Прытков Максим

Варианты заданий и ответы

Вариант 12

1. Русское слово из четырех букв закодировано при помощи алгоритма RSA открытым ключом $e = 23$, $m = 51$). Шифрованное сообщение имеет вид (45; 18; 26; 24). Подберите закрытую часть ключа и прочитайте исходное слово. Буквам русского алфавита соответсвуют числа в диапазоне от 2 до 33 (без буквы Ё).

2. С помощью алгоритма Хаффмана построить код Шеннона-Фэно для текстового сообщения, состоящего из символов с частотами: В: 50; Г: 65; Д: 86; Е: 45; Ж: 93; З: 59; И: 35.

3. Какое число задаётся данным кодом Грея: 10011101?

4. Восстановить при помощи алгоритма Рида-Соломона исходное сообщение длины 3 в Z_5, переданное с не более чем одной ошибкой (точки, в которых вычислены значения, упорядочены от 0 до 4): 2, 3, 2, 4, 3.

№	Ответ
1.	БРАК.
2.	В(100); Г(110); Д(00); Е(1111); Ж(01); З(101); И(1110).
3.	233.
4.	$(2, 2, 4)$.

Задание 1.

Определим закрытую часть ключа d:

$\varphi(m) = \varphi(51) = \varphi(3) \cdot \varphi(17) = 2 \cdot 16 = 32;$

$23d \equiv 1\ mod\ 32;$

$23d + 32y = 1;$

Распишем алгоритм Евклида:

$32 = 23 \cdot 1 + 9;$
$23 = 9 \cdot 2 + 5;$
$9 = 5 \cdot 1 + 4;$
$5 = 4 \cdot 1 + 1;$

Обратный ход:

$1 = 5 - 4 \cdot 1 = 5 - (9 - 5 \cdot 1) \cdot 1 = 5 \cdot 2 - 9 \cdot 1 = (23 - 9 \cdot 2) \cdot 2 - 9 \cdot 1 =$
$= 23 \cdot 2 - 9 \cdot 5 = 23 \cdot 2 - (32 - 23 \cdot 1) \cdot 5 = 23 \cdot 7 - 32 \cdot 5 \rightarrow d = 7;$

Подставим корни для проверки: $23 \cdot 7 - 32 \cdot 5 = 161 - 160 = 1;$

Необходимо вычислить:

$45^7 mod\ 51,\ 18^7 mod\ 51,\ 26^7 mod\ 51,\ 24^7 mod\ 51;$

$7_{10} = 111_2;$

Возводим в степень по модулю:

a_i	c	c^2	$c^2 a^{a_i}$	$c^2 a^{a_i}\ mod\ 51$
1	1	1	45	45
1	45	2025	91125	39
1	39	1521	68445	3

a_i	c	c^2	$c^2 a^{a_i}$	$c^2 a^{a_i}\ mod\ 51$
1	1	1	18	18
1	18	324	5832	18
1	18	324	5832	18

a_i	c	c^2	$c^2 a^{a_i}$	$c^2 a^{a_i}\ mod\ 51$
1	1	1	26	26
1	26	676	17576	32
1	32	1024	26624	2

a_i	c	c^2	$c^2 a^{a_i}$	$c^2 a^{a_i} \, mod \, 51$
1	1	1	24	24
1	24	576	13824	3
1	3	9	216	12

Значит слово имеет вид $(3; 18; 2; 12)$, сопоставим найденным номерам буквы алфавита и получим: БРАК.

Ответ: БРАК.

Задание 2.

В: 50; Г: 65; Д: 86; Е: 45; Ж: 93; З: 59; И: 35;

Отсортируем по возрастанию частот:

И: 35; Е: 45; В: 50; З: 59; Г: 65; Д: 86; Ж: 93;

Соединяем:

50(В); 59(З); 65(Г); 80(ИЕ); 86(Д); 93(Ж);

65(Г); 80(ИЕ); 86(Д); 93(Ж); 109(ВЗ);

86(Д); 93(Ж); 109(ВЗ); 145(ГИЕ);

109(ВЗ); 145(ГИЕ); 179(ДЖ);

179(ДЖ); 254(ВЗГИЕ);

Расщепляем:

0(ДЖ); 1(ВЗГИЕ);

0(ДЖ); 10(ВЗ); 11(ГИЕ);

00(Д); 01(Ж); 10(ВЗ); 11(ГИЕ);

00(Д); 01(Ж); 100(В); 101(З); 11(ГИЕ);

00(Д); 01(Ж); 100(В); 101(З); 110(Г); 111(ИЕ);

00(Д); 01(Ж); 100(В); 101(З); 110(Г); 1110(И); 1111(Е);

Сведем данные в таблицу:

Символ	Частота	Код
В	50	100
Г	65	110
Д	86	00
Е	45	1111
Ж	93	01
З	59	101
И	35	1110

Ответ: В(100); Г(110); Д(00); Е(1111); Ж(01); З(101); И(1110).

