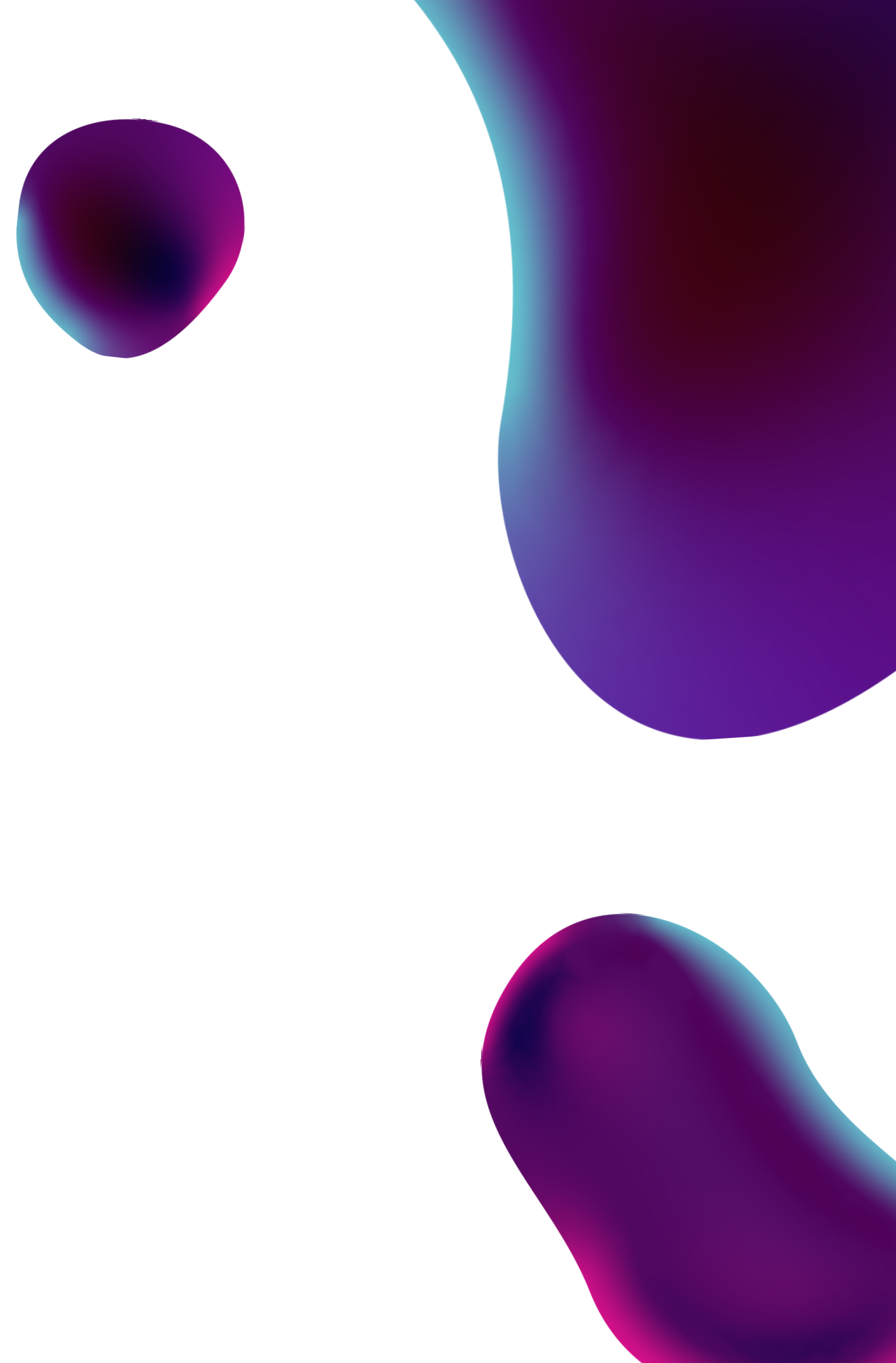


Universidad Industrial de Santander

ESCUELA DE INGENIERÍA DE SISTEMAS E
INFORMÁTICA

PROYECTO PARA LA ASIGNATURA DE MATEMÁTICAS
DISCRETAS 2021-2



Chat en tiempo real cifrado de extremo a extremo

by Carlos Daniel Peñaloza Torres

Introducción

Uno de los principales problemas de las comunicaciones son los ataques ***Man in the middle*** los cuales pueden ser muy peligrosos ya que pueden suplantar identidades en las comunicaciones y capturar información delicada, el objetivo de este proyecto fue brindar un canal de comunicación seguro para organizaciones que necesiten de un canal de comunicación privada y seguro.

Métodología

Para solucionar este problema se implementara mediante ***sockets***, una comunicación en tiempo real en la cual cada mensaje estará cifrado de extremo a extremo usando el ***algoritmo asimétrico RSA***, pues es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

The background features three large, abstract, organic shapes in shades of purple and blue. One shape is in the top right corner, another is a large, elongated shape on the right side, and a smaller one is at the bottom center. The text is centered on the left side of the image.

