TP1Ex2

March 16, 2020

1 TP1 - 2)

Neste exercício temos como objetivo implementar o mesmo esquema do exercício anterior, mas agora com o uso de curvas elíticas substituindo: * A cifra simétrica por ChaCha20Poly1305 * Diffie–Hellman por Elliptic-curve Diffie–Hellman * Digital Signature Algorithm p Elliptic Curve Digital Signature Algorithm .

[1]:
```
import os
import time

from PipeCommunication import PipeCommunication

from cryptography.exceptions import *

from cryptography.hazmat.backends import default_backend

from cryptography.hazmat.primitives.asymmetric import ec
from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC
from cryptography.hazmat.primitives import hashes, hmac, serialization
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
```

[2]:
```
#print('Gerando os parâmetros para o Diffie-Hellman . . .')
#parameters_dh = dh.generate_parameters(generator=2,␣
 ↪key_size=1024,backend=default_backend())
#print(' . . . Parâmetros criados!')
#print('')
#print('Gerando agora os parâmetros para as assinaturas DSA . . .')
#parameters_dsa = dsa.
 ↪generate_parameters(key_size=1024,backend=default_backend())
#print(' . . . Parâmetros criados!')
```

[3]:
```
class ECDiffieHellman:
    def generate_ECDH_PrivateKey(self):
        private_key = ec.generate_private_key(ec.SECP384R1(),default_backend())
        return private_key

    def generate_ECDH_PublicKey(self, private_key):
```

```
        public_key = private_key.public_key()
        return public_key

    def generate_ECDH_PublicBytes(self, public_key):
        return public_key.public_bytes(
            encoding=serialization.Encoding.PEM,
            format=serialization.PublicFormat.SubjectPublicKeyInfo)
```

[21]:
```
class ECDSASignatures:
    def generate_ECDSA_PrivateKey(self):
        private_key = ec.generate_private_key(ec.SECP384R1(),default_backend())
        return private_key

    def generate_ECDSA_PublicKey(self,private_key):
        public_key = private_key.public_key()
        return public_key

    def generate_ECDSA_PublicBytes(self, public_key):
        return public_key.public_bytes(
            encoding=serialization.Encoding.PEM,
            format=serialization.PublicFormat.SubjectPublicKeyInfo)

    def sign_message(self, message,own_private_key):
        signature = own_private_key.sign(
            message,
            ec.ECDSA(hashes.SHA256())
        )
        return signature

    def verify_Signature(self, message, signature, other_public_key):
        other_public_key.verify(
            signature,
            message,
            ec.ECDSA(hashes.SHA256())
        )
```

[23]:
```
dsaSig = ECDSASignatures()

emitter_ecdsa_privateKey = dsaSig.generate_ECDSA_PrivateKey()
emitter_ecdsa_publicKey = dsaSig.
 ↪generate_ECDSA_PublicKey(emitter_ecdsa_privateKey)

receiver_ecdsa_privateKey = dsaSig.generate_ECDSA_PrivateKey()
receiver_ecdsa_publicKey = dsaSig.
 ↪generate_ECDSA_PublicKey(receiver_ecdsa_privateKey)
```

[24]:
```
class Encription:
    def kdf(self, password, mySalt=None):
        if mySalt is None:
            auxSalt = os.urandom(16)
        else:
            auxSalt = mySalt
        kdf = PBKDF2HMAC(
            algorithm = hashes.SHA256(),   # SHA256
            length=32,
            salt=auxSalt,
            iterations=100000,
            backend=default_backend()        # openssl
        )
        key = kdf.derive(password)
        if mySalt is None:
            return auxSalt, key
        else:
            return key

    def mac(self, key, msg, tag=None):
        h = hmac.HMAC(key,hashes.SHA256(),default_backend())
        h.update(msg)
        if tag is None:
            return h.finalize()
        h.verify(tag)

    def encript(self, Ckey, Hkey, msg):
        iv = os.urandom(16)
        cipher = Cipher(algorithms.AES(Ckey), modes.CTR(iv), default_backend())
        encryptor = cipher.encryptor()
        ciphertext = encryptor.update(msg) + encryptor.finalize()
        tag = self.mac(Hkey,ciphertext)
        return iv, ciphertext, tag

    def decript(self, Ckey, iv, msg):
            cipher = Cipher(algorithms.AES(Ckey), modes.CTR(iv),␣
↪default_backend())
            decryptor = cipher.decryptor()
            cleant = decryptor.update(msg) + decryptor.finalize()
            return cleant
```

