1 Задание 7

1.1 Задача 1

$$e_A = (107, 187); e_B = (7, 253)$$

$$\phi_A = \phi(187) = 16 \cdot 10 = 160; \phi_B = \phi(253) = 22 \cdot 10 = 220$$

$$d_A = e_A^{-1} \bmod 160; d_B = e_B^{-1} \bmod 220$$

a	b	r	x	y
160	107		-2	3
107	53	1	1	-2
53	1	2	0	1
1	0	53	1	0

$$220 \cdot (-2) + 7 \cdot 63 = 1 \to d_B = 63$$

$$m = 17; m_B = m^{e_B} \bmod 253 = 17^7 \equiv 250 mod 253$$

$$17^7 = 17^6 \cdot 17 = 104 \cdot 17 \equiv 250 \bmod 253$$

$$17^6 = (17^3)^2 = 106^2 \equiv 104 \bmod 253$$

$$17^3 = 17^2 \cdot 17 = 36 \cdot 17 = 106 \bmod 253$$

$$17^2 = 17^2 = 289 = 51 \bmod 253$$

Сертификат: $c = m^{d_A} = 17^3 \equiv 51 mod 187$

1.2 Задача 2

$$s_y = y^d = r^{ed}x^d \equiv rx^d \bmod n \to r^{-1}s_y \equiv x^d \bmod n$$

1.3 Задача 3

$$\begin{cases} M^3 \equiv_{N_1} C_1 \\ M^3 \equiv_{N_2} C_2 \\ M^3 \equiv_{N_3} C_3 \end{cases}$$

Используя китайскую теорему об остатках решим эту систему сравнений. Вычислим $N = N_1N_2N_3$. Для каждого $i \in \{1, 2, 3\}$ найдем $K_i = \frac{N}{N_i}$. Расширенным алгоритмом Евклида найдем $K_i^{-1} \bmod N_i$. Теперь найдем решение $M^3 = \sum\limits_{i=1}^{3} C_iK_iK_i^{-1} \bmod N$. По китайской теореме об остатках, существует ровно один вычет по модулю N, удовлетворяющий системе. Поскольку $M < N_i, M^3 < N$. Тогда полученное решение по модулю N равно M^3, а значит, можно вычислить $M = \sqrt[3]{M^3}$, например, итеративным методом Ньютона.

Асимптотика: При решении системы использовались арифметические операции и алгоритм Евклида – полиномиальное время. Каждая итерация метода Ньютона состоит из арифметических операций, при этом с каждой итерацией количество верно вычисленных цифр удваивается – получается полинамиальный алгоритм от длины числа.

1.4 Задача 4

Сначала определим количество чисел от 2 до $N - 1$, которые подходят на роль d. Для начала рассмотрим все числа, меньшие $\phi(N)$. Из этих чисел среди принадлежащих $\mathbb{Z}_{\phi(\mathbb{N})}$ не подходит, т.к. иначе

$$ex \equiv_{\phi(N)} 1 \to x \equiv_{\phi(N)} e^{-1}$$

Поскольку $x \neq e^{-1}$, x должен быть больше $\phi(N)$. Теперь рассмотрим числа, большие либо равные $\phi(N)$. Таких чисел всего $pq - pq + p + q - 1 = p + q - 1 \ll \phi(N)$. Поэтому с очень большой точностью чисел, удовлетворяющих d, найдется всего одно. Теперь подсчитаем матожидание количества попыток по определению:

$$\mathbb{E}[T] = 1\frac{1}{n-2} + 2 \cdot \frac{n-3}{n-2}\frac{1}{n-3} + 3\frac{n-3}{n-2}\frac{n-4}{n-3}\frac{1}{n-4} + ...$$

$$\mathbb{E}[T] = \frac{1}{n-2} + 2\frac{1}{n-2} + 3\frac{1}{n-2} + ... + (n-2)\frac{1}{n-2} = \frac{(n-2)(n-1)}{2(n-2)} = \frac{n-1}{2}$$

Теперь подсчитаем матожидание количества попыток при полном переборе. Формула получится такой же, что и при случайном выборе, поэтому матожидание будет таким же $\frac{n-1}{2}$

1.5 Задача 5

Докажем индукицей по n. Считаем, что всюду $m \leq n$, т.к. в противном случае алгоритм не завершит работу корректно.

1. База индукции $n = 0, 1$ В первом случае возможно только пустое множество, оно и будет возвращено. Во втором случае при $m = 0$ возможно тольео пустое множество, оно и возвращается, при $m = 1$ рекурсивный вызов возвращается пустое множество, поэтому единственный элемент случайно выбирается функцикй $Random(0, 1)$

2. Индукционный переход: пусть алгоритм случайно и равновероятно возвращает множество для некоторого $n = k$.

3. Докажем, что это так и для $n = k + 1$. Покажем что вероятности вхождения каждого элемента из $[1, n+1]$ в итоговое множество равны. В ходе выполнения алгоритма будет рекурсивный вызов, который по предположению индукции вернет случайное равновероятное множество S размера m из первых n элементов. Рассмотрим произвольный элемент, не равный $n + 1$. Тогда вероятность вхождения этого элемента в множество равна сумме вероятностей вхождения этого элемента в S, и вероятности вхождения этого элемента при добавлении в S: $P = \frac{m}{n} + \frac{n-m}{n}\frac{1}{n+1} = \frac{m+1}{n+1}$. Рассмотрим $n + 1$-й элемент. Он входит в множество, если был выбран элемент, который уже принадлежит S, или если был выбран $n + 1$. Поскольку в S m элементов, эта вероятность равна $\frac{m}{n+1} + \frac{1}{n+1} = \frac{m+1}{n+1}$. Таким образом, у всех элементов одинаковые вероятности дополнить случайное монжество. Значит полученное при дополнении множество будет случайным.