Matheus Rafalski

TIAGO MALLMANN ROHDE

Segurança de Dados

17 de Março de 2025

Criptografia

INTRODUÇÃO

O trabalho foi realizado em Python em específico a versão 3.9, a escolha do python foi principalmente devido a sua função acadêmica que permite a abstração de diversos fatores para focar na parte principal da comunicação encriptada de mensagens além de eu possuir um conhecimento prévio com a linguagem. Para realização do trabalho foi utilizado quatro bibliotecas principais:

cryptography

Para fazer a criptografía das mensagens, a escolha dela foi pelo fato de ela conseguir abstrair a complexidade de forma eficiente, tornando a implementação extremamente intuitiva, possui todas a funcionalidades necessárias e além disso eu tinha um conhecimento prévio de outras utilizações

socket

Para realização da comunicação entre os servidores, é uma biblioteca padrão do python que cumpre o objetivo de forma eficiente.

• base64 e json

Ambas bibliotecas padrões do python que cumprem o mesmo objetivo a transformação dos dados para serem possíveis serem enviados através da biblioteca socket, ambas já existem no python por padrão então optei por utiliza-las também.

EXECUÇÃO

A execução segue um fluxo base onde se inicia o servidor, o cliente conecta-se ao servidor por outra porta, o cliente se registra no servidor mandando a chave pública serializada, o servidor recebe a chave pública serializada então desserializar a chave pública criptografa uma mensagem e manda de volta para o cliente, o cliente recebe a mensagem criptografada então descriptografa com sua chave secreta e exibe a mensagem criptografada.

```
base) → rsa-server-client python3 main.py
Server] Servidor iniciado em 127.0.0.1:8888
[Cliente] Chave pública cliente: b'-----BEGIN PUBLIC KEY-----\mMIIBIjANBokohkiG9w0BAOEFAAOCAO8AMIIBCoKCAOEA0Lkey42Y6PNDXcGRxbaA\npMO+o9vGSsvk8+ZoPIHjXA
82a+YTK5qjpB0BTbkcWhnjjcZjzPwubJ4ByPdri4\npxAh8Vx0CbWmgNG0JQ3AXNyPtkCCU+hFLHol+f8Vcg6D4C0XsaMio0QCtXIs3KLd\nKX2+f75TQLEJheSggfqRlNcM9pC6JeKpplmZwN9F2r
EX0rjYJOq415YKysiUXb\n/+9DipAY7xuyy+PGY83/VbpYACdr8CrkyUt3k8j4q+iLYE6toGr9C1NdDnPTbcHi\nOoIz/g9DTYasCovRoBgQ+aUPAsOdPgbpJvTxmM12XFs7ZkSPs/cwLRciDK3ghF
n8QIDAQAB\n----END PUBLIC KEY----\n'
Cliente] Chave privada cliente: b'-----BEGIN PRIVATE KEY-----\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQuR6/jZjo80Nd\nwZHFtoCkxD6j28ZKzKTz5
8geNcBF/zZr5hMrmq0kE4FNuRxaGe0NxmPM/C5sng\nHI92uLimsCHxXHQJtaaA0Y4lDcBc3I+2QIJT6EUseiX5/xVyDoPgI5exoyKjRAK1\ncizcot0pfb5/vlNAsQmF5KCB+pGU1wz2kLo14qmm
