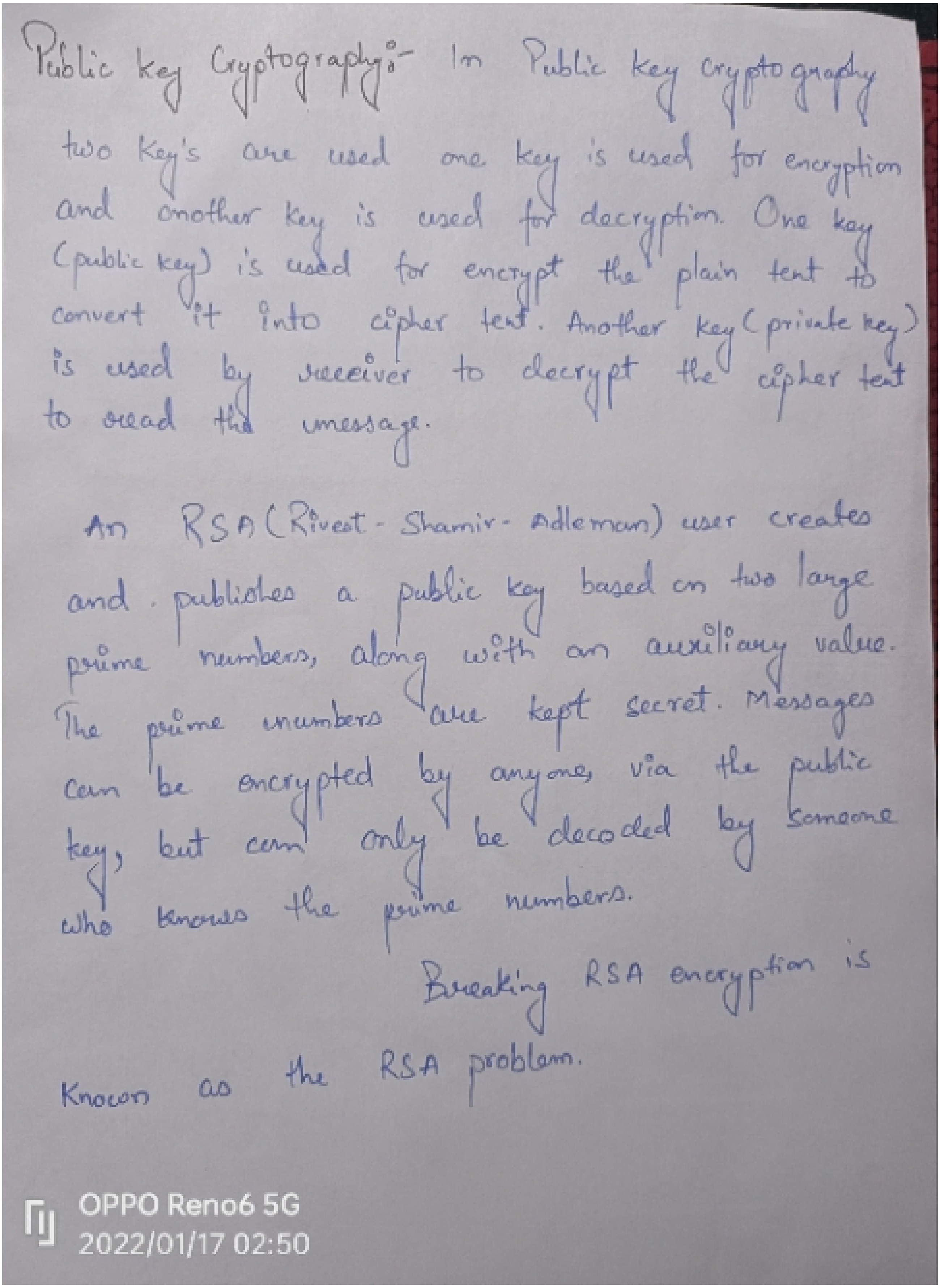
1 What is cryptography. Explain the details about Public Key Cryptography and private key cryptography? How RSA public key cryptography work.

Cryptography is a technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "Crypt" means "hidden" and suffix 'graphy' means "writing"

Private Key Cryptography :- In Private key cryptography, the same key (secret key) is used for encryption and decryption. In this key is symmetric because the only key is copy or share by another party to decrypt the cipher text. It is faster than the public key cryptography.



Public key Cryptography:- In Public key cryptography two key's are used one key is used for encryption and another key is used for decryption. One key (public key) is used for encrypt the plain text to convert it into cipher text. Another key (private key) is used by receiver to decrypt the cipher text to read the message.

An RSA (Rivest - Shamir - Adleman) user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

Breaking RSA encryption is Known as the RSA problem.

2. Define Hash Function and explain the working of Digital Signature Hash function and also write the difference between hash function and digital signature.