Solución del problema

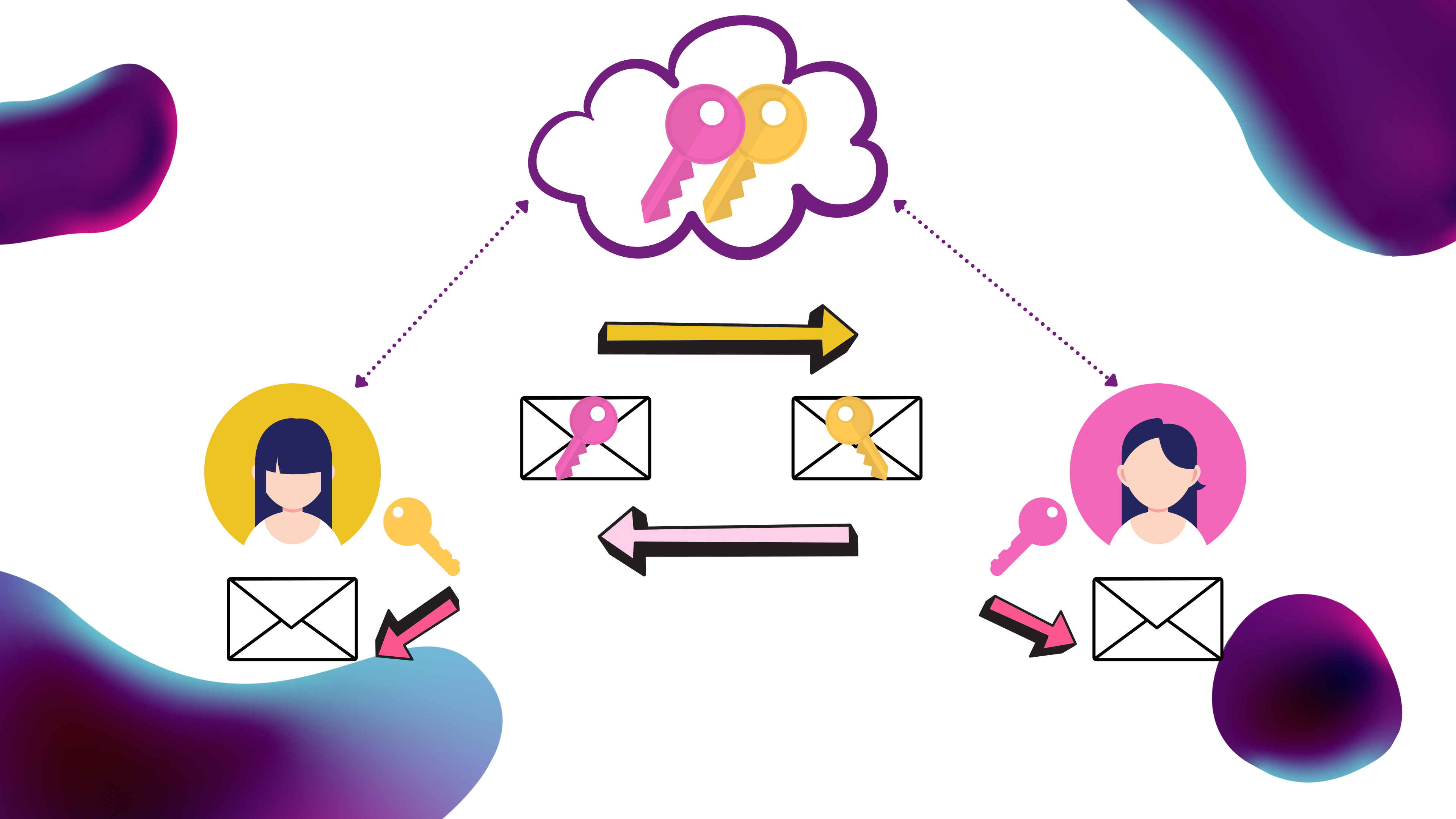
RSA

Rivest, Shamir y Adleman (RSA) es un sistema criptográfico de clave pública de clave pública para cifrar y firmar mensajes, desarrollado en 1979, que utiliza **factorización de números enteros**.

RSA

Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de **dos números primos grandes elegidos al azar** y mantenidos en secreto.

Actualmente estos primos son del orden de **10^{300}**

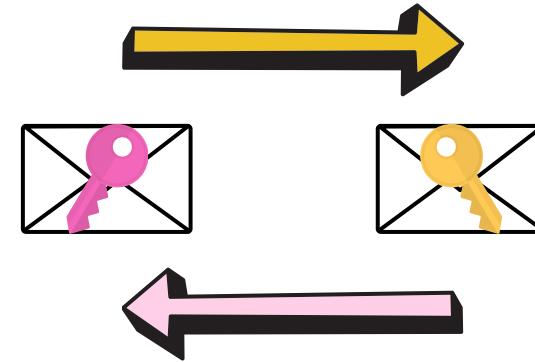


Claves públicas de A y B

Clave privada de A



A



Clave privada de B



B



Como en todo sistema de clave pública, **cada usuario posee dos claves de cifrado: una pública y otra privada.**

Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, **cifra su mensaje con esa clave**, y una vez que el mensaje cifrado llega al receptor, este se ocupa de **descifrarlo usando su clave privada.**

RSA

Se cree que **RSA** será seguro mientras no se conozcan formas rápidas de descomponer un número grande en producto de primos.

Herramientas utilizadas

Flask es un framework minimalista escrito en Python, utilizado para realizar el backend del aplicativo.



HTML, CSS, JavaScript, Bootstrap y JQuery son las tecnologías utilizadas para realizar la funcionalidad e interfaz del proyecto

Visual Studio Code fue editor de código fuente utilizado para la realización del proyecto



The background features three large, abstract, organic shapes in shades of purple and blue. One shape is in the top right corner, another is a large, elongated shape on the right side, and a smaller one is at the bottom center. The word "Resultado" is centered on the left side of the image.