A30Xac70Rf5uNgk6rjXlg\nrkyJRdv/700KkBjvG7LL4/pjzf9VulgAJ2vwKuTJ53eTyPir6ItgTq2gav0LU100\nc9NtweI6gjP+D0NNhqwKi9GgGBD5pQ8Cw50+Bukm9PGYyXZcWztmRI+z9zAtF
M\nreCEUV7xAgMBAAECggEAFcI2omFwf1hcvXlgaOwNnR+YKBzRHxsWVxa95xDjUsRh\n/E3JqvhOwqAwDFigSyH/Jy9mSoIsZnUItoRDsGyxUy8pWq/4qMp3ARbXaqV0WDnm\nAWnYLEcabviM3PU
xlJ9i0/vJT1F3APmDq+0oFn7Nte8JI2u5e5FmwvD12/r3RL\nf5T7MtN9UTuJ8FePG60Rqj5ih/YdOgV0HnOImbPVIK5RB2V2vPul27aU56BSVJ3i\n6LgjLe2Px4tC77T6SMeHNmG/e0Ud0Yj952G
<u>vF6EsHbh+l+vDLhMZal</u>ou+2VW8m\nYcyNJ25yuETtGdE10J0tCx2/JyESPxOm7xxJ5BE0wQKBgQDtNaiOoxmkiA/kxQaQ\na/0TyvvSbGmcQpx6xFlb2EqxnZxAUPF46kSHI2YHAkXAB3dI8uVTaxz
usyz/02\nN2pRV6VqE2PfnI6bHPnIu0X6NEwmoSvREEH4Y/qcRYiLqAVOAUh1EAk8imtlstZu\nEunvApDewXNUpqy1QBogJ2YgjwKBgQDhQcnKGB416mV3YujqqyjSXnwSvwyDCrbo\n4ZWZVpXje
33aXjrJ65nwzEFcufC7SwFAnku5V/vHOCecHHCRgBwZSo+8TTcOlZ\nnF0uC1n82WYUM08wE9cVznEpmoKVUDgxFSfcfUs7pdflRyMCOSSlaLGCAEu/801M\n66HN1hF1fwKBgQDoCn5pkZjq/wJ1k
iedCmRQETtWOWLP7/hQVYt/tRRjlsHQIp\n4xjIDVOn9Ywfre39GUZF1NkSLtq7XDJ5j7nb+l3gpzkiq/ZAPBcISlHI0NHRVAYV\ny86M2dh0d/x7iRAvX0fu45H1e/5VDJ2ALdZTLPJkRV65ZxY5c
a+c+IdwKBgQCI\n7/adThYd1KYEcvPHnW++m8PvnYccrsnNPz4zrqiGVWrxxgkQJK0FkoQvPFTCBlq8\n5CGzlLnooobSHfTIa+XVQ3p9VDkulSi22lDnKe11wi/FPI5b+u05lPvEX/LclJzk\nccj
IIO5VwdakOFGXoGuGOY9VcXg3xAz8pYaoPhPwKBgFwiPc0lcUowcNYKcLbp\nsvaFmDFVc4R49H7oidhx1n9NEncAonSssEmB7/cDRMHJOL8uJRcd2P9UavIswd9u\nlvWFcZdOn3FcgWsm0I0/sm0
nrzAe2EVZOotaySLPW3BPxU/9trEBUlVVZWIiNm\nsxerngW0FRhufH1dAVMuNd66\n-----END PRIVATE KEY-----\n
 lient.Client object at 0x7bcb45df81d0>
 nectado ao servidor 127.0.0.1:8888 a partir da porta 8904
  rver] Nova conexão de ('127.0.0.1', 8904)
```

```
aEUvzX1dmamjnmtl/+mGeKJt7nUPSsysi/MKX84Bzv38fraDM/FMWdz2ChIR85\nJiQkDIIAeDEWqS0QqlYr6DhJHyFC/VI/dHTGRIaRvaTu+Ijy1rrLk9Ua6sKngEw0\n9ERf3T0wciiIgLDu8KT5J
ddzteNksGO7i4shOrorVNUOZ0mJrWuMr0ZvXxaGLOW\nR4MfpSJ3StU+GTEl28nfHtG55YGfA5Tm5tbuSH2HoopElcCByR2Q78OooYsiuoO/\nr9RIxmWb53ERiHytau7Vw+AFCl6jEDMPQ5Lo+2cJS
[Cliente] Mensagem criptografada recebida: QSBti0R8IuG5azocErtGq3Lfvm3SNASgLHv/dzJ0WlnW0djvLp3D2dFG3JmKk0NuYohAV+P1qlVULDCuLrGlnHL22HVTVhIDoQ8cp2yRLXZN
dLUaFmwKYYB720hJKl18fH2nYwsGi07275FXaIiGPgisAImZVCTI0QSKK2pQvYfEXRb43BAnmtk66ZKDmxLisf/vYqVqiaqnJPRUeesI9Yy/RQR/geyMnRevQBmmrxmOKG1BNwYRVNuJD5Q7+/6zIsN
WghY13CtI9JxnALM22cWw5cmJhGmP/IuRD4fZOLtNIVaElWcAyM9omgjNuDEfcBzRrM3xk3HQVgJa25A==
[Cliente] Descriptografando mensagem com chave privada: b'---
                                                          --BEGIN PRIVATE KEY-----\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDBAPa1JiEqRzRN
2QM+wna1hoRS/NfV2ZqaOea2X/6YZ4om3udQ9KzKyL8wpfzgHO/fx+toMz8UxZ3P\nYKEhHzkmJCQMggB4MRapLRCqVivoOEkfIÜL9Uj90dMZEhpG9p074iPLWusuTl\overline{x}rq\nwqeATDT0RF/dM7ByKI.
