|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |

**Институт информационных технологий (ИИТ)**

**Кафедра математического обеспечения и стандартизации информационных технологий**

**ОТЧЁТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ**

**Научно-исследовательская работа**

**Тема практики**: «Гражданская Оборона - Русское поле экспериментов»

приказ Университета о направлении на практику от «28» августа 2020 г. 3301-С

|  |  |  |  |
| --- | --- | --- | --- |
| Отчет представлен к  рассмотрению:  Студент группы ИКБО-06-17 | «01» сентября 2020 | (подпись) | Карпушина С.К. |
| Отчет утвержден.  Допущен к защите: |  |  |  |
| Руководитель практики от кафедры | «21» декабря 2020 | (подпись) | Григорьев В.К. |

Москва 2020 г.

|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |

**Институт информационных технологий (ИИТ)**

**Кафедра математического обеспечения и стандартизации информационных технологий**

**ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРОИЗВОДСТВЕННУЮ ПРАКТИКУ**

**Научно-исследовательская работа**

**Студенту 4 курса учебной группы ИКБО-06-17**

**Карпушиной Софье Константиновне**

**Место и время практики:** РТУ МИРЭА, кафедра МОСИТ, с 01 сентября 2020 г. по 21 декабря 2020 г.

**Должность на практике:**  студент

**1. ЦЕЛЕВАЯ УСТАНОВКА:** Получение первичных профессиональных умений и опыта профессиональной деятельности по теме: «Гражданская Оборона - Русское поле экспериментов».

**2. Подробное содержание проделанной работы ПРАКТИКИ:**

2.1. Изучить: география подлости, орфография ненависти

2.2. Практически выполнить: трогательным ножичком пытать свою плоть

2.3. Ознакомиться: апология невежества, мифология оптимизма

**3. ДОПОЛНИТЕЛЬНОЕ ЗАДАНИЕ:** набить до отказа собой могилу

**4. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ УКАЗАНИЯ:** пройти инструктаж по охране труда, технике безопасности, пожарной безопасности и правилам внутреннего распорядка Университета, в течение всей научно-исследовательской работы осуществлять устойчивое взаимодействие с научным руководителем.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Заведующий кафедрой: | | | | | |
| «01» сентября 2020 г. | | | *(подпись)* | | (Головин С.А.) |
| **СОГЛАСОВАНО:** | |  |  | |  |
| Руководитель практики от кафедры  «01» сентября 2020 г. | | | *(подпись)* | | (Григорьев В.К.) |
| Задание получил | |  |  | |  |
| «01» сентября 2020 г. | |  | *(подпись)* | | (Карпушина С.К.) |
| **Проведенные инструктажи:** |  | | |  | |
| Охрана труда: |  | | | «01» сентября 2020 г. | |
| Инструктирующий | *(подпись)* | | | Григорьев В.К., к.т.н., доцент кафедры МОСИТ | |
| Инструктируемый | *(подпись)* | | | Карпушина С.К. | |
|  |  | | |  | |
| Техника безопасности: |  | | | «01» сентября 2020 г. | |
| Инструктирующий | *(подпись)* | | | Григорьев В.К., к.т.н., доцент кафедры МОСИТ | |
| Инструктируемый | *(подпись)* | | | Карпушина С.К. | |
|  |  | | |  | |
| Пожарная безопасность: |  | | | «01» сентября 2020 г. | |
| Инструктирующий | *(подпись)* | | | Григорьев В.К., к.т.н., доцент кафедры МОСИТ | |
| Инструктируемый | *(подпись)* | | | Карпушина С.К. | |
|  | | | |  | |
| С правилами внутреннего распорядка ознакомлен: | | | | «01» сентября 2020 г. | |
|  | *(подпись)* | | | Карпушина С.К. | |

|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |

**РАБОЧИЙ ГРАФИК ПРОВЕДЕНИЯ  
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ**

студента Карпушиной С.К. 4 курса группы ИКБО-06-17 очной формы обучения, обучающегося по направлению подготовки 09.03.04 «Программная инженерия», профиль «Системная инженерия».

