Задачи к лабораторным занятиям по дисциплине
«Криптографические методы и средства защиты информации»
VII семестр 2023/2024 учебного года
специальность 10.05.01 Компьютерная безопасность
Жаркова А. В.

Задачи реализуются письменно (по условию) и программно (в общем случае).

1) I) Берется слово МАТЕМАТИКА. Из него с равной вероятностью выбирается каждая из 10 букв. Пространство X состоит из 6 различных букв этого слова с вероятностями, отвечающими данному выбору. Определить энтропию $H(X)$.

II) Пусть задан алфавит из n букв, занумерованных обычным образом. На платформе $\mathbb{Z}_n$ определен шифр, ключом которого является вычет $k \in \mathbb{Z}_n$. Шифрование осуществляется по правилу:

$$E_k : m \to k - m(mod n).$$

Показать, что этот шифр на самом деле является аффинным.

2) I) Придумать схему разделения секрета между n пользователями для $n \geq 3$ такую, что секрет могут восстановить только любые m пользователей (m – фиксированное число меньшее n), но не могут восстановить любые $\leq m - 1$ пользователей.

II) Доказать, что в любом поле $\mathbb{F}_{p^k}$ содержится единственный (тривиальный) корень p-й степени из 1.

3) I) Доказать, что абелева группа порядка pq, где p, q – различные простые числа, обязательно циклическая. Верно ли это утверждение в случае абелевой группы порядка p^2 (p – простое)? Построить пример неабелевой

(заведомо нециклической) группы порядка pq, где p, q – также различные простые числа.

II) Найти обратную к матрице, используемой при замене байтов (SubBytesTransformation).

4) I) Что можно сказать о композиции двух шифров перестановки с ключами $\tau_1 \in S_m$, $\tau_2 \in S_k$?

II) Алфавит русский – 33 буквы. Разбит на блоки величины $n = 8$. Буквы внутри каждого блока переставляются перестановкой:

$$s = (1,6,4,8,7,2,3)(5).$$

1. Зашифровать текст (убрав знаки и пробелы): «На портрете была изображена действительно необыкновенной красоты женщина» – Достоевский.

2. Расшифровать текст (убраны кавычки, пробелы и тире, но оставлена запятая): епбмовллеощркавсыдвопабммреашок, щаюкйавееслйиакрпдйохокорийнномалоукабвг.

5) …

…

Список источников

1) Кукина Е. Г., Романьков В. А. Введение в криптографию: сборник задач и упражнений / Е.Г. Кукина, В.А. Романьков. – Омск: Изд-во Ом. гос. ун-та, 2013. – 91 с. ISBN 978-5-7779-1588-7.

2) Романьков В. А. Введение в криптографию. Курс лекций / В.А. Романьков. М. : ФОРУМ, 2012. - 240 с. - (Высшее образование). ISBN 978-5-91134-573-0