AsO7wpPklV3j0142SwY7uLiyE6uitU1Q5nSYmta4yvRm9\nfFoYs5ZHgx+lIndK1T4ZMSXbyd8eØbnlgZ8DlObm1u5IfYeiikQhwIG9HZDvw6ih\niyK6g7+v1EjGZZvncRGIfK1q7tXD4AUKXqMQM
C97\nY9tf5sq4HoBHQKf7BBmcWOCBKvcK+EanStVrgPpgVq1a7SSU60ZErLpK69XVkAqF\nL97nm9jvHi50Lwxc9RpdlYol5GX9eXDX0EHkrCqB/9NXJg1Sf9PvqbvfdhgDtSS1\nKM+VH51WNmB7
0xWB6h/euH5KLqEgwoZBxL4aw+8vxYEi6X2cKss6KcMvu8i2qa\nH27FGA2jjnCXzXvwIRDLfQBn+gNE1yD9faO1IKpU/QKBgQDx8q5KxFLvbRF7IPIE\ncfygbMV8aFzCE4mYxSCvfzOKGwnwIemW
Cky0vm/oQIQme8Gtkv0B1Lm+kczhVLE\nFfs15LY0DV1BDMEjC/LHcCLru/k4UagTQGt3KabSTNylbCJ/gaXe4h95w8mL31YM\nnvj5lVnOs4IToMSJN250iffYdQKBgQDMNpKt8terVEhPwBbUtwYsl
GCBUQquEF/\n4XZ8WOzYvYeCFkOcb/1vH3pbFlky9yEn1fbWn4yZS10jRJePwE+If5/KPLHHOrwB\nodJR/hm1pVe/b2VPdYDuf+rz/u+j9ld79xpaBPqil0e1G5dSB//1y0f0ToDxWfkE\n1pEGH
ZQKBgQCv/Z3IJuxI2mZH0RwaHavsKZKxPtySEiIYPPPclEMyJx7gfFqE\nDe312T7vpDdzSfVzRXEULaug9daK5GTi2zZi6l2amUoHAjcOvic36RqNrKrIy6Td\ndBN3l2WQPXaWIYUqiGzWJldM5&
p0LWv8ocaTQgJccuhaWTshtSG7pbI7QKBgQCn\n4wnN1kL2iND2N67NbDa4N7e8NAYptNesgbh+XEFDovWfvhwRpYROciuObR4iJ0fr\nzx0ir4LQmDwHkyGjPfBk/r5mXmWtrBzanqYhYGzUiD101g
NNwYrjaCkvedX/fNl\naAsTDNj03Wps22UZPJhzaZuon02knlp6XshVpgRCfQKBgHdTuDNBT78+u/zTURdN\n9Mg0GPRMEf1PdhoPoG4sFLirHM+2spRcCtLGu0PY9Kv/S9p0Vi6xf0eqwfvc/QpJ\r
TPDG3fc+BD0x3HdGGUCX6f2ctdSKmSDMQv70NuNoyFbhmGRI8Th4jTdVBd1NKF1\nLxVjnMQaFn0LUzYeOyHF4nNX\n-----END PRIVATE KEY-----\n
SBti0R8IuG5azocErtGq3Lfvm3SNASgLHv/dzJ0WlnW0djvLp3D2dFG3JmKk0NuYohAV-P1qlVVLDCuLrGlnHL22HVTVhIDoQ8cp2yRLXzNqdLUaFmwKYYB720hJK118fH2nYwsGi07275FXaIiGPg
AImZVCTIØQSkK2pQvYfEXRb43BAnmtk662KDmxLisf/vYqVqiaqnJPRUeesI9Yy/RQR/geyMnRevQBmmrxmOKG1BNwYRVNuJD5Q7+/6zIsNcQWghY13Ct19JxnALM22cWw5cmJhGmP/IuRD4f2OLtN
aElWcAyM9omgjNuDEfcBzRrM3xk3HQVgJa25A==
Cliente] Mensagem descriptografada: teste
```

POSSÍVEIS CENÁRIOS

Entre os cenários mais comuns de uso do RSA está a transmissão segura de dados, como ocorre quando um cliente precisa enviar informações confidenciais a um servidor. Nesse caso, o cliente utiliza a chave pública do servidor para criptografar os dados, que só poderão ser descriptografados com a chave privada do servidor, garantindo que apenas o destinatário consiga acessar as informações.

Outro uso importante é na assinatura digital, utilizada para garantir a autenticidade e integridade de documentos e softwares. O emissor gera uma assinatura criptografando o hash do conteúdo com sua chave privada, e o receptor pode verificar a autenticidade usando a chave pública do emissor. Essa técnica é essencial, por exemplo, na distribuição de software confiável.