Resultado

Pantalla de Login

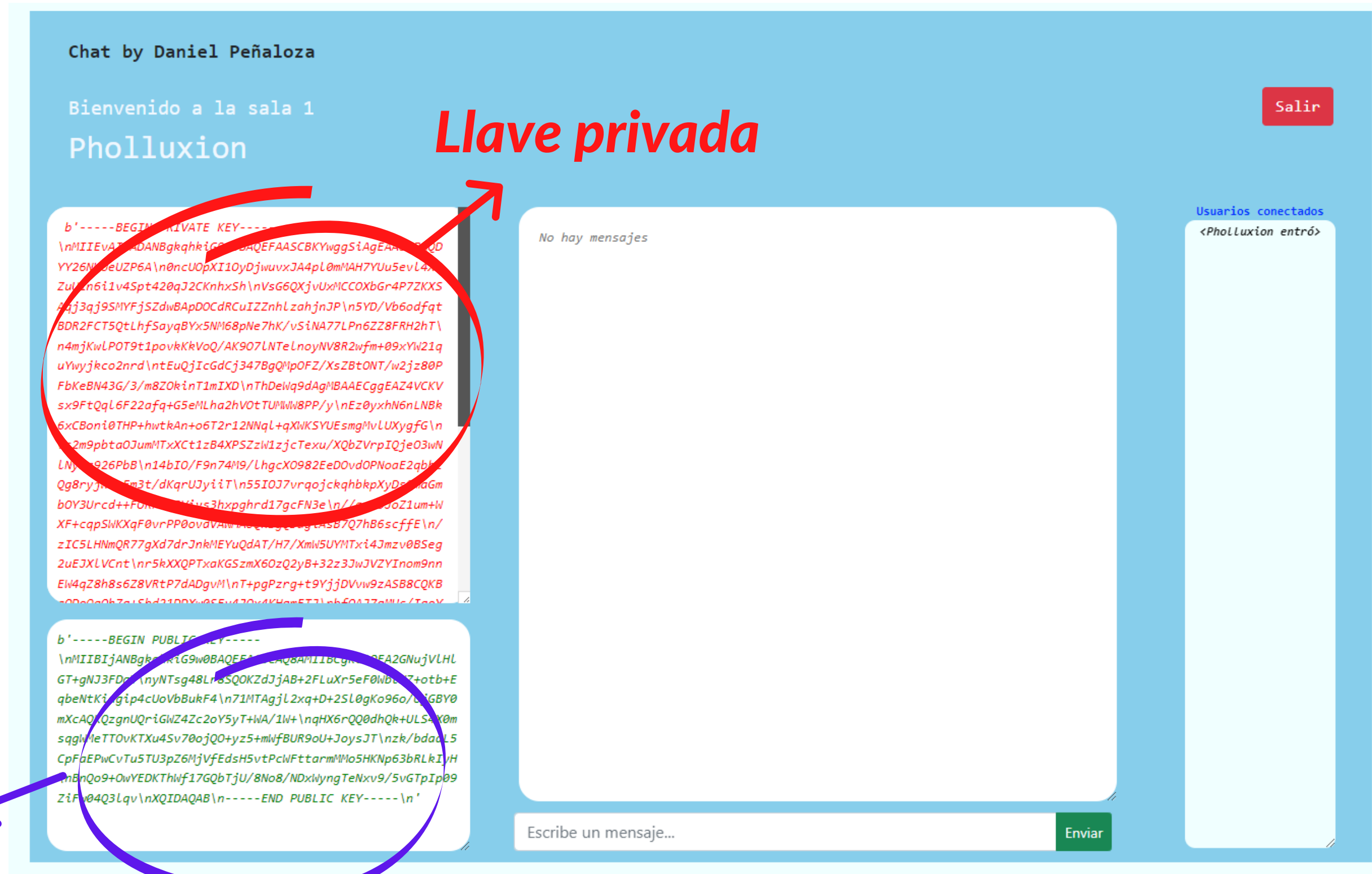


Inicio de sesión

Entrar

© Universidad Industrial de Santander 2022

Pantalla del Chat



Llave publica

Chat by Daniel Peñaloza

Bienvenido a la sala 1

Pholluxion

Salir

Usuarios conectados

<Pholluxion entró>

Pholluxion : b'Hola'

Escribe un mensaje...

Enviar

Mensaje encriptado

Pholluxion :

