

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ФЕДЕРАЛЬНОЕ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)

Факультет прикладной математики, информатики и механики
Кафедра Системного анализа и управления

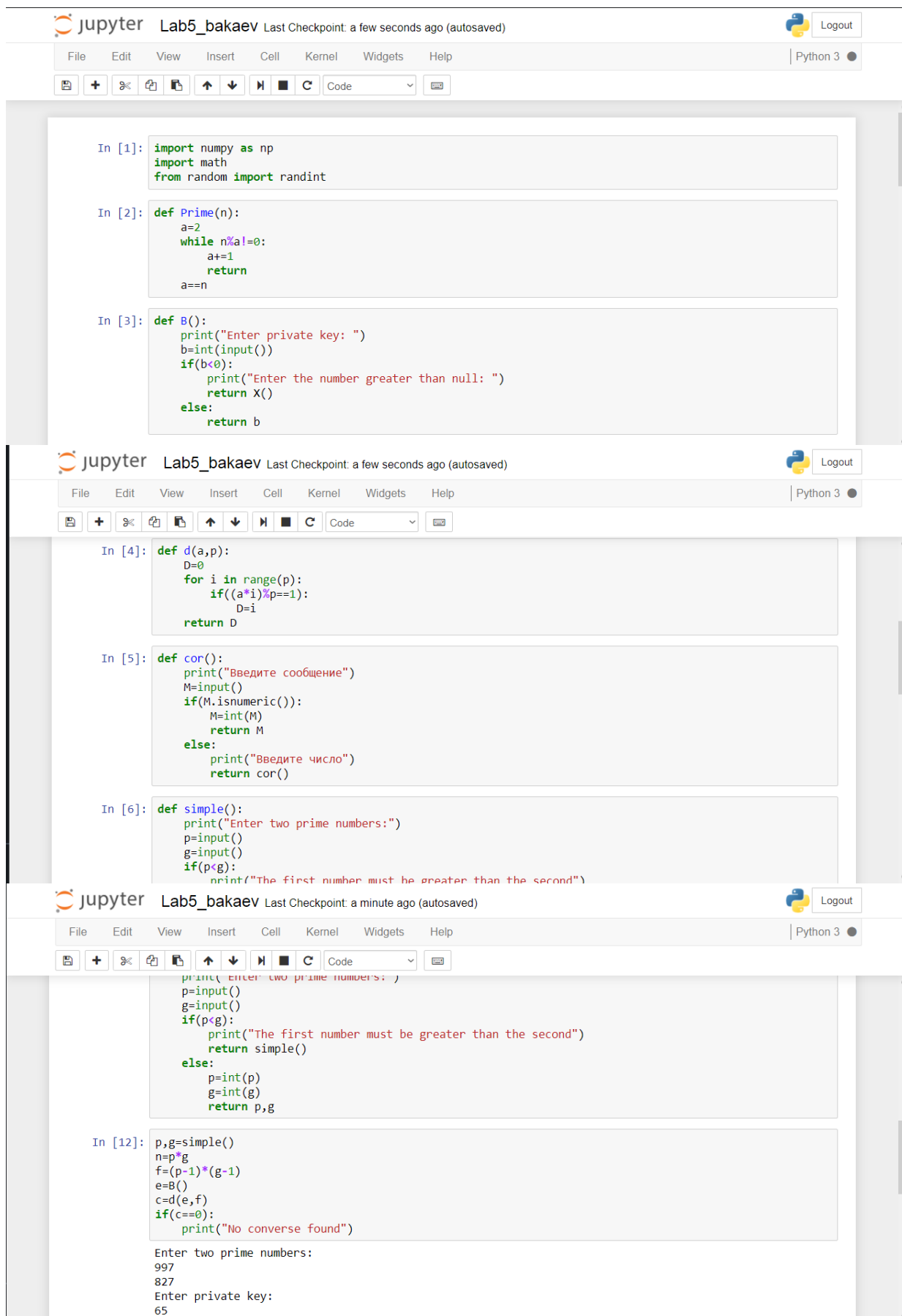
Лабораторная работа №5
«Алгоритм генерации цифровой подписи»

Выполнил: студент 4 к. 6 гр. ПМИ
Бакаев Илья Игоревич

Воронеж – 2021

1. Цель работы:

Программно реализовать алгоритм генерации цифровой подписи.



The image displays three sequential screenshots of a JupyterLab notebook interface, showing the implementation of a digital signature algorithm. The notebook is titled "Lab5_bakaev" and shows the following code:

```
In [1]: import numpy as np
import math
from random import randint

In [2]: def Prime(n):
a=2
while n%a!=0:
a+=1
return a
a==n

In [3]: def B():
print("Enter private key: ")
b=int(input())
if(b<0):
print("Enter the number greater than null: ")
return X()
else:
return b

In [4]: def d(a,p):
D=0
for i in range(p):
if((a*i)%p==1):
D=i
return D

In [5]: def cor():
print("Введите сообщение")
M=input()
if(M.isnumeric()):
M=int(M)
return M
else:
print("Введите число")
return cor()

In [6]: def simple():
print("Enter two prime numbers:")
p=input()
g=input()
if(p<g):
print("The first number must be greater than the second")
return simple()
else:
p=int(p)
g=int(g)
return p,g

In [7]: def X():
print("Enter two prime numbers: ")
p=input()
g=input()
if(p<g):
print("The first number must be greater than the second")
return simple()
else:
p=int(p)
g=int(g)
return p,g

In [12]: p,g=simple()
n=p*g
f=(p-1)*(g-1)
e=B()
c=d(e,f)
if(c==0):
print("No converse found")

Enter two prime numbers:
997
827
Enter private key:
65
```

.....

.....

.....

.....

.....

Выполнено в Jupyter Notebook (Anaconda)