|  |  |  |  |
| --- | --- | --- | --- |
| **Неделя** | **Сроки**  **выполнения** | **Этап** | **Отметка о выполнении** |
| 1 | 01.09.2020 | Выбор темы НИР. Оформление задания на НИР и рабочего графика. Прохождение инструктажей |  |
| 1-4 | 09.09.2020-13.10.2020 | Изучить География подлости, орфография ненависти |  |
| 5-7 | 14.10.2020-17.11.2020 | Ознакомиться Апология невежества, мифология оптимизма |  |
| 8-10 | 18.11.2020-  16.12.2020 | Набить до отказа собой могилу |  |
| 11-16 | 17.12.2020-  20.12.2020 | Трогательным ножичком пытать свою плоть |  |
| 17 | 21.12.2020 | Оформление отчета по НИР, зачет |  |

**Согласовано:**

Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Головин С.А., д.т.н., профессор/

Руководитель практики от  
кафедры \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Григорьев В.К., к.т.н., доцент/

Обучающийся \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Карпушина С.К./

**ОТЧЁТ**

**по производственной практике**

**студента 4 курса учебной группы ИКБО-06-17 института Университета**

Карпушиной Софьи Константиновны

1. Практику проходил с 01.09.2020 г. по 21.12.2020 г. в\_\_ФГБОУ ВО «МИРЭА – Российский технологический университет», на кафедре МОСИТ, студент

*(место прохождения практики и должность)*

1. Задание на практику выполнил

в полном объеме

*(указать: в полном объеме или частично)*

Не выполнены следующие задания:

*(указать также причины невыполнения)*

Подробное содержание выполненной на практике работы и достигнутые результаты: Подробное содержание проделанной работы

Предложения по совершенствованию организации и прохождения практики:

предложений нет

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Карпушина С.К.)

*(подпись)*

«21» декабря 2020 г.

Заключение руководителя практики

Заключение научного руководителя о выполненной работе

Проявил себя как: дисциплинированный ответственный, за срок прохождения практики не получил ни одного замечания - проявляет инициативу и творческое отношение к работе, а, сроков выполняет задания; в любой ситуации адекватен и уважителен в общении с другими.

«21» декабря 2020 г.

**Отчет проверил:**

**Руководитель практики от Университета**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Григорьев В.К.)

*(подпись)*

1. **Шифрование методом простой замены**

Исходный алфавит:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |

Смещенный алфавит:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё |

Буквы исходного алфавита сдвигаем на n=7 позиции вправо.

Исходный текст: **устойчивое выражение**

Кодированный текст: **ъшщхрюпихл ивчжнлфпл**

Расшифрованный текст: **ъшщхрюпихл ивчжнлфпл** → **устойчивое выражение**

1. **Шифрование методом многоалфавитной замены**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |
| 2 | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а |
| 3 | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б |
| 4 | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в |
| 5 | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г |
| 6 | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д |
| 7 | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е |
| 8 | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё |
| 9 | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж |
| 10 | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з |
| 11 | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и |
| 12 | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й |
| 13 | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к |
| 14 | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л |
| 15 | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м |
| 16 | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н |
| 17 | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о |
| 18 | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п |
| 19 | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р |
| 20 | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с |
| 21 | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т |
| 22 | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у |
| 23 | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф |
| 24 | ц | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х |
| 25 | ч | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц |
| 26 | ш | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч |
| 27 | щ | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш |
| 28 | ъ | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ |
| 29 | ы | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ |
| 30 | ь | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы |
| 31 | э | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь |
| 32 | ю | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э |
| 33 | я | а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю |

При шифровании каждая буква исходного слова заменяется на букву (в той же позиции) из другого алфавита, номер которого соответствует номеру буквы в слове (предложении) или же соответствует n mod 33, где n ≥ 33.

Исходный текст: **фразеологизм**

Кодированный текст: **фсвкиусхкссч**

Расшифрованный текст: **фсвкиусхкссч** →**фразеологизм**

1. **Шифрование методом вертикальных перестановок**

Ключ: (3, 5, 1, 2, 4)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3 | 5 | 1 | 2 | 4 |
| о | т | в | л | е |
| к | а | ю | щ | и |
| й |  | м | а | н |
| е | в | р |  |  |

Шифруем:

Исходный текст: **отвлекающий маневр**

Записываем столбцы в порядке, который указан в ключе.

Получаем шифрованный текст: **вюмр|лща |окйе|еин |та в**

Расшифровываем:

Кол-во символов N в зашифрованном сообщении: 18

Длина ключа K: 5

Сделаем следующий вывод: N/K= 18/5. Получаем целую часть, равную 3 и остаток 3. Таким образом, получаем три полных строки, содержащих по пять символов, и одну строку, содержащую 3 символа → 3 полных столбца (3, 5, 1) по 4 символа и 2 столбца (2, 4) по 3 символа.

