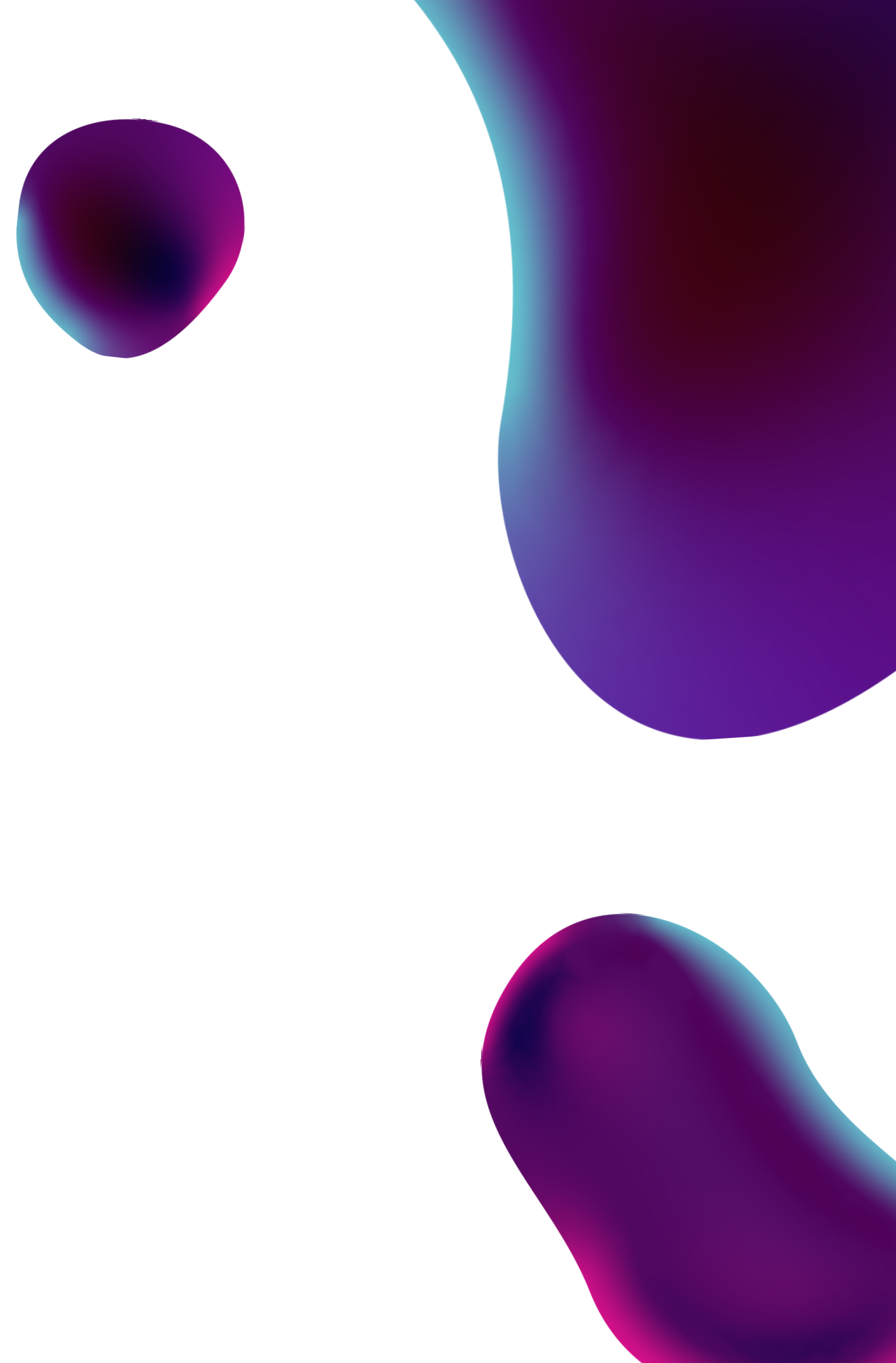


Universidad Industrial de Santander

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

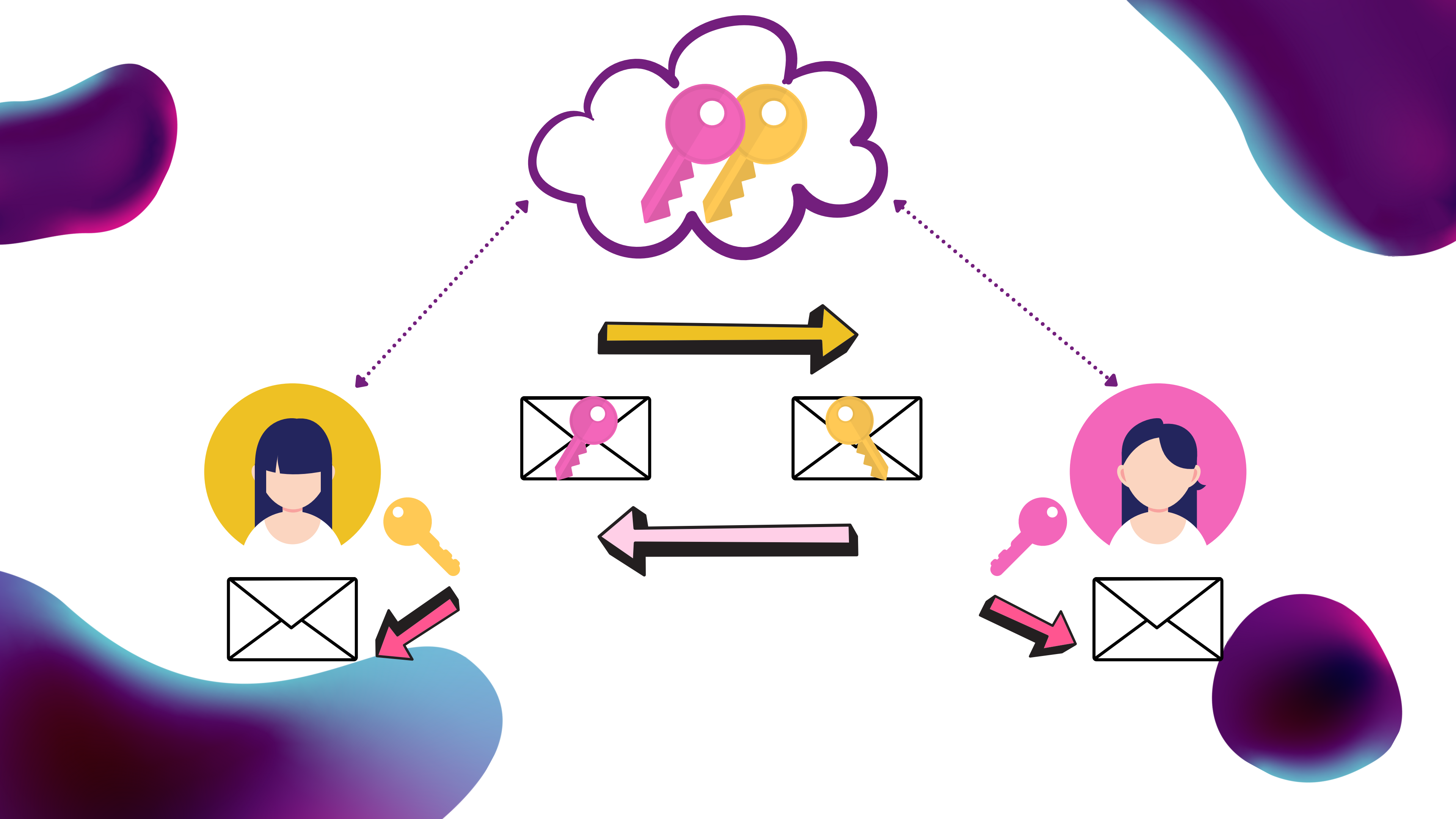
Uno de los principales problemas de las comunicaciones son los ataques ***Man in the middle*** los cuales pueden ser muy peligrosos ya que pueden suplantar identidades en las comunicaciones y capturar información delicada, el objetivo de este proyecto fue brindar un canal de comunicación seguro para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



