|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Hope Foundation’s,**  **Finolex Academy of Management and Technology, Ratnagiri** | | | | | | | | | |
| **Department of Information Technology** | | | | | | | | | |
| Subject name: SECURITY LAB | | | | | | | | Subject Code: ITL502 | | | |
| Class | | TE IT | | Semester – V (CBCGS) | | | | Academic year: 2018-19 | | | |
| Name of Student | |  | | | | | **QUIZ Score :** | | | | |
| Roll No | |  | | | Experiment No. | | | | | 02 | |
| Title**:**  **Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA/El Gamal** | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. **Course objectives applicable:**   **LOB1**- To be able to analyze and implement public key algorithms like RSA and El Gamal | | | | | | | | | | | |
| 1. **Course outcomes applicable:**   **LO1**- Analyze and implement public key algorithms like RSA and El Gamal | | | | | | | | | | | |
| **3. Learning Objectives:**   * Understand how the RSA public key encryption algorithm works * Understand how the El Gamal public key encryption algorithm works * To be able to illustrate the above schemes using small numbers * To know about some implementation issues | | | | | | | | | | | |
| 1. **Practical applications of the assignment/experiment:**  * Whatsapp end-to-end encryption is implemented using asymmetric cryptography or public key systems. Recall, that in asymmetric encryption, when one key is used to encrypt (here, the public key), the other key is used to decrypt (here, the private key) the message. Once ‘Whatsapp’ is installed on a user’s smartphone, the public keys of ‘Whatsapp’ clients are registered with the Whatsapp server. It is important to note here that the private key is not stored on Whatsapp servers. * ElGamal cryptosystem, called Elliptic Curve Variant, is based on the Discrete Logarithm Problem. It derives the strength from the assumption that the discrete logarithms cannot be found in practical time frame for a given number, while the inverse operation of the power can be computed efficiently. | | | | | | | | | | | |
| **5. Prerequisites**: Understanding working of cryptosystem. | | | | | | | | | | | |
| **6. Hardware Requirements**:   1. PC with 4GB RAM, 500GB HDD.   **7. Software Requirements:**  1. Programming language C, C++, Java, Python | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **8. Quiz Questions (if any): (Online Exam will be taken separately batch wise, attach the certificate/ Marks obtained)**   1. What is Asymmetric Key cryptography? 2. What is Digital Signature? 3. Compare RSA and El-Gamal Schemes. | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **9. Experiment/Assignment Evaluation:** | | | | | | | | | | | |
| **Sr. No.** | **Parameters** | | | | | | | | **Marks obtained** | | **Out of** |
| **1** | Technical Understanding (Assessment may be done based on Q & A **or** any other relevant method.) Teacher should mention the other method used - | | | | | | | |  | | 6 |
| **2** | Neatness/presentation | | | | | | | |  | | 2 |
| **3** | Punctuality | | | | | | | |  | | 2 |
| **Date of performance (DOP)** | | |  | | | **Total marks obtained** | | |  | | **10** |
| **Date of checking (DOC)** | | |  | | | **Signature of teacher** | | | | | |

**Results:**

**SOURCE CODE:**

#Rivest Shamir Adleman

print("Select two prime numbers")

p=(int)(input())

q=(int)(input())

n=p\*q

pn=(p-1)\*(q-1)

print("Select e such that GCD(e,",pn,")=1\n")

e=(int)(input())

m=(int)(input("Enter plain text\n"))

for d in range(0,1000):

j=d\*e

j=j%pn

if(j==1):

print("d=",d)

break

c=(int)((pow(m,e))%n)

m=(int)((pow(c,d))%n)

print("Cipher text=",c)

print("Plain text=",m)

**OUTPUT:**

Select two prime numbers

3

11

('Select e such that GCD(e,', 20, ')=1\n')

7

Enter plain text

5

('d=', 3)

('Cipher text=', 14)

('Plain text=', 5)

**SOURCE CODE:**

#ElGamal Algorithm

print("Select a prime number")

p=(int)(input())

print("Enter primitive root of ",p,"\n")

e1=(int)(input())

print("Select private key d")

d=(int)(input())

e2=(int)(pow(e1,d)%p)

print("e2=",e2)

print("Select random integer r such as r<",p,"\n")

r=(int)(input())

print("Enter plain text")

pt=(int)(input())

c1=(int)(pow(e1,r)%p)

c2=(int)((pt\*pow(e2,r))%p)

c1=(int)(pow(c1,p-1-d))

pt=(c2\*c1)%p

print("c1=",c1,"\n")

print("c2=",c2,"\n")

print("Plain text=",pt,"\n")

**OUTPUT:**

Select a prime number

11

('Enter primitive root of ', 11, '\n')

2

Select private key d

3

('e2=', 8)

('Select random integer r such as r<', 11, '\n')

4

Enter plain text

7

('c1=', 78125, '\n')

('c2=', 6, '\n')

('Plain text=', 7, '\n')

**References** :

1. Build your own Security Lab, Michael Gregg, Wiley India.

2. CCNA Security, Study Guide, TIm Boyles, Sybex.