**Лабораторна робота №4**

Самостійно ознайомитися з блоковим алгоритмом шифрування відповідно до варіанту, номер якого співпадає з порядковим номером у списку. Програмно реалізувати зашифрування і розшифрування текстового файлу вказаним алгоритмом. На захисті коротко розповісти про алгоритм (можна з декількома слайдами для наглядності) та продемонструвати роботу програми.

*Література*:

1. **Панасенко С.** *Алгоритмьі шифрования.* *Специальньій справочник*. СПб.:БХВ-Петербург, 2009.- 576 с.
2. **Корченко О. Г**. *Прикладна криптологія : системи шифрування : підручник /* О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.
3. **Остапов С. Е**. *Технології захисту інформації* : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

|  |  |  |
| --- | --- | --- |
| № пп | Прізвище та імя | Алгоритм |
|  | Баранович Марта-Владислава | **Akelarre** |
|  | Библів Богдан | **CAST-256** |
|  | Білозор Андрій | **Crypton** |
|  | Богоніс Олеся-Марія | **CS-Cipher** |
|  | Голяш Дмитро | **DES** |
|  | Горбан Назарій | **FROG** |
|  | Загородник Артур | **Hierocrypt-3** |
|  | Зубик Вікторія | **ICE** |
|  | Кіндрат Соломія | **IDEA** |
|  | Ковальчук Софія | **Khazad** |
|  | Копач Андрій | **MAGENTA** |
|  | Кравців Роман | **Mercy** |
|  | Крикливець Олександр | **Noekeon** |
|  | Кушка Андрій | **NUSH** |
|  | Луців Павло | **Q** |
|  | Перчак Анна-Марія | **RC5** |
|  | Саакян Нікіта | **SAFER+** |
|  | Сельменський Руслан | **Sha-zam** |
|  | Сорочинський Михайло | **SHARK** |
|  | Тупичак Василь | **SPEED** |
|  | Юрас Віталій | **TEA** |