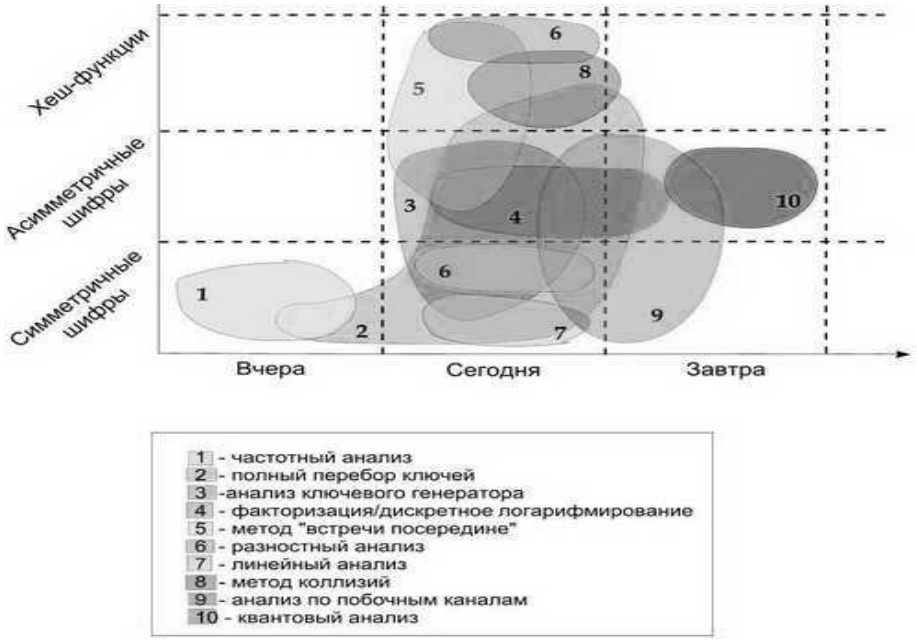

Рисунок 1 – Методы криптоанализа

С того момента, как У. Диффи и М. Хеллман в 1976 г. предложили концепцию криптографии с открытым ключом, проблемы факторизации целых чисел и дискретного логарифмирования стали объектом пристального изучения математиков всего мира.

Метод факторизации (разложения на множители) Ферма состоит в вычислении квадратов по модулю n для целых x, чуть больших $\sqrt{n}$, в надежде встретить полный квадрат y^2. Метод быстро работает, если $n = p \otimes q$ и числа p и q близки друг к другу [3] .

Пусть надо разложить на множители число n. Если удастся найти два числа x и y такие, что $x^2 - y^2 = n$, то $(x + y) * (x - y) = n$.

Числа $(x + y)$ и $(x - y)$ являются множителями n, возможно, тривиальными (т.е. одно из этих чисел 1, а другое n.)

Эти два числа x и y, дающие $x^2 - y^2 = n$, найдутся, если найдётся такое целое x, что $x^2 - n$ является квадратом. Тогда $x^2 - (x^2 - n)$ — разность квадратов, равная n.

Поиск начинают с $x = \sqrt{n} + 1$ - наименьшего возможного числа, при котором разность $x^2 - n$ положительна. Увеличивают x на 1 и вычисляют $x^2 - n$, пока $x^2 - n$ не окажется точным квадратом. Если это произошло, пытаются разложить n как $\left(x - \sqrt{x^2 - n}\right) \otimes \left(x + \sqrt{x^2 - n}\right)$. Если это разложение тривиально, продолжают увеличивать x. Метод имеет экспоненциальную сложность.

Вывод

В процессе работы было выявлено, что на сегодняшний день видное место в криптоанализе занимают методы факторизации. Самые эффективные из известных алгоритмов факторизации, например, Ферма, имеют большую вычислительную сложность. Таким образом актуальной является задача поиска путей уменьшения вычислительной сложности метода Ферма.

Список литературы

1. Алферов А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – Москва: Издательский дом «Гелиос АРВ», - 2005. 480 с.
2. А.А. Болотов. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – Москва: Издательский дом «КомКнига», - 2006. 274 с.
3. Н. Смарт. Криптография / Н. Смарт. – Москва: Издательский дом «ТЕХНОСФЕРА», - 2005 г. 526 с.