NAME; Pratheeshkumar.N
REG NO; 20BCI0195

Assignment-3:CryptographyAnalysisandImplementation

Objective: The objective of this assignment is to analyze cryptographic algorithmsand implementthem inapractical scenario.

Instructions:
Research:Beginbyconductingresearchondifferentcryptographicalgorithmssuchassymmetric key algorithms (e.g., AES, DES), asymmetric key algorithms (e.g., RSA,Elliptic Curve Cryptography), and hash functions (e.g., MD5, SHA-256). Understandtheirproperties,strengths,weaknesses,andcommonusecases.

Analysis: Choose three cryptographic algorithms (one symmetric, one asymmetric,and one hash function) and write a detailed analysis of each. Include the followingpoints inyouranalysis:

Brieflyexplainhowthealgorithmworks.
Discussthekeystrengthsandadvantagesofthealgorithm.Identifyanyknownvul
nerabilities orweaknesses.
Providereal-worldexamplesofwherethealgorithmiscommonlyused.

Implementation:
Select one of the cryptographic algorithms you analyzed and implement it in apractical scenario. You can choose any suitable programming language for theimplementation.
Clearly define the scenario or problem you aim to solve using cryptography.Provide step-by-step instructions on how you implemented the chosen algorithm.Includecodesnippetsandexplanationstodemonstratetheimplementation.
Testtheimplementationanddiscusstheresults.

SecurityAnalysis:
Performasecurityanalysisofyourimplementation,consideringpotentialattackvectors andcountermeasures.

Identify potential threats or vulnerabilities that could be exploited.Proposecountermeasuresorbestpracticestoenhancethesecurityofyourimple mentation.
Discussanylimitationsortrade-offsyouencounteredduringtheimplementationprocess.
Conclusion:Summarizeyourfindingsandprovideinsightsintotheimportanceofcryptography in cybersecurityand ethicalhacking.

SubmissionGuidelines:
Prepareawell-structuredreportthatincludestheanalysis,implementationsteps,codesnippets,and security analysis.
Useclearandconciselanguage,providingexplanationswherenecessary.Includeany references orsourcesused forresearch and analysis.
Compilealltherequiredfiles(report,codesnippets,etc.)intoasinglezipfileforsubmission.

Analysis:

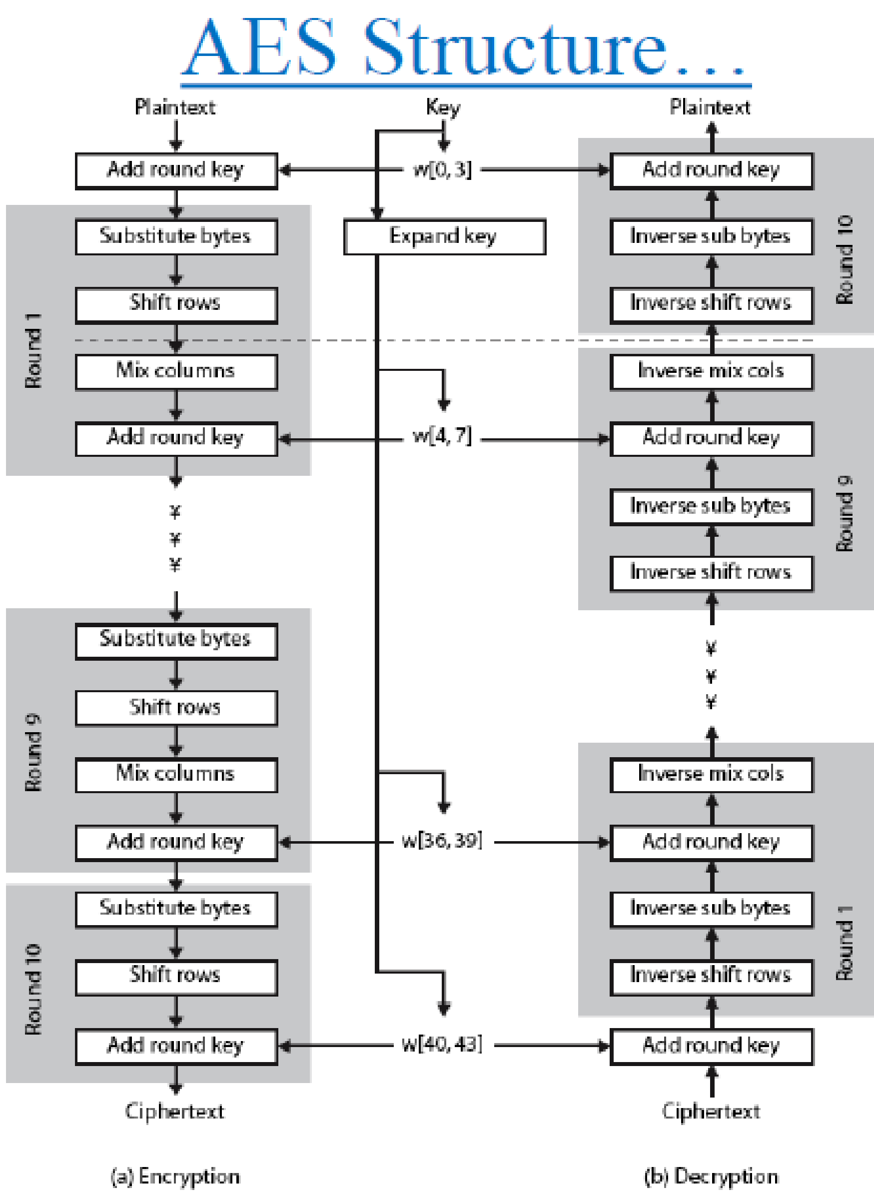
SymmetricAlgorithm:AES
TheAdvancedEncryptionStandard(AES)isasymmetricblockcipherchosenbythe U.S. government to protect classified information. AES is implemented in softwareandhardwarethroughouttheworldtoencryptsensitivedata.Itisessentialforgovernmentcomputersecurity,cybersecurityand electronicdataprotection.

