GRIFFITH COLLEGE DUBLIN

Tutorial Cover Sheet

Student name:	BANDARU KIRAN SUBRAHAMANYA SAI
Student number:	3178784
Faculty:	Computing Science
Course:	Computing Science **Stage/year:** 1/1
Subject:	Information Security
Study Mode:	Full time **yes** *Part-time*
Lecturer Name:	Sheresh Zahoor
Assignment Title:	Tutorial 02
No. of pages:	06
Disk included?	Yes *No*
Additional Information:	(ie. number of pieces submitted, size of assignment, A2, A3 etc)
Date due:	14/04/2025
Date submitted:	14/04/2025

Plagiarism disclaimer:

I understand that plagiarism is a serious offence and have read and understood the college policy on plagiarism. I also understand that I may receive a mark of zero if I have not identified and properly attributed sources which have been used, referred to, or have in any way influenced the preparation of this assignment, or if I have knowingly allowed others to plagiarise my work in this way.

I hereby certify that this assignment is my own work, based on my personal study and/or research, and that I have acknowledged all material and sources used in its preparation. I also certify that the assignment has not previously been submitted for assessment and that I have not copied in part or whole or otherwise plagiarised the work of anyone else, including other students.

Signed: _ B.kiransai___ Date: 13/04/2025_

Please note: Students **MUST** retain a hard / soft copy of **ALL** assignments

1.Explain how to generate a pair of RSA encryption keys given two prime numbers, p = 11 and q = 3.

Sol :

RSA :

One popular asymmetric or public-key cryptography technique is Rivest Shamir Adleman (RSA). It uses a private key pair for encryption and decryption to safeguard sensitive data. Steps to be followed for RSA Generation:

Steps to be followed for RSA Generation:

Steps 1: Key Generation

Given

1. p = 11, q = 3.

2. Calculate n = p * q

= 11 * 3

= 33

3. Calculate $\Phi(n) = (p -1)(q -1)$

$\Phi(n) = (11 -1)(3 -1)$

$\Phi(n) = (10)*(2)$

$\Phi(n) = 20$

Select integer e $gcd(\Phi(n),e) =1; 1< e <\Phi(n)$

$1< e < 20$

And $1< e < 20$ should be $gcd(\Phi(n),e) =1$

Gcd(3,20)=1

e = 3

4. Calculate d

$d = e -1 \bmod \Phi(n)$

de = mod $\Phi(n)$

$de \bmod \Phi(n) = 1$

$d(3) \bmod 20 = 1$

$7 * 3 \bmod 20 = 1$

$21 \bmod 20 = 1$

d = 7

5. Public Key KU = {e,n}
{e,n} = (3, 33)

6. private key KR = {d,n}

{d,n} = (7, 33)

2. Find out the secret key that Alice and Bob will share using the Diffie-Hellman key exchange when they start with: g=7 and n = 11. Alice generates a=3 and Bob generates b= 5 as their initial secret prime numbers.

Sol:

The following values are used to determine the secret key that Alice and Bob will exchange via the Diffie-Hellman key exchange:

- g = 7
- n=11
- Alice generated secret key : a = 3
- Bob generated secret key : b = 5

Step 1: Public Parameters:

- A large prime number n=11.
- A base g=7(primitive root modulo n).

These values can be seen and used by anyone

Step 2: Alice Computes Her Public Key

- Alice's private (secret) number is a=3

- She computes her public value:

$A = g^a \ mod\ n$

$A = 7^3 \ mod\ 11$

$= 343 \bmod 11$

$= 2$

Alice sends: A = 2

Step 3: Bob Computes His Public Key

- Bob's private (secret) number is b=5
- He computes his public value

$B = g^b \ mod \ n$

$B = 7^5 \ mod \ 11$

=16807 mod 11

=10

Bob sends: B= 10

Step 4: Both Parties Exchange Public Values

- Alice receives B=10
- Bob receives A=2

Step 5: Shared Secret Calculation

Alice Computes: $s = B^a \bmod n$

$= 10^3 \bmod 11$

$= 1000 \bmod 11$

$= 10$

Bod Computes: $s = A^b \bmod n$

$= 2^5 \bmod 11$

$= 32 \bmod 11$

$= 10$

Both compute the same shared secret key: 10

Final **Shared secret key = 10**

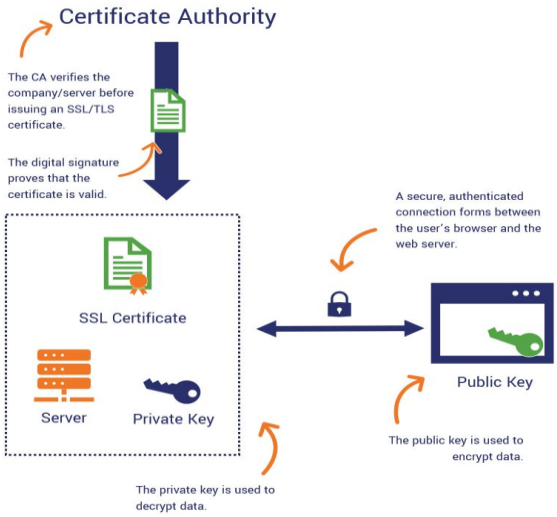
This secret key can now be used to encrypt further communication between Alice and Bob - and **no one else can compute it**, even if they know g, n, A, B because the private values a and b are never shared.

