КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ ШИФРОВ ЗАМЕНЫ

Бигеза Я. О., Рыбак Д. В.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Стройникова Е. Д. – ассистент каф. информатики

В настоящее время данные являются самой ценной информацией, поэтому существует множество методов защиты. Их изучает наука криптография. Изначально она изучала методы шифрования информации.

Шифр — это сам алгоритм, по которому преобразуется сообщение, которое мы хотим передать. Шифрованное сообщение – это сообщение, прошедшее процесс шифрования. Расшифровать его можно с помощью ключа.

Криптостойкость шифра определяется по количеству времени, необходимому для его взлома. Шифры разделяются на **шифры перестановки**, **композиционные шифры** и **шифры замены**. Шифрами замены называются такие шифры, преобразования из которых приводят к замене каждого символа исходного сообщения на другие символы, причем порядок их следования совпадает с порядком следования соответствующих им символов исходного сообщения.

Математическая модель произвольного шифра замены:

$$S_A = (x, k, y, e, d)$$

где *x* — символ открытого текста в алфавите A,, y — символ шифротекста в алфавите B, *k* — ключ шифра, E_k — преобразование шифра с ключом $k_з$, D_k – преобразование расшифрования с ключом $k_р$.

Шифров замены существует множество, мы выделили некоторые из них.

1. **Шифр Вернама (XOR-шифр) (1890 г. - 1960 г.).**

Шифр основан на бинарной логике и обладает криптографической стойкостью. Без знания ключа расшифровать его невозможно (доказано Клодом Шенноном(1916 - 2001)).

Исходный алфавит — латиница, символы шифротекста - двоичный код по таблице ASCII, ключ шифра - слово на языке исходного сообщения, где каждому символу также присвоен двоичный код. Ключ записывается столько раз, сколько потребуется для того, чтобы каждому символу исходного сообщения соответствовал символ ключа. Между символами сообщения и ключа проводится операция XOR - “исключающее или” (если все сигналы равны между собой: 0-0 или 1-1, то на выходе получаем 0, если сигналы не равны: 0-1 или 1-0, то на выходе получаем 1). Таким образом, мы получаем новую запись в виде двоичного кода.

С образцом программы, выполняющей алгоритм данного шифра на языке C++ вы можете ознакомиться по ссылке.

2. **Аффинный шифр.**

Для реализации аффинного шифра необходимо выбрать 2 числа для использования в качестве ключа шифрования, обозначим их как a и b. Число a должно быть взаимно простым с 26. Пусть каждая буква текста, который необходимо зашифровать, имеет соответствующий числовой индекс от 0 до 25. Затем для каждой буквы текста нужно вычислить новый индекс, умножив ее индекс на число a и прибавив остаток от деления на 26. Полученный результат будет соответствовать другой букве в алфавите. Таким образом, каждая буква текста заменяется на другую букву, образуя зашифрованный текст.

Чтобы расшифровать текст, используется обратная формула:

$$y = a^{-1} * (x - b) \ (mod\ 26)$$

где *x* — индекс зашифрованной буквы, a^{-1} — обратное число к *a*, y — индекс расшифрованной буквы. Используя таблицу соответствия букв и индексов, мы можем найти соответствующую букву для каждого вычисленного значения y, чтобы получить исходный текст.

С образцом программы, выполняющей алгоритм данного шифра на языке C++ вы можете ознакомиться по ссылке.

3. Шифр «Квадрат Полибия» (ок. 200 до н. э., — ок. 120 до н. э.)

Квадрат Полибия представляет собой квадрат 5×5, столбцы и строки которого нумеруются цифрами от 1 до 5. В каждую клетку этого квадрата записывается по алфавиту одна буква.

Существует несколько методов шифрования с помощью квадрата Полибия. Ниже приведены три из них.

Метод 1: Для шифрования на квадрате находили букву текста и вставляли в шифр нижнюю от неё в том же столбце. Если буква была в нижней строке, то брали верхнюю из того же столбца.

Метод 2: Сообщение преобразуется в координаты по квадрату Полибия, координаты записываются вертикально. Затем координаты считывают по строкам: Далее координаты преобразуются в буквы по этому же квадрату:

Метод 3: Полученный первичный шифротекст шифруется вторично. При этом он выписывается без разбиения на пары. Полученная последовательность цифр сдвигается циклически влево на нечетное количество шагов. Эта последовательность вновь разбивается в группы по два. И по таблице заменяется на окончательный шифротекст.

Квадрат Полибия является примером шифра замены, поэтому неустойчив к частотной атаке.

4. Шифр Плейфера

Шифр Плейфера использует матрицу 5x5 для латинского алфавита, содержащую ключевое слово. Чтобы составить ключевую матрицу, нужно сначала заполнить пустые ячейки матрицы буквами ключевого слова без повторяющихся символов, потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку.

Для того чтобы зашифровать сообщение, необходимо разбить его на группы из двух символов. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем, руководствуясь следующими 4 правилами, зашифруем пары символов исходного текста.

Если два символа биграммы совпадают (или если остался один символ), заменяем второй символ на «X», зашифровываем новую пару символов и продолжаем.

Если символы биграммы исходного текста встречаются в одной строке, то эти символы заменяются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, убрав из алфавита символы «X» (или «Q»), если они не несут смысла в исходном сообщении.

В настоящее время, в связи с быстрым развитием технологий, многие из шифров замены уже не способны обеспечить необходимую степень безопасности. Поэтому необходимо постоянно совершенствовать методы защиты информации, а в случае шифров замены необходимо еще правильно подбирать ключи. Также некоторые из них неустойчивы к некоторым атакам, что делает их менее надежными.

Список использованных источников:

1. Шнайер Б. Прикладная криптография. 2012. Гл. 1.4-1.5.

2. Криптографическая защита информации: учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. Тамбов : ТГТУ, 2020.140 с.

3. Алферов А.П., Зубов А.Ю. Основы криптографии. - М.: Гелиос АРВ, 2005.