**Практическое задание №4.1**

**Тема «Криптографическая защита информации»**

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.

В англоязычной литературе зашифрование / расшифрование – enciphering / deciphering.

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).

Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.

Обмен информацией осуществляется в 3 этапа:

* отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар);
* отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;
* получатель получает сообщение и расшифровывает его.

Если для каждого дня и для каждого сеанса связи будет использоваться уникальный ключ, это повысит защищенность системы.

При блочном шифровании информация разбивается на блоки фиксированной длины и шифруется поблочно. Блочные шифры бывают двух основных видов:

· шифры перестановки (transposition, permutation, P-блоки);

· шифры замены (подстановки, substitution, S-блоки).

Шифры перестановок переставляют элементы открытых данных (биты, буквы, символы) в некотором новом порядке. Различают шифры горизонтальной, вертикальной, двойной перестановки, решетки, лабиринты, лозунговые и др.

Шифры замены заменяют элементы открытых данных на другие элементы по определенному правилу. Paзличают шифры простой, сложной, парной замены, буквенно-слоговое шифрование и шифры колонной замены. Шифры замены делятся на две группы:

· моноалфавитные (код Цезаря);

· полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma).

В моноалфавитных шифрах замены буква исходного текста заменяется на другую, заранее определенную букву. Например в коде Цезаря буква заменяется на букву, отстоящую от нее в латинском алфавите на некоторое число позиций.



Очевидно, что такой шифр взламывается совсем просто. Нужно подсчитать, как часто встречаются буквы в зашифрованном тексте, и сопоставить результат с известной для каждого языка частотой встречаемости букв.

В полиалфавитных подстановках для замены некоторого символа исходного сообщения в каждом случае его появления последовательно используются различные символы из некоторого набора. Понятно, что этот набор не бесконечен, через какое-то количество символов его нужно использовать снова. В этом слабость чисто полиалфавитных шифров.

В современных криптографических системах, как правило, используют оба способа шифрования (замены и перестановки). Такой шифратор называют составным (product cipher). Oн более стойкий, чем шифратор, использующий только замены или перестановки.

В асимметричных алгоритмах шифрования (или криптографии с открытым ключом) для зашифровывания информации используют один ключ (открытый), а для расшифровывания - другой (секретный). Эти ключи различны и не могут быть получены один из другого.

Схема обмена информацией такова:

· получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует);

· отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю;

· получатель получает сообщение и расшифровывает его, используя свой секретный ключ.

**Задание к выполнению**

1. Изучить теоретические сведения по данной теме.
2. Зашифровать сообщение с использованием шифра
   1. Цезаря,
   2. Трисемуса,
   3. Плейфейра,
   4. Вижинера и полученного секретного ключа (**по номеру варианта** и ключевому слову «**Защита**»). В качестве сообщения использовать свою **Фамилию Имя Отчество**.
3. Расшифровать следующие сообщения:

