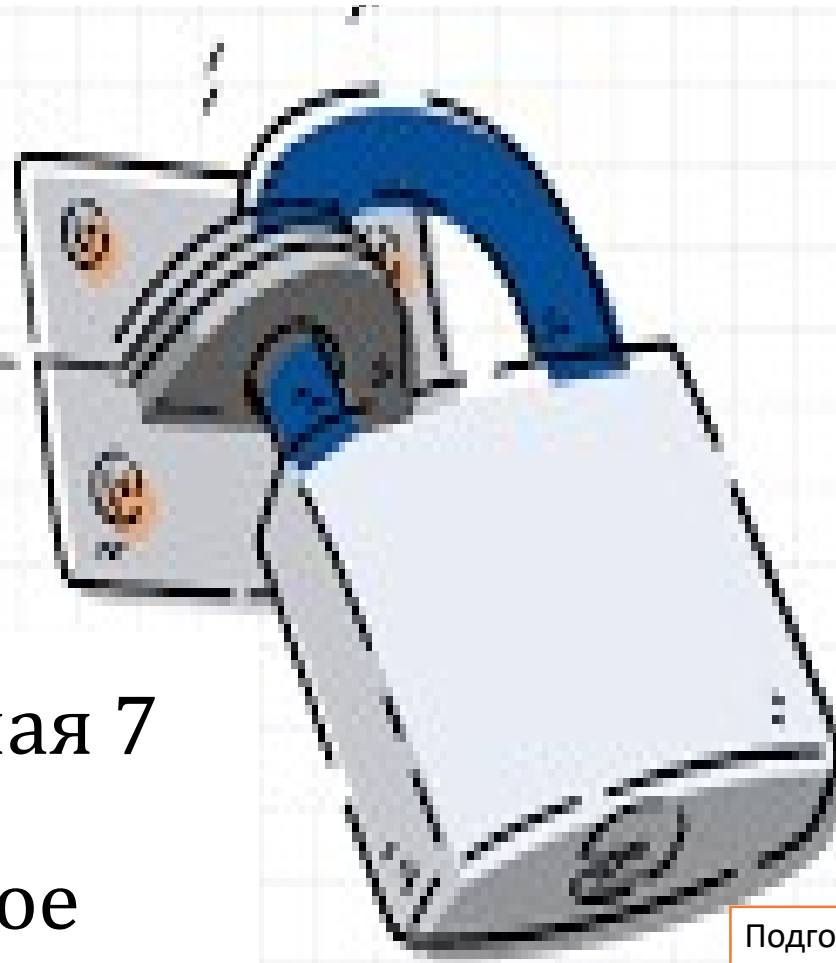


# Российский университет дружбы народов Научный факультет

Математические  
основы защиты  
информации и  
информационной  
безопасности



## Лабораторная 7

## Дискретное логарифмирование

Подготовлено студентом:  
Елиенис Санчес Родригес.  
Преподаватель: Дмитрий Сергеевич

# Логарифм

**Логарифм - это показатель степени, до которого необходимо увеличить положительную величину, чтобы в результате получить определенное число. Следует помнить, что показатель степени-это число, обозначающее степень, до которой должна быть увеличена другая цифра.**

**Таким образом, логарифм числа-это показатель степени, до которого должно быть увеличено основание, чтобы получить это число. Часто арифметические вычисления можно выполнить более простым способом, обратившись к логарифмам..**

# Дискретные логарифмы

Дискретные логарифмы - это теоретическая группа аналогов обычного логарифма. Этот тип логарифмов-это логарифмы, которые из  $x$  на основе  $a$  по модулю  $p$  для  $a$  решают уравнение  $x=a$  по модулю  $p$ , где  $x$ ,  $p$  и  $a$  постоянны, а  $y$  неизвестно. Модульная арифметика - это система арифметики, используемая для различных классов эквивалентности целых чисел, называемых классами конгруэнтности. Обычный логарифм - это решение уравнения  $ax = b$  над комплексными числами. В противном случае мы можем в качестве примера привести уравнение  $gx = h$  в виде дискретного логарифма к основанию  $g$   $h$  в группе  $G$ . Но если  $g$  и  $h$  являются элементами конечной циклической группы  $G$ , то это решение  $x$ .

