

Представленные здесь исторические исследования объединяет общий момент: в обоих случаях ученым удалось добиться успеха вследствие применения к зашифрованным текстам той или иной давности современных криптоаналитических методов.

В первом случае в архивах Национальной библиотеки Франции коллекция писем, написанных необычными символами, лежала забытой в папке с неправильной маркировкой, пока группа энтузиастов не заинтересовалась их историческим происхождением. Используя для взлома шифра специальный алгоритм и ручной анализ, они смогли расшифровать документы и идентифицировать их как неизвестные ранее письма королевы Шотландии Марии I Стюарт в годы, предшествовавшие ее казни в 1587 году. Результаты были опубликованы в журнале *Cryptologia* в начале 2023 года.

Второй материал посвящен одному из наиболее широко освещавшихся нераскрытых дел о серийных убийцах. В 1968–1969 годах человек, называвший себя Зодиаком, убил, по меньшей мере, пять человек в Северной Калифорнии. Тогда же убийца отправил ряд писем в местные газеты вместе с четырьмя шифрами. Один из них, часто упоминаемый как Z340, на протяжении 51 года ставил в тупик и любителей криптозагадок, и профессиональных криптографов. Однако в декабре 2020 года международная команда исследователей объявила, что ей удалось расшифровать Z340, и опубликовала научный труд, который раскрывает масштабы проделанной работы. Последующая проверка, проведенная ФБР, подтвердила корректность решения, предложенного авторами статьи.

I. Расшифровка утерянных писем Марии Стюарт 1578–1584 годов

1. Введение

2. Мария, королева Шотландии

3. Источники

- 3.1. Письма Марии к Кастельно
- 3.2. Расшифрованные нами шифртексты
- 3.3. Шифры Марии

4. Дешифрование писем

- 4.1. Шифры описываемого времени
- 4.2. Транскрибирование писем
- 4.3. Первоначальная расшифровка
- 4.4. Восстановление символов-омофонов
- 4.5. Восстановление символов для слов и частей слов
- 4.6. Восстановление символов, обозначающих имена и географические названия
- 4.7. Восстановление символов, обозначающих названия месяцев
- 4.8. Полностью реконструированный шифр Марии – Кастельно
- 4.9. Сравнение шифра Марии – Кастельно с родственными шифрами

5. Расшифрованные письма

- 5.1. Инвентаризация писем и их временные рамки
- 5.2. Основные темы, затронутые в письмах
- 5.3. Краткое содержание писем
 - Письма, датированные 1576–1579 годами*
 - Письма, датированные 1580–1581 годами*
 - Письма, датированные периодом с начала 1582 года по середину 1583 года*
 - Письма, датированные периодом с середины 1583 года по 1584 год*

6. Секретные каналы связи Марии Стюарт

- 6.1. Официальные и секретные каналы
- 6.2. Доставка и перехват писем
- 6.3. Меры предосторожности
- 6.4. Тайные курьеры
- 6.5. Кодовые имена и псевдонимы

7. Заключение

Приложение А. Алгоритм взлома кода

Приложение В. Ошибки шифрования и перекрестная контаминация шифров

Приложение С. Обновленный перечень известных писем Марии, адресованных Кастельно

Литература

II. Разгадка 340-символьной криптограммы убийцы Зодиака

1. Предыстория

- 1.1. Омофонические шифры
- 1.2. Шифры перестановки
- 1.3. Первый шифр Зодиака: Z408
- 1.4. Второй шифр Зодиака: Z340
- 1.5. Остальные шифры Зодиака

2. Исторические попытки взлома Z340

- 2.1. Заявления о решении в популярных СМИ (2011 – настоящее время)
- 2.2. Представление предыдущих работ авторов (2012–2017)
- 2.3. Предыдущие научные исследования (1993–2019)
- 2.4. Вычислительные средства и методы (1969–2020)

3. Наблюдения и измерения

- 3.1. Наблюдения и гипотезы ФБР

4. Гипотеза: Z340 – это шифр транспонирования и омофонической замены

5. Атака на Z340

- 5.1. Краудсорсинговые исследования
- 5.2. Количество повторяющихся биграмм
- 5.3. Исследования по перемещению
- 5.4. Прорывное решение: первые 9 строк
- 5.5. Прорывное решение: оставшиеся секции

6. Оценка фон цур Гатеном расстояния единственности Z340

7. Обсуждение и открытые вопросы

- 7.1. Рассуждения о методе перестановки
- 7.2. Безопасность через скрытность
- 7.3. Криптографические способности Зодиака

8. Направления будущих исследований

- 8.1. Личность Зодиака
- 8.2. Оставшиеся криптограммы Зодиака
 - 8.2.1. Z13 и Z32
 - 8.2.2. Z18
 - 8.2.3. Прочие символы
- 8.3. Усовершенствование криптоаналитических инструментов
- 8.4. Классификация типов шифров

Литература