HowAESencryptionworks:
AESincludesthreeblockciphers:

1.AES-128usesa128-bitkeylengthtoencryptanddecryptablockofmessages.2.AES-192 uses a 192-bit key length to encrypt and decrypt a block of messages.3.AES-256 uses a 256-bit key length to encrypt and decrypt a block of messages.Eachcipherencryptsanddecryptsdatainblocksof128bitsusingcryptographickeysof128,192and256bits,respectively.Symmetric,alsoknownassecretkey,ciphersusethesamekeyforencryptinganddecrypting.Thesenderandthereceivermustboth know--anduse--the samesecretkey.

Thegovernmentclassifiesinformationinthreecategories:Confidential,SecretorTopSecret. All key lengths can be used to protect the Confidential and Secret level. TopSecretinformationrequires either192-or256-bitkeylengths.

There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for256-bit keys. A round consists of several processing steps that include substitution,transposition and mixing of the input plaintext to transform it into the final output ofciphertext.



The AES encryption algorithm defines numerous transformations that are to beperformedondatastoredin anarray.Thefirststepofthecipheris toputthedatainto an array, after which the cipher transformations are repeated over multipleencryption rounds.

The first transformation in the AES encryption cipher is substitution of data using asubstitution table. The second transformation shifts data rows. The third mixescolumns. The last transformation is performed on each column using a different partoftheencryption key.Longerkeys needmoreroundsto complete.

StrengthsofAES:

AES data encryption is a more mathematically efficient and elegant cryptographicalgorithm,butitsmainstrengthrestsintheoptionforvariouskeylengths.AESallowsyou to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger thanthe56-bitkeyof DES.

BenefitsoradvantagesofAES

- As it is implemented in both hardware and software, it is most robust securityprotocol.
- It uses higher length key sizes such as 128, 192 and 256 bits for encryption.Henceit makes AESalgorithmmorerobust againsthacking.
- It is most common security protocol used for wide variety of applications suchas wireless communication, financial transactions, e-business, encrypted datastorageetc.
- It is one of the most widely used commercial and open source solutions acrosstheworld.
- Noonecanhackyourpersonalinformation.
- For128bit,about2128attemptsareneededtobreak.Thismakesitverydifficulttohackitasa resultitisverysafeprotocol.

DrawbacksordisadvantagesofAES

- Itusestoosimplealgebraicstructure.
- Everyblockis alwaysencryptedinthesameway.
- Hardtoimplementwithsoftware.
- AESincountermodeiscomplextoimplementinsoftwaretakingbothperformanceandsecurity intoconsiderations.

Weakness:

The biggest problem with AES symmetric key encryption is that you need to have awaytogetthekeytothepartywithwhomyouaresharingdata.Symmetricencryptionkeysareoftenencrypt edwithanasymmetricalgorithmlikeRSAandsentseparately.

Examples where AES technology is used: **VPN** Implementations. File transferprotocols (FTPS, HTTPS, SFTP, OFTP, AS2, WebDAVS) Wi-Fi security protocols(**WPA-PSK,WPA2-PSK**)

AsymmetricAlgorithm:ElGamalEncryption

ElGamal cryptosystem can be defined as the cryptography algorithm that uses thepublicandprivatekeyconceptstosecurecommunicationbetweentwosystems.Itcanbe considered the asymmetric algorithm where the encryption and decryption happenby using public and private keys. In order to encrypt the message, the public key isused by the client, while the message could be decrypted using the private key on theserver end. This is considered an efficient algorithm to perform encryption anddecryptionasthekeysareextremelytoughtopredict.Thesolepurposeofintroducingthemessagetrans action'ssignatureistoprotectitagainst**MITM**,whichthisalgorithmcould veryeffectivelyachieve.

