Лабораторная работа № 4

Шифры подстановки и замены

Цель работы

Освоить основные алгоритмы шифрования перестановки и замены.

Указание к работе

Ознакомиться с лекционным материалом, а также с литературой [1], [8]–[11].

Подстановочные шифры

Шифр простой подстановки.

В таком шифре производится замена каждой буквы сообщения на некоторый определенный символ (обычно также на букву).

Таким образом, сообщение $M = m_1 m_2 ... m_n$, где $m_1 m_2 ... m_n$ – последовательные буквы, переходит в шифротекст $C = [c_1 c_2 ... c_n] = [\varphi(m_1)\varphi(m_2)...\varphi(m_n)]$, причем функция φ имеет обратную функцию. Ключ является просто перестановкой алфавита (если буквы заменяются на буквы).

Шифр Виженера и его варианты.

В шифре Виженера ключ задается набором из T букв. Такие наборы подписываются с повторением под сообщением и полученные две последовательности складываются по модулю, равному мощности алфавита исходного сообщения (каждая буква рассматриваемого алфавита нумеруется). Таким образом: $c_t = (m_t + k^\tau) \bmod |X|$, где $t = (i-1)\cdot T + \tau, \quad i = 1,2...; \quad \tau = \overline{1,T}$, $|X|$ – мощность алфавита сообщений. Обратное преобразование: $m_t = (c_t - k^\tau + |X|) \bmod |X|$.

Шифр Виженера с периодом $T = 1$ называется ***шифром Цезаря***[1]. Он представляет собой простую подстановку, в которой каждая буква сообщения M сдвигается вперед на фиксированное число мест по алфавиту.

Так называемый ***шифр Бофора*** и ***видоизмененный шифр Бофора*** подобны шифру Виженера. В них сообщения зашифровываются с помощью равенств $c_i = (k_i - m_i) \bmod |X|$ и $c_i = (m_i - k_i) \bmod |X|$ соответственно.

Повторное применение двух или более шифров Виженера будет называться ***составным шифром Виженера***. Он имеет уравнение $c_i = (m_i + k_i + ... + s_i) \bmod |X|$, где $k_i,..., s_i$ вообще говоря, имеют различные периоды. Период их суммы $k_i + ... + s_i$ будет наименьшим общим кратным отдельных периодов.

Если используется шифр Виженера с неограниченным неповторяющимся ключом, то мы имеем ***шифр Вернама***, в котором k_i выбираются случайно и независимо среди чисел $\overline{0,|X|}$. Если ключом служит текст, имеющий смысл, то имеем ***шифр «бегущего ключа»***.

Шифр Виженера с перемешанным один раз алфавитом представляет собой простую подстановку с последующим применением шифра Виженера: $c_i = \varphi(m_i) + k_i$, тогда $m_i = \varphi^{-1}(c_i - k_i)$.

Диграммная, триграммная и n-граммная подстановки.

Вместо подстановки одной буквы можно использовать подстановку диграмм, триграмм и т.д. Для диграммной подстановки в общем виде требуется ключ, состоящий из перестановок $|X|^2$ диграмм. Он может быть представлен с помощью таблицы, в которой ряд соответствует первой букве диграммы, а столбец – второй букве, причем клетки таблицы заполнены заменяющими символами (обычно также диграммами).

Имеется один метод подстановки *n*-грамм, который заключается в применении к последовательным *n*-граммам некоторой матрицы, имеющей обратную (***матричная система***). Предполага-

[1] 1 век до н.э. Данный шифр был описан историком Древнего Рима Светонием. Гай Юлий Цезарь использовал в своей переписке шифр собственного изобретения.

ется, что буквы занумерованы от 0 до $|X|-1$ и рассматриваются как элементы некоторого алгебраического кольца. Если к *n*-грамме сообщения применить матрицу *A*, то получится *n*-грамма криптограммы: $A\cdot[m_1, m_2,..., m_n]=[c_1, c_2,..., c_n]$.