Более жесткое определение было бы следующим:

Пусть  $G$ -конечная циклическая группа с  $n$  элементами, тогда  $G=\{e, g, g^2, \dots, g^{n-1}\}$ .

# Дискретные логарифмы

Для вычисления и решения дискретных логарифмов используются алгоритмы, которые в информатике и математике представляют собой конечный набор инструкций, используемых для выполнения задачи или действия. Существуют популярные варианты дискретной криптографии логарифмов. Например, система шифрования и дешифрования ElGamal, основанная на математических задачах с дискретными логарифмами. Еще одна из используемых систем — это система Диффи-Хеллмана.



# Дискретные логарифмы

```
# Python3 program to calculate  
# discrete logarithm  
import math
```

```
def discreteLogarithm(a, b, m):  
    n = int(math.sqrt(m) + 1)
```

```
    # Calculate  $a^n$   
    an = 1  
    for i in range(n):  
        an = (an * a) % m
```

```
    value = [0] * m
```

```
    # Store all values of  $a^{(n*i)}$  of LHS  
    cur = an  
    for i in range(1, n + 1):  
        if (value[cur] == 0):  
            value[cur] = i  
        cur = (cur * an) % m
```

```
    cur = b  
    for i in range(n + 1):
```

```
        # Calculate  $(a^n)^i * b$  and check  
        # for collision  
        if (value[cur] > 0):  
            ans = value[cur] * n - i  
            if (ans < m):  
                return ans  
        cur = (cur * a) % m
```

```
    return -1
```

```
print("calculo de logaritmo discreto")
```

```
a = int(input("ingrese el primer número entero positivo: "))
```

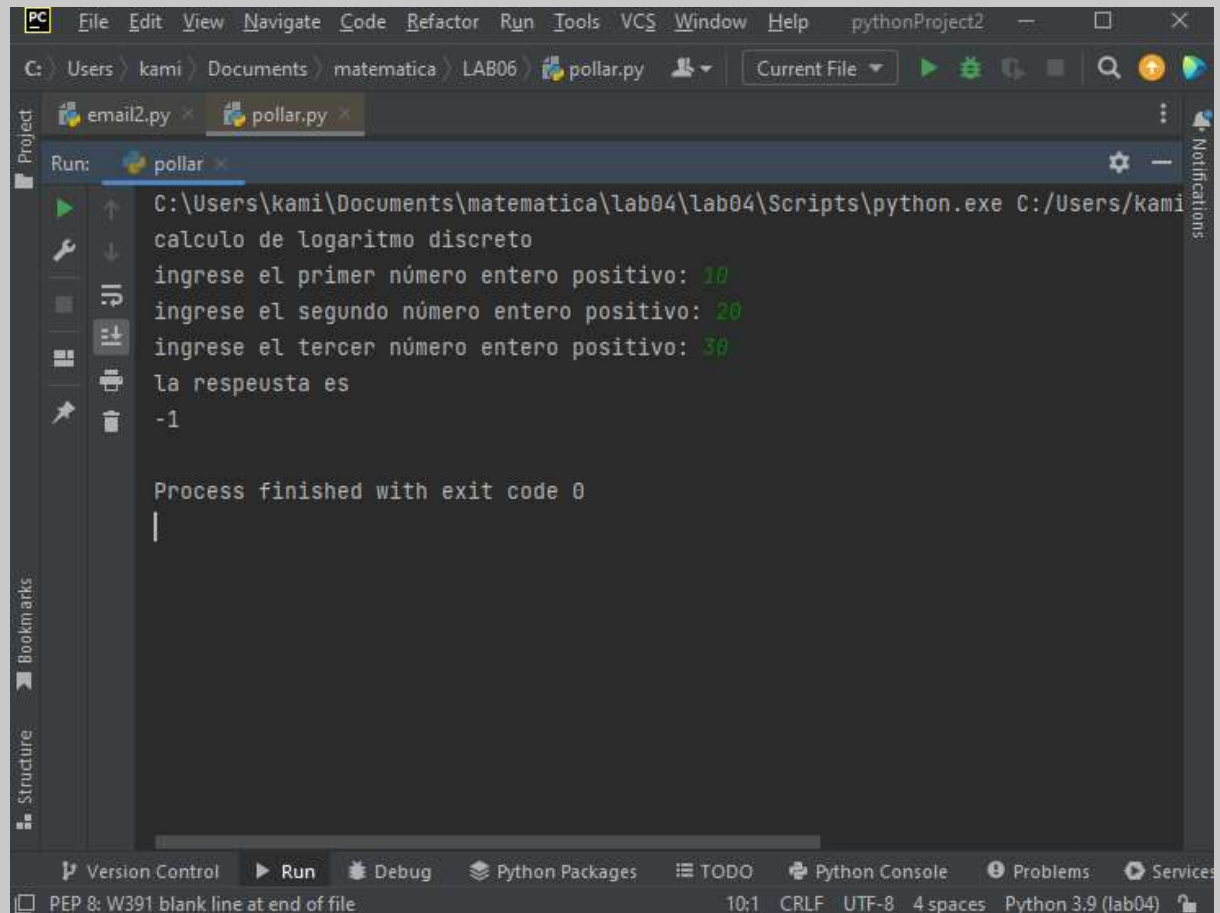
```
b = int(input("ingrese el segundo número entero positivo: "))
```

```
m = int(input("ingrese el tercer número entero positivo: "))
```