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



Resultado

Pantalla de Login



Inicio de sesión

Entrar

© Universidad Industrial de Santander 2022

Pantalla del Chat

Chat by Daniel Peñaloza

Bienvenido a la sala 1

Pholluxion

Salir

b'-----BEGIN PRIVATE KEY-----

%nMIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYYggSiAgEAAoIBAQD
YY26NWUeUzP6A\n\ncUOpXIIOyDjwuvxJA4pl0mIAH7YUu5evL4XR
ZuU1n6i1v4Spt420qJ2CKnhxSh\nVs66QXjVUXiCCOXbGr4P7ZXKS
Aaj3jq9SMYfJSzdWBApDOCDRCuIZZhnlzahjnJP\n\5YD/Vb6odfqL
BDR2FCT5QtLhfSayqBYx5NM68Pne7hk/vSiNA77LPn6ZZ8FRH2htV
n4mjKwLPOT9t1povkKkVoQ/AK907LNTeLnoyNV8R2wfjm+89xYW21q
uYwyjkco2nrnd\ntEuQjJCgdCj347BgQMPOFZ/XszBZONT/w2jz80P
FBkEBN43G/3/m8ZOkt1T1mIXD\n\ThDeWg9dAgMBAAECggEAZ4VCKV
sx9FtQql6F22afq+G5eMLha2hvOTUMWW8PP/y\n\nEz0yxhN6nLNbk
6xCBonioTHP+hwtKAn+o6T2r12NNql+qXWKSYUEsmgMvLUxygfG\n\nvs2m9pbtaOJumMTxXCt1zB4XPSSzW1zjcTexu/XQBZVrpIQjeO3wN
Lnywa926PbB\n\nn14bIO/F9n74M9/LhgCXO982EEODvodOPNoaE2qbhc
Qg8ryjWrMfm3t/dKqrUJyiit\n\n55IOJ7vrqojckqhbkpXyDsQmaGm
boY3Urcd++FORFi7JVIs3hxpghrd17gcFN3e\n\n/gurDJozIum+W
XF+cqpSKXqF0vrPP0ovdVAImAoQKBgQDugiAsB7QjhB6scffE\n\n/n/
ZIC5LHNmQR77gXd7drJnkMEYuQdAT/H7/Xmlw5UYMTxi4Jmzv0BSeg
2uEJXLVCnt\n\nlr5kXXQPXTxaKG5zmX60ZyB+3z23JwJVZYInom9nn
EW4q28hs6SZ8rtP7AdgvMt1T+pgPzrg+t9Yjdvw9ZASBB8CQg
E090qhzLcshd31DDXvE5Fu43704Vhe5TL3jcfDM37zhUuLTC

```
b'-----BEGIN PUBLIC KEY-----
```

```

\nMIIBIjAnBgqknriG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAG2GnujVVLH
GT+gNJ3FDqV\nyNtsg48Lr8SQOKZdJjAB+2FLuXr5eF0wblNZ+otb+E
qbeNtKidgip4cUoVbBukF4\n7n1MTAgjl2xq+D+2SLgKo96o/UjGBY0
mXcAQKQZgnUQriGWZ4Zc2oY5yT+wA/1w+\nqHX6rQQ0dhqK+ULS4X0m
sqglWmETToVtXU4Sv70ojQ0+yz5+mlvFBUR9oU+JoysJT\nzk/bdaaL5
CpFaEPcVtU5TU3pZ6jVfEdSh5vtPcWfTttarmMm05HKNp63bRLkIyh
\nBnQo9+0wYEDKThWf17GQBtJjU/8No8/NDxWlyngTeNxv9/5vGtPip09
ZiFw04Q3Lqv\nXQIDAQAB\n-----END PUBLIC KEY-----\n'

```

No hay mensajes

Escribe un mensaje...

Enviar

Usuarios conectados

<PhoLLuxion entró>

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\x04\x87\xdd\x04\xdc\xee\x
10\xaa\x89*\xf0(\xe7\x88\x86\x19/\x95\xe3999\xca
\x07IP\xca\x00\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\xf1\xa3\t\xe7
\xadJ\xf8\xa6\xfe\xdc:\xcd\xf0,=\xf2\xfc\x193KA\x14
5\xcc\x96\xb4\xc3^\x96\xf5\x02\xb5\x91\t\xe6\xc0!
\x0bGC\x1e?
d\xce*\x87\r\x0f6\xba\xb8\xb7\xa6\xd0\xb7\x02\x8
8\xe4w\xda\x1d-\xbdX\xba\xe1\x9b\xa1\xdf?
z\x91t\xf0\xc2#\xb3\xff\xd5\x0c\x8f0F\xd7\x85\xa4I
\xbf'

b'-----BEGIN PRIVATE KEY-----
\nMIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKYYwggSiAgEAAoIBAQD
YY26NWUeUZP6A\n0ncUOpXI10yDjwuvxJA4pL0mMAH7YUu5evL4XR
ZuU1n6i1v4Spt420qJ2CKnhxSh\nnVsG6QXjvUxMCCOXbGr4P7ZKXS
MYFjSZdwBApDOCdRCuIZZnhLzahjnJP\nn5YD/Vb6odfqt
QTLhfSayqBYx5NM68pNe7hK/vSiNA77LPn6ZZ8FRH2hT\
n4mjKwLpOT9t1povkKkVoQ/AK9O7LNTelnoyNV8R2wfm+09xYw21q
uYwyikcc2nrd\ntEuQjIcGdCj347BgQMpOFZ/XsZBtONT/w2jz80P
G/3/m8ZOkint1mIXD\nnThDeWq9dAgMBAAECggEAZ4VCKV
6F22afq+G5eMLha2hV0tTUMWw8PP/y\nnEz0yxhN6nLNBk
THP+hwtkAn+o6T2r12NNqL+qXWKSyUESmgMvLUXygfG\nn
aOJumMTxXCt1zB4XPSZzW1zjcTexu/XQbZVrpIQje03wN
PbB\nn14bIO/F9n74M9/LhgC
XO982EeDOvdOPNoaE2qbhc
WmFm3t/dKqrUJyiit\nn55IOJ7vrqojckqhbKpXyDsQmaGm
co++FORFi7JViys3hxpghrd17gcFN3e\nn//gurDJoZ1um+W
SKXqF0vrPP0ovdVAwMAoQKBgQDugiAsB7Q7hB6scffe\nn/
TCtWMeQR77gXd7drJnkMEYuQdAT/H7/XmW5UYMTxi4Jmzv0BSeg
2uE3YVCnt\nnr5kXXQPTxaKGSzmX60zQ2yB+32z3JwJVZYInom9nn
s6Z8VRtP7dADgvM\nnT+pgPzrg+tt9YjjDVvw9zASB8CQKB
7eL5hd3100Xw0SE5u470u4KHg
ETJ\ncb60A77eMLc/TeeY
-----END PRIVATE KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA2GnujVLHL
3fDqV\nnyNTsg48Lr8SQOKZdJjAB+2FLuXr5eF0WbLNZ+otb+E
qbeNtKigip4cUoVbBukF4\nn71MTAgjL2xq+D+2SL0gKo96o/UjGBY0
gnUQriGWZ4Zc2oY5yT+WA/1W+\nnqHX6rQQ0dhQk+ULS4X0m
sqgWMeTTOvKTXu4Sv70ojQO+yz5+mWfBUR9oU+JoysJT\nnzK/bdaaL5
CpFaEPwCuTu5TU3pZ6MjVfEdsH5vtPcWfTtarMMo5HKNp63bRLkIyH
\nBnQo9+OwYEDKThWf17GQbTjU/8No8/NDxWlyngTeNxxv9/5vGTpIp09
ZiFw04Q3Lqv\nnXQIDAQAB\nn-----END PUBLIC KEY-----\n'

Pholluxion : b'Hola'

Usuarios conectados

<Pholluxion entró>

Escribe un mensaje...

Enviar

Chat by Daniel Peñaloza

Bienvenido a la sala 1

Juan

Salir

Usuarios conectados

<Juan entró>

```
b'-----BEGIN PRIVATE KEY-----  
\\nMIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQD  
Q9dK5h7AG5g2z\\n9Qbg3v3nB51FFCqhaJ/aE3mt0i5ZakI9d3dzxc  
XGpQTAAguqq+ZH+JktUihhhY8A\\n4aealCk4xK2LpxkamrSI63hY  
XzhU4k/W0u1cQdezNVae/fIexr1KPFD+\\nZCGVhy6LmHp  
ufwfGuAIHjiRHyQ6cd9wh1Lo6v73re01Fh3zDsw0zml\\n  
Tetz1h+FSYS7EnICttsUzV0CQCWEIRXcQPQz8am8i35iXU37NkEUI  
ka4f4ki8DRVB\\n11zqp6vYaLnVAhiC1+SZNaiO1QHMLWz3Id39/pa  
2xc5lmgg7obGO0MZi6HU5\\n54n/S531AgMBAAECggEAep4VL0  
xd5|x8fhLneUchspgDH4klWezkChrvJwgZ8wi4\\ndos5DDWctdE1t  
e|\\n94vd1KbQNb6IISVKFICMEJZO79H8jhIUxw7fuG9e5ROSS\\n  
baQvdTIL+ZpycHWUlLmRR+DqiAbFit+8A1tMpCKD3vjCuduxa2cfr  
x86wIhz4\\nIGzLtxieaPBnUJrzPtPB5Wb2qi74+1pra7Deo7Nj  
9|x92q|F+yH/a7fJk3mwVCVEw\\ntTsJJ9hgds09/8kW+U5Pdw8NsMTK  
H6mHmq5xzJILSLGOML3r3iJVALtDhVzcj1LnE\\nYsxlwq6YKK050w/  
4RAk2KeftatS/4HeT1zaJuX8bm7QKBgQD3GLTyRo7L1HZBE7d\\n9  
x95|x42CyeUFZiyZLw+gRR+eZKUysjhCRWNr8NFR83mNXnaRM4S4  
8z+4bj1ed+\\nuQI/nRrk5oLL1ui+VDMr220L4NBiO8wx2k9tK8GsK0  
951S|xBTFTxNw6EeqZYgn\\n4EALIGRWVP+UmubmK4qFNeYNwwKB  
xce|xbb147f-8VwF5wB5E-KL6ssYQ0QwU\\nDAMJ3KO27VE/NfE  
b'-----BEGIN PUBLIC KEY-----  
\\nMIIIBIJBANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKQAQEA0PXSuYewB  
cf\\nxdxfxG\\n79\\n5wedRRQqowif2hN5rdIuwWpCPXD3c8XFxqUEWhgrgo  
5|xbl|xUih4YWPAOGnmI3C\\numStri6cZGpq0iOt4WCVe9sri8M4VOJ  
90|x05|EHXszVwnv3yHsa9SjxQ/mQhoFYc\\nuis5h6YC7E4co7bn1nxrg  
CISYokR8kOnHfcIdZaOr+963tNRYd8w7MMMSpU3s9Yfh\\newEuXJyAr  
bbFM1daKHfHIkv3ED0M/GpvIt+YL1N+zZBFCAJAH+JIvMgbwddc6j+r  
\\n2GpVLQIQYgtfkMtWojuTBUpVs9yHd/f6WgdKdfa6LJDzQo6GxjtDGy  
uh10eeJ/0ud\\n9QIDAQAB\\n-----END PUBLIC KEY-----\\n'
```

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

Escribe un mensaje...

[Enviar](#)

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?