ElGamalEncryptionAlgorithmwithExample

The ElGamal Encryption algorithm method's sole concept is to make it nearlyimpossible to calculate the encryption approach even if certain important informationis known to the attacker. It is mainly concerned about the difficulty of leveraging thecyclicgrouptofindthediscrete logarithm.

It will be very easy to understand, using a simple example. Suppose that even if thevalue like g^a and g^b are the values known to the attacker, the attacker will find itextremelydifficulttofindoutthevalueofg^abwhichisnothingbutthecrackedvalue.

Inordertounderstandtheentirescenario,weneedtogoinastepwisemanneronhowthe encryption and decryption of messages happen actually. We will be consideringthe example of two peers who are willing to exchange data in a secure manner byleveraging the ElGamal algorithm. Let's suppose user1 and user2 want to exchangetheinformationsecretly;inthat case,thefollowingprocedurewillbefollowed.

Step1:Generationofthepublicandprivatekeys.

Theuser1willtrytoselectaverylongorlargenumberx,andmeanwhile,hewillalsochoose a cyclic group Fx. From this cyclic group, he will be further choosing anothercomponent b and one more element c. The values will be selected in the manner thatifpassed through aparticularfunction,theoutcomewillbeequivalent to1.
Once the value selection phase is over, a value will be calculated that will be furtherused to generate the private key. By applying the formula fm=b^c, the value will becalculated. In the current scenario, user1 will select F, fm = b^c, a, b as their publickey, while the values of a will be saved as the private key, which will be further usedas theprivate key.

Step2:User2willencryptthedatausingthepublickeyofUser1.

In order to begin the encryption of the message, there are certain values that user2needs to pick. The user2 will also require to pick one of the values p from the cyclicgroup. The cyclic group will be the same as it was for the user1. The value should bepickedinamannersothatIncpasseswithaintheparticularfunctionwillgeneratetheoutcome1.
know the user2 will generate some other values that will be used to encrypt themessageusingthepublickey.ThevaluegenerateswillbePm=b^p.Theotherrevalueb^c will be equal to b^ap. The outcome of this computation will be multiplied to theother value Z in order to get closer to the encryption method. Eventually, the valuewillbesentusing theoutcomeof computations onb^p,Z*b^ap.

Step3:Decryptionofthemessageatuser1end.

The user1 will then use the computation of the values picked in the first and secondphase to identify the appropriate number, which will be used to decrypt the encryptedmessage. The User1 will be processing b^ap, and then the outcome will be used todivide the by Z in order to get the decrypted value. The decrypted value is somethingthat isthatwasencryptedinthesecondphase.

Intheabovescenario,theuser1hasinitiatedtheprocessbycalculatingtheprivateandpublic key, which is the algorithm's soul. The key is further used by user2 in thesecond stepinordertoencryptthe method.

The message is encrypted so that they value computed in that initial phase could beleveraged to decrypt the message. In the third step, it could be witnessed that afterdiving the entire value with the number that is computed in the third step itself totallydecrypts the message making it readable for the end-user. The same approach isfollowed everywhentheurge topass the messagesecurely occurs

AdvantageofElGamalalgorithm:

The advantage of the ElGamal algorithm is the generation of keys using discretelogarithms. Encryption and decryption techniques use a large computing process sothat theencryption resultsaretwicethe sizeoftheoriginal size.

DisadvantageofEl-Gamal

Themaindisadvantage ofEl-Gamalisheneedforrandomness,anditsslowerspeed(especiallyforsigning).Anotherpotentialdisadvantageofthe El-Gamalalgorithmisthatthemessageexpansionbyafactoroftwotakesplaceduringencryption.

Example: Alice chooses p**A** = 107, **A** = 2, d**A** = 67, and she computes **A** = 267 ≡94(mod107).Herpublickeyis(p**A**, **A**, **A**)=(2,67,94),andherprivatekeyisd**A** = 67. sends the encrypted message (28, 9) to Alice. −d**A** = 9·28 −67 ≡ 9·28106−67 ≡9·43 ≡66(mod107).

Hashfunction:MD5

MD5isacryptographichashfunctionalgorithmthattakesthemessageasinputofanylength and changes it into a fixed-length message of 16 bytes. MD5 algorithm standsfor the message-digest algorithm. MD5 was developed as an improvement of MD4,withadvancedsecuritypurposes.TheoutputofMD5(Digestsize)isalways128bits.MD5 wasdevelopedin1991 byRonaldRivest.

HowdoesMD5work?

