Министерство образования Республики Беларусь

Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Факультет компьютерных систем и сетей

Кафедра гуманитарных дисциплин

РЕФЕРАТ  
На тему: «Симметричная криптосистема»

Выполнил: студент 3 курса

группы №250541

Тарасенко К. А.

Проверил:

\_\_\_\_\_\_\_\_\_

МИНСК 2025

План

1. Шифр Цезаря
2. Шифр Виженера
3. Принципы построения блочных симметричных алгоритмов. Алгоритм 34.191 31-2011

**1. Шифр Цезаря.**

Шифр Цезаря — классический пример моноалфавитной подстановки, где каждая буква открытого текста заменяется на букву, стоящую в алфавите на фиксированное число позиций (сдвиг) дальше. Этот метод назван в честь Гая Юлия Цезаря, который использовал его с ключом **3** для защиты военной переписки. Принцип работы крайне прост: алфавит циклически сдвигается, а буквы за пределами **Z** возвращаются к началу (например, **X** при сдвиге +3 становится **A**).

Математически шифрование описывается формулой:

где *P* — числовой код исходной буквы (A=0, B=1, …, Z=25), *K* — ключ (сдвиг), *C* — код зашифрованной буквы. Дешифровка выполняется обратной операцией:

Шифр Цезаря обладает двумя критическими уязвимостями:

* Малое пространство ключей. Для английского алфавита существует всего 25 значимых ключей (сдвиг 0 или 26 не меняет текст). Злоумышленник может перебрать все варианты за секунды;
* Уязвимость к частотному анализу. Буквы в зашифрованном тексте сохраняют частотные характеристики языка. Например, в английском чаще всего встречается E (12.7%), затем T, A и т.д. Сопоставив частоты, атакующий легко определит сдвиг.

Методы взлома:

* Полный перебор (brute force) — проверка всех 25 возможных ключей.
* Автоматический частотный анализ — сравнение распределения букв с эталонным (например, через хи-квадрат тест).
* Использование известных фрагментов текста. Если известна часть исходного сообщения (например, стандартное начало письма), ключ вычисляется за одну операцию.

Для повышения стойкости применялись вариации модифицированного шифра:

Ключевое слово. Перед сдвигом алфавит переставляли по ключевому слову (например, KEY → K E Y A B C D…), что усложняло частотный анализ. Однако это всё равно оставалось моноалфавитным шифром.

Нециклический сдвиг. Например, сдвиг увеличивался на 1 для каждой следующей буквы (A→D, B→F, C→I…). Это прообраз полиалфавитных систем, но без должной криптостойкости.

Историческое значение и современное применение

Несмотря на примитивность, шифр Цезаря сыграл ключевую роль в развитии криптографии:

Образовательная ценность. На его примере изучают базовые принципы шифрования, частотный анализ и атаки.

Основы для сложных алгоритмов. Идея сдвига легла в основу ROT13 (частный случай с ключом 13, где шифрование = дешифровка) и компонентов современных шифров (например, операции сложения по модулю в AES).

Использование в низкоуровневой защите. Иногда применяется для обфускации (например, в простых программах или играх), где важна не стойкость, а быстрота реализации.

Шифр Цезаря — фундаментальный, но абсолютно небезопасный метод. Его изучение помогает понять базовые принципы криптографии и необходимость сложных преобразований в современных алгоритмах.

**2. Шифр Виженера**

Шифр Виженера, разработанный в XVI веке французским дипломатом Блезом де Виженером, стал революционным шагом в криптографии, преодолев ключевые ограничения моноалфавитных шифров. В отличие от шифра Цезаря с его фиксированным сдвигом, здесь применяется полиалфавитная подстановка, где для каждой буквы используется свой сдвиг, определяемый ключевым словом.

Принцип работы

Ключевое слово повторяется до длины открытого текста. Каждая его буква задаёт величину сдвига для соответствующей буквы сообщения (A=0, B=1, ..., Z=25).

Результат: "LXFOPVEFRNHR".

Криптостойкость и атаки

Шифр Виженера долгое время считался "неразрушимым" (le chiffre indéchiffrable), но в XIX веке были найдены методы его взлома:

Определение длины ключа:

Метод Казиски: поиск повторяющихся последовательностей в шифротексте. Их расстояния могут быть кратны длине ключа. Тест Фридмана: статистический анализ индекса совпадений для разных предположительных длин ключа.

После определения длины текст разбивается на n групп, каждая из которых шифровалась одним сдвигом. К каждой группе применяется частотный анализ, как к шифру Цезаря.

Если ключ короче текста (например, "KEY" для сообщения "SECRETMESSAGE"), повторения в ключе создают паттерны, раскрывающие его длину. Для ключа "KEY":

Группа 1 (1-я, 4-я, 7-я буквы): S, R, S → частотный анализ указывает на сдвиг K.

Группа 2: E, E, A → сдвиг E.

Группа 3: C, M, G → сдвиг Y.

Для повышения стойкости использовались:

Автоключ: ключём становится сам открытый текст (например, начальный ключ "KEY", далее "KEYSECRETME..."). Устраняет цикличность, но уязвим к известному тексту.

Бесконечный ключ: ключевая последовательность генерируется из случайного источника (прародитель одноразового блокнота).