b"\x9d\xe8s\x9b\xa9\x999\xca\x08f\x8f\xbc\xcb\x0e
\xf5\x90\x92h\x88\xb8\xfa\xc2R\xce\xbd=\xcb\x94\
xec\x86:\xcaS\x1c\xbf\xaa^\x16\x8b\x04\x86\x9c\xce
eC\xdb\xa4(\xa5\xe5\xef\x13\x9d\x8bXu\xd2\x00:\xf
4\\|xeaE\xe0\xc4Nh\xa1A\xc6\xcapb\\|xa5\x1d\xbf
\xa2\x8aG\\|x96E\x19\xce\x98j_\xa5\xc4\x03Q\x17K
r\x19\xd2\r\xae\xfe\xfb\x13\x9d\x8bXu\xd2\x00:\xf
10\xaa\x89*\xf0(\xe7\x88\x86\x19/\x95\xe3999\xca
\x07IP\xca\x0c\xce'\x01\xfa\xa1\xa9\x8f\xb6D\x18\
xe1\xae\xb2\xfe0`p\x18\x12\x85\xef"\x02\x0b\xe43]
\x13\xb2\xfe\x0`kQ\xb5\xc6\x1b\xc6\xfb\x13\x1e7
\xadJ\xfb\x8a\xfe\xdc:\xcd\xfb,=\xf2\xfb\x193KA\x14
5\xcc\x96\xb4\xcb^\x96\xfb\x02\xb5\x91\t\xe6\xcb!
\x0bGC\x1e?
d\xce*\x87\r\x0f6\xba\x8b\x87\xa6\xd0\xb7\x02\x8
8\xe4w\xda\x1d-\xbdX\xba\x1e\x9b\xa1\xdf?
z\x91t\xfb\x0c#\xb3\xff\xdb\x0c\xfb0F\xdb7\x85\xa4I
\xbf'

Mensaje encriptado

Chat by Daniel Peñaloza

Bienvenido a la sala 1

Juan

Salir

Mensaje encriptado

Juan :

