ВАРИАНТ ЗАДАНИЯ И ОТВЕТЫ К ЗАДАЧАМ

Вариант 14

1. Русское слово из четырех букв закодировано при помощи алгоритма RSA открытым ключом $e = 25$, $m = 35$). Шифрованное сообщение имеет вид (33; 13; 20; 2). 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: Ф: 90; Х: 46; Ц: 98; Ч: 24; Ш: 59; Щ: 89; Ъ: 51.

3. Какое число задаётся данным кодом Грея: 10110111?

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): 3, 3, 2, 2, 2.

№	Ответ
1	ЯЛТА
2	00(Ф), 1101(Х), 01(Ц), Ч(1100), 101(Ш), 111(Щ), 100(Ъ)
3	218
4	(3; 3; 2)

Выполнил: Радионов Роман, 0362

1. $e = 25, m = 35, (33; 13; 20; 2)$

   1) $de \equiv 1\ mod\ \varphi(m)$

   $\varphi(35) = \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 24$

   $25d \equiv 1\ mod\ 24$

   $25d + 24y = 1$

r	25	24	1	0
q		1	24	
d	1	0	1	

   $d = 1\ mod\ 24 = 1$

   2) $a_i^d\ mod\ m$

   $33\ mod\ 35 = 33$

   $13\ mod\ 35 = 13$

   $20\ mod\ 35 = 20$

   $2\ mod\ 35 = 2$

   3) 33 = Я, 13 = Л, 20 = Т, 2 = А

   Ответ: ЯЛТА.

2. Ф: 90, Х: 46, Ц: 98, Ч: 24, Ш: 59, Щ: 89, Ъ: 51

   1) Соединяем:

   98(Ц), 90(Ф), 89(Щ), 59(Ш), 51(Ъ), 46(Х), 24(Ч)

   98(Ц), 90(Ф), 89(Щ), 70(ХЧ), 59(Ш), 51(Ъ)

   110(ШЪ), 98(Ц), 90(Ф), 89(Щ), 70(ХЧ)

   159(ЩХЧ), 110(ШЪ), 98(Ц), 90(Ф)

   188(ЦФ), 159(ЩХЧ), 110(ШЪ)

   269(ЩХЧШЪ), 188(ЦФ)

   2) Расщепляем

   0(ЦФ), 1(ЩХЧШЪ)

   0(ЦФ), 10(ШЪ), 11(ЩХЧ)

   00(Ф), 01(Ц), 10(ШЪ), 11(ЩХЧ)

00(Ф), 01(Ц), 10(ШЪ), 110(ХЧ), 111(Щ)

00(Ф), 01(Ц), 100(Ъ), 101(Ш), 110(ХЧ), 111(Щ)

00(Ф), 01(Ц), 100(Ъ), 101(Ш), 1100(Ч), 1101(Х), 111(Щ)

3) Фильтруем:

Ф: 00

Х: 1101

Ц: 01

Ч: 1100

Ш: 101

Щ: 111

Ъ: 100

Ответ: 00(Ф), 1101(Х), 01(Ц), Ч(1100), 101(Ш), 111(Щ), 100(Ъ).

3. 10110111

0: 1

1: $1 + 0 = 1$

2: $1 + 0 + 1 = 0$

3: $1 + 0 + 1 + 1 = 1$

4: $1 + 0 + 1 + 1 + 0 = 1$

5: $1 + 0 + 1 + 1 + 0 + 1 = 0$

6: $1 + 0 + 1 + 1 + 0 + 1 + 1 = 1$

7: $1 + 0 + 1 + 1 + 0 + 1 + 1 + 1 = 0$

$11011010 = 128 + 64 + 16 + 8 + 2 = 218$

Ответ: 218.

4. $P(x)$ – исходн.

$\hat{P}(x)$ – фактич.

$D(x)$ – ошибка

$Q(x) = P(x) \cdot D(x) \equiv \hat{P}(x) \cdot D(x)$

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

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

(0) $x = 0$: $q_0 + 3d = 0$

(1) $x = 1$: $q_0 + q_1 + q_2 + q_3 + 3d = 3$

(2) $x = 2$: $q_0 + 2q_1 + 4q_2 + 3q_3 + 2d = 4$

(3) $x = -2$: $q_0 - 2q_1 + 4q_2 - 3q_3 + 2d = -4$

(4) $x = -1$: $q_0 - q_1 + q_2 - q_3 + 2d = -2$

Решение системы уравнений:

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

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

$$\sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 3 & 0 \\ 0 & 1 & 1 & 1 & 0 & 3 \\ 0 & 0 & 1 & \frac{1}{2} & -\frac{1}{2} & -1 \\ 0 & 0 & 0 & -4 & 2 & 8 \\ 0 & 0 & 0 & -1 & 0 & 3 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 3 & 0 \\ 0 & 1 & 1 & 1 & 0 & 3 \\ 0 & 0 & 1 & \frac{1}{2} & -\frac{1}{2} & -1 \\ 0 & 0 & 0 & 1 & -\frac{1}{2} & -2 \\ 0 & 0 & 0 & -1 & 0 & 3 \end{array}\right) \sim$$

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

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

$$\sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & 6 \\ 0 & 1 & 0 & 0 & 0 & \frac{13}{2} \\ 0 & 0 & 1 & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & 0 & 1 & 0 & -3 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{array}\right).$$

$$\begin{cases} q_0 = 6 \equiv 1 \\ q_1 = \frac{13}{2} \\ q_2 = -\frac{1}{2} \\ q_3 = -3 \equiv 2 \\ d = -2 \equiv 3 \end{cases}$$

$q_1 = \frac{13}{2}\ mod\ 5$

$2q_1 = 13\ mod\ 5$

$2x - 5y = 13$

$2x + 5y' = 1$

r	2	5	2	1	0
q		0	2	2	
x	1	0	1	-2	
y	0	1	0	1	

$x_0 = -2$

$x = -26 + 5n$

$x = q_1 = 4$

$q_2 = -\frac{1}{2} mod\ 5$

$2q_2 = -1\ mod\ 5$

$q_2 = 2$

$D(x) = x - 3 \equiv x + 2$

$$
\begin{array}{l|l}
2x^3+2x^2+4x+1 & x+2 \\
\cline{2-2}
2x^3+4x^2 & 2x^2+3x+3 \\
\cline{1-1}
\quad 3x^2+4x & \\
\quad 3x^2+x & \\
\cline{1-1}
\quad\quad 3x+1 & \\
\quad\quad 3x+1 & \\
\cline{1-1}
\quad\quad\quad 0 &
\end{array}
$$

$P(x) = 3 + 3x + 2x^2 \Rightarrow$ исходное сообщение $(3; 3; 2)$

Ответ: $(3; 3; 2)$.