# Оглавление

# Глава 1

# Кодирование

## 1.1 Код Хэмминга

**Алгоритм.** Есть сообщение

$$y = (0, 1, 0, 1, 0, 1, 1)$$

Заводим шаблон

$$\overline{y} = (x_1, x_2, \_, x_3, \_, \_, \_, x_4, ...)$$

Записываем сообщение на свободные места

$$\overline{y} = (x_1, x_2, 0, x_3, 1, 0, 1, x_4, 0, 1, 1)$$

$$A\overline{y} = b$$

Назначаем такие значения $x$-ам, чтобы $b \underset{2}{\equiv} 0$

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \left(\overline{y}\right) = \begin{pmatrix} x_1 + 3 \\ x_2 + 3 \\ x_3 + 2 \\ x_4 + 2 \end{pmatrix}$$

Чтобы везде были чётные числа, определим

$$x_1 = 1 \quad x_2 = 1 \quad x_3 = 0 \quad x_4 = 0$$

Получаем

$$\overline{y} = (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$$

Отправляем его

## 1.2 Криптография

Терминология:
Ключ, Алгоритм, Сообщение, Зашифрованное сообщение

### 1.2.1 RSA

**Лемма 1.** $a$ взаимно просто с $n$

$$\Longrightarrow a^{\varphi} \underset{\varphi}{\equiv} 1$$

**Лемма 2.** $e$ взаимно просто с $\varphi$

$$\Longrightarrow \exists! d \in 1 : \varphi : e \cdot d \underset{\varphi}{\equiv} 1$$

**Алгоритм.** Выбираем два простых числа $p$ и $q$

$$n = pq$$

$p, q$ – закрытые, $n$ – открытый. При достаточно большом $n$ найти $p$ и $q$ практически невозможно

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

$e$ – секретный ключ, $d$ – публичный ключ, $d, e \in 1 : (n-1)$

$$y_i = x_i^d \mod (n)$$

$$x_i = y_i^e \mod (n)$$

**Пример.**

$$n = 33$$

$$p = 3 \quad q = 11$$

$$\varphi = 20$$

$$e = 7 \implies d = 3$$

Сообщение: 312

$$y_1 = 3^7 \mod 33$$

$$y_2 = 1$$

$$y_3 = 2^7 \mod 33$$

Можно скомбинировать с предыдущим шифрованием:

**Алгоритм.** 1. Генерируем ключ $\boxed{\text{сессии}}$:

$$c = (0,1,0,1) \xrightarrow{RSA} f$$

$$a \xrightarrow{c} b$$

$$(b, f)$$

$$f \to c$$

$$b \xrightarrow{c} a$$