Практическое занятие №5

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ АЛГОРИТМОВ СИММЕТРИЧНОГО ШИФРОВАНИЯ

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель работы:**

Овладение основными криптографическими алгоритмами симметричного и асимметричного шифрования, их применение для защиты данных и проверки целостности информации.

**Теоретические сведения**

**Криптография и ее задачи**

Криптография – это наука о методах защиты информации от несанкционированного доступа путем шифрования и хеширования. Основные задачи криптографии:

* **Конфиденциальность** – защита данных от несанкционированного доступа.
* **Целостность** – предотвращение изменения данных без обнаружения.
* **Аутентификация** – подтверждение подлинности отправителя.
* **Неотрекаемость** – невозможность отказа от факта отправки сообщения.

**Алгоритмы шифрования**

Существует два основных типа криптографических систем:

1. **Симметричное шифрование** – один и тот же ключ используется как для шифрования, так и для расшифрования.
   * **Преимущества:** высокая скорость работы.
   * **Недостатки:** сложность безопасного обмена ключами.
   * **Примеры алгоритмов:** AES, DES, Triple DES.
2. **Асимметричное шифрование** – используются два ключа: открытый (для шифрования) и закрытый (для расшифрования).
   * **Преимущества:** безопасный обмен ключами.
   * **Недостатки:** низкая скорость работы.
   * **Примеры алгоритмов:** RSA, Diffie-Hellman, ElGamal.

**Алгоритм RSA (512 бит)**

RSA – один из самых известных алгоритмов асимметричного шифрования. Он основан на сложности факторизации больших чисел.  
**Принцип работы RSA:**

1. Генерируется пара ключей: **открытый ключ (public key)** и **закрытый ключ (private key)**.
2. Сообщение шифруется с помощью открытого ключа.
3. Расшифрование возможно только с использованием закрытого ключа.

Формулы RSA:

* **Шифрование:** C=Memod  NC = M^e \mod NC=MemodN
* **Расшифрование:** M=Cdmod  NM = C^d \mod NM=CdmodN  
  где:
* MMM – исходное сообщение,
* CCC – зашифрованное сообщение,
* eee – открытая экспонента,
* ddd – секретная экспонента,
* NNN – модуль (произведение двух простых чисел).

**Хеширование и алгоритм MD5**

Хеширование – это процесс получения уникального цифрового отпечатка (хеша) данных фиксированной длины.

**Принцип работы MD5:**

1. Сообщение разбивается на блоки по 512 бит.
2. Каждый блок обрабатывается функцией сдвигов и нелинейных преобразований.
3. В результате получается хеш длиной **128 бит (32 шестнадцатеричных символа)**.

**Недостатки MD5:**

* Уязвимость к коллизиям (разные сообщения могут давать одинаковый хеш).
* Не рекомендуется для критически важных приложений.

**Применение криптографии**

* **Безопасная передача данных в интернете (SSL/TLS).**
* **Электронная цифровая подпись (ЭЦП).**
* **Шифрование файлов и сообщений.**
* **Защита паролей в базах данных.**

**Задание для выполнения**

1. Изучите теоретические сведения по данной теме.

2. Зашифруйте сообщение с использованием нижеперечисленных шифров и полученного секретного ключа (по номеру варианта (см. номер студента в журнале группы) и ключевому слову «Защита»):

− шифр Цезаря;

− шифр Трисемуса;

− шифр Плейфейра;

− шифр Виженера.

В качестве сообщения используйте свое полное имя (Фамилия Имя Отчество).

3. Расшифруйте сообщения по индивидуальному заданию.

|  |  |  |
| --- | --- | --- |
| Номер Варианта | Сообщение | Способ |
| 4 | Лжбзеииеизиачзнр | Расшифровать с помощью магического квадрата   |  |  |  |  | | --- | --- | --- | --- | | 7 | 12 | 1 | 14 | | 2 | 13 | 8 | 11 | | 16 | 3 | 10 | 5 | | 9 | 6 | 15 | 4 | |

**Выполнение задания:**

**2** Васильев Владислав Васильевич

Ключ: 4

**Шифр Цезаря**

Исходный алфавит

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Ж | З | И | Й | К | Л | М |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| Н | О | П | Р | С | Т | У |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| Ф | Ч | Ц | Ч | Ш | Щ | Ъ |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| Ы | Ь | Э | Ю | Я |
| 29 | 30 | 31 | 32 | 33 |

|  |  |  |  |
| --- | --- | --- | --- |
| Буква | Исходная позиция | Новая позиция(+4) | Зашифрованная буква |
| В | 3 | 7 | Ж |
| А | 1 | 5 | Д |
| С | 19 | 23 | Х |
| И | 10 | 14 | М |
| Л | 13 | 17 | П |
| Ь | 30 | 34 -> 1 | А |
| Е | 6 | 10 | И |
| В | 3 | 7 | Ж |

|  |  |  |  |
| --- | --- | --- | --- |
| Буква | Исходная позиция | Новая позиция(+4) | Зашифрованная буква |
| В | 3 | 7 | Ж |
| Л | 13 | 17 | П |
| А | 1 | 5 | Д |
| Д | 5 | 9 | З |
| И | 10 | 14 | М |
| С | 19 | 23 | Х |
| Л | 13 | 17 | П |
| А | 1 | 5 | Д |
| В | 3 | 7 | Ж |

|  |  |  |  |
| --- | --- | --- | --- |
| Буква | Исходная позиция | Новая позиция(+4) | Зашифрованная буква |
| В | 3 | 7 | Ж |
| А | 1 | 5 | Д |
| С | 19 | 23 | Х |
| И | 10 | 14 | М |
| Л | 13 | 17 | П |
| Ь | 30 | 34 -> 1 | А |
| Е | 6 | 10 | И |
| В | 3 | 7 | Ж |
| И | 10 | 14 | М |
| Ч | 26 | 30 | Ь |