[25]:
```
def Emitter_ECDH(conn):
    diffieHellman = ECDiffieHellman()
    dsaSign = ECDSASignatures()
    print('EmitterECDH: Iniciar Processo de DiffieHellman')

    emitter_ecdh_privateKey = diffieHellman.generate_ECDH_PrivateKey()
```

```
    #print('Emitter: Chave privada criada')
    emitter_ecdh_publicKey = diffieHellman.
↪generate_ECDH_PublicKey(emitter_ecdh_privateKey)
    #print('Emitter: Chave pública criada')
    print('EmitterDH: Enviando a minha chave pública')
    emitter_ecdh_public_bytes_key =diffieHellman.
↪generate_ECDH_PublicBytes(emitter_ecdh_publicKey)
    conn.send(emitter_ecdh_public_bytes_key)

    while True:
        print('EmitterDH: Esperando a chave pública do Receiver')
        pubkey = conn.recv()
        break
    while True:
        print('EmitterDH: Esperando a assinatura da chave pública')
        signature = conn.recv()
        break

    try:
        aux = emitter_ecdh_public_bytes_key + pubkey
        dsaSign.verify_Signature(aux,signature,receiver_ecdsa_publicKey)
        print('EmitterDH: Assinatura válida!')
        receiver_ecdh_public_key = pubkey
        print('EmitterDH: Já obtive a chave pública do Receiver')
        sign = dsaSign.sign_message(aux,emitter_ecdsa_privateKey)
        conn.send(sign)
    except(InvalidSignature):
        print('EmitterDH: Assinatura não válida! Conexão fechada!')

    while True:
        msg = conn.recv()
        break
    while True:
        sig = conn.recv()
        break
    try:
        dsaSign.verify_Signature(msg,sig,receiver_ecdsa_publicKey)
        print('EmitterDH: Assinatura válida!')

        emitter_ecdh_shared_key = emitter_ecdh_privateKey.exchange(ec.
↪ECDH(),serialization.load_pem_public_key(
            receiver_ecdh_public_key,
            backend = default_backend()))
        print('EmitterDH: Shared Key criada!')
        return emitter_ecdh_shared_key
    except(InvalidSignature):
        print('Emitter: Assinatura inválida! Conexão fechada!')
```

[26]:
```
def Receiver_ECDH(conn):
    diffieHellman = ECDiffieHellman()
    dsaSigns = ECDSASignatures()
    print('ReceiverDH: Iniciar Processo de DiffieHellman.')

    receiver_ecdh_privateKey = diffieHellman.generate_ECDH_PrivateKey()
    #print('Receiver: Chave privada criada.')
    receiver_ecdh_publicKey = diffieHellman.
↪generate_ECDH_PublicKey(receiver_ecdh_privateKey)
    #print('Receiver: Chave pública criada - - - ')
    receiver_ecdh_public_bytes_key = diffieHellman.
↪generate_ECDH_PublicBytes(receiver_ecdh_publicKey)

    #print('Receiver: Esperando chave pública do Emitter')
    while True:
        emitter_ecdh_public_key = conn.recv()
        #print('Receiver: Já obtive a chave pública do Emitter')
        #print(emitter_ecdh_public_key)
        break;

    publicKeys = emitter_ecdh_public_key + receiver_ecdh_public_bytes_key
    sign = dsaSigns.sign_message(publicKeys, receiver_ecdsa_privateKey)
    print('ReceiverDH: Enviando a minha chave pública')
    conn.send(receiver_ecdh_public_bytes_key)
    conn.send(sign)

    while True:
        ''' Esperando pela assinatura do emitter (ultimo passo do␣
↪Diffie-Hellman)'''
        msg = conn.recv()
        break;

    try:
        dsaSigns.verify_Signature(publicKeys,msg,emitter_ecdsa_publicKey)
        print('ReceiverDH: Assinatura válida!')
        print('\n\n Acordo Realizado!\n\n')
        msg = b'ACORDO REALIZADO!'
        sig = dsaSigns.sign_message(msg,receiver_ecdsa_privateKey)
        conn.send(msg)
        conn.send(sig)
    except:
        print('Receiver DH: Assinatura inválida')

    receiver_ecdh_shared_key = receiver_ecdh_privateKey.exchange(ec.
↪ECDH(),serialization.load_pem_public_key(
            emitter_ecdh_public_key,
            backend=default_backend()))
```

```
    print('ReceiverDH: Shared Key criada!')
    return receiver_ecdh_shared_key
```