Шифр Виженера заложил основы для современных потоковых шифров. На его примере изучают криптоанализ, включая методы Казиски и Фридмана. ROT13 как вырожденный случай: При ключе "N" (сдвиг 13) шифр Виженера превращается в ROT13, где шифрование = дешифровка. Шифр Виженера — важный этап в криптографии, продемонстрировавший силу полиалфавитных систем, но его ручное применение уязвимо. Современные аналоги (например, AES в режиме CFB) используют схожие принципы, но с нелинейными преобразованиями и длинными псевдослучайными ключами.

Таблица 2 - Сравнение шифров Цезаря и Виженера

|  |  |  |
| --- | --- | --- |
| Критерий | Шифр Цезаря | Шифр Виженера |
| Тип | Моноалфавитный | Полиалфавитный |
| Ключ | Число (сдвиг) | Слово |
| Пространство ключей | 25 (для латиницы) | ~26^len(ключ) |
| Уязвимость | Частотный анализ | Метод Казиски и Фримдмана |
| Скорость взлома | Мгновенно | Зависит от ключа |

**3. Принципы построения блочных симметричных алгоритмов. Алгоритм 34.191 31-2011**

Современные симметричные криптосистемы используют блочное шифрование, где данные разбиваются на фиксированные блоки по 64 или 128 бит, каждый из которых обрабатывается отдельно или во взаимосвязи с другими в различных режимах работы. Основу таких алгоритмов составляют несколько ключевых принципов: конфузия, обеспечивающая запутывание связи между ключом и шифротекстом; диффузия, распространяющая влияние отдельных битов на весь блок; нелинейные преобразования через S-блоки; и многораундовая итерационная структура обработки данных. Эти принципы в совокупности обеспечивают высокий уровень криптостойкости.

Российский стандарт ГОСТ 34.191-2011, известный как "Кузнечик", представляет собой современный блочный шифр, принятый в 2011 году. Он работает с блоками по 128 бит, использует 256-битные ключи и выполняет 10 раундов преобразований. В каждом раунде последовательно применяются три основных типа преобразований: нелинейная подстановка через 8-битные S-блоки, линейная перестановка битов через P-блок и наложение раундового ключа с помощью операции XOR. Такая структура обеспечивает как конфузию (благодаря S-блокам), так и диффузию (за счет P-блока), что делает алгоритм устойчивым к различным видам криптоанализа.

Генерация раундовых ключей в "Кузнечике" осуществляется путем разделения исходного 256-битного ключа на две 128-битные части и их итеративного преобразования по схеме Фейстеля. Особенностью алгоритма является использование в процессе генерации ключей констант, полученных из дробной части числа e. Это добавляет дополнительную сложность потенциальным атакующим. В результате формируется 10 раундовых подключей, каждый из которых используется в соответствующем раунде шифрования.

Криптостойкость алгоритма ГОСТ 34.191-2011 подтверждена многочисленными исследованиями. Он демонстрирует устойчивость к дифференциальному и линейному криптоанализу, а также к атакам по времени выполнения. Однако теоретически возможны атаки на связанных ключах, особенно при уменьшенном числе раундов (менее 8). На практике для обеспечения максимальной безопасности всегда используется полный набор из 10 раундов.

Алгоритм находит широкое применение в российской криптографической инфраструктуре. Он входит в состав стандартов ГОСТ Р 34.11-2012 для хеширования, ГОСТ Р 34.10-2012 для электронной цифровой подписи, а также используется в российских модификациях протоколов TLS. По сравнению с американским стандартом AES-256, "Кузнечик" показывает сопоставимый уровень безопасности, но отличается внутренней структурой преобразований. В то время как AES использует операции SubBytes и ShiftRows, российский алгоритм опирается на S-блоки и P-блоки, что обеспечивает ему преимущество в скорости реализации на российских процессорах.

Реализация алгоритма возможна как аппаратными, так и программными средствами. Специализированные криптопроцессоры позволяют достигать тактовой частоты до 1 ГГц, а программные реализации могут быть оптимизированы с использованием современных инструкций x86 и SIMD-расширений. В перспективе рассматриваются направления адаптации алгоритма для постквантовой криптографии, оптимизации для устройств интернета вещей и интеграции с новыми протоколами защиты данных, такими как российский аналог IPsec. Таким образом, ГОСТ 34.191-2011 представляет собой современный, стойкий блочный шифр, который продолжает развиваться, сохраняя баланс между безопасностью и производительностью в условиях меняющихся технологических вызовов.

Список используемых источников

1. Гребенников В.В. Основы криптографии. М.: Гелиос АРВ, 2018. 320 с.
2. Романец Ю.В. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 2001. 376 с.
3. ГОСТ Р 34.191-2011. Информационная технология. Криптографическая защита информации. Алгоритм блочного шифрования. М.: Стандартинформ, 2011.
4. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хеширования. М.: Стандартинформ, 2012.
5. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012.
6. Аграновский А.В. Криптографические методы защиты информации. СПб.: БХВ-Петербург, 2019. 496 с.
7. Рекомендации по стандартизации (Р 50.1.111-2016). Методы криптографической защиты информации. М.: Стандартинформ, 2016.
8. Черёмушкин А.В. Криптографические протоколы. М.: МЦНМО, 2017. 272 с.