**ЛАБОРАТОРНАЯ РАБОТА 3**

**РЕАЛИЗАЦИЯ АЛГОРИТМА ШИФРОВАНИЯ ПЛЕЙФЕЙРА**

**Содержание задания**

Зашифруйте сообщение, используя алгоритм Плейфейра согласно своему варианту (табл. 1). Размер шифрующей таблицы 4 × 8.

Т а б л и ц а 1

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