Докомпьютерные шифры

Кевролетин В.В.

28 декабря 2011 г.

Задание3.3.1

Условие

Какие из докомпьютерных шифров являются групповыми, а какие нет (с доказательством)?

Решение

Модулярный шифр

Дважды применим шифр к исходному символу m:

$$c_1 = n_1 * m + k_1(modM)$$
$$c_2 = n_2 * c_1 + k_2(modM) =$$
$$= n_2 * (n_1 * m + k_1) + k_2(modM) =$$
$$= n_2 * n_1 * m + n_2 * k_1 + k_2(modM) =$$
$$= N * m + K(modM), N = n_2 * n_1, K = n_2 * k_1 + k_2$$

Таким образом шифр является групповым.

шифр Вижнера

Применим процедуру шифрования дважды, с ключами K_1, K_2. Если ключи одинаковой длины, то все сводится к предыдущему случаю. Если ключи разной длины, то длина нового ключа будет равна наименьшему общему кратному длин ключей K_1, K_2, а сам ключ выражается несложной формулой:

$$K_1 = k_1^1, k_2^1, ..., k_{s1}^1$$
$$K_2 = k_1^2, k_2^2, ..., k_{s1}^2$$

Новый ключ(т.к. мы 2 раза делаем сдвиг):

$$(K)_i = (k_{imods1}^1 + k_{imods2}^2)(modM)$$

T.e. шифр является групповым

шифр Плейфейера

Приведём контрпример, показывающий, что шифр негрупповой.

Пусть первое шифрование с ключём K_1 переводит пару символов

$$AB \to CD$$

А второе шифрование с ключём K_2, обратно

$$CD \to AB$$

Тогда если бы шифр был групповым, то должен был бы существовать ключ, шифрование которым эквивалентно шифрованием с ключем K_1, а затем K_2. Но тогда бы пара символов AB переводилась бы сама в себя, что невозможно в системе Плейфейера.

Таким образом, шифр не групповой.

шифр Хилла

В этом шифре применяются линейные преобразования:

$$\vec{c_1} = A_1 * \vec{m} + \vec{b_1}(modM)$$

$$\vec{c_2} = A_2 * \vec{c_1} + \vec{b_2}(modM)$$

$$\vec{c_2} = A_2 * (A_1 * \vec{m} + \vec{b_1}) + \vec{b_2} =$$

$$A_1 * A_2\vec{m} + A_2 * \vec{b_1} + \vec{b_2} =$$

$$A * \vec{m} + \vec{b}, A = A_1 * A_2, \vec{b} = A_2 * \vec{b_1} + \vec{b_2}$$

Таким образом, шифр групповой.

Задание3.3.2

Условие

Показать, что шифр перестановки является линейным преобразованием в $B^n, B = 0, 1$

Решение

Перестановку n-элементного вектора можно представить матрицей размерности n*n, где в каждой строке один элемент, равной 1, а остальные нули, и в каждом столбце один элемент, равной 1, а остальные нули.

Задание3.3.3

Условие

Сколько существует нелинейных криптопреобразований $B^3 -> B^3$?

Решение

Посчитаем сколько всего приобразований: существует 2^3 разных бинарных векторов длины n => существует $2^3!$ различных преобразований $B^3 -> B^3$. Чтобы посчитать количество линейных преобразований в B^3 необходимо посчитать число различных бинарных матрицы размерности 3x3: 2^9. Таким образом нелинейных преобразований: $2^3! - 2^9$

Задание3.3.4

Условие

Доказать, что перестановка П:$0, 1, 2, \ldots, 2^n - 1$(взаимно однозначное отображение n-битовых целых чисел в себя) в более, чем 60% случаев % имеет неподвижную точку, $n \geq 2$

Решение

Как было отмечено ранее, перестановку можно записать в виде матрицы, имеющей в каждой строке и столбце одну 1, а остальные 0. Если перестановка имеет неподвижную точку, то она имеет хотя бы одну 1 на диагонали. Таким образом задача сводится к подсчёту нужных нам матриц с 1 на диагонали. Для подсчёта будем использовать принцип включения и исключения(множество матриц, содержащих хотя бы одну 1 на диагонали включает множество матриц с хотя бы 2мя единицами на диагонали и т.д)

Количество вершин без неподвижной точки выражается формулой (которая называется субфакториалом числа)

$$!n = n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} + \cdots + (-1)^n \frac{n!}{n!} = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!}$$

Известно, что субфакториал асимптотически ведёт себя, как $\frac{n!}{e}$

Тогда при больших n процент перестановок без неподвижной точки

$$\frac{\frac{n!}{e}}{n!} = \frac{1}{e}$$

Соответственно процент перестановок с неподвижной точкой примерно

$$1 - \frac{1}{e} \approx 0,63$$

ч.т.д.