УДК 519.2

ОТ ТАЙНОПИСИ К ТЕОРИИ ЧИСЕЛ: КАК МАТЕМАТИКА ПРЕВРАТИЛА РЕМЕСЛО ШПИОНОВ В ТОЧНУЮ НАУКУ

Сторублев Р.А., студент гр. ИБс-231, III курс
Липина Г.А., старший преподаватель
Кузбасский государственный технический
университет имени Т.Ф. Горбачева
г. Кемерово

Аннотация

В статье рассматривается эволюция криптографии от искусства придумывать шифры до строгой математической дисциплины. Анализируется исторический путь развития методов защиты информации, особое внимание уделяется математическим основам современных криптосистем. На примерах алгоритмов RSA и эллиптических кривых демонстрируется, каким образом теория чисел обеспечивает стойкость шифрования. Показывается парадоксальный вывод: математика позволила сделать криптографию прозрачной — алгоритмы публикуются открыто, однако безопасность гарантируется вычислительной сложностью математических задач.

Ключевые слова: криптография, теория чисел, RSA, факторизация, дискретное логарифмирование, эллиптические кривые, информационная безопасность.

Введение

С момента возникновения письменности у человечества появилась потребность скрывать информацию от посторонних. На протяжении тысячелетий криптография развивалась как искусство — искусство придумывать хитроумные замены, перестановки и коды, доступные лишь посвященным. Однако во второй половине XX века произошла фундаментальная трансформация: секретное ремесло превратилось в точную науку, фундаментом которой стала математика, и прежде всего — теория чисел [1].

Актуальность темы обусловлена ключевой ролью криптографических методов в обеспечении безопасности современного цифрового пространства. Электронная коммерция, банковские операции, государственное управление, военная связь — все эти сферы невозможны без надежных алгоритмов шифрования. Цель настоящей работы — проследить эволюцию криптографии и показать, каким образом математические понятия (простые числа, факторизация, дискретный логарифм) стали основой современных систем защиты информации.

1. Криптография как искусство: от древности до Нового времени

1.1. Истоки тайнописи

Зарождение криптографии относится к глубокой древности. В переводе с древнегреческого «криптография» означает «тайнопись» [2]. Археологические находки свидетельствуют, что уже в Древнем Египте применялись методы сокрытия информации. Сохранившиеся папирусы демонстрируют использование своеобразного криптографического ключа: узкая длинная лента папируса наматывалась на палку строго определенного диаметра, текст наносился вдоль палки, после чего лента сматывалась и отправлялась адресату. Прочесть сообщение мог только тот, кто обладал палкой такого же диаметра.

В древнеиндийских текстах упоминаются 64 способа изменения текста, некоторые из которых можно отнести к криптографическим. В Месопотамии найдены таблички с рецептами изготовления глазури, где использовались редкие обозначения, а буквы заменялись цифрами.

1.2. Античность и Средневековье

Значительного развития криптография достигла в Древней Греции. В Спарте (V–VI вв. до н.э.) использовался шифр «скитала» — жезл, на который наматывалась полоса пергамента. Текст писался вдоль оси жезла, после снятия с жезла буквы оказывались переставленными [3].

Арабский мир внес огромный вклад в развитие криптографии. Само слово «шифр» имеет арабское происхождение. В 855 году появилась «Книга о большом стремлении человека разгадать загадки древней письменности», где описывались системы шифров, в том числе с применением нескольких шифроалфавитов. Арабы первыми обратили внимание на возможность использования стандартных слов и выражений для дешифрования.

В эпоху Возрождения криптография получила новый импульс. Леонардо да Винчи, кардинал Ришелье, Джованни Порта, Блез Виженер — эти имена связаны с разработкой методов замены букв на цифры, созданием анаграмм и более сложных шифровальных систем. Труд Виженера «Трактат о шифрах» (1585) обобщил известные к тому времени криптографические методы.

