УДК 624.21

Криптография и шифрование: как математика защищает данные

***Хасанов Давуд Маратович**, студент 1-го курса*
кафедры «Строительные конструкции»
Белорусский национальный технический университет, г. Минск
(Научный руководитель – Ковалёнок Н.В., старший преподаватель)

Криптография — это наука о защите информации с помощью математических методов. Её история охватывает века, но особенно важную роль она сыграла в годы Великой Отечественной войны, когда надёжная шифровальная связь имела стратегическое значение. Советские криптографы разработали ряд уникальных шифровальных машин и методов, которые обеспечивали безопасность передачи приказов и разведданных.

Математические основы криптографии. Криптография опирается на несколько ключевых математических дисциплин:

Теория чисел:

- **Простые числа и факторизация** – основа RSA (сложность разложения больших чисел).
- **Модульная арифметика** – используется в шифрах (например, $A \equiv B \bmod m$).
- **Функция Эйлера** – важна для генерации ключей в RSA.

Алгебра и теория групп:

- **Дискретные логарифмы** – являются основой алгоритма Диффи-Хеллмана.
- **Эллиптические кривые** – используются в ECC (Elliptic Curve Cryptography).

Теория вероятностей и статистика:

- Криптоанализ часто использует статистические методы для взлома шифров (например, частотный анализ в шифре Цезаря).

Шифровальные машины СССР в годы Великой Отечественной войны. Роторная шифровальная машина "М-100" ("Спектр") - самая известная советская шифровальная машина, использовавшаяся в годы войны.

Принцип работы:

- Основана на роторном механизме, схожим с более ранним зарубежным аналогом, но с усовершенствованной схемой.
- Состояла из нескольких вращающихся дисков (роторов), каждый из которых выполнял замену букв по сложному алгоритму.

- После каждой буквы роторы сдвигались, меняя схему шифрования (как в современных потоковых шифрах).

Математическая основа:

- Каждый ротор реализовывал подстановочный шифр (перестановку алфавита).
- Общая зашифрованность определялась числом роторов и их начальным положением.

Пример шифрования:

1. Исходное сообщение: "АТАКА"
2. Каждая буква заменялась по текущему положению роторов.
3. После обработки каждой буквы роторы поворачивались, меняя таблицу замены.

Недостатки:

- Требовала высокой точности синхронизации на принимающей и передающей стороне.
- При потере исходных настроек расшифровка становилась почти невозможной.

Книжный шифр и ручные методы. Помимо машинных шифров, активно использовались ручные методы, особенно в условиях нехватки техники.

Метод «двойной табличной замены»:

1. **Ключ 1** – перестановка алфавита (например, по кодовому слову "ПОБЕДА").
2. **Ключ 2** – сдвиг на фиксированное число (например, +3).

Пример шифрования слова «АТАКА»:

1. Замена по таблице: А→П, Т→У, К→Н → "ПУПНП".
2. Сдвиг (+3): П→С, У→Х, Н→Р → "СХСРС".

Уязвимость:

- При перехвате большого числа сообщений возможен частотный анализ.

Современная криптография: пример RSA. Генерация ключей:

1. Выбираются два больших простых числа p и q (например, p=61, q=53).
2. Вычисляется n = p * q = 3233 и φ(n) = (p-1)(q-1) = 3120.
3. Выбирается e (обычно 65537), взаимно простое с φ(n).
4. Вычисляется $d \equiv e^{-1} \bmod \varphi(n)$ (с помощью расширенного алгоритма Евклида).

Открытый ключ: (e=17, n=3233)

Закрытый ключ: (d=2753, n=3233)

Шифрование числа 65

- $c \equiv 65^{17} \bmod 3233 = 2790$

Расшифровка

- $m \equiv 2790^{2753} \bmod 3233 = 65$

Почему это безопасно? Факторизация n=3233 на p=61 и q=53 проста, но для n из 2048 бит (~600 цифр) это требует миллионов лет вычислений.

Заключение. Работа над этим рефератом позволила мне глубже понять, как математика и криптография защищают информацию. Раньше я не задумывался, что даже в годы Великой Отечественной войны использовались сложные шифровальные машины, такие как советская «М-100». Меня удивило, как роторные механизмы и табличные шифры обеспечивали безопасность связи, несмотря на ограниченные технологии того времени.

Особенно интересным оказался разбор математической стороны шифрования: я узнал, что такие понятия, как простые числа, модульная арифметика и функция Эйлера, лежат в основе современных алгоритмов вроде RSA. Теперь я понимаю, почему взломать хороший шифр так сложно — всё упирается в вычислительную сложность математических операций.

Этот реферат показал мне, что криптография — это не просто абстрактная наука, а важный инструмент, который спасал жизни в войну и сейчас защищает наши данные в интернете. Хотелось бы и дальше изучать, как развиваются методы шифрования, особенно с появлением квантовых компьютеров.

Литература:

1. Коутинхо С. — "Введение в теорию чисел. Москва: Постмаркет, 2001.
2. Статьи о советских шифровальных машинах в журнале "Защита информации".
3. Материалы музея криптографии (Москва).