МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Рыбинский государственный авиационный технмческий университет имени П.А. Соловьева»

КАФЕДРА ЭМиЭИС

Информационная безопасность

|  |  |
| --- | --- |
|  | Группа: ЗИП-14  Студент: Лебедев Е. В.  Преподаватель: Михайлов Н. Л.  Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Рыбинск 2017

Содержание

[Задача 1 код Хэмминга 3](#_Toc499927817)

[Задача 2 Полиграммная замена 6](#_Toc499927818)

[Задача 3 Код Виженера 7](#_Toc499927819)

# Задача 1 код Хэмминга

Сообщение: 01101100

К=8, 2m > k+m, m=4

Проверочные биты 1, 2, 4, 8 и 13 бит четности

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|  |  | 0 |  | 1 | 1 | 0 |  | 1 | 1 | 0 | 0 |  |

И3: 3 = 20 + 21 = 1 + 2 => Информационный бит И3 проверяется контрольными битами П1 и П2.

И5: 5 = 20 + 22 = 1 + 4 => Информационный бит И5 проверяется контрольными битами П1 и П4.

И6: 6 = 21 + 22 = 2 + 4 => Информационный бит И6 проверяется контрольными битами П2 и П4.

И7: 7 = 20 + 21 + 22 = 1 + 2 + 4 => Информационный бит И7 проверяется контрольными битами П1, П2 и П4.

И9: 9 = 20 + 23 = 1 + 8 => Информационный бит И9 проверяется контрольными битами П1 и П8.

И10: 10 = 21 + 23 = 2 + 8 => Информационный бит И10 проверяется контрольными битами П2 и П8.

И11: 11 = 20 + 21 + 23 = 1 + 2 + 8 => Информационный бит И11 проверяется контрольными битами П1, П2 и П8.

И12: 12 = 22 + 23 = 4 + 8 => Информационный бит И12 проверяется контрольными битами П4 и П8.

П1 = И3 + И5 + И7 + И9 + И11 = 0 + 1 + 0 + 1 + 0 = 0

П2 = И3 + И6 + И7 + И10 + И11= 0 + 1 + 0 + 1 + 0 = 0

П4 = И5 + И6 + И7 + И12 = 1 + 1 + 0 + 0 = 0

П8 = И9 + И10 + И11 + И12 = 1 + 1 + 0 + 0 = 0

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |

Если 4й симовл искажен 01111100

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |

П1: П1 + И3 + И5 + И7 + И9 + И11 = 0 + 0 + 1 + 1 + 1 + 0 = 1 http://all-ht.ru/inf/systems/img/00_22.gif 0

П2: П2 + И3 + И6 + И7 + И10 + И11 = 0 + 0 + 1 + 1 + 1 + 0 = 1 http://all-ht.ru/inf/systems/img/00_22.gif 0

П4: П4 + И5 + И6 + И7 + И12 = 0 + 1 + 1 + 1 + 0 = 1 http://all-ht.ru/inf/systems/img/00_22.gif 0

П8: П8 + И9 + И10 + И11 + И12 = 0 + 1 + 1 + 0 + 0 = 0 http://all-ht.ru/inf/systems/img/00_31.gif 0

Проверка для бита П1 П2 П4 не пройдена, найдем бит с ошибкой, найдем биты принадлежащие всем ошибочным группам, это бит И7 , инвертировав его значение получим исходное сообщение.

Если 5й и 6й символы искажены 01100000

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

П1: П1 + И3 + И5 + И7 + И9 + И11 = 0 + 0 + 1 + 0 + 0 + 0 = 1 http://all-ht.ru/inf/systems/img/00_22.gif 0

П2: П2 + И3 + И6 + И7 + И10 + И11 = 0 + 0 + 1 + 0 + 0 + 0 = 1 http://all-ht.ru/inf/systems/img/00_22.gif 0

П4: П4 + И5 + И6 + И7 + И12 = 0 + 1 + 1 + 0 + 0 = 0 http://all-ht.ru/inf/systems/img/00_31.gif 0

П8: П8 + И9 + И10 + И11 + И12 = 0 + 0 + 0 + 0 + 0 = 0 http://all-ht.ru/inf/systems/img/00_31.gif 0

Обнаружено 2 ошибки.

# Задача 2 Полиграммная замена

Сообщение: СКОРО\_МОРОЗЫ

Алфавит:

|  |  |  |  |
| --- | --- | --- | --- |
| ­\_ | А | Б | В |
| Г | Д | Е | Ж |
| З | И | К | Л |
| М | Н | О | П |
| Р | С | Т | У |
| Ф | Х | Ц | Ч |
| Ш | Щ | Ъ | Ы |
| Ь | Э | Ю | Я |

Шифр: ИТТМБМНПМТШЛ

# Задача 3 Код Виженера

Сообщение: доброе утро вам

Ключ: бекон

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Д | О | Б | Р | О | Е | У | Т | Р | О | В | А | м |
| Б | Е | К | О | Н | Б | Е | К | О | Н | Б | Е | К |

(Д (5) + Б (2)) mod 32 = Ж (7)

(О (14) + Е (6)) mod 32 = Ф (20)

(Б (2) + К (11)) mod 32 = Н (13)

(Р (16) + О (14)) mod 32 = Ю (30)

(О (14) + Н (13)) mod 32 = Ы (27)

(Е (6) + Б (2)) mod 32 = З (8)

(У (19) + Е (6)) mod 32 = Щ (25)

(Т (18) + К (11)) mod 32 = Э (29)

(Р (16) + О (14)) mod 32 = Ю (30)

(О (14) + Н (13)) mod 32 = Ы (27)

(В (3) + Б (2)) mod 32 = Д (5)

(А (1) + Е (6)) mod 32 = Ж (7)

(М (12) + К (11)) mod 32 = Ч (23)

Шифр: жфнюыз щэюы джч