1.3. Криптография в России

В России датой появления криптографической службы принято считать 1549 год — время образования Посольского приказа, в котором имелось «цифирное отделение». В XVII–XVIII веках, с развитием математического образования (выход «Арифметики» Л.Ф. Магницкого в 1703 году), создавались предпосылки для математизации криптографии.

Однако вплоть до конца XIX века криптография оставалась преимущественно искусством. Ее основу составляли лингвистика, смекалка и изобретательность. Шифры замены (как в знаменитых «Пляшущих человечках» Конан Дойля), шифры перестановки, кодовые таблицы — все эти методы объединяло одно: их стойкость основывалась на секретности алгоритма. Если противник узнавал способ шифрования, сообщение оказывалось раскрытым.

2. Математизация криптографии

2.1. Первые шаги: математика в криптоанализе

Во второй половине XIX века математика начала проникать в криптографию. Были открыты основные полиномы, имеющие значение для крипто-

анализа. Однако подлинная революция произошла в XX веке, и связана она с двумя факторами: появлением электронно-вычислительных машин и развитием теории информации.

Работы Клода Шеннона в 1940-х годах заложили теоретический фундамент криптографии. Шеннон ввел понятия «рассеивание» (diffusion) и «перемешивание» (confusion), показал возможность создания абсолютно стойкого шифра (одноразового блокнота) и, что важнее, доказал: стойкость шифра может быть строго математически обоснована.

2.2. Открытый ключ: революция в криптографии

Подлинный переворот произошел в 1976 году, когда Уитфилд Диффи и Мартин Хеллман предложили концепцию криптографии с открытым ключом. Идея заключалась в том, что ключи шифрования и дешифрования могут быть разными, причем ключ шифрования можно публиковать открыто. В 1977 году Рональд Ривест, Ади Шамир и Леонард Адлеман реализовали эту идею в алгоритме RSA, который стал первым практически применимым асимметричным шифром.

3. Теоретико-числовые основы современной криптографии

3.1. Базовые понятия теории чисел

Современная криптография опирается на несколько фундаментальных понятий теории чисел:

Простые числа — натуральные числа, большие единицы, которые делятся без остатка только на 1 и на самих себя. Простые числа являются «кирпичиками», из которых строятся все остальные числа (основная теорема арифметики).

Функция Эйлера $\varphi(n)$ — количество натуральных чисел, не превосходящих n и взаимно простых с n. Для простого числа p $\varphi(p) = p - 1$. Для произведения двух простых p и q $\varphi(pq) = (p-1)(q-1)$.

Сравнения по модулю — фундаментальный аппарат модульной арифметики. Запись $a \equiv b\,(mod\ n)$ означает, что числа a и b дают одинаковые остатки при делении на n.

Малая теорема Ферма: если p — простое число и a не кратно p, то $a^{p-1} \equiv 1\,(mod\ p)$. Обобщением является теорема Эйлера: $a^{\varphi(n)} \equiv 1\,(mod\ n)$ для взаимно простых a и n.

Эти, казалось бы, абстрактные математические факты образуют основу практических криптосистем.

3.2. Вычислительная сложность как основа стойкости [4]

Ключевое отличие современной криптографии от классической заключается в том, что стойкость шифра опирается не на секретность алгоритма, а на вычислительную сложность определенных математических задач. Наиболее важными являются две задачи:

Задача факторизации (разложения на множители). Дано большое составное число n, являющееся произведением двух простых чисел p и q. Требуется найти p и q. При достаточной величине n (более 300 десятичных зна-

ков) эта задача считается практически неразрешимой — даже самые мощные современные компьютеры не могут решить ее за приемлемое время.

Задача дискретного логарифмирования. Даны простой модуль p, образующий элемент g и число $y = g^x mod\ p$. Требуется найти x. Эта задача также является вычислительно трудной.

4. Криптосистема RSA: математика в действии

4.1. Генерация ключей

Рассмотрим процесс создания ключей в системе RSA на конкретном числовом примере.

Выбираются два простых числа. Возьмем p = 7, q = 11.

Вычисляется модуль $n = p \times q = 7 \times 11 = 77$.

Вычисляется функция Эйлера $\varphi(n) = (p-1)(q-1) = 6 \times 10 = 60$.