Готовый результат: ВАСИЛЬЕВ ВЛАДИСЛАВ ВАСИЛЬЕВИЧ ––>

* + ЖДХМПАИЖ ЖПДЗМХПДЖ ЖДХМПАИЖМЬ

**Шифр Трисемуса**

Ключевое слово: Защита

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

Готовый результат: ВАСИЛЬЕВ ВЛАДИСЛАВ ВАСИЛЬЕВИЧ ––>

МЕЫЙФТПМ МФЕОЙЫФЕМ МЕЫЙФТПМЙЗ

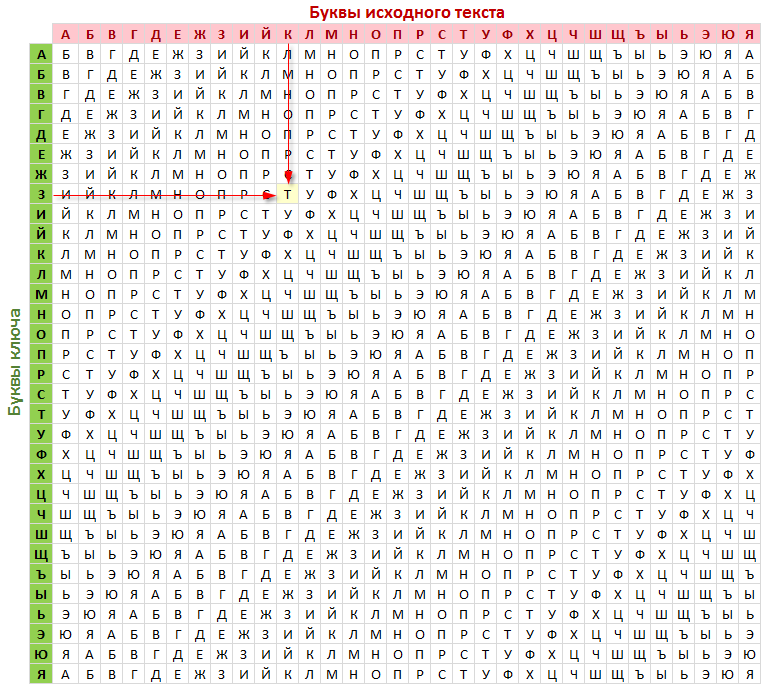
**Шифр Плейфейра**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

ВА-СИ-ЛЬ-ЕВ-ВЛ-АД-ИС-ЛА-ВЪ-ВА-СИ-ЛЬ-ЕВ-ИЧ

ГЩ-ЫЙ-КЭ-МА-БМ-ЗЕ-ЙЫ-ЕБ-ЩЮ-ГЩ-ЫЙ-КЭ-МА-ЗЫ

**Шифр Вижинера**



ВАСИЛЬЕВ ВЛАДИСЛАВ ВАСИЛЬЕВИЧ 27 символов

ЗАЩИТАЗА ЩИТАЗАЩИТ АЗАЩИТАЗАЩ

|  |  |  |
| --- | --- | --- |
| В | З | К |
| А | А | Б |
| С | Щ | Л |
| И | И | С |
| Л | Т | Ю |
| Ь | А | Э |
| Е | З | Н |
| В | А | Г |

|  |  |  |
| --- | --- | --- |
| В | Щ | Ь |
| Л | И | Ф |
| А | Т | У |
| Д | А | Е |
| И | З | Р |
| С | А | Т |
| Л | Щ | Е |
| А | И | Й |
| В | Т | Х |

|  |  |  |
| --- | --- | --- |
| В | А | Г |
| А | З | И |
| С | А | Т |
| И | Щ | В |
| Л | И | Ф |
| Ь | Т | П |
| Е | А | Ж |
| В | З | К |
| И | А | Й |
| Ч | Щ | С |

Полученное зашифрованное сообщение:  
КБЛСЮЭНГ ЬФУЕРТЕЙХ ГИТВФПЖКЙС

3. Расшифруйте сообщения по индивидуальному заданию.

|  |  |  |
| --- | --- | --- |
| Номер Варианта | Сообщение | Способ |
| 4 | Лжбзеииеизиачзнр | Расшифровать с помощью магического квадрата   |  |  |  |  | | --- | --- | --- | --- | | 7 | 12 | 1 | 14 | | 2 | 13 | 8 | 11 | | 16 | 3 | 10 | 5 | | 9 | 6 | 15 | 4 | |

ЛЖБЗ ЕИИЕ ИЗИА ЧЗНР

|  |  |  |  |
| --- | --- | --- | --- |
| 7 Л | 12 Ж | 1 Б | 14 З |
| 2 Е | 13 И | 8 И | 11 Е |
| 16 И | 3 З | 10 И | 5 А |
| 9 Ч | 6 З | 15 Н | 4 Р |

Расшифрованное сообщение:  
БЕЗРАЗЛИЧИЕ ЖИЗНИ

**Использованные источники**

1. Соловьев В. И. Основы криптографии. — М.: Издательство МГТУ, 2020.
2. Шеннон К. Работы по теории информации и кибернетике. — М.: Мир, 1963.
3. Кнут Д. Искусство программирования. Том 2: Получисленные алгоритмы. — М.: Вильямс, 2007.
4. Столбов С. Н. Методы и средства защиты информации. — СПб.: Питер, 2019.
5. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая.
6. Официальная документация по криптографическим алгоритмам [Электронный ресурс]. Доступ: <https://cryptography.io>
7. История и принципы работы шифров Цезаря, Вижинера, Плейфера и магических квадратов [Электронный ресурс]. Доступ: <https://crypto-history.com>