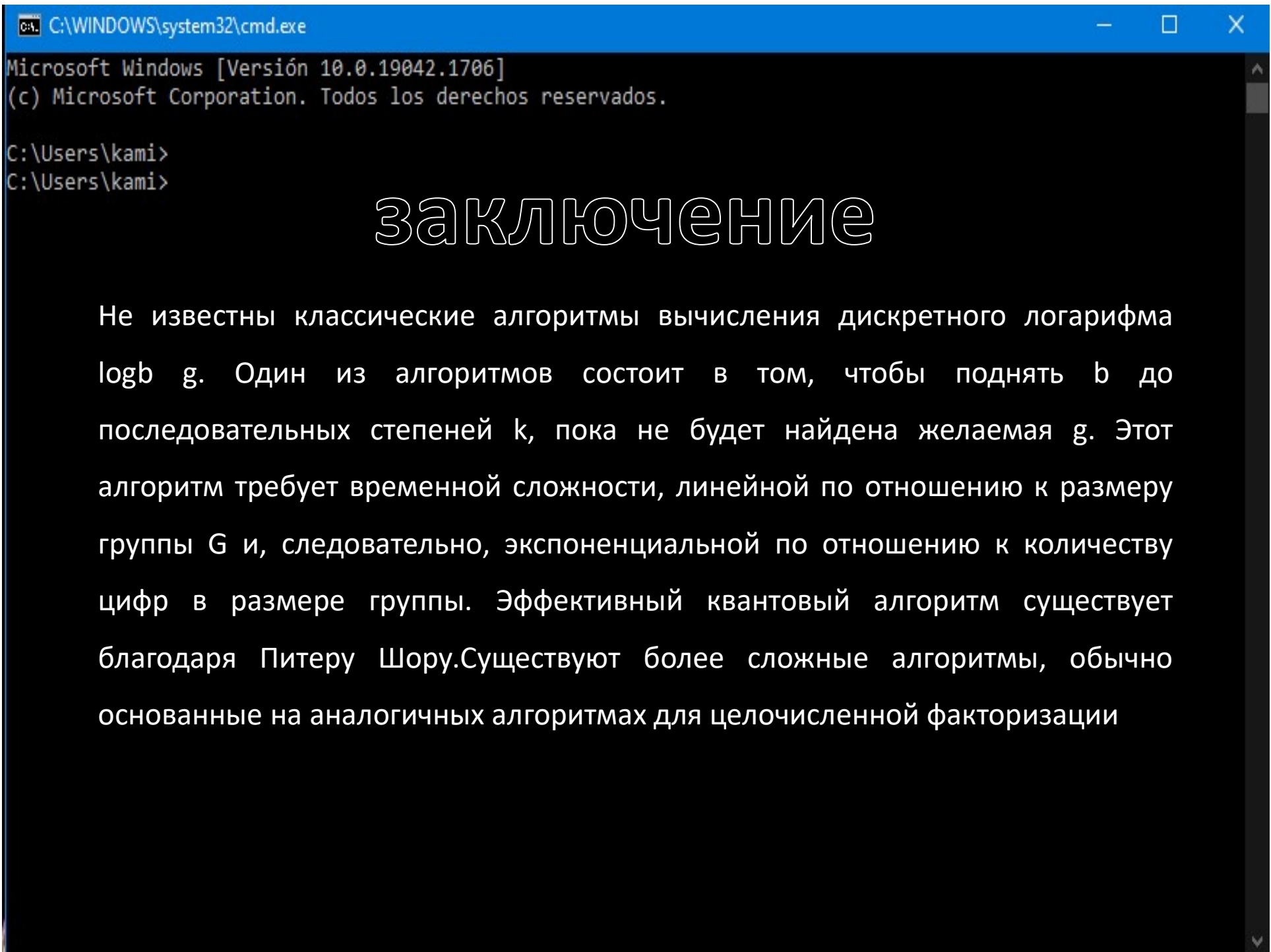
```
# Driver code
```

```
print("la respeusta es ")
```

```
print(discreteLogarithm(a, b, m));
```