Выбирается открытая экспонента e, взаимно простая с $\varphi(n)$. Пусть e = 13. Проверим: НОД(13, 60) = 1.

Вычисляется секретная экспонента d как число, обратное e по модулю $\varphi(n)$: $e \times d \equiv 1\ (mod\ 60)$. Находим d = 37, поскольку $13 \times 37 = 481 \equiv 1\ (mod\ 60)$.

Открытый ключ: (n, e) = (77, 13). Секретный ключ: d = 37.

4.2. Шифрование и дешифрование

Пусть Алиса хочет передать Бобу сообщение, которое представляется числом m = 5 (на практике сообщение преобразуется в число по определенным правилам).

Шифрование (используется открытый ключ Боба): $c = m^e mod\ n = 5^{13} mod\ 77$.

Вычислим: $5^2 = 25;\ 5^4 = 25^2 = 625 \equiv 625 - 8 \times 77 = 625 - 616 = 9\ (mod\ 77)$;

$5^8 = 9^2 = 81 \equiv 4 (mod 77)$;

$5^{13} = 5^8 \times 5^4 \times 5^1 = 4 \times 9 \times 5 = 180 \equiv 180 - 2 \times 77 = 180 - 154 = 26\ (mod\ 77)$.

Зашифрованный текст: c = 26.

Дешифрование (используется секретный ключ Боба): $m = c^d mod\ n = 26^{37} mod\ 77 = 5$ (получатель восстанавливает исходное сообщение).

4.3. Почему это работает?

Корректность расшифрования обеспечивается теоремой Эйлера: $(m^e)^d = m^{e \times d} = m^{1\ +\ k \times \varphi(n)} = m \times \left(m^{\varphi(n)}\right)^k \equiv m \times 1^k = m\ (mod\ n)$.

Безопасность RSA основана на том, что для нахождения d необходимо знать φ(n), а для этого требуется разложить n на простые множители. Если n достаточно велико (рекомендуется не менее 2048 бит), эта задача практически невыполнима.

4.4. Сравнение стойкости

В таблице приведены соотношения между длиной модуля и уровнем стойкости для RSA и белорусского стандарта СТБ 1176.2 (основанного на дискретном логарифмировании):

Уровень стойкости	Длина модуля RSA (бит)	Длина модуля СТБ (бит)
1	638	143
3	1022	175
5	1310	195
8	2046	235
10	2462	257

Из таблицы видно, что RSA-1024 примерно соответствует третьему уровню стойкости, а RSA-2048 — восьмому.

5. Эллиптические кривые: новый этап развития

5.1. Математический аппарат

Криптосистемы на эллиптических кривых [5] (ECC — Elliptic Curve Cryptography) представляют собой современную альтернативу RSA. Они позволяют достичь того же уровня безопасности при значительно меньшей длине ключа.

Эллиптическая кривая над полем действительных чисел задается уравнением:

$$y^2 = x^3 + ax + b$$

Для криптографических целей используются кривые над конечными полями — простыми (GF(p)) или двоичными (GF(2^m)). Условие несингулярности: дискриминант $4a^3 + 27b^2 \neq 0$.

5.2. Операция сложения точек

На множестве точек эллиптической кривой вводится операция сложения, обладающая свойствами абелевой группы. Геометрический смысл: сумма трех точек, лежащих на одной прямой, равна нулю (бесконечно удаленной точке).

Для двух различных точек $P = (x_1, y_1)$ и $Q = (x_2, y_2)$ (при $x_1 \neq x_2$) сумма $R = P + Q = (x_3, y_3)$ вычисляется по формулам:

$$\lambda = (y_2 - y_1)/(x_2 - x_1)$$
$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

Для удвоения точки P = (x_1, y_1) (при $y_1 \neq 0$):

$$\lambda = (3{x_1}^2 + a)/(2y_1)$$
$$x = \lambda^2 - 2x_1$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

5.3. Задача дискретного логарифмирования на эллиптической кривой

Стойкость ECC основана на сложности задачи дискретного логарифмирования в группе точек эллиптической кривой: даны точки P и Q = k×P, требуется найти k. Для этой задачи не известно субэкспоненциальных алгоритмов (подобных решету числового поля), поэтому при одинаковом размере ключа ECC обеспечивает существенно более высокую стойкость, чем RSA [6].

