Подготовка к контрольной работе

по истории криптографии

Собрал Мигалин Сергей

05.03.17

№1. Дать определение шифра, описав его компоненты

Шифр омофонной замены

$X = \{x_i,\ i = \overline{1,n}\}$

$A = \{a_1 \dots a_n\}$ – алфавит естественного языка

$|A| = n$

m – количество замен

$Y = \{y_1 = \{y_{1_1} \dots y_{1_{j_1}}\}, \dots y_n = \{y_{n_1} \dots y_{n_{j_n}}\}\}$

$\sum_{k=1}^{n} |y_k| = m$

p_i – частота встречаемости x_i

$\lfloor p_i m \rfloor$ – количество замен для i буквы

$K = \{k_1 = \begin{pmatrix} y_{1_1} & \dots & y_{n_{j_n}} \\ 1 & \dots & m \end{pmatrix}, \dots, k_m = \begin{pmatrix} y_{1_1} & \dots & y_{n_{j_n}} \\ m & \dots & 1 \end{pmatrix}$

$E_{k_j}(x_i) = \forall y_{i_s} \in y_i / k_j$

$D_{k_j}\left(y_{i_j}\right) = x_i / k_j$

Шифр маршрутной перестановки

$S = n * m$

$X = \{x_i = \left(a_1, \dots a_{nm_i}\right)\ \ a_{ji} \in A \quad i = \overline{1, t^{nm}}$

$Y = X$

$K = \{k_i = \left(k_{i_1},\ k_{i_2}\right)\}$

$E_{k_i}(x_j) = \{$вписывание вектора x_j в таблицу S по маршруту k_{i_1}
и выписывание по маршруту $k_{i_2}\}$

$D_{k_i}(y_j) = \{$вписывание вектора y_i в таблицу S по маршруту k_{i_2}
и выписывание по маршруту $k_{i_1}\}$

Шифр простой замены

$$A = \{а, б, в, \dots, я\}$$

$$|A| = 33$$

$$X = A$$

$$Y = \{1, 2, 3, 4, 5, \dots, 33\}$$

$$K = \begin{pmatrix} a_1 & \dots & a_{33} \\ y_{n_1} & \dots & y_{n_{33}} \end{pmatrix}, \qquad a_i \in A, \qquad i, j = \overline{1,33}, \ y_n \in Y$$

$$E_{k_i}(x_j) = y_{i_j}$$

$$D_{k_i}(y_j) = a_{i_j} \text{ — это } a_j \text{ в } k_i$$

A={a1,a2,…at} – алфафит
|A|=t
33=t везде

Шифр простой перестановки в блоке

m – длина блока

$$X = \{x_i = (x_{i_1}, \dots, x_{i_m}), \ x_{i_j} \in A, \qquad i, j = \overline{1, m}$$

$$Y = X$$

$$K = \{k_i = \begin{pmatrix} 1 & \dots & m \\ s_i & \dots & s_{i_m} \end{pmatrix}, \qquad s_i \in N, \qquad i, j = \overline{1, m}\}$$

$$U_{k_i} = \left|\left|U_{fg}\right|\right| \qquad U_{fg} = \begin{cases} 1, \text{если } f = i_t, \quad g = s_{i_t} \\ 0, \text{ в других случаях} \end{cases}$$

$$E_{k_i}(x_j) = U_{k_i} * x_j^T, \quad x_j \in X, k_i \in K$$

$$D_{k_i}(y_j) = U_{k_i}^{-1} y_j^T, \ y_j \in Y, k_i \in K$$

№2. Привести примеры исторических шифров, которые являются простой заменой или маршрутной перестановкой

Простая замена	Маршрутная перестановка
Шифр Цезаря	Сцитала ? На вики написано
Диск Энея	Шифр вертикальной перестановки
АТБАШ	Решетка Кардано
«Иные письмена»	?
Геометрические шифры простой замены или шифры в квадратах	?
Мудрая литорея	?

№3. Описать некий алгоритм

Частотный анализ + закономерности

1. Посчитать количество вхождений каждого из *y*
2. Упорядочить их в порядке от наиболее часто встречаемых к менее встречаемым
3. Сделать гипотезы, что 2-3 наиболее частых символа шифра заменяют 2-3 наиболее частых символа открытого текста. (Необходимо для точности, чтобы шифртекст был в 10 раз больше мощности алфавита)
4. Проверить гипотезу по запретным сочетаниям (Например, АА или ЫЪ)
5. Если гипотеза неверна, сделать другое предположение. Также делать гипотезы для других групп. Можно также угадывать слова (Например, часто двухбуквенное слово – это ЕЁ) или предугадывать окончания

Дешифрование шифра простой перестановки

1. Разбить текст на блоки, совпадающие по длине с заданным значением длины блока
2. Записать получившиеся блоки в прямоугольную таблицу, с количеством столбцов, равным длине блока. Каждый блок в отдельную строку, пронумеровать столбцы
3. Разделить таблицу на столбцы
4. Переставлять столбцы между собой до получения осмысленного текста.(Переставлять, исходя из известных правил языка, например, запретных биграмм)
5. Если в шифртексте сохранились знаки препинания, заглавные буквы, пробелы, то переставляем столбцы с их учетом
6. Зафиксировать порядок следования столбцов с дешифрованном тексте – это будет ключ.

Дешифрование омофонной замены

1. Выбрать букву с минимальной частотой встречаемости – 1 вариант замены.
2. Из особенностей языка установить ее возможных соседей слева и справа – s и t букв
3. Определить число вариантов замен ее соседей – сумма количества вариантов замен для s и t, букв S и T
4. Отыскать в тексте символ, у которого слева не более чем S различных символов и T символов справа
5. Сделать предположение, что данный символ является заменой выбранной нами буквы
6. Проверить данную гипотезу на основе особенностей языка
7. Повторять данную процедуру (1-6) для следующей по частоте буквы.

Определение длины ключа шифра многоалфавитной замены

1. Найти пары последовательностей совпадающих символов длиной от 4-х
2. Посчитать расстояние между одинаковыми символами из пар
3. Составить таблицу расстояний и их делителей
4. Выбрать общий делитель
5. Проверить гипотезу о том, что делитель является длиной ключа
6. Начать пункт 4 для другого общего делителя, если не подошла такая длина

№4. Составить ключ и зашифровать текст (30+ символов)

Шифром Плейфера

Шифром «Два квадрата»

№5. Описать закономерности связи открытого текста с шифртекстом, полученным шифром:

Плейфера

1. Биграмма не может перейти в инверсию себя
2. Две одинаковые буквы переходят в одинаковую биграмму
3. HT->BM => TH->MB (надо доказать на КР)

«Два квадрата»

1. HT->BM => MB->TH (надо доказать на КР)
2. BI->IB (Если совпадает строка и номер столбца)
3. Для одинаковых букв могут получиться разные биграммы

Джеферсона

Буква сама в себя перейти не может (т.к. алфавит без повторов)

Решетка Кардано

1. Первой буквой может стать только первая буква каждой четверти
2. Буквы в каждой четверти не перемешиваются