НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н. Тихонова

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Задания (с разбором): материал 16

Подстановочные шифры

Евсютин О.О.

Москва 2020

1 ЦЕЛЬ РАБОТЫ

Целью данной работы является приобретение навыков программной реализации и криптоанализа применительно к простым подстановочным шифрам.

2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Простейшим примером подстановочного шифра является шифр простой замены.

Математически данный шифр может быть описан на языке подстановок.

Каждой букве алфавита A мощностью m ставится в соответствие число из диапазона $1 \dots m$ — другими словами, все символы алфавита нумеруются.

Множество возможных ключей шифра простой замены является симметрической группой степени m, то есть группой подстановок длины m: $K = S(A) = S_m$.

Открытый текст обозначим $x = (x_1,\ \dots,\ x_l)$, где $x_i \in A$, $i = \overline{1,\ l}$, соответствующий шифртекст — $y = (y_1,\ \dots,\ y_l)$.

Зашифрование открытого текста $x = (x_1,\ \dots,\ x_l)$ на ключе $k \in K$ может быть записано как $E_k(x) = \big(k(x_1),\ \dots,\ k(x_l)\big)$, расшифрование шифртекста $y = (y_1,\ \dots,\ y_l)$ на том же ключе — $D_k(y) = \big(k^{-1}(y_1),\ \dots,\ k^{-1}(y_l)\big)$, где $k^{-1} \in K$ — подстановка, обратная k.

Проще говоря, при шифровании каждый символ текста заменяется на другой символ с помощью ключевой подстановки.

Известным частным случаем шифра простой замены является шифр Цезаря, названный так по имени использовавшего его всю жизнь древнеримского полководца. Данный шифр основан на использовании одного-единственного ключа — подстановки, полученной циклическим сдвигом элементов второй строки относительно первой на три позиции влево.

Другим частным случаем шифра простой замены является аффинный шифр, основанный на так называемом аффинном преобразовании.

Данный шифр реализует замену символов открытого текста с использованием операций в кольце классов вычетов. Символы алфавита A мощностью m представляются элементами кольца классов вычетов $\mathbb{Z}_m$.

В качестве ключа аффинного шифра выступает пара значений $k = (\alpha, \beta)$, $\alpha \in \mathbb{Z}_m^*$, $\beta \in Z_m$, соответственно ключевое пространство имеет вид $K = \mathbb{Z}_m^* \times \mathbb{Z}_m$.

Открытый текст и шифртекст обозначим соответственно $x = (x_1,\ \dots,\ x_l)$ и $y = (y_1,\ \dots,\ y_l)$, где $x_i \in Z_m$, $y_i \in \mathbb{Z}_m$, $i = \overline{1,\ l}$.

Зашифрование отдельного символа открытого текста осуществляется по формуле $y_i = \alpha x_i + \beta$, $i = \overline{1,\ l}$, расшифрование — по формуле $x_i = (y_i - \beta)\alpha^{-1}$, $i = \overline{1,\ l}$.

Усилением аффинного шифра является аффинный рекуррентный шифр, когда для каждого символа открытого текста вычисляется новое ключевое значение на основе предыдущего. Для этого необходимо задать две ключевые пары $k_1 = (\alpha_1,\ \beta_1)$, $k_2 = (\alpha_2,\ \beta_2)$, и тогда ключевая пара для произвольного символа преобразуемой последовательности будет иметь вид $k_i = (\alpha_{i-1}\alpha_{i-2},\ \beta_{i-1} + \beta_{i-2})$, $i = \overline{3,\ l}$.

3 ЗАДАНИЕ

1) написать программную реализацию следующих шифров:
   - шифр простой замены:
   - аффинный шифр;

- аффинный рекуррентный шифр;

2) изучить методы криптоанализа моноалфавитных подстановочных шифров с использованием дополнительных источников;
3) провести криптоанализ данных шифров;
4) подготовить отчет о выполнении работы.

Программа должна обладать следующей функциональностью для каждого из реализованных в ней шифров:

1) принимать на вход произвольную последовательность символов, вводимую пользователем в качестве открытого текста или шифртекста;
2) принимать на вход секретный ключ вида, соответствующего конкретному шифру;
3) осуществлять зашифрование или расшифрование введенного текста по выбору пользователя.

Отчет должен содержать следующие составные части:

1) раздел с заданием;
2) раздел с краткой теоретической частью;
3) раздел с двумя-тремя примерами «ручного» шифрования для произвольных последовательностей символов;
4) раздел с результатами работы программы для тех же последовательностей символов, что и в предыдущем разделе;
5) раздел с примерами криптоанализа реализованных шифров;
6) раздел с выводами о проделанной работе.