Задание 3.

Код: 10011101

0: 1
1: $1 + 0 = 1$
2: $1 + 0 + 0 = 1$
3: $1 + 0 + 0 + 1 = 0$
4: $1 + 0 + 0 + 1 + 1 = 1$
5: $1 + 0 + 0 + 1 + 1 + 1 = 0$
6: $1 + 0 + 0 + 1 + 1 + 1 + 0 = 0$
7: $1 + 0 + 0 + 1 + 1 + 1 + 0 + 1 = 1$

Получено число: $11101001_2 = 128 + 64 + 32 + 8 + 1 = 128 + 105 = 233_{10}$;

Выполним проверку:

$N = 233, \left[\frac{N}{2}\right] = 116;$

$233_{10} = 128 + 64 + 32 + 8 + 1 = 11101001_2;$

$116 = 64 + 32 + 16 + 4 = 1110100_2;$

x	y	$x \oplus y$
1	0	1
1	1	0
1	1	0
0	1	1
1	0	1
0	1	1
0	0	0
1	0	1

Значит для числа 233_{10} код Грея имеет вид: 10011101, что совпадает с начальным условием, значит число было найдено верно.

Ответ: 233.

Задание 4.

x	y
0	2
1	3
2	2
3	4
4	3

$P(x) - \text{исх}, \deg\ P(x) \leq 2;$

$\widehat{P(x)} - \text{факт.}, \deg\ \widehat{P(x)} \leq 4;$

$D(x) - \text{ошибка};$

$D(x) = 0 \to P(x) \overset{5}{\equiv} \widehat{P(x)};$

$Q(x) = P(x) \cdot D(x) = \widehat{P(x)} \cdot D(x) = \widehat{P(x)} \cdot (x - d);$

$Q(x) = q_0 + q_1 x + q_2 x^2 + q_3 x^3;$

$P(x) = \frac{Q(x)}{D(x)};$

$q_0 + q_1 x + q_2 x^2 + q_3 x^3 = (x - d)y;$

$(0)\ x \equiv 0: \quad q_0 = -2d$
$(1)\ x \equiv 1: \quad q_0 + q_1 + q_2 + q_3 = 3(1 - d)$
$(2)\ x \equiv 2: \quad q_0 + 2q_1 + 4q_2 + 3q_3 = 2(2 - d)$
$(3)\ x \equiv -2: \quad q_0 - 2q_1 + 4q_2 - 3q_3 = 4(-2 - d)$
$(4)\ x \equiv -1: \quad q_0 - q_1 + q_2 - q_3 = 3(-1 - d)$

$$\begin{cases} q_0 + 2d = 0, \\ q_0 + q_1 + q_2 + q_3 + 3d = 3, \\ q_0 + 2q_1 + 4q_2 + 3q_3 + 2d = 4, \\ q_0 - 2q_1 + 4q_2 - 3q_3 + 4d = 2, \\ q_0 - q_1 + q_2 - q_3 + 3d = -3 \equiv 2\ mod\ 5. \end{cases};$$

Решаем систему методом Гаусса:

$$\left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 2 & 0 \\ 1 & 1 & 1 & 1 & 3 & 3 \\ 1 & 2 & 4 & 3 & 2 & 4 \\ 1 & -2 & 4 & -3 & 4 & 2 \\ 1 & -1 & 1 & -1 & 3 & 2 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 & 3 \\ 0 & 2 & 4 & 3 & 0 & 4 \\ 0 & -2 & 4 & -3 & 2 & 2 \\ 0 & -1 & 1 & -1 & 1 & 2 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 & 3 \\ 0 & 0 & 2 & 1 & -2 & -2 \\ 0 & 0 & 6 & -1 & 4 & 3 \\ 0 & 0 & 2 & 0 & 2 & 0 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 & 3 \\ 0 & 0 & -2 & -1 & 2 & 2 \\ 0 & 0 & 0 & -4 & 0 & 4 \\ 0 & 0 & 0 & -1 & 4 & 2 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 & 3 \\ 0 & 0 & -2 & -1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 4 \end{array}\right)$$

$d = 4;$

$q_3 = 4;$

$q_2 = 1;$

$q_1 = 4;$

$q_0 = 2;$

$$\begin{array}{rrrrrrr|lrrrr} & 4x^3 & + & x^2 & + & 4x & + & 2 & x & - & 4 & \\ \cline{8-11} - & 4x^3 & + & 4x^2 & & & & & 4x^2 & + & 2x & + & 2 \\ \cline{1-5} & & - & 2x^2 & + & 4x & & & & & & \\ & & & 2x^2 & + & 2x & & & & & & \\ \cline{3-6} & & & & - & 2x & + & 2 & & & & \\ & & & & & 2x & + & 2 & & & & \\ \cline{5-8} & & & & & & & 0 & & & & \end{array}$$

Ответ: $(2, 2, 4)$.