**ЛАБОРАТОРНАЯ РАБОТА 4**

**РЕАЛИЗАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ**

**4.1. ВИЖИНЕРА**

**4.2. ДВОЙНОЙ КВАДРАТ УИТСОНА**

**Содержание задания**

Зашифруйте сообщение, используя алгоритмы согласно своему варианту (табл. 1).

2). Ключевое слово – Фамилия и имя

Т а б л и ц а 1

|  |  |
| --- | --- |
| Вариант | Сообщение |
|  | За пару секунд компьютер успевает сделать ошибку таких размеров, что сотни людей трудятся над ней месяцами |
|  | Смысл жизни подобен карабканию по канату, который мы же сами подкинули в воздух |
|  | Первые каналы связи были очень простыми, их организовывали с помощью надежных курьеров |
|  | Проблемы конфиденциальности и целостности тесно связаны между собой |
|  | Параметр, с помощью которого выбирается отдельное используемое преобразование, называется криптографическим ключом |
|  | В симметричной криптосистеме секретный ключ передается по защищенному каналу |
|  | Знания бывают двоякого рода: либо мы что-нибудь знаем, либо мы знаем, где найти сведения об этом |
|  | Оптимист – это человек, который еще не читал утренних газет |
|  | Криптосистема является криптостойкой, если предпринятые криптоаналитические атаки не достигают поставленных целей |
|  | Стойкость шифра должна определяться только секретностью ключей |
|  | Весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитикам противника |
|  | Криптосистема, реализующая семейство криптографических преобразований, обычно является открытой системой |
|  | Если мечтаешь о радуге, будь готов к дождю |
|  | Самый непобедимый человек – это тот, кому не страшно быть глупым |
|  | Системы шифрования дисковых данных могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков |
|  | Другим классификационным признаком систем шифрования является способ их функционирования |
|  | Тот, кто смотрит на дело с обеих сторон, обычно не видит ни одной из них |
|  | Системы второго типа являются утилитами шифрования, которые необходимо специально вызывать |
|  | В случае канального шифрования защищается информация, передаваемая по каналу связи, включая служебную |
|  | Лотерея – наиболее точный способ учета количества оптимистов |
|  | Защищается только содержание сообщений, служебная информация остается открытой |
|  | При обмене данными по сетям возникает проблема установления подлинности авторов |
|  | Получатель проверяет цифровую подпись, используя при этом открытый ключ |
|  | В системах прозрачного шифрования преобразования осуществляются незаметно для пользователя |
|  | Счастливые обстоятельства создают друзей, печальные – их испытывают |