b"\x90x\|tmO\|xe8|x0f\|xce,,K)\|x04~B\|xee\|xe2\|xc2\|xc5
\|xc3\|x0c\|xd0ZP\|xc9V\|xa0\|xb8\|xb0\|x9b1"T>\|xd5\|x8
a\|xe3w\|xde~gy\|x1d\|xa9\|xe6Z%M\|xdd\|xe7\|xe1\|x94\|
xb0\|xe7d\|xc6\|xd7"\|xac\|x1f\|x9f\|x88-
"\|xc2\|xd7\|x97\|xb98X9L\|x9d\|xe3\|x8a\|xde\|xce\|x86w
@\|x05\|xa5qt\|xea^\|xc0\|x15\|xa1C\|xaa\|x92\|x99\|x92q\|f-
xd3\|x087\|x87?
\|xc7\|xc15\|hf=\|x94\|xaf\|x88\|xb9\|x9bX6\|xba>?
\|x1b9\|x89\|x1a\|xd1\|xc3\|xf0H\|x9b\|xe6B\|x80p\|x95\|xd
5-
(t\|x99{<D\|xaf\|xcd\|xc4.\|xa5:ZB\|x13\|xc2:\|xf4\|x95!3S\|x
f0\|xe0\|xf4\|xd8\|xbbrF\|x9a\|x1b0\|xa5.\|xfdVN=\|xce\|xb
3\|rNqykrY>\|xbb[X\|xd7J\|xd1\|xb0U\|xe4\|xf7\$?
b\|x84\|xa6\|x8f\|x82\|x1e\|x83\|xd7\|xaa\|xd2?
\|x0b\|x89\|xcc\|xee\|f\|xad\|xf4\|xcbG\|xfaO\|xa2\|xcf\|xdf\|x6-
0f\|x8f\|xa0c\|xb7\|xbc6\|xcf\|x80\|x84\|x84\|x0e\|xf5\|xb1\|x1V
95,L\|xf1\|xc8~\|xd0\|x0b\|x83\|xb5i\|x80\$|x7f\|x90\|x05\|E
\|xd8'

```
b'-----BEGIN PRIVATE KEY-----
\nMIIEvwIBADANBgkqhkiG9w0BAQEFAASCBAQwggSLAgEAAoIBAQD
Q9dK5h7AG5g2z\n9Qbg3v3nB51FFCqhaJ/aE3mt0i5ZakI9d3dzxc
XGpQTAAguqg+ZH+JktUiHhhY8A\n4aeaLcK4xK2uLpxkamrSI63hY
88T2\nzhU4k/W0u1cQdezNVae/fIexr1KPFd+\nZCGgVhy6LmHp
ufwfGuAIhJiIRHyQ6cd9wh1o6v73re01Fh3zDsw0zml\
nTez1h+f5YS7EnICttsUzV0CQcWEiRXcQPQz8am8i35iXU37NkEUI
kAf4ki8yDRvB\n11zqP6vYaLWVAhiC1+SZNai01QHWLWz3Id39/pa
\n1mqq7obGO0MZi6HU5\n54n/S531AgMBAAECggEAep4VLo
\nhLneUchspgDh4kWezkCHrvJwGz8wI4\ndos5DDWctdE1t
\nVd1KbQNb6II5VKFICMEJZo79H8jhIUxw7fuG9e5ROSS\n
baQVdTiL+ZpycHWulLmRR+DqiAbFit+8A1tMpCKD3vjCuduxa2cfr
\nh3rz4\nIGzLtxieaPBnUJrzPtPB5Wb2qI74+1pra7Deo7Nj
\nyH/a7fJk3mWVCVEw\nTsJJ9hgd5o9/8kW+U5Pdw8NsMTK
H6mHmQ5zJiLsLGOML3r3iJVALtDhVzcj1LnE\nYsxlWq6YKK050w/
\nRAk2KerataT5/4HeT1zaJuX8bm7QK8gQD33GLTyRo7L1HZBE7d\nn9