|  |  |  |
| --- | --- | --- |
| Номер варианта | Сообщение | Способ |
|  | Ие михежцчжшйч сшихуцчб | Расшифровать с помощью шифра Цезаря. Ключ 5 |
|  | съчпщг окхчхиге ичлкпщг | Расшифровать с помощью шифра Цезаря. Ключ 7 |
|  | ьоъщочто т лечшыхтлшыьё | Расшифровать с помощью шифра Цезаря. Ключ 10 |
|  | Лжбзеииеизиачзнр | Расшифровать с помощью магического квадрата   |  |  |  |  | | --- | --- | --- | --- | | 7 | 12 | 1 | 14 | | 2 | 13 | 8 | 11 | | 16 | 3 | 10 | 5 | | 9 | 6 | 15 | 4 | |
|  | тяеонаыбиьсрль\_т | Расшифровать с помощью магического квадрата   |  |  |  |  | | --- | --- | --- | --- | | 9 | 16 | 2 | 7 | | 6 | 3 | 13 | 12 | | 15 | 10 | 8 | 1 | | 4 | 5 | 11 | 14 | |
|  | иоарткдпвл\_натоа | Расшифровать с помощью магического квадрата   |  |  |  |  | | --- | --- | --- | --- | | 7 | 12 | 1 | 14 | | 2 | 13 | 8 | 11 | | 16 | 3 | 10 | 5 | | 9 | 6 | 15 | 4 | |
|  | гэ ишн зижшпэг оюжи | Расшифровать с помощью шифра Цезаря.  Ключ 8. Ключевое слово – ВЕСНА |
|  | дороюё дъ нозбъвё жодщйц | Расшифровать с помощью шифра Цезаря.  Ключ 5. Ключевое слово – ОСЕНЬ |
|  | жъйтаьъщ ёьръ клъюё жёйлал | Расшифровать с помощью шифра Цезаря.  Ключ 6. Ключевое слово – ЗИМА |
|  | Боитдиултоьтдгь-псеоснояшмяил\_ьу-бу\_дччуч\_ | Расшифровать с помощью метода простой перестановки. Таблица 6х7 |
|  | гг\_ \_ ип-оомитрдр\_ос,яубогп\_  мбадираоитнла\_гноаавуоа | Расшифровать с помощью метода простой перестановки. Таблица 7х7 |
|  | нотеч\_е\_ \_кем\_кчалемре,осеал\_втссоаеотив\_к\_ | Расшифровать с помощью метода простой перестановки. Таблица 6х7 |
|  | \_яетож\_нксучнтуотдеыужбьатйдны\_,  с\_ао\_о\_яс,\_ндк,е\_иаиу\_ккддндаруто\_  а\_еди.в\_нта\_ \_ахе:\_ | Расшифровать с помощью одиночной перестановки по ключу. Ключ – СЧАСТЬЕ. Таблица 12х7 |
|  | Онлгвишлеиоутньмшттьишньо\_ \_мио\_всп\_нгоиеодсичтгзнтеесодев \_няднможь\_не\_ \_и\_жяеб | Расшифровать с помощью одиночной перестановки по ключу. Ключ – ОКТЯБРЬ. Таблица 11х7 |
|  | \_ \_еоовипи\_ \_ \_ы\_о\_ввв\_тттыыытуоо\_ \_ \_атмтерем\_у,сес,б\_ \_тшт \_ычкьиьгттт,л,дь | Расшифровать с помощью одиночной перестановки по ключу. Ключ – ФЕВРАЛЬ. Таблица 10х7 |
|  | НТЕЬСЯЛБЬЫРТОИА\_ | Расшифровать с помощью двойной перестановки по ключу. Ключ 1 – Мама. Ключ 2 – 3142 |
|  | И\_ЛБКЧУОПЧТУ\_ОЬР | Расшифровать с помощью двойной перестановки по ключу.Ключ 1 – ЛЕТО. Ключ 2 – 4213 |
|  | АМУМАФАССИ\_ТКРК\_ | Расшифровать с помощью двойной перестановки по ключу. Ключ 1 – ЗИМА. Ключ 2 – 2341 |
|  | ъгчгл кыпргл бгнщзг | Расшифровать с помощью шифра Трисемуса. Ключ – «ПРАВИТЕЛЬ» |
|  | иецеж пецен, пй ыд зещеъез | Расшифровать с помощью шифра Трисемуса. Ключ – «МОСКВА» |
|  | зчгы очхей, й зчгы гйък щчрейв | Расшифровать с помощью шифра Трисемуса. Ключ – «МИНСК» |
|  | нп тр яч дн ка бо ат дъ ка цр кб щг уф уч тб ты | Расшифровать с помощью шифра Плейфейра. Ключ – АБСТРАКЦИЯ |
|  | вт пм зл ко ту нщ кж ек да ъл тс дш ыд пц къ ац ми лф | Расшифровать с помощью шифра Плейфейра.Ключ – РЕПЛИКАЦИЯ |
|  | рп пд оф бл гщ мф ыи мф цг гн оп см тп гн въ ив жя | Расшифровать с помощью шифра Плейфейра. Ключ – КЛАССИФИКАЦИЯ |
|  | у ь т ц в ю к п ч ю ч у в у и з к щ й ю т у ф б х к ф э у е в д б е ь б ч о | Расшифровать с помощью шифра Виженера. Ключ – ВЕТЕР |
|  | д с я ш о ж у в я и х ь с я с б е у ю т в х я ю т к ф я ъ и о е п я | Расшифровать с помощью шифра Виженера. Ключ – ВЕСНА |
|  | х ш п ф и с ъ ш а с ъ м щ ю ш х ю к п я ц д ю о ы г х з г и ь р с щ с с у х щ м ь т п | Расшифровать с помощью шифра Виженера. Ключ – ПРИЗМА |
|  | кл ез рц ьй уа бц пв вй ая хй ущ хй бш | Расшифровать с помощью шифра «Двойной квадрат Уитстона». Ключ 1 – ХАЛЯВА. Ключ 2 – РАБОТА |
|  | пх кю гй яг зо ад зн йр юм тш кь | Расшифровать с помощью шифра «Двойной квадрат Уитстона». Ключ 1 – ХАЛЯВА. Ключ 2 – РАБОТА |
|  | ба хи хх ьй ля сс эж ап це ък бш | Расшифровать с помощью шифра «Двойной квадрат Уитстона». Ключ 1 – ХАЛЯВА. Ключ 2 – РАБОТА |