[27]:
```
def Emitter(conn):
    shared_key = Emitter_ECDH(conn)
   # print('E: sharedKey- ' + str(shared_key))
    time.sleep(2)
    print('Emitter: Tenho o segredo partilhado.\n\n')

    encription = Encription()
    dsaSig = ECDSASignatures()

    text1 = b'Ola! Vamos enviar 4 mensagens(sendo esta a primeira) para o␣
↪Receiver!'
    text2 = b'Todas estas mensagens serao encriptadas. Sera ele capaz de as␣
↪desencriptar?'
    text3 = b'Cada criptograma sera autenticado com um HMAC e vai assinado com a␣
↪minha chave privada DSA'
    text4 = b'Se correr bem, todas estas 4 mensagens foram printadas!'
    text5 = b'Assinado: Emitter'
    text6 = b'PS: afinal foram 6'
    msgs=[text1,text2,text3,text4,text5,text6]

    i = 0
    while(i < 6):
        salt,key = encription.kdf(shared_key)
        Ckey = key[0:16]
        #print('E: Ckey- ' + str(Ckey))
        Hkey = key[16:32]
        #print('E: Hkey- ' + str(Hkey))
        iv,cipher_text, tag = encription.encript(Ckey,Hkey, msgs[i])
        sig = dsaSig.sign_message(cipher_text, emitter_ecdsa_privateKey)
        conn.send(salt)
        #print('E: SALT- ' + str(salt))
        conn.send(iv)
        #print('E: IV- ' + str(iv))
        conn.send(cipher_text)
        #print('E: MSG- ' + str(cipher_text))
        conn.send(tag)
        #print('E: TAG- ' + str(tag))
        conn.send(sig)
        #print('E: SIG- ' + str(sig))
        #time.sleep(2)
        i+=1
    print('ALL MESSAGES SENDED!')

    #conn.send(b'welelele')
```

[28]:
```
max_msg = 6
def Receiver(conn):
    sharedKey = Receiver_ECDH(conn)
    #print('R: sharedKey- ' + str(sharedKey))
    time.sleep(2)
    print('Receiver: Tenho o segredo partilhado.\n\n')
    encription = Encription()
    dsaSig = ECDSASignatures()
    i = 0
    while (i < max_msg):
        '''
        Esperemos sempre 5 mensagem por cada criptograma. Um com o salt, outra
↪com o iv, outra com a tag,
            outra com a assinatura e outra com a mensagem cifrada
        '''
        while True: #salt
            mySalt = conn.recv()
            #print('R: SALT- '+ str(mySalt))
            while True: #iv
                iv = conn.recv()
                #print('R: IV- '+str(iv))
                while True: #mensagem
                    msg = conn.recv()
                    #print('R: MSG- '+ str(msg))
                    while True: #tag
                        tag = conn.recv()
                        #print('R: TAG- ' + str(tag))
                        while True: #sign
                            sig = conn.recv()
                           # print('R: SIG- ' + str(sig))
                            break
                        break
                    break
                break
            break

        try:
            dsaSig.verify_Signature(msg, sig, emitter_ecdsa_publicKey)
            key = encription.kdf(sharedKey, mySalt)
            Ckey = key[0:16]
            Hkey = key[16:32]
            #print('R: CKEY- ' + str(Ckey))
            #print('R: HKEY- ' + str(Hkey))
            try:
                encription.mac(Hkey,msg,tag)
                plaintext = encription.decript(Ckey, iv, msg)
                print(plaintext)
```

```
            except(InvalidSignature):
                print('Tag inválida!')
        except(InvalidSignature):
            print('Assinatura inválida!')

        i += 1

    print('MAX MESSAGE REACHED')
```

[29]:
```
def main():
    PipeCommunication(Emitter,Receiver,timeout=600).run()
```

[30]:
```
main()
```

```
EmitterECDH: Iniciar Processo de DiffieHellman
ReceiverDH: Iniciar Processo de DiffieHellman.
EmitterDH: Enviando a minha chave pública
EmitterDH: Esperando a chave pública do Receiver
ReceiverDH: Enviando a minha chave pública
EmitterDH: Esperando a assinatura da chave pública
EmitterDH: Assinatura válida!
EmitterDH: Já obtive a chave pública do Receiver
ReceiverDH: Assinatura válida!


 Acordo Realizado!


EmitterDH: Assinatura válida!
ReceiverDH: Shared Key criada!
EmitterDH: Shared Key criada!
Receiver: Tenho o segredo partilhado.


Emitter: Tenho o segredo partilhado.


b'Ola! Vamos enviar 4 mensagens(sendo esta a primeira) para o Receiver!'
b'Todas estas mensagens serao encriptadas. Sera ele capaz de as desencriptar?'
b'Cada criptograma sera autenticado com um HMAC e vai assinado com a minha chave
privada DSA'
b'Se correr bem, todas estas 4 mensagens foram printadas!'
ALL MESSAGES SENDED!
b'Assinado: Emitter'
b'PS: afinal foram 6'
MAX MESSAGE REACHED
```

[ ]: