

Защита лабораторной 4

по предмету мат. основы защиты информации

Дидусь К.В.

Российский университет дружбы народов, Москва, Россия

Информация

- Диудусь Кирилл Валерьевич
- Студент кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- 1132223499@rudn.ru
- <https://github.com/kirilldi/>



Введение

Актуальность

- Изучение базовых принципов шифрования
- Важность знания основ шифрования для работы в сфере информационных технологий

Цели и задачи лабораторной

Целью данной лабораторной работы является ознакомление с алгоритмом Евклида, а так же с его реализацией в программном виде.

- ТУИС РУДН
- Язык программирования Python

Выполнение лабораторной

Алгоритм Евклида

Алгоритм Евклида – эффективный алгоритм для нахождения наибольшего общего делителя двух целых чисел

$$106 / 16 = 6, \text{ остаток } 10$$

$$16 / 10 = 1, \text{ остаток } 6$$

$$10 / 6 = 1, \text{ остаток } 4$$

$$6 / 4 = 1, \text{ остаток } 2$$

$$4 / 2 = 2, \text{ остаток } 0$$

Расширенный алгоритм Евклида

Расширенный алгоритм Евклида — это расширение алгоритма Евклида, которое вычисляет кроме наибольшего общего делителя (НОД) целых чисел a и b ещё и коэффициенты соотношения Безу, то есть целые x и y , такие что $ax+by=\text{НОД}(a,b)$

индекс i	частное q_{i-1}	остаток r_i	s_i	t_i
0		240	1	0
1		46	0	1
2	$240 \div 46 = 5$	$240 - 5 \times 46 = 10$	$1 - 5 \times 0 = 1$	$0 - 5 \times 1 = -5$
3	$46 \div 10 = 4$	$46 - 4 \times 10 = 6$	$0 - 4 \times 1 = -4$	$1 - 4 \times -5 = 21$
4	$10 \div 6 = 1$	$10 - 1 \times 6 = 4$	$1 - 1 \times -4 = 5$	$-5 - 1 \times 21 = -26$
5	$6 \div 4 = 1$	$6 - 1 \times 4 = 2$	$-4 - 1 \times 5 = -9$	$21 - 1 \times -26 = 47$
6	$4 \div 2 = 2$	$4 - 2 \times 2 = 0$	$5 - 2 \times -9 = 23$	$-26 - 2 \times 47 = -120$

Figure 2: Рис. 2. Пример работы расширенного алгоритма

Бинарный алгоритм Евклида

- 1) если оба числа a и b четные, то $\text{НОД}(a, b) = 2 \cdot \text{НОД}(\frac{a}{2}, \frac{b}{2})$;
- 2) если число a – нечетное, число b – четное, то $\text{НОД}(a, b) = \text{НОД}(a, \frac{b}{2})$;
- 3) если оба числа a и b нечетные, $a > b$, то $\text{НОД}(a, b) = \text{НОД}(a - b, b)$;
- 4) если $a = b$, то $\text{НОД}(a, b) = a$.

Figure 3: Рис. 3. Пример работы расширенного алгоритма

Применение алгоритма

- Шифрование открытым ключом
- Для поиска взаимно-простых чисел

Вывод

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: я ознакомился с алгоритмом Евклида, а так же мне удалось реализовать вариации этого алгоритма на языке программирования Python.