Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Практическое задание №5

«Криптографическая защита информации»

Подготовил: студент ФИТ 2 курса 5 группы Древотень Е.В.

Проверил: асс. Берников В.О.

Цель: Овладение основными криптографическими алгоритмами симметричного шифрования.

Теоретическое введение

Криптография - наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства) информации.

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа.

Помимо этого современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Шифрованием (encryption) называют процесс преобразования открытых данных (plaintext) в зашифрованные (шифртекст, ciphertext) или зашифрованных данных в открытые по определенным правилам с применением ключей.

Классификация алгоритмов шифрования

1. Симметричные (с секретным, единым ключом, одноключевые, single-key).

1.1. Потоковые:

· с одноразовым или бесконечным ключом (infinite-key cipher);

· с конечным ключом;

· на основе генератора псевдослучайных чисел.

1.2. Блочные:

1.2.1. Шифры перестановки (permutation, P-блоки);

1.2.2. Шифры замены (substitution, S-блоки):

· моноалфавитные;

· полиалфавитные;

2. Асимметричные (с открытым ключом, public-key):

· Диффи-Хеллман DH (Diffie, Hellman);

· Райвест-Шамир-Адлeман RSA (Rivest, Shamir, Adleman);

· Эль-Гамаль (ElGamal).

Задание на выполнение

1. Зашифровать сообщение с использованием шифра Цезаря, Трисемуса, Плейфейра и Вижинера и полученного секретного ключа (12 и ключевому слову «Защита»). В качестве сообщения использовать «ДРЕВОТЕНЬ ЕВГЕНИЙ ВЛАДИМИРОВИЧ».

Шифрование с помощью шифра Цезаря:

Изначальный алфавит русского языка без сдвига на 12 символов: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.

Сдвинем каждый символ со своей позиции на 12 символов: ЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙК.

Зашифрованное сообщение: ПЬРНЪЮРЩЗ РНОРЩФХ НЧЛПФШФЬЪНФГ.

Шифрование с помощью шифра Трисемуса:

Рис. 1.1 позволяет легко сопоставить буквы с их порядковыми номерами.



Рисунок 1.1 Алфавит с порядковыми номерами символов

Пусть уравнение зашифрования имеет вид k=3р^2+8р-4. Смещение вправо. Тогда зашифрованное сообщение имеет вид: ЙБЮЩБШЮЧОШЮЩОЮЧЕБШЩКЮЙЕШЕББЩЕО.

Шифрование Плейфейра:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| З | А | Щ | И | Т | Б | В | Г |
| Д | Е | Ж | Й | К | Л | М | Н |
| О | П | Р | С | У | Ф | Х | Ц |
| Ч | Ш | Ъ | Ы | Ь | Э | Ю | Я |

Таблица 1.2 Ключевая матрица

Разобьём сообщение на биграммы:

ДР ЕВ ОТ ЕН ЬЕ ВГ ЕН ИЙ ВЛ АД ИМ ИР ОВ ИЧ.

Зашифрованная последовательность биграмм:

ЖО МА УЗ ЖД ШК ГЗ ЖД ЙС БМ ЗЕ ВЙ ЩС ХЗ ЗЫ.

Шифрование Вижинера:

На рис. 1.3 можно увидеть таблицу Вижинера для русского алфавита.

Запишем ключ на 28 символов (число символов в шифруемом сообщении): ЗАЩИТАЗАЩИТАЗАЩИТАЗАЩИТАЗАЩИТАЗАЩИТАЗАЩИ.

Тогда Зашифрованное сообщение имеет вид: ЛРЮКАТМНХ НФГМНБС ФЛЗДБФЪРХВБЯ.

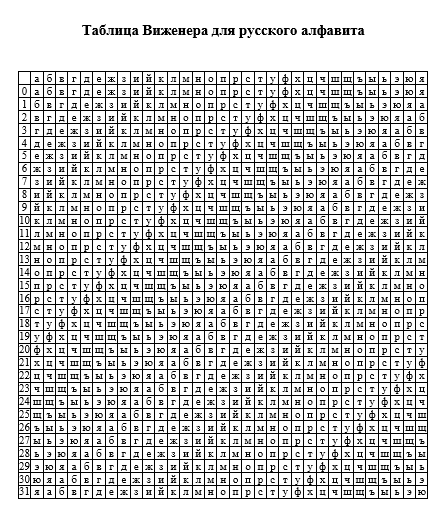


Рисунок 1.3 Таблица Вижинера для русского алфавита

1. Расшифровать следующее сообщение с помощью метода простой перестановки (таблица 6×7): «нотеч\_е\_ \_кем\_кчалемре,осеал\_втссоаеотив\_к\_».

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Н | О | Т | Е | Ч | \_ |
| Е | \_ | \_ | К | Е | М |
| \_ | К | Ч | А | Л | Е |
| М | Р | Е | , | О | С |
| Е | А | Л | \_ | В | Т |
| С | С | О | А | Е | О |
| Т | И | В | \_ | К | \_ |

Таблица 2.1 Таблица для шифрования

По таблице получаем дешифрованное сообщение:

НЕ\_МЕСТО\_КРАСИТ\_ЧЕЛОВЕКА,\_А\_ЧЕЛОВЕКА\_МЕСТО\_.

Вывод. Овладел основными криптографическими алгоритмами симметричного шифрования: шифры Цезаря, Трисемуса, Плейфейра и Вижинера, метод простой перестановки.