

1. ИССЛЕДОВАНИЕ ПРОЦЕССА ЗАШИФРОВАНИЯ С ПОМОЩЬЮ ПРОСТОЙ ЗАМЕНЫ И РЕШЕТКИ КАРДАНО

Теоретическая часть

Одними из самых простых и известных шифров являются шифры простой однозначной замены. Данные шифры используют в качестве шифрующего алгоритма замены или подстановки, при которых осуществляется замена символов (слов) открытого текста соответствующими символами, принадлежащими алфавиту шифротекста.

Рассмотрим модель шифра подстановки (замены). Определим модель $\varepsilon_A = (X, K, Y, E, D)$ произвольного шифра замены. Будем считать, что открытые и шифрованные тексты являются словами в алфавитах A и B соответственно: $X \subset A^*$, $Y \subset B^*$, $|A| = n$, $|B| = m$. Здесь и далее C^* обозначает множество слов конечной длины в алфавите C .

Перед зашифрованием открытый текст предварительно представляется в виде последовательности подслов, называемых шифрвеличинами. При зашифровании шифрвеличины заменяются некоторыми их эквивалентами, которые назовем шифробозначениями. Как шифрвеличины, так и шифробозначения представляют собой слова из A^* и B^* соответственно.

Пусть $U = \{u_1, \dots, u_N\}$ – множество возможных шифрвеличин, $V = \{v_1, \dots, v_M\}$ – множество возможных шифробозначений. Эти множества должны быть такими, чтобы любые тексты $x \in X$, $y \in Y$ можно было представить словами из U^* , V^* соответственно. Требование однозначности расшифрования влечет неравенства $N \geq n$, $M \geq m$, $M \geq N$.

Для определения правила зашифрования $E_k(x)$ в общем случае нам понадобится ряд обозначений и понятие распределителя, который, по сути, и будет выбирать в каждом такте шифрования замену соответствующей шифрвеличине.

Поскольку $M \geq N$, множество V можно представить в виде объединения непересекающихся непустых подмножеств V^j . Семейство биекций, соответствующее этому семейству разбиений множества V , обозначим через $\{\varphi_\alpha\}$: $V \Rightarrow \{V_\alpha^{(1)}, \dots, V_\alpha^{(N)}\}$ и будем предполагать, что $\varphi_\alpha(u_i) = V_\alpha^{(i)}$, $i = 1, \dots, N$.

Рассмотрим также произвольное отображение $\Phi: K \times N \Rightarrow N_r^*$, где $N_r = \{1, 2, \dots, r\}$, такое, что для любых $k \in K$, $l \in N$ выполнено $\Phi(k, l) = a_1^{(k)} \dots a_l^{(k)}$, $a_j^{(k)} \in N_r$, $j = 1, \dots, r$.

Назовем последовательность $\Phi(k, l)$ распределителем, отвечающим данным значениям $k \in K, l \in N$.

Теперь мы сможем определить правило зашифрования произвольного шифра замены. Пусть $x \in X, x = x_1 \dots x_l, x_i \in U, i = 1, \dots, l, k \in K$ и $\Phi(k, l) = a_1^{(k)} \dots a_l^{(k)}$. Тогда $E_k(x) = y$, где $y = y_1 \dots y_l, y_i \in \varphi_{a_j^{(k)}}^{(k)}(x_j), j = 1, \dots, l$.

В качестве y_j можно выбрать любой элемент множества $\varphi_{a_j^{(k)}}^{(k)}(x_j)$. Всякий раз при шифровании этот выбор можно производить случайно. Подчеркнем, что такая многозначность при зашифровании не препятствует расшифрованию, т. к. $V_a^{(i)} \cap V_a^{(j)} = \emptyset$ при $i \neq j$.

Рассмотрим пример реализации шифра одноалфавитной замены. Вскрытие одноалфавитного шифра осуществляется на учете частоты появления отдельных букв или сочетаний (биграмм, триграмм, и т. д.) в языке. Примером одноалфавитного шифра замены является шифр Цезаря. Шифрование осуществляется по таблице, представляющей собой матрицу, содержащую 2 строки и n столбцов, где n – число символов алфавита (для русского алфавита – 32). Первая строка содержит все символы алфавита. Вторая строка получается из предыдущей путем циклического сдвига вправо или влево на несколько символов (букв алфавита).

Выбирается циклический сдвиг шифра. После чего процесс зашифровывания осуществляется следующим образом:

1) строится матрица для осуществления зашифрования с установленным циклическим сдвигом;

2) каждая буква шифротекста находится на пересечении столбца таблицы, определяемого буквой открытого текста, и строки, определяемой буквой ключа.

Пример. Пусть надо зашифровать текст *А нам все равно*.

В качестве ключа используем циклический сдвиг влево на 11 букв русского алфавита (буква *А* заменяется на букву *К*).

Тогда процесс зашифрования можно представить в следующем виде. Таблица 1 для циклического сдвига на 11 символов русского алфавита представлена ниже.

Таблица 1.1

Шифр одноалфавитной замены

Исходный алфавит															
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	Р
Циклический сдвиг на 11 символов															
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Исходный алфавит															
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	–
Циклический сдвиг на 11 символов															
Ы	Ь	Э	Ю	Я	–	А	Б	В	Г	Д	Е	Ж	З	И	Й

В результате процедуры шифрования получаем текст, представленный в таблице 1.2.

Таблица 1.2

Пример шифрования текста с помощью шифра одноалфавитной замены

Исходный текст														
А	–	Н	А	М	–	В	С	Е	–	Р	А	В	Н	О
Зашифрованный текст														
К	Й	Ч	К	Ц	Й	М	Ы	П	Й	Ъ	К	М	Ч	Щ

Расшифровка осуществляется следующим образом. Во второй строке происходит поиск соответствующей буквы шифротекста. Находящаяся над ней в первой строке буква и будет соответствовать букве исходного текста.

Шифры перестановки, или транспозиции, изменяют только порядок следования символа или других элементов исходного текста. Пример – решетка Кардано, которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. При зашифровке буквы сообщения вписываются в эти отверстия. При расшифровке сообщение вписывается в диаграмму нужных размеров, затем накладывается решетка, после чего на виду оказываются только буквы открытого текста.

Решетки можно использовать двумя способами.

В первом случае зашифрованный текст состоит только из букв исходного сообщения. Решетка изготавливается таким образом, чтобы при ее последовательном использовании в различных положениях каждая клетка лежащего под ней листа бумаги оказалась занятой (это поворотная решетка).

1	2	3	4	5	1
5	1	2	3	1	2
4	3	1	1	2	3
3	2	1	1	3	4
2	1	3	2	1	5
1	5	4	3	2	1

Рис. 1.1. Пример решетки Кардано

Если решетку поворачивать на 90° последовательно, то при возврате к исходному состоянию все клетки будут заполнены. Причем в каждом окаймлении должна быть вырезана только одна цифра (внешнее обрамление имеет 5 дырок – отмечены серым цветом, во внутреннем – 1, в среднем – 3). Пример простейшей решетки Кардано приведен на рис. 1.1.

Второй – стеганографический – метод использования решетки позволяет скрыть факт секретного сообщения. В этом случае заполняется только часть листа, а в остальное место дописываются буквы или слова ложного текста.

Задания

1. Изучить теоретический материал работы.
2. Провести исследование системы шифрования на основе алгоритма одноалфавитной замены.
3. Провести исследование системы шифрования на основе алгоритма Кардано.

Содержание отчета

Отчет по лабораторной работе оформляется в виде документа Word и должен включать:

- 1) название лабораторной работы;
- 2) цель лабораторной работы;
- 3) формулировку индивидуального задания и результат его выполнения;
- 4) краткие выводы по результатам выполнения лабораторной работы.

Контрольные вопросы для защиты работы

1. Дайте определение шифра. Какие виды шифров вы знаете?
2. Дайте определение шифра одноалфавитной замены.
3. Назовите основные достоинства и недостатки шифра одноалфавитной замены.
4. Дайте определение шифра простой подстановки замены.
5. Назовите основные достоинства и недостатки шифра Кардано.

Индивидуальное задание 1

Задача 1. Используя данные своего варианта, реализуйте шифр одноалфавитной замены

Вариант	Исходный текст	Ключ
1	прекрасная_погода	вправо 13
2	дождливый_вечер	влево 13
3	красный_закат	вправо 14
4	удивительная_радуга	влево 14
5	утренний_туман	вправо 15
6	поздний_закат	влево 15
7	западный_ветер	вправо 16
8	неожиданный_шторм	влево 16
9	весенняя_гроза	вправо 17
10	неукротимая_пурга	влево 17
11	осенняя_погода	вправо 18
12	летний_зной	влево 18

Задача 2. Осуществите процесс дешифрования, используя зашифрованное сообщение и примененный сдвиг шифра одноалфавитной замены.

Вариант	Зашифрованный текст	Ключ
1	ятютсцынмъ_ютхшн	вправо 14
2	чъяутчѐць	влево 14
3	юуячыуаяняэypo	вправо 15
4	цытячдвсэвехт	влево 15
5	юазюспэшфоб_пяфешш	вправо 16
6	вг_б_ясрдфэс	влево 16
7	ёхювапытрфарвр	вправо 17
8	бахфюоопыщющю	влево 17
9	свьюаг_гсръбъу_ы	вправо 18
10	я_юшчсюэпногвзъешш	влево 18
11	фнгадтсбывтяыцн	вправо 19
12	_уеуъчунщэъб_о	влево 19