MD5 runs entire files through a mathematical hashing algorithm to generate asignaturethatcanbematchedwithanoriginalfile.Thatway,areceivedfilecanbe authenticated as matching the original file that was sent, ensuring that theright filesgetwhere theyneedtogo.

The MD5 hashing algorithm converts data into a string of 32 characters. Forexample,theword"frog"alwaysgeneratesthishash:938c2cc0dcc05f2b68c4287040cfcf71.Similarly,afileof1.2GBalsogeneratesahashwiththesamenumberofcharacters.Whenyousendthatfiletosomeone,theircomputerauthenticatesitshashtoensureitmatchestheoneyousent.

Ifyouchange,justonebitinafile,nomatterhowlargethefileis,thehashoutputwill be completely and irreversibly changed. Nothing less than an exact copywillpassthe MD5test.

StrengthsofMD5:

MD5 (Message Digest Method 5) is a cryptographic hash algorithm used to generatea 128-bit digest from a string of any length. It represents the digests as 32 digithexadecimal numbers. Ronald Rivest designed this algorithm in 1991 to provide themeans for digitalsignature verification.

AdvantagesoftheMD5algorithm

- It'seasiertocompareandstoresmallerhashesusingMD5Algorithmsthanitistostore alarge variable-lengthtext.
- ByusingMD5,passwords arestoredin128-bit format.
- Youmaycheckforfilecorruptionbycomparingthehashvaluesbeforeandafter transmission. To prevent data corruption, file integrity tests are validoncethehashesmatch.

- AmessagedigestcaneasilybecreatedfromanoriginalmessageusingMD5.

DisadvantagesoftheMD5algorithm

- WhencomparedtootheralgorithmsliketheSHAalgorithm,MD5iscomparatively slow.
- Itispossibletoconstructthesamehashfunctionfortwodistinctinputsusing MD5.
- MD5islesssecurewhen comparedtotheSHA algorithmsinceMD5ismorevulnerable tocollisionattacks.

Real-WorldExampleofHashing: OnlinePasswords

Every time you attempt to log in to your email account, your email provider hashesthe password YOU enter and compares this hash to the hash it has saved. Only whenthetwohashes matchareyou authorizedtoaccessyouremail.

IMPLEMENTATIONS:

Aimandabstract:

Securityiseveryone'stopconcerninthemodernera.Everyoneusestheinternetthesedaysforavarietyofpurposes,includingdataandmoneytransfers.Therefore,webuilda cryptosystem that leverages the Discrete Logarithm Problem (DLP) for encryption,whichmakestheencryptionmethodmoresafe,inordertoincreasethesecurityofthecurrent system. It's known as Elgamal encryption. A public key cryptosystem is used.Both the encryption and decoding processes require asymmetric keys. The currentElgamalcryptosystemencryptsdatausingjustonekey.Thesedays,therearesomanyinstanceswhereunauthorisedclientsgetaccesstocrucialinformation.Inordertoaddanadditionallayerofsecuritytothesystem,wesuggestthattheElgamalCryptosystembemodifiedinthiswork.Withthisupdate,theuserisabletoencryptthemessagewithnumerous private keys. The text will be converted into integer values by an existingalgorithm,increasingthefilesizeby2*n.Bytranslatingtheintvaluestothecorresponding characters,wewereable toreducethe file size.

Keywords: Security,cryptosystem,DiscreteLogarithmProblem,encryption,Elgamal,privatekey

s.

ExistingMethod

ExistingElgamalencryptionconsistsofthreeparts.Theyarekeygeneration,encryptionand decryption.

1. Bobgeneratespublicandprivatekey:
   - Bob chooses averylargeprimenumberp.
   - Fromthep,hefindsg whichisthe primitive rootofp.
   - Thenhecomputesy= g^xmodp.
   - Bob publishes p, g and y as his public key and retains x

asprivatekey.

2. AliceencryptsdatausingBob'spublickey:
   - Aliceselects arandomintegerk<p.
   - Thenshecomputes c1=g^kmodp.
   - Shemultiplesy^{k}withMthatisconsiderasc2.
   - Thenshesends(c1,c2).

3. Bobdecryptsthemessage:
   - Bobcalculatess'=(c1x^{-}1)modp.
   - Thenhemultiplies c2bys'toobtain M.

PROPOSEDSYSTEM:

Existing algorithm uses discrete logarithmic problem it is very hard to crack the keyusing brute force attack. With modified and dedicated hardware, we can crack thekey. ButourgoalistodevelopanenhancedElgamalencryptionsystemwhichsystem is not crack easily. Existing encryption method is using integer as a ciphertext. But, in our proposed system we use character string as a cipher text so it reducethe file size. In this proposed algorithm it is impossible to break it via brute-forceattack.AndalsoCiphertextattackisnotpossiblesinceattackerhasnoideaaboutthekeys andlengthofthe message.