A hash function in cryptography is a unique identifier for any given piece of content. It's also a process that takes plaintext data of any size and converts it into a unique ciphertext of a specified length.

A digital signature is a cryptographic mechanism used to verify the authenticity and Integrity of digital data. We may consider it as a digital version of the ordinary handwritten signatures, but with higher levels of complexity and security.

WORKING OF DIGITAL SIGNATURE

In the content of cryptocurrencies, a digital signature system often consists of three basic steps: hashing, signing & verifying.

- Hashing the data:- The first step is to hash the message or digital data. This is done by submitting the data through a hashing algorithm so that a hash value is generated. The messages can vary significantly in size, but when they are hashed, all their hash values have the same length. This is the most basic property of hash function.

Signing:- After the information is hashed, the sender of the message needs to sign it. This is the movement where public-key cryptography comes into play. There are several types of digital signature algorythims, each with its own particular mechanism. But essentially, the hashed message will be signed with a private key, and the receiver of the message can then check its validity by using the corresponding public key

The major difference between hash function & digital Signature is:-

A hash is used to only verify the message Integrity. If a message changes, the hash of a message will also change.

A digital signature is used to gurantee that a Known source generated the message and that the message was not altered in transit.

3 Explain Public key distribution and its type.

In cryptography, it is a very tedious task to distribute the public and private keys between sender and receiver. If there Key is Known to the third party then the whole security mechanism becomes worthless. So, there comes the need to secure the exchange of keys.

There are two aspects of key Management.

→ Distribution of public keys.

→ Use of public-Key encription to distribute secrets.

DISTRIBUTION OF PUBLIC KEY

The public key can be distributed in four ways.

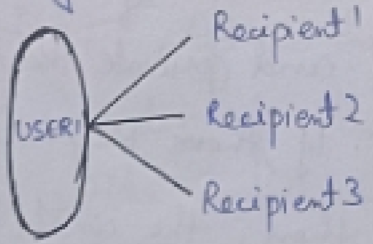
→ Public announcement

→ Public available directory

→ Public - Key authority

→ Public - Key certificates.

1 Public Announcement — Here the public key is broadcasted to everyone. The major weakness of this method is a forgery. Anyone can create a key claiming to be someone else and broadcast it.



Public Key Announcement

2 Public Available Directory:- Here the public key is stored in a public directory. Directories are trusted here, with properties like Participant Registration, access and allow to modify values at any time, contains entries like {name, public-key}. Diretories can be accessed electronically still vulnerable to

3 Public key Authority:- It is similar to the directory but, improves security by tightening control over the distribution of keys from the directory. It requires users to know the public key for the directory. Whenever the keys are needed, real-time access to the directory is made by the user to obtain any desired public key.

4 Public Certification:- This time authority provides a certificate to allow key enchange without real-time access to the public authority each time. The certificate is accompanied by some other info such as period of validity, rights of use, etc. All of this content is signed by the private key of the certificate authority and it can be verified by anyone possesing the authority's public key.

4. What is Real world protocol. Describe its type with the help of their working protocol.

A cryptographic protocol is a procedure carried out between two parties which is used to perform some security task. We need to discuss several widely used real world security protocols. Next, we look at real protocols.

IPSec (IP Security) - security at IP level

TLS - provide privacy and integrity.

SSH - A simple and useful security protocol

Kerberos - Symmetric key, single sign on. etc.

Each has advantages and disadvantages, many of them overlap somewhat in functionality, but tends to be used in different areas.

→ IPSec The IP security is an Internet Engineering Task Force standard suite of protocols between two communication points across IP network that provide data authentication, integrity, confidentiality.

→ Transport Layer Security- TLS is a cryptographic protocol that provides end-to-end communications security over networks and its widely used for internet communication and online transactions. It is particularly useful for private and sensitive information such as passwords, credit card numbers, and personal correspondence. It prevents eavesdropping, tampering and message forgery.

→ Secure Shell Protocol:- The SSH protocol uses encryption to secure the connection between a client and a server. It makes possible for a client to open an interactive sessions on a remote machine to send commands or files over a secure channel.

5 What is the Similarity and difference about the Gmail security certificate and Transport layer certificate? Explain its working process. And also explain the applicatn.

TLS is developed from a previous encryption protocol called SSL, which was developed by Netscape. TLS version 1.0 actually began development as SSL version 3.1, but the name of the protocol was changed before publication in order to indicate that it was no longer associated with Netscape.

Working of SSL/TLS

These are the essential principles to grasp for understanding how SSL/TLS work.