**вюмр|лща |окйе|еин |та в**

**1 2 3 4 5**

Записываем полученные группы в столбцы и расставляем их в порядке, указанном в ключе.

Получаем расшифрованный текст: **отвлекающий маневр**

1. **Блочное шифрование с помощью шифра Плейфера**

Исходный текст: **семимильными шагами.**

Ключевая таблица:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| г | ! | , | с | ъ | к |
| ж | и | о | т | а | х |
| р | ш | й | н | щ | ? |
| . | ч |  | б | я | е |
| ё | & | ф | ы | ь | з |
| ь | п | м | э | л | ю |

Исходный текст разделяем на биграммы:

**се|ми|ми|ль|ны|ми| ш|аг|ам|и.**

При шифровании буквы биграммы, оказавшиеся в одной строке, заменяются на находящиеся непосредственно справа от них; буквы биграммы, оказавшиеся в одном столбце, заменяются на находящиеся непосредственно под ними. В противном случае мысленно рисуем прямоугольник с углами, соответствующими 2 буквам биграммы, и заменяем их буквами противоположных углов по горизонтали.

Кодированный текст:

**кб|по|по|ъл|бэ|по|чй|жъ|ол|жч**

Расшифрованный текст, применяя обратный алгоритм:

**кб|по|по|ъл|бэ|по|чй|жъ|ол|жч** → **се|ми|ми|ль|ны|ми| ш|аг|ам|и.**

1. **Блочное шифрование методом двойного квадрата**

Исходный текст: **потерянность**

Ключевые таблицы:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| м | я | к | : | э | ы |
| ь | ? | ю | н | е | в |
| а | у | ъ | щ | . | ё |
| з | п | л | ж | д | р |
| и | ! | о | г | й | х |
| т | б | ф | ч | с | , |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| . | ю | н | й | ш | , |
| : | 7 | ъ | г | с | е |
| м | ж | о | я | л | у |
| з | т | ы | ! | в | д |
| ? | б | щ | э | ь | ч |
| ё | а | ь | ф | п | р |

Разбиваем исходный текст на блоки:

**по|те|ря|нн|ос|ть**

При кодировании данным способом первый символ из блока всегда берется из первой таблицы, а заменяется символом из второй таблицы, и наоборот. Мы или мысленно рисуем прямоугольник и делаем замену, или заменяем в соответствии с позицией, если символы в одной строке.

Кодированный текст:

**ыу|рь|!ё|ъ:|ью|пи**

Расшифровываем по обратному алгоритму.

Расшифрованный текст:

**ыу|рь|!ё|ъ:|ью|пи** → **по|те|ря|нн|ос|ть**

1. **Шифр Хилла**

Таблица соответствия:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

Исходный текст: **абсолютизировать**

*В* – исходная матрица

*В* = =

Выберем ключевую матрицу *A* четвёртого порядка, такую, чтобы определитель матрицы не был равен 0 и не имел общих делителей с модулем n (кроме единицы), где n – количество символов в алфавите.

*А* =

Определитель матрицы: Δ*А* = 1

Найдем обратную ей матрицу:

*А*-1 =

*C* – зашифрованная матрица

Шифрование: *C* = (*А* \* *В*) mod 33

*C* = (*А* \* *В*) *mod* 33 = mod 33 =

= *mod* 33 =

=

Зашифрованный текст: **зчфзытжпщщссвсьа**

Расшифрование: *В* = (*А*-1 \* *C*) mod 33

*В* = (*А*-1 \* *C*) *mod* 33 =

mod 33 = *mod* 33 =

=

Расшифрованный текст: **абсолютизировать**

1. **Шифрование (упрощенное) с помощью шифра с открытым ключом RSA**

Алфавит:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

Исходный текст: **ценность**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ц | е | н | о | с | т | ь |
| 23 | 5 | 14 | 15 | 18 | 19 | 28 |

Открытый ключ - Коткр = (*n*, *e*); закрытый ключ Кзакр = (*n*, *d*).