\nCyeUFZiYzLw+gRR+eZKUysjhCRiWnr8NFR83mNxnaRM4S4
8z+4bj1Ed+\nuQI/nRk5oLL1uI+VDMr220L4NBi08wx2k9tK8GsK0
\nBTFTxNw6EeqzYGn\n4EALIGRWVP+UmubmK4qFNeYNwvKB
\n1H7f6RYuFavBcF6Kl\unpYX0Qvdt\nD4M73KQ37V6/NF8
b'-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAPXSuYewB
\nN79\n5wedRRQqoWif2hN5rdIuWlpCPXd3c8XFxqUEwGhrqo
\nIh4YwPAOGnmi3C\nnuMStri6cZGpq0i0t4WCvE9sri8M4VOJ
95,L\|xf1\|xc8~\|xd0\|x0b\|x83\|xb5i\|x80$|x7f\|x90\|x05\|E
\nXszVWnv3yHsa9SjxQ/mQhoFYc\nui5h6YC7E4co7bn1nxrg
CISYokR6kOnHfcIdZaOr+963tNRYd8w7MMN5pU3s9Yfh\nneWExJyAr
bbFM1dA\nHFhIkV3ED0M/GpvIt+YL1N+zZBFCJAH+JiVMg0bwd6c6j+r
\n2GpVLQIYgtfkmTWOjtUB1pVs9yHd/f6WgKdfa6LJdZqo06GxjtDGY
uh10eeJ/0ud\n9QIDAQAB\n-----END PUBLIC KEY-----\n'
```

Pholluxion : b'Hola'
Juan : b'Hola Daniel'

Mensajes desencryptados

Escribe un mensaje...

Enviar

Usuarios conectados

<Juan entró>

¿Cómo usar?

1. Tener instalado Python 3.+ y Git
2. Clonar el repositorio
 - *git clone https://github.com/Pholluxion/Proyecto-Matematicas-Discretas-2021-2-UIS.git*
3. Instalar **virtualenv** para crear un entorno virtual.
 - *pip install virtualenv*
 - *py -m venv env*
4. Activar entorno virtual en la raíz del proyecto y ejecutar el comando
 - *pip install -r .\requirements.txt*
5. Ejecutar el archivo *app.py*

Referencias

- RSA — cryptography 37.0.0.Dev1 documentation. (s/f). Cryptography.io. Recuperado el 7 de marzo de 2022, de <https://cryptography.io/en/latest/hazmat/primitives/asymmetric/rsa/>
- Vollebregt, B. (s/f). Asymmetric encryption and decryption in Python. Nitratine.Net. Recuperado el 7 de marzo de 2022, de <https://nitratine.net/blog/post/asymmetric-encryption-and-decryption-in-python/>



¿Tienes alguna pregunta?