Матрица *A* является ключом, и расшифровка выполняется с помощью обратной матрицы: $[m_1, m_2,..., m_n]=A^{-1}\cdot[c_1, c_2,..., c_n]$. Обратная матрица будет существовать тогда и только тогда, когда определитель $|A|$ имеет обратный элемент в данном кольце.

Перестановочные шифры

Перестановка с фиксированным периодом T.

В этом случае сообщение делится на группы символов длины *T* и к каждой группе применяется одна и та же перестановка. Эта перестановка является ключом; она может быть задана некоторой перестановкой первых *T* целых чисел.

Последовательное применение двух или более перестановок будет называться составной перестановкой. Если периоды этих перестановок равны $T_1,...,T_s$ то, очевидно, в результате получится перестановка периода *T*, где *T* – наименьшее общее кратное $T_1,...,T_s$.

Дробные шифры.

В этих шифрах каждая буква сначала зашифровывается в две (или более) буквы или в два (или более) числа, затем полученные символы каким-либо способом перемешиваются (например, с помощью транспозиции), после чего их можно снова перевести в первоначальный алфавит. После того, как полученный ряд чисел подвергнут некоторой перестановке, его можно снова разбить на пары чисел и перейти к буквам.

Пример.

Необходимо предложить вариант шифра матричной системы (триграмма). Пусть алфавит сообщений $X=\{a,b,c,d,e,f\}$. Буква *a* кодируется 0, $b\to 1,...,\ f\to 5$. Надо подобрать такую матрицу *A*, чтобы $|A|^{-1}$ был равен одному из возможных значений $0\div 5$: $A=\begin{bmatrix}1 & 1 & 0\\ 4 & 3 & 1\\ 4 & 1 & 2\end{bmatrix}$, $|A|=1$. Сообщение для отправки: *badeff*. Делим его на блоки по три символа, кодируем: $M_1=[1\ \ 0\ \ 3]$, $M_2=[4\ \ 5\ \ 5]$. Каждый полученный вектор преобразуем в шифр: $M_1^T\cdot A=[1\ \ 7\ \ 10]$, $M_2^T\cdot A=[9\ \ 36\ \ 31]$. Передаем по каналу связи C_1, C_2; злоумышленник, не зная код матричного шифрования, пытается прочесть сообщение, используя, например, $B=\begin{bmatrix}3 & 4 & 0\\ 3 & 3 & 1\\ 4 & 3 & 2\end{bmatrix}$ (из достоверных источников ему всё же стал известен определитель матрицы-кода). И получает: $N_1=B^{-1}C_1=[-13\ \ 10\ \ 16]$: ничего не вышло, хотя кодировку $a\to 0, b\to 1,...,\ f\to 5$ он все же знает! Тот же, кому адресовано наше сообщение, получив его, дешифрует: $M_1=A^{-1}C_1=[1\ \ 0\ \ 3]$, $M_2=A^{-1}C_2=[4\ \ 5\ \ 5]$, и декодирует: *badeff*.

Задание

I. Реализовать приложение для шифрования:
   1. Шифруемый текст должен храниться в одном файле, а ключ шифрования (если есть) – в другом.
   2. Шифрование производится согласно заданному в варианте алгоритму. Конкретную реализацию алгоритма нужно выбрать самостоятельно. В алфавит шифруемых сообщений, который задан в варианте, нужно добавить символ '_', который является разделителем слов.
   3. Зашифрованный текст должен сохраняться в файл.

II. Реализовать приложение для дешифрования:

1. Зашифрованный текст должен храниться в одном файле, ключ (если есть) – в другом.
2. Расшифрованный текст должен сохраняться в файл.

III. С помощью реализованных приложений выполнить следующие задания:
1. Протестировать правильность работы разработанных приложений при различных сообщениях и ключах.
2. Выполнить шифрование нескольких сообщений аналитически (вручную) и сравнить полученные шифротексты с результатами работы шифрующего приложения.
3. Проанализировать шифр на приведённые в лекции типы криптоаналитического вскрытия.
4. Проанализировать шифр с точки зрения совершенной криптостойкости, т.е. проверить выполнение условий теорем (о совершенной криптостойкости симметричной криптосистемы). Ответить на вопрос об идеальной стойкости данного шифра.
5. Сделать выводы о проделанной работе.