ModuleandDescription:

1- Keygeneration(Server):

- Choosearandomprimenumber(p)andchoosearandomprimitiveroot(g)of the prime number.

- Choosearandominteger(n)asthenumberofkeys (rounds)inourprivatekey
- Generate n random integers (xn) which will act as our private key, applyyn =gxmod pto each oftheintegers togenerateY (list ofintegers).
- Sendp,g,Y toclient which acts asourpublickey.

2- Encryption(Client):

- Choosenlength(Y)randomnumbers(kn)
- Compute Ykmod p using all numbers in Y and a and multiply themand storeinonevariablec and then compute c=cmod p.
- ComputealistA=gk modpusing all integersin akn
- Padthemessagewithcrandomcharactersinthebeginning andc/2intheend.
- Encrypt message by multiplying c with message and then convert themto charactersresulting inencrypted message B
- Send A,BtoServer.

3- Decryption(Server):

- ReceiveA,Bfrom client
- ComputecbyapplyingAxmodpon alltheintegersinAcorrespondstox thenmultiplythem togetherandmod themwith p.
- Beginprocessingmessagefrompositioncasthecharactersbeforeitare,justpadding andendthedecryptionatc/2.
- DividetheUnicodevalueofeachcharacterinthemessagebycandthen convertthem backto acharacter.
- Thisisourdecryptedmessage

ImplementationDetailsandAnalysis:

Weareimplementingthisusing**python**language.

elgamal.py

```
import
math,randomimport
string

primel=[]
for i in range(76432,652423):f=1
    for j in range(2,int(math.sqrt(i))+1):if
        i%j==0:
            f=0br
            eak
    if f:
        primel.append(i)

def primitive_root(p):if
    p == 2:
        return1
    p1=2
    p2 = (p-1) //
    p1while(1):
        g=random.randint(2,(p-1))
        ifnot(pow(g,(p-1)//p1,p)==1):
            if not pow(g, (p-1)//p2, p) ==
                1:returng

def genkey():p=primel[random.randint(0,len(primel)
    -1)]g =primitive_root(p)
    n = random.randint(4,9)b=[]
    B=[]
    whilelen(b)!=n:
```

```
        x = random.randint(2,p-2)ifx
        notinb:
            b.append(x)f
    oriin range(n):
        B.append(pow(g,b[i],p))ret
    urn [p,g,B,b]

defencrypt(z,n,p,g,B):a=[]
    while
        len(a)!=n:x=random.randint(
        2,p-2)if x notina:
            a.append(x)
    c=1A
    =[]
    foriin range(n):
        sec=pow(B[i],a[i],p)
        A.append(pow(g,a[i],p))c*=s
        ec
    c%=pif(c=
    =1):
        c=5while(c>2
    25):
        c=c//2
    mes=random.choices(string.ascii_letters+string.digits,k=c)for i inz:
        mes.append(i)
    mes+=random.choices(string.ascii_letters+string.digits,k=c//2)fori
    inrange(0,len(mes)):
        w=(c*ord(mes[i]))m
        es[i]=chr(w)
    return[A,''.join(mes)]

defdecrypt(n,A,b,p,l):
    s=[];l2=[]
    fori
        inrange(n):l2.append(pow(A[i],
        b[i],p))
    c=1
    for i in
        l2:c*=i
```

```
    c%=pif(c=
    =1):
       c=5while(c>2
    55):
       c=c//2
    s=""
    ll=len(l)-c//2
    for        i        in
       range(c,ll):w=(or
       d(l[i])//c)s+=chr
       (w)
    returns
```

Bob.py

```
import socketimport
stringimport
randomimport math
as mimportpickle
fromelgamalimport


cs=socket.socket(socket.AF_INET,socket.SOCK_STREAM)host
=socket.gethostname()
port =
12345cs.connect((host,port))w
hileTrue:
    k =genkey()
    recv = cs.recv(10000)serverkey
    = pickle.loads(recv)key =
    pickle.dumps(k[0:3])cs.send(key)
    # key exchange
    doneprint("\nEnter message:
    ")mes =input()
    x =
    encrypt(mes,len(serverkey[2]),serverkey[0],serverkey[1],serverkey[2])encmes=pi
    ckle.dumps(x)
    cs.send(encmes)
```

```
    recv =
    cs.recv(10000)encmes=pickle.l
    oads(recv)
    print("\nEncryptedmessage:",encmes[1])
    decmes =
    decrypt(len(k[3]),encmes[0],k[3],k[0],encmes[1])print("\nDecrypt
    edmessage:",decmes)
```

Alice.py:

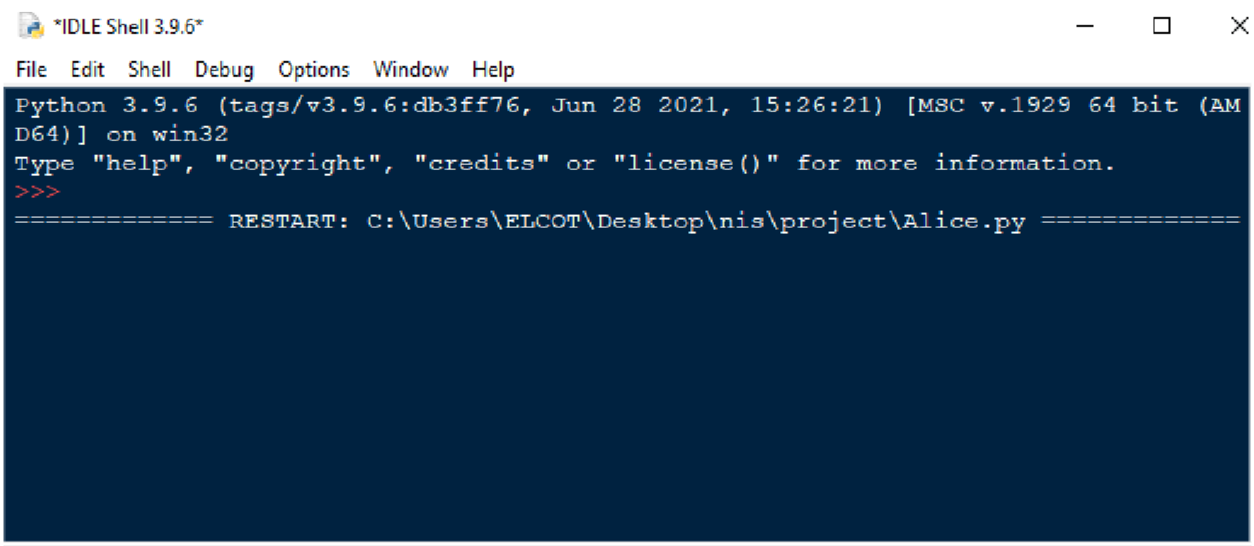
```
import socketimport
stringimport
randomimport math
as mimportpickle
fromelgamalimport*

ss=socket.socket(socket.AF_INET,socket.SOCK_STREAM)host
=socket.gethostname()
port =
12345ss.bind((host,port)
)ss.listen(1)c,addr=ss.a
ccept()whileTrue:
    k=genkey()key=pickle.dumps(
    k[0:3])c.send(key)recv=c.recv
    (10000)
    clientkey=pickle.loads(recv)#key
    exchangedone
    recv =
    c.recv(10000)encmes=pickle.loads(recv)print
    ("\nEncrytedmessage:",encmes[1])
    decmes=decrypt(len(k[2]),encmes[0],k[3],k[0],encmes[1])print("\nDe
    cryptedmessage:",decmes)
```

```
print("\nEnter
message:")mes=input()
x=encrypt(mes,len(clientkey[2]),clientkey[0],clientkey[1],clientkey[2])encmes
=pickle.dumps(x)
c.send(encmes)
```

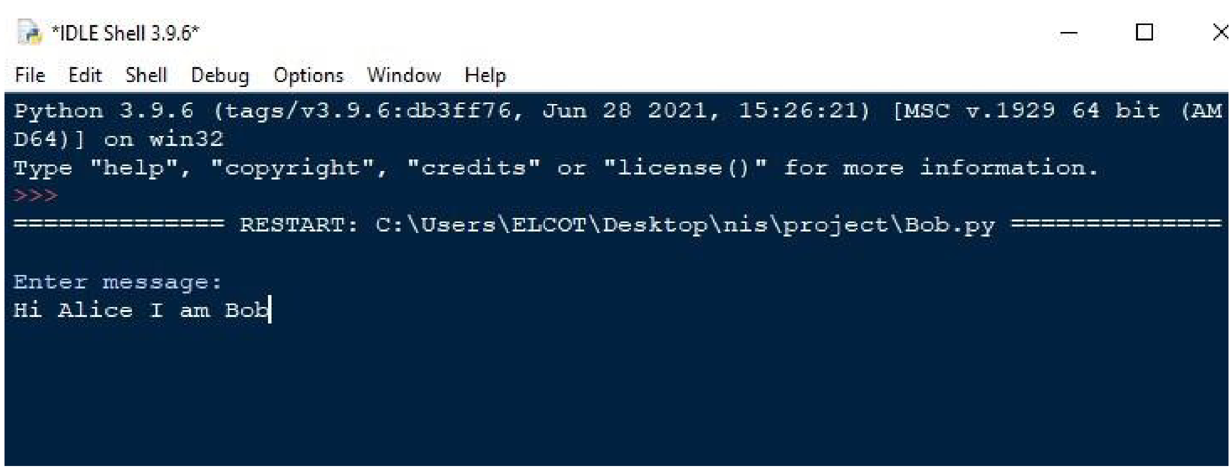
Output:

Alice.py:

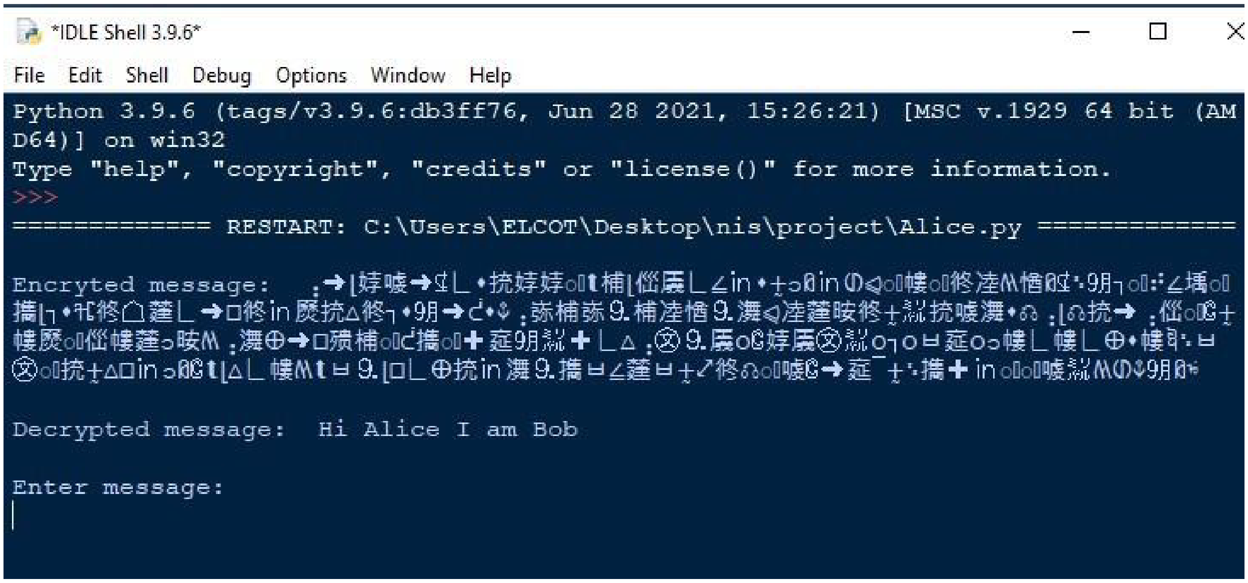


Bob.py:

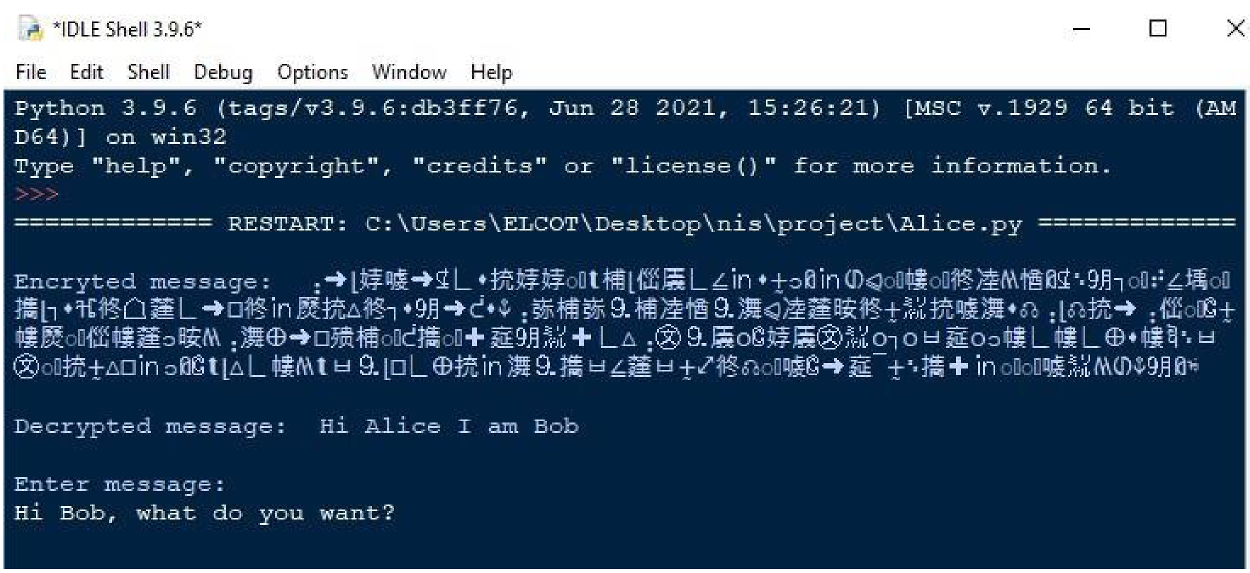
BobsendingmessagetoAlice:



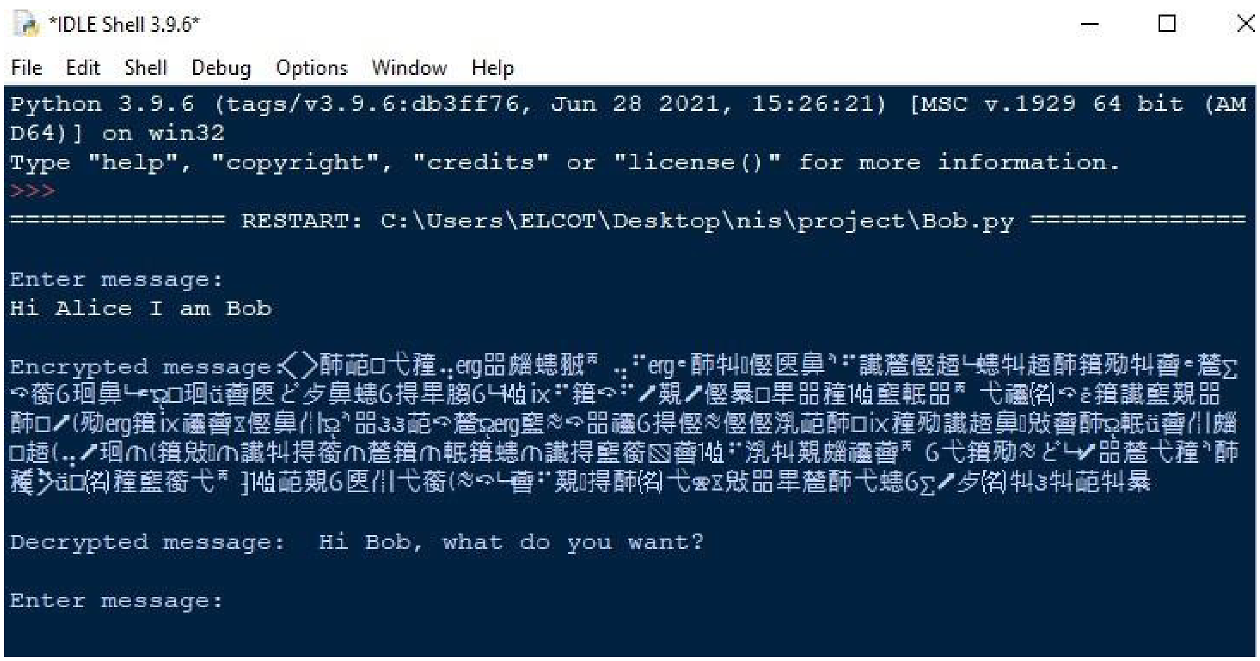
Encrypted&decrypted messagereceived byAlicefromBob:



Alicesending replytoBob:



BobreceivingreplyfromtheAlice:



SecurityAnalysis:

(In)securityofElGamalinOpenPGP

IBM cryptographers in Zurich report two new vulnerabilities they discovered inOpenPGP.Thevulnerabilitiesmakeemailseasilydecryptablebyanymathematically skilledhackerwithmodestresources.

IBM cryptographers in Zurich report two new vulnerabilities they discovered inOpenPGP.Thevulnerabilitiesmakeemailseasilydecryptablebyanymathematically skilledhackerwithmodestresources.

OpenPGP is a popular standard for end-to-end encrypted email, supported by manyemailapplicationsforbothPCsandmobiledevicesincludingOutlook,Thunderbirdand Apple Mail.Whilepopular,turnsoutthatitisalsoinsecure.

Limitations:

1. Itsneedforrandomness,anditsslowerspeed(especiallyforsigning).
2. The potential disadvantage of the ElGamal system is that message ex- pansionby a factor of two takes place during encryption(means the ciphertext is twice aslong astheplaintext.)

Conclusion:

Weobtainedanencryptedcyphertextversionofthecommunicationthatisdifficult for brute force attacks to crack. We safely exchange messages betweenthesender and receiver using our improved Elgamal technique. In the currentlyusedencryptionmethod, integersareusedascyphertext.However,thefilesizeis reduced in our suggested approach by using character strings as cypher text. Itis difficult to defeat this proposed method with a brute-force attack. Additionally,since the attacker is unaware of the message's length and encryption keys, acyphertextattackisnotfeasible.Therefore, comparedtotheElgamalalgorithm,it reducesoveralprocessingtimesduetothesecharacteristics.