**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

**федеральное государственное бюджетное образовательное учреждение высшего**
**профессионального образования**

**«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ»**

СОГЛАСОВАНО:
Выпускающей кафедрой
«Вычислительная техника»
Зав. кафедрой
_____В.Ю. Горелик
(подпись, Ф.И.О.)
« ___ » _____ 20 ____ г.

УТВЕРЖДАЮ:
Проректор - директор Российской открытой академии транспорта
_____ В.И. Апатцев
(подпись, Ф.И.О.)
« ___ » _____ 20 ____ г.

**Кафедра:** «Вычислительная техника»
(название кафедры)

**Авторы:** Ермаков А.Е., к.тех.н, доц.
(ф.и.о., ученая степень, ученое звание)

# ЗАДАНИЕ НА КОНТРОЛЬНУЮ РАБОТУ ПО ДИСЦИПЛИНЕ

## «Информационная безопасность»
(название дисциплины)

*Направление/специальность:* **230700.62. Прикладная информатика**
(код, наименование специальности /направления)

*Профиль/специализация:* **«Прикладная информатика в информационной сфере» (ИИ)**

*Квалификация (степень) выпускника:* **бакалавр**

*Форма обучения:* **заочная**

| | |
|---|---|
| Одобрена на заседании<br>Учебно-методической комиссии РОАТ<br>Протокол №_____<br>« ___ » _____ 20 ____ г.<br>Председатель УМК _____ А.В.Горелик<br>(подпись, Ф.И.О.) | Одобрена на заседании кафедры<br>«Вычислительная техника»<br>Протокол №_____<br>« ___ » _____ 20 ____ г.<br>Зав. кафедрой _____ В.Ю. Горелик<br>(подпись, Ф.И.О.) |

Москва 2013 г.

## ОБЩИЕ УКАЗАНИЯ

Контрольная работа выполняется на листах формата А4. На титульном листе должны быть указаны данные студента и его учебный шифр.

Для выполнения контрольной работы необходимо:

- изучить методические указания и рекомендуемую литературу;
- определить свой вариант задания;
- изучить заданные алгоритмы шифрования;
- зашифровать свою фамилию и полное имя методом гаммирования и по алгоритму RSA;
- выполнить проверку путем дешифрования шифротекста.

В контрольной работе должны быть выполнены все пункты задания, которое приводится в начале работы. Контрольные работы, не соответствующие указанным требованиям, возвращаются студенту без рецензии.

## ЗАДАНИЕ НА КОНТРОЛЬНУЮ РАБОТУ

Контрольная работа состоит из двух задач.

### ЗАДАЧА 1

Зашифровать фамилию и полное имя студента методом гаммирования. Под гаммированием понимают процесс наложения по определенному закону (чаще всего с использованием операции сложения по модулю 2) гаммы шифра на открытые данные. Гамма шифра – это псевдослучайная последовательность целых чисел, для генерации которых наиболее часто применяется так называемый линейный конгруэнтный генератор. Закон функционирования такого генератора описывается соотношением:

$$T_i = (T_{i-1} \cdot A + C) \bmod M \qquad (1)$$

где $T_i$ – текущее число последовательности; $T_{i-1}$ - предыдущее число последовательности; A, C и M – константы; M – модуль; A – множитель; C – приращение; $T_0$ – порождающее число.

Текущее псевдослучайное число $T_i$ получают из предыдущего числа $T_{i-1}$ умножением его на коэффициент A, сложением с приращением C и вычислением целочисленного остатка от деления на модуль M. Данное уравнение генерирует псевдослучайные числа с периодом повторения, который зависит от выбираемых значений параметров A, C и M. Значение модуля M берется равным $2^n$, либо равным простому числу, например $M = 2^{31} - 1$. Приращение C должно быть взаимно простым с M, коэффициент A должен быть нечетным числом.

Вариант задания определяется в соответствии с табл. 1.

Таблица 1

| Константа | Значение |
|---|---|
| $T_0$ | 7 |
| A | 9 |
| C | Сумма двух последних цифр шифра |
| M | 64 |

Шифрование текста методом гаммирования рекомендуется выполнять в следующей последовательности:

1. Определить константы шифрования по табл. 1.

2. Каждой букве шифруемого текста поставить в соответствие десятичное число по табл. 2.

Таблица 2

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

2. Сгенерировать гамму шифра в соответствии с выражением (1).

3. Полученные числа (шифруемый текст и гамма шифра) перевести в двоичный. Замечание. Каждое число представляется байтом.

4. Наложить гамму шифра на шифруемый текст по формуле (2):

$$Ш_i = C_i \oplus T_i, \qquad (2)$$

где $Ш_i - i$ - ый символ шифрограммы, представленный в двоичном коде; $C_i - i$ - ый символ исходного текста, представленный в двоичном коде.

5. Полученную шифрограмму перевести в десятичный код и по табл. 2 получить текстовую форму шифрограммы. Замечание. В процессе выполнения операции сложение по модулю 2 могут получиться числа больше 32. В этом случае рекомендуется выполнить операцию $\mathrm{mod}32$. Однако при дешифровке необходимо использовать исходное число.

6. Выполнить проверку шифрования путем наложения гаммы шифра на шифрограмму.

## ЗАДАЧА 2

Зашифровать фамилию и полное имя студента по алгоритму RSA. Порождающие числа выбрать в соответствии с табл. 3. Причем число $p$ выбирается по последней цифре шифра, а число $q$ – по предпоследней цифре.

Таблица 3

| Цифра | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $p$ | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 19 | 17 | 13 |
| $q$ | 23 | 19 | 29 | 7 | 13 | 11 | 19 | 11 | 23 | 29 |

Замечание. Если числа $p$ и $q$ совпадают, то следует взять другое большее простое число.

Шифрование текста по алгоритму RSA рекомендуется выполнять в следующей последовательности:

1. Определить порождающие числа по табл. 3.

2. Каждой букве шифруемого текста поставить в соответствие десятичное число по табл. 2.

3. Вычислить произведение порождающих чисел $N = p \cdot q$.

4. Вычислить функцию Эйлера по формуле:

$$\varphi(n) = (p-1) \cdot (q-1)$$

5. Выбрать открытый ключ шифрования $K_{OTK}$, который должен удовлетворять следующим неравенствам:

$$1 < K_{OTK} < \varphi(n);$$

$$НОД(K_{OTK}, \varphi(n)) \equiv 1$$

Значение $K_{OTK}$ выбирается произвольным образом из указанного диапазона чисел, а наибольший общий делитель (НОД) $K_{OTK}$ и функции Эйлера должен быть равен 1, т.е. эти два числа должны быть взаимно простыми. Так как порождающие числа с точки зрения криптографии ничтожно малы, то рекомендуется соблюдать два дополнительных условия: $K_{OTK} \neq p,\ K_{OTK} \neq q$.

6. Вычислить секретный ключ $K_{CEK}$ по формуле:

$$K_{CEK} = K_{OTK}^{(\varphi(n)-1)} \bmod \varphi(n)$$

При вычислении $K_{CEK}$ рекомендуется выполнить ряд последовательных умножений, выполняя каждый раз приведение по модулю. Например, необходимо вычислить 25 степень некоторого числа *a* по модулю *n*: $a^{25} \bmod n$. Представим степень 25 в виде целых степеней 2:

$$25 = 2^4 + 2^3 + 2^0.$$

Таким образом, нам необходимо вычислить 8 и 16 степени числа *a*. Для вычисления 8 степени воспользуемся выражением:

$$((a^2 \bmod n)^2 \bmod n)^2 \bmod n.$$

Для вычисления 16 степени, полученное на предыдущем шаге число необходимо возвести в квадрат и привести его по модулю.

7. Зашифровать исходный текст по формуле:

$$Ш_i = C_i^{K_{OTK}} \bmod N,$$

где $Ш_i - i$ - ый символ шифрограммы, представленный в десятичном коде; $C_i - i$ - ый символ исходного текста, представленный в десятичном коде.

8. Выполнить проверку, дешифровав шифрограмму по формуле:

$$Ш_i = C_i^{K_{CEK}} \bmod N.$$