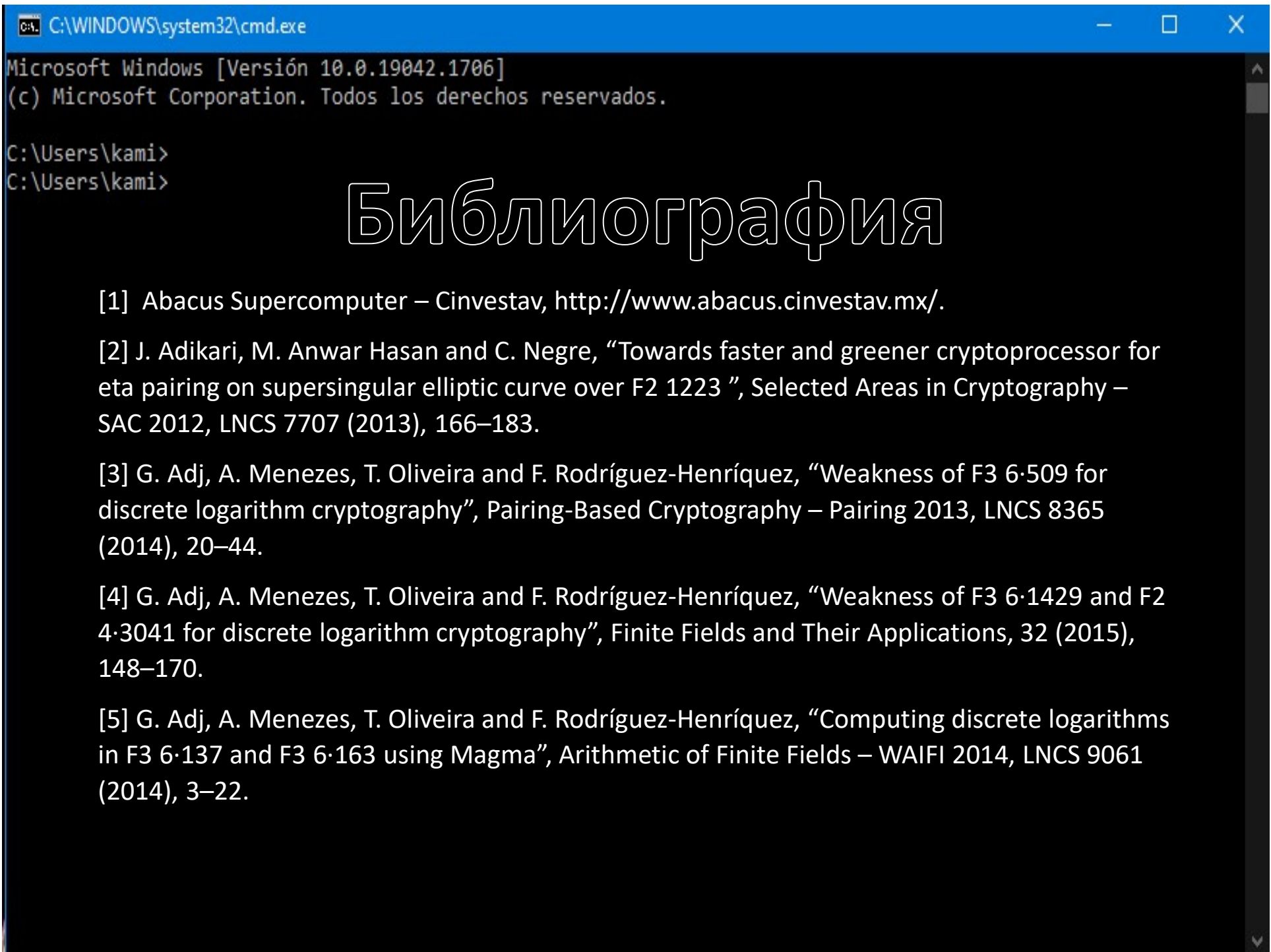


The screenshot shows an IDE window titled 'pythonProject2'. The file explorer on the left shows the project structure with files 'email2.py' and 'pollar.py'. The 'Run' tab is active, showing the command: `C:\Users\kami\Documents\matematica\lab04\lab04\Scripts\python.exe C:/Users/kami\Documents\matematica\lab04\lab04\Scripts\python.exe C:/Users/kami\Documents\matematica\lab04\lab04\Scripts\python.exe C:/Users/kami\Documents\matematica\lab04\lab04\Scripts\python.exe`. The output console displays the following text:   
calculo de logaritmo discreto  
ingrese el primer número entero positivo: 10  
ingrese el segundo número entero positivo: 20  
ingrese el tercer número entero positivo: 30  
la respeusta es  
-1  
Process finished with exit code 0



# ЗАКЛЮЧЕНИЕ

Не известны классические алгоритмы вычисления дискретного логарифма  $\log_b g$ . Один из алгоритмов состоит в том, чтобы поднять  $b$  до последовательных степеней  $k$ , пока не будет найдена желаемая  $g$ . Этот алгоритм требует временной сложности, линейной по отношению к размеру группы  $G$  и, следовательно, экспоненциальной по отношению к количеству цифр в размере группы. Эффективный квантовый алгоритм существует благодаря Питеру Шору. Существуют более сложные алгоритмы, обычно основанные на аналогичных алгоритмах для целочисленной факторизации



# Библиография

- [1] Abacus Supercomputer – Cinvestav, <http://www.abacus.cinvestav.mx/>.
- [2] J. Adikari, M. Anwar Hasan and C. Negre, "Towards faster and greener cryptoprocessor for eta pairing on supersingular elliptic curve over  $F_{2^{1223}}$ ", Selected Areas in Cryptography – SAC 2012, LNCS 7707 (2013), 166–183.
- [3] G. Adj, A. Menezes, T. Oliveira and F. Rodríguez-Henríquez, "Weakness of F3 6·509 for discrete logarithm cryptography", Pairing-Based Cryptography – Pairing 2013, LNCS 8365 (2014), 20–44.
- [4] G. Adj, A. Menezes, T. Oliveira and F. Rodríguez-Henríquez, "Weakness of F3 6·1429 and F2 4·3041 for discrete logarithm cryptography", Finite Fields and Their Applications, 32 (2015), 148–170.
- [5] G. Adj, A. Menezes, T. Oliveira and F. Rodríguez-Henríquez, "Computing discrete logarithms in F3 6·137 and F3 6·163 using Magma", Arithmetic of Finite Fields – WAIFI 2014, LNCS 9061 (2014), 3–22.

C:\WINDOWS\system32\cmd.exe

Microsoft Windows [Versión 10.0.19042.1706]  
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\kami>

C:\Users\kami>Большое спасибо