Произвольно выберем простые числа *p* = 7 и *q* = 13

Найдем их произведение *n* = *p* \* *q* = 7 \* 13 = 91

Определим для *n* функцию Эйлера (*φ*(*n*))

*φ*(*n*) = (*p* – 1) \* (*q* -1) = 6 \* 12 = 72

Выберем число *e* = 17, взаимно простое с *φ*(*n*)

Теперь по расширенному алгоритму Евклида подберём число *d* такое, чтобы остаток от деления произведения чисел *e* и *d* на *φ*(*n*) равнялся 1:

*e* \* *u* + *φ*(*n*) \* *v* = 1

*φ*(*n*) = *e* \* *k* + остаток

Нашли наибольший делитель:

72 = 17 \* 4 + 4

17 = 4 \* 4 + 1

1 = 17 – 4 \* 4 = 17 – 4 \* (72 – 17 \* 4) = 17 – 4 \* 72 + 17 \* 16 = 17 \* 17 –

- 4 \* 72

*u* = 17; *v* = 4

Если *u* > 0, то *d* = *u*, т.е. *d* = 17 (*e* \* *d* = 17 \* 17 = 289; 72 \* 4 = 288)

Коткр = (*n*, *e*) = (91, 17)

Кзакр = (*n*, *d*) = (91, 17)

Зашифруем исходный текст: *ci* = *mod* *n*, где *Mi*  - блок шифруемого текста

|  |  |
| --- | --- |
| Вход | Шифрование |
| Ц (23) | (Д) |
| Е (5) | (Ю) |
| Н (14) | (Н) |
| Н(14) | (Н) |
| О (15) | 71 |
| С (18) | 44 |
| Т (19) | 80 |
| Ь (28) | 84 |

Однако в нашем алфавите всего 33 символа. Введем дополнительные символы для *Сi*, к которым нельзя подобрать символы из алфавита: *C5*=«!», *C6*=«?», *C7*=«@», *C8*=«%».

Зашифрованный текст: **дюнн!?@%**

Расшифруем зашифрованный тескт: *Mi* = *mod* *n*

|  |  |
| --- | --- |
| Вход | Дешифрование |
| Д (4) |  |
| Ю (31) | (Е) |
| Н(14) | (Н) |
| Н(14) |  |
| ! (71) | (О) |
| ? (44) | (С) |
| @ (80) | 19 (Т) |
| %(84) | 28 (Ь) |

Расшифрованный текст: **ценность**

1. **Создание цифровой подписи на базе алгоритма RSA**

* шифруем закрытым ключом некоторое слово
* передаем зашифрованное слово и исходное
* расшифровываем полученный текст открытым ключом
* сравниваем расшифрованный с исходным текстом
* если тексты совпадают, то *цифровая подпись* действительна

Ключи и алфавит возьмем из предыдущего примера для усеченного RSA.

Исходный текст: **абсурд**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| а | б | с | у | р | д |
| 0 | 1 | 18 | 20 | 17 | 4 |

Коткр = (*n*, *e*) = (91, 17) – открытый ключ

Кзакр = (*n*, *d*) = (91, 17) – закрытый ключ

Зашифруем исходный текст закрытым ключом:

|  |  |
| --- | --- |
| Вход | Шифрование |
| А (0) | (А) |
| Б (1) | (Б) |
| С (18) |  |
| У(20) |  |
| Р (17) | 75 |
| Д (4) | 23(Ц) |

Введем дополнительные символы для *Сi*, к которым нельзя подобрать символы из алфавита: *C3*=«?», *C4*=«[», *C5*=«]», *C5*=«\».

Зашифрованный текст: **аб?[]\**

Посылаем исходный и зашифрованный текст адресату. Адресат должен знать открытый ключ для расшифровки.

Расшифровываем зашифрованный текст открытым ключом:

|  |  |
| --- | --- |
| Вход | Дешифрование |
| А (0) |  |
| Б (1) | (Б) |
| ? (44) | (С) |
| [(76) |  |
| ] (75) | (Р) |
| \ (4) | (Д) |

Расшифрованный текст: **абсурд**

На практике данный метод почти не применяется из-за того, что затруднительно передавать адресату и исходный, и зашифрованный текст. Вместо этого пользуются специально сгенерированной хеш-функцией. В этом случае алгоритм цифровой подписи имеет вид:

1. По открытому тексту (документу) вычисляется его хэш-функция;
2. Зашифровывается хэш-функция закрытым ключом некоторой ассиметричной системы шифрования (зашифрованная хэш-функция играет роль цифровой подписи);
3. Посылается документ и зашифрованная хэш-функция;
4. По открытому тексту (документу) вычисляется хэш-функция;
5. Присланная зашифрованная хэш-функция расшифровывается открытым ключом;
6. Сравнивается вычисленная и расшифрованная хэш-функции;
7. Если они совпали, то цифровая подпись действительна.
8. **Разработка алгоритма обмена защищенной информацией в открытой сети на базе асимметричной системы шифрования**

