Лабораторная работа № 1

3 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

3.1 Провести шифрование текста простейшими перестановочными шифрами.

3.2 Провести шифрование текста подстановочным методом (аффинное преобразование). Первый ключ равен k_1 = № студента в журнале (если он не удовлетворяет условию взаимной простоты, то берется ближайшее целое).

3.3 Оформить отчет по проделанной работе.

В качестве исходного текста взять **ФАМИЛИЯ_ИМЯ_ОТЧЕСТВО** (не менее 20 символов).

Лабораторная работа № 2

ИСПРАВЛЕНИЯ ПО ТЕКСТУ

1) Стр. 9.

   В п. 1.7 написано:

«Доказательство: по теореме Эйлера: $n^{\varphi(n)} = 1 \bmod r$ или

$$1 = n^{\varphi(n)} \bmod r. \qquad (2)$$

Перемножив (1) и (2), получим: $n \cdot m = n^{\varphi(n)} \bmod r$, разделив обе части на n, получим: $m = n^{\varphi(n)-1} \bmod r$.»

Следует читать:

«Нахождение взаимообратных чисел: если НОД(n,r) = 1, то по теореме Эйлера: $n^{\varphi(r)} = 1 \bmod r$ или

$$1 = n^{\varphi(r)} \bmod r. \qquad (2)$$

Перемножив (1) и (2), получим: $n \cdot m = n^{\varphi(r)} \bmod r$, разделив обе части на n, получим: $m = n^{\varphi(r)-1} \bmod r$ (справедливо при НОД(n,r) = 1).»

2) Стр. 10.

   Пункты 2.1, 2.2 исключить.

3) Стр. 11.

   Вариант 11.

   Написано:

«5. $r = 28$, $m = 7$»

Следует читать:

«5. $r = 28$, $m = 9$»

Лабораторная работа № 3

ИСПРАВЛЕНИЯ ПО ТЕКСТУ

4) Стр. 13, п. 2)
Приведены формулы:
«$C(i)$=($M(i)K$о) mod r»,
«$M(i)$=($C(i)K$с) mod r»

Следует читать:
«$C(i)=(M(i)^{Ko})$ mod r»,
«$M(i)=(C(i)^{Kc})$ mod r»

2) Стр. 14, п. 6.
Написано:
«$C(1)$ = (57) mod 33 = 78125 mod 33 = 14,
$C(2)$ = (37) mod 33 = 2187 mod 33 = 9,
$C(3)$ = (47) mod 33 = 16384 mod 33 = 16.»

Следует читать:
«$C(1) = (5^7)$ mod 33 = 78125 mod 33 = 14,
$C(2) = (3^7)$ mod 33 = 2187 mod 33 = 9,
$C(3) = (4^7)$ mod 33 = 16384 mod 33 = 16.»

3) Стр. 14, п. 7.
Написано:
«M(1) = (143) mod 33 = 2744 mod 33 = 5,
M(2) = (93) mod 33 = 729 mod 33 = 3,
M(3) = (163) mod 33 = 4096 mod 33 = 4.»

Следует читать:
«M(1) = (14^3) mod 33 = 2744 mod 33 = 5,
M(2) = (9^3) mod 33 = 729 mod 33 = 3,
M(3) = (16^3) mod 33 = 4096 mod 33 = 4.»

4) Стр. 15, п. 2.2.
Написано:
«Используя заданные в соответствии с вариантом значения p, q и закрытого ключа *Kc* вычислить открытый ключ *Ko* при помощи расширенного алгоритма Евклида и выполнить шифрование по алгоритму *RSA* открытым ключом (*Ko*) своей фамилии. Для представления букв в

числовой форме использовать следующее соответствие: ‘А’ – 2, ‘Б’ – 3, ‘В’ – 4, ..., ‘Ё’ – 8, ..., ‘Я’ – 34.»

Следует читать:

«Используя заданные в соответствии с вариантом значения p, q и закрытого ключа Kc вычислить открытый ключ Ko при помощи расширенного алгоритма Евклида и выполнить шифрование по алгоритму RSA открытым ключом (Ko):

а) Числа M = 15.

б) Своей фамилии. Для представления букв в числовой форме использовать следующее соответствие: ‘А’ – 2, ‘Б’ – 3, ‘В’ – 4, ..., ‘Ё’ – 8, ..., ‘Я’ – 34.»

Приложение. Алгоритм быстрого возведения в степень по модулю.

На первом шаге степень представляется в двоичном виде (1-я строчка).

Пусть требуется вычислить $249^{321} \bmod 499$. Представим степень в виде $321 = 256 + 64 + 1 = 2^8 + 2^6 + 2^0$.

Представим $249^{321} \bmod 499$ в виде $249^{321} \bmod 499 = 249^{2^8+2^6+2^0} \bmod 499 =$

$$= (((((((249^2)^2)^2)^2)^2)^2)^2(((((249^2)^2)^2)^2)^2 249 \bmod 499 = [249^2 \equiv 125(\bmod 499)] =$$

$$= ((((((125^2)^2)^2)^2)^2)^2((((125^2)^2)^2)^2)^2 249 \bmod 499 = [125^2 \equiv 156(\bmod 499)] =$$

$$= (((((156^2)^2)^2)^2)^2(((156^2)^2)^2)^2 249 \bmod 499 = [156^2 \equiv 384(\bmod 499)] =$$

$$= ((((384^2)^2)^2)^2)^2((384^2)^2)^2 249 \bmod 499 = [384^2 \equiv 251(\bmod 499)] =$$

$$= (((251^2)^2)^2)^2(251^2)^2 249 \bmod 499 = [251^2 \equiv 127(\bmod 499)] =$$

$$= ((127^2)^2)^2 127^2 249 \bmod 499 = [127^2 \equiv 161(\bmod 499)] =$$

$$= (161^2)^2 161 * 249 \bmod 499 = [161^2 \equiv 472(\bmod 499)] =$$

$$= 472^2 161 * 249 \bmod 499 = [472^2 \equiv 230(\bmod 499)] =$$

$$= 230 * 161 * 249 \bmod 499 = 447$$