Требования к оформлению отчёта

Отчёт должен содержать:
- титульный лист (обязат.);
- задание на лабораторную работу (обязат.);
- описание метода решения заданий;
- описание разработанного программного средства;
- описание проведённых исследований (обязат.);
- программный код, написанный непосредственно студентами (обязат.);
- тестирование программы.

Отчёт не должен содержать орфографических, пунктуационных и смысловых ошибок.
Все его разделы должны быть выдержаны в едином стиле оформления.

Критерии оценивания качества работы

1. Графический интерфейс пользователя:
   1 – приложения имеют графический интерфейс пользователя;
   0 – приложения имеют интерфейс командной строки;
   Л.р. не принимается – иначе.
2. Выполнение требований к оформлению отчёта:
   1 – отчёт удовлетворяет всем требованиям;
   0 – отчёт не удовлетворяет всем требованиям, но содержит обязательные разделы;
   Л.р. не принимается – в отчёте нет хотя бы одного обязательного раздела.
3. Обработка ошибок:
   1 – все возможные ошибки и нестандартные ситуации (например, неудачная попытка открытия файла) обрабатываются программой, которая выдаёт соответствующее сообщение;
   0 – не все возможные ошибки обрабатываются программой.
4. Применение принципов структурного программирования:
   1 – все повторяющиеся либо логически целостные фрагменты программы выделены в качестве функций; работа каждой функции полностью определяется её параметрами (т.е. не используются глобальные переменные, все данные, нужные функции для работы, передаются ей через параметры); программа позволяет без перекомпиляции изменять все параметры, от которых зависит её работа; в тексте программы отсутствуют числовые константы (все необходимые константы объявляются как поименованные);
   0 – иначе (не выполняется что-либо из перечисленного).
5. Наличие комментариев в тексте программы:
   1 – комментариев достаточно для документирования исходных кодов;
   0 – комментариев недостаточно.
6. Глубина понимания материала лабораторной работы каждым членом бригады:
   1 – быстрые и правильные ответы на все вопросы;
   0 – не на все вопросы ответы правильные и быстрые;
   Л.р. не принимается – на половину вопросов ответы неправильные.

Варианты

Вариант	Алгоритм шифрования	Алфавит сообщения	Дополнительная информация
1	Шифр Виженера	$A \div Z$	Период $T = 5$
2	Шифр Бофора	$a \div z$	
3	Шифр Цезаря	$a \div я$	
4	Видоизмененный шифр Бофора	$A \div Z$	
5	Составной шифр Виженера	$0 \div 9$	Периоды $T_1 = 5$, $T_2 = 2$
6	Шифр простой подстановки	$А \div Я$	
7	Шифр Вернама	•,–	
8	Диграммная подстановка	$A \div Z$	
9	Матричная система	$a \div h$	(диграммная подстановка)
10	Матричная система	$a \div к$	(3-граммная подстановка)
11	Перестановка с периодом	$A \div Z$	Период $T = 6$
12	Дробные шифры	$А \div Я$	
13	Шифр Виженера	$a \div z$	Период $T = 2$
14	Шифр Бофора	$A \div Z$	
15	Шифр Виженера с перемешанным один раз алфавитом	$a \div я$	

Контрольные вопросы

1. Основные понятия криптографии.
2. Протоколы обмена ключами.
3. Основные аспекты криптоанализа.
4. Общая схема симметричных криптосистем.
5. Математические модели элементарных криптосистем.
6. Криптостойкость симметричных криптосистем.
7. Пессимистическое утверждение Шеннона (теорема).
8. Показатели криптостойкости.
9. Требования, предъявляемые к современным криптографическим системам.