3.With the help of a diagram, describe in detail how a Certification Authority can be used to provide a secure communication

Sol:

Secure Communication Using a Certification Authority (CA)

A Certification Authority (CA) is a trustworthy organization that issues digital certificates and verifies identities to help guarantee safe and secure connection between users, websites, and services. With the use of these certificates, consumers can be sure they are speaking with the right person.



The above figure shows how a Certificate Authority (CA) uses SSL/TLS encryption to allow safe communication between a user's browser and a web server.

1. Identity Verification and Certificate Issuance

- **Verification Process**: The CA confirms the identity of the applicant when a website or organization requests a digital certificate. Verifying domain ownership, corporate information, and other credentials may be part of this.
- **Certificate Issuance**: A digital certificate with the entity's public key and identifying details is issued by the CA following a successful verification. The CA digitally signs the certificate, giving clients confidence in its legitimacy.

2. Installation of SSL/TLS Certificate on the Server

- The web server of the company has the issued certificate installed.
- This certificate, which uses protocols like HTTPS to create secure connections with clients, contains the public key of the server.

3. Establishing a Secure Connection

- **Client Request**: When a user visits the page on the website, their browser asks for the digital certificate from the server.
- **Certificate Validation**: In order to make sure the certificate is signed by a reliable CA and hasn't expired or been revoked, the browser verifies its authenticity.
- **Session Key Exchange**: In order to create a shared session key, the browser and server must first handshake if the certificate is genuine. Usually, the server's public key is used to safely communicate this data.
- **Encrypted Communication**: All data sent between the browser and server is encrypted after the session key is created, guaranteeing security and privacy.

4. Role of Public and Private Keys

- **Public Key**: Included in the server's certificate, it is used by clients to encrypt data sent to the server.
- **Private Key**: Securely stored on the server, it is used to decrypt data received from clients.
- This asymmetric encryption ensures that even if data is intercepted during transmission, it cannot be read without the private key.

5. Ensuring Trust and Security

- **Authentication**: Clients can communicate with the authentic server with confidence thanks to the CA's signature on the certificate.
- **Data Integrity**: Digital certificates aid in preventing data manipulation while it is being transmitted.
- **Confidentiality**: Sensitive data transferred between clients and servers remains protected from unauthorized entry using encryption.

Why Certificate Authorities Are Important

- They assist users with determining the legitimacy and dependability of a website.
- They ensure that all user and website data is securely encrypted.
- They prevent hackers from altering or stealing data while it is being transmitted.
- By making websites safe (HTTPS), they contribute to the development of online trust.

4. What is a public key certificate? And what information does it contain?

Sol :

Public Key Certificate:

It is also called as Digital Certificate**.** A digital document known as a public key certificate confirms that the sender of information sent online has the right to distribute that information. In essence, a public key certificate links a key holder to a particular entity using sophisticated cryptography.

An **SSL** (secure sockets layer) certificate is the most well recognized kind of public key certificate. These have grown in importance and prevalence to guarantee user and e-commerce security and are used to verify the legitimacy of a website. If you have ever been notified that a website is "unsafe," it was probably due to an SSL certificate issue.

A certificate authority, a neutral third party that will validate the credentials for the public key certificate, is required for anyone who wants to obtain one for a particular entity or organization.

What's in a Public Key Certificate

A public key certificate has a lot of information that may be used to confirm the legitimacy of the user and the transaction that follows. A public key certificate could include the following elements:

- **Issuer Name -** One of the most important parts of the public key certificate is the issuer name, which attests to the fact that it was issued by a legitimate certificate authority.
- **Certificate Validity Information -** Public key certificates have a temporal limit on their issuance. The certificate has a validity period and may expire if it is not renewed in a timely manner. It will provide information on when the certificate was acquired and when it will expire, according to the public key certificate.
- **Serial Number of the Certificate -** A distinct serial number is assigned to each public key certificate, and this number is shown on the certificate. This certificate's serial number serves as authentication and evidence that it was acquired from a reliable third-party certificate authority.
- **Identity Name -** This is the name of the person, group, or website that made the public certificate request.
- **Public Key Information -** Information about the public key that was acquired by the designated person or entity is contained in the public key information.
- **Algorithm Data -** The certificate is signed and validated by the certificate authorities using sophisticated procedures. The public key certificate contains the algorithm information.

Purpose of Public key certificate :

- Authenticate the certificate holder's identity.
- enables digital signatures and safe encryption.
- Helps in establishing trust between strangers online.