6. «Прозрачная» криптография: математика позволяет прятать секрет на виду

Проведенный анализ позволяет сформулировать парадоксальный, на первый взгляд, вывод: математика сделала криптографию прозрачной.

В классической криптографии секретность сообщения обеспечивалась секретностью алгоритма. Шифровальщики прятали свои методы, использовали нестандартные замены, создавали тайные коды. Если алгоритм становился известным, шифр переставал быть надежным.

Современная криптография основана на совершенно ином принципе. Алгоритмы RSA, Эль-Гамаля, ECC опубликованы в открытой печати, они изучаются в университетах, описаны в международных стандартах. Тем не менее, они остаются надежными. Почему? Потому что их стойкость обеспечивается не неизвестностью алгоритма, а математической сложностью обратной задачи.

Любой может взять открытый ключ RSA — пару чисел (n, e) — и попытаться расшифровать сообщение. Для этого нужно найти секретную экспоненту d, а для этого — разложить n на множители. Но если n выбрано правильно (произведение двух больших простых чисел), эта задача практически неразрешима, хотя прямая задача (возведение в степень по модулю) решается легко.

Таким образом, математика позволила спрятать секрет «на виду у всех». Мы публикуем полное описание алгоритма, но без знания конкретных простых чисел (ключа) прочесть текст нельзя. Информация защищена не стеной секретности, а стеной вычислительной сложности.

Заключение

Эволюция криптографии от примитивных шифров древности до современных криптосистем представляет собой яркий пример того, как абстрактные математические идеи находят практическое применение, меняющее мир.

На протяжении тысячелетий криптография развивалась как искусство, основанное на лингвистике, изобретательности и скрытности алгоритмов.

Во второй половине XX века произошла математизация криптографии — она превратилась в строгую научную дисциплину.

Фундаментом современных криптосистем стали теория чисел и теория вычислительной сложности. Понятия простого числа, факторизации, дискретного логарифмирования, эллиптических кривых образуют основу алгоритмов защиты информации.

Стойкость современных шифров опирается не на секретность алгоритма, а на вычислительную сложность обратных математических задач.

Математика сделала криптографию «прозрачной» — алгоритмы можно публиковать открыто, не опасаясь компрометации системы.

Дальнейшее развитие криптографии связано с появлением квантовых компьютеров, которые могут поставить под угрозу существующие алгоритмы (благодаря алгоритму Шора, эффективно решающему задачи факторизации и дискретного логарифмирования). Это стимулирует развитие постквантовой криптографии, основанной на иных математических задачах (теория решеток, коды, исправляющие ошибки, многомерные квадратичные системы).

Список литературы:

1. День шифровальщика // Предметно-методическая кафедра информатики и ИКТ Оренбургского президентского кадетского училища. — 2015. — URL: http://ikt.1pku.ru/?p=1446
2. Марухина Л.В., Ребковец П.А. Интегрированный урок «Криптография и тайнопись» // Первое сентября. — 2016. — URL: https://urok.1sept.ru/articles/662498
3. Криптосистемы // Национальный открытый университет «ИНТУИТ». Лекция 15. — 2010. — URL: https://intuit.ru/studies/educational_groups/1320/courses/408/lecture/9373
4. О стойкости // НИИ прикладных проблем математики и информатики БГУ. — URL: https://apmi.bsu.by/blog/cryptology/rsa-vs-stb.html
5. Криптография с использованием эллиптических кривых // Национальный открытый университет «ИНТУИТ». Лекция 11. — 2003. — URL: https://intuit.ru/studies/courses/28/28/lecture/20430
6. Черепнев М.А. О вычислительной сложности алгоритмов факторизации и дискретного логарифмирования. — 2017. — 25 с.