Данный обмен может происходить по следующей схеме:

1. Некоторый *i*-ый пользователь (*i*=1..*N*) шифрует текст *T* своим закрытым ключом *Kзi*

*T* → [*Kзi*] → *TKзi*

1. Затем он шифрует этот текст *TKзi* открытым ключом *j*-го (*j*=1..*N*) пользователя *Kоj*

*TKзi* → [*Kоj*] → *TKзi* *Kоj* и посылает текст по открытой сети

1. *j*-й пользователь расшифровывает своим закрытым ключом *Kзi*, полученное сообщение *TKзi*

*Kоj* → (*Kзi*) → *TKзi*

1. Далее он расшифровывает текст *TKзi* открытым ключом *i*-го пользователя *Kоi* и получает открытый текст *TKзi* → (*Kоi*) → T
2. **Построение циклического кода по заданному порождающему полиному**

Пусть требуется закодировать исходную комбинацию вида *А* = 10010011101, что соответствует:

*G*(*x*) = *x*10 + *x*7 + *x*4 + *x*3 + *x*2 + 1

Выберем образующий полином:

*P*(*x*) = *x*3 + *x* + 1

Число контрольных разрядов равно 3, умножим *G*(*x*) на *x*3:

*F*(*x*) = *G*(*x*) \* *x*3 = *x*13 + *x*10 + *x*7 + *x*5 + *x*3 → 10010011101000

Разделим полученное произведение на *P*(*x*):

*x*13 + *x*10 + *x*7 + *x*5 + *x*3  *x*3 + *x* + 1

*x*13 + *x*11 + *x*10 *x*10 + *x*8 + *x*6 + *x*5 + 1

*x*11 + *x*7 + *x*5

*x*11 + *x*9 + *x*8

*x*9 + *x*8 + *x*7

*x*9 + *x*7 + *x*6

*x*8 + *x*6 + *x*5

*x*8 + *x*6 + *x*5

*x*3

*x*3 + *x* + 1

*x* + 1

Остаток от деления: *x* + 1

*F*(*x*) = *G*(*x*) \* *x*3 = *x*13 + *x*10 + *x*7 + *x*5 + *x*3 + *x* + 1→ 10010011101011

Проверка:

*x*13 + *x*10 + *x*7 + *x*5 + *x*3 + *x* + 1 *x*3 + *x* + 1

*x*13 + *x*11 + *x*10 *x*10 + *x*8 + *x*6 + *x*5 + 1

*x*11 + *x*7 + *x*5

*x*11 + *x*9 + *x*8

*x*9 + *x*8 + *x*7

*x*9 + *x*7 + *x*6

*x*8 + *x*6 + *x*5

*x*8 + *x*6 + *x*5

*x*3 + *x* + 1

*x*3 + *x* + 1

0

Ошибок не найдено.

1. **Построение кода Хэминга для заданного двоичного сообщения**

Исходный текст: 1000101111

Вставляем контрольные биты (1, 2, 4, 8): ??1?000?101111

Перевернутое сообщение: 111101?000?1??

Вычисляем значения контрольных бит:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 1 | 1 | 1 | 1 | 0 | 1 | ? | 0 | 0 | 0 | ? | 1 | ? | ? |  |
|  | X |  | X |  | X |  | \* |  | \* |  | X |  | \* | 1 |
| X |  |  | X | \* |  |  | \* | \* |  |  | X | \* |  | 2 |
| X | X | X |  |  |  |  | \* | \* | \* | \* |  |  |  | 3 |
| X | X | X | X | \* | X | \* |  |  |  |  |  |  |  | 4 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |

Вычисление контрольных бит происходит следующим образом: берём каждый контрольный бит и смотрим сколько среди контролируемых им битов единиц, получаем некоторое целое число и, если оно чётное, то ставим ноль, в противном случае ставим единицу, причем контрольный бит с номером N контролирует все последующие N бит через каждые N бит, начиная с позиции N.

Таким образом, получаем закодированное сообщение: 11110110001110

Если была допущена ошибка, мы вновь пересчитываем значение контрольных бит, сравниваем комбинацию со значением, которое получили ранее. Если в сообщении была допущена одна ошибка, мы можем вычислить поврежденный бит путем сложения не совпавших контрольных бит.