- Secure communication begins with a TLS handshake, in which the two communicating parties open a secure connection & exchange the public key
- During the TLS handshake, the two parties generate session keys, and the sessions keys encrypt and decrypt all communications after the TLS handshake.
- Different session keys are used to encrypt communicati in each new session.
- TLS ensures that the party on the server side, or the website the user is interacting with, is actually who they claim to be
- TLS also ensures that the data has not been altered, since a message authentication code (MAC) is included with transmissions

E mail Security Certificate:- An email certificate is a digital file that is installed to your email application to enable secure email communication. These certificates are known by many names- email security certificates, email encryption certificate, S/MIME certificates, etc. S/MIME, which stands for "secure/multipurpose internet mail extension", is a certificate that allows users to digitally sign their email communications as well as encrypt the content and attachments included in them. Not only does this authenticate the identity of the sender to the recipient, but it also protects the integrity of the email data before it is transmitted across the Internet.

Why Email Signing SSL Certificate

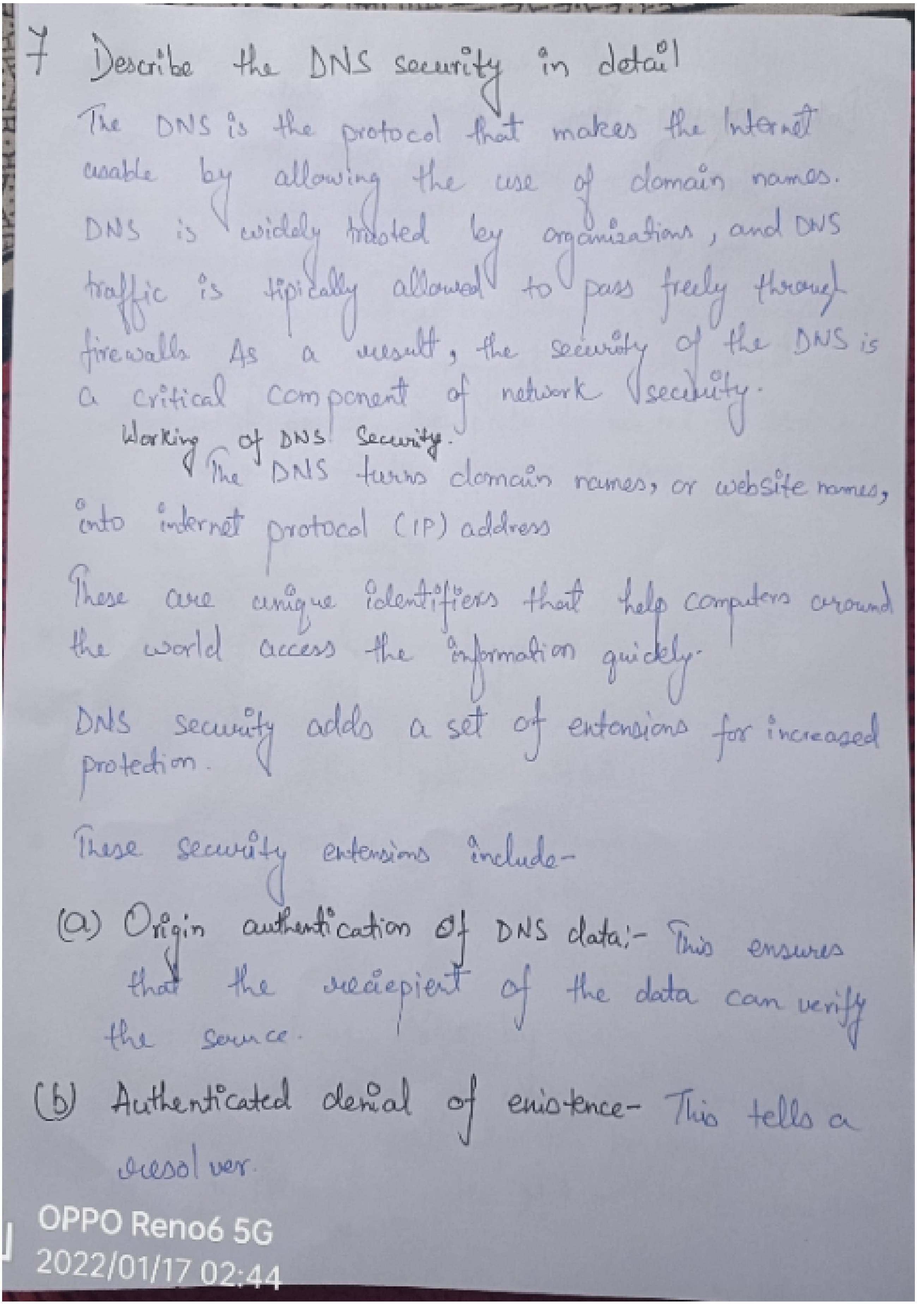
- Issued and Installed within minutes
- Compatible with every email clients and web browsers.
- Compatible with all mobile & desktop devices & OS.
- Available within minutes and easily accessible

6 Why IP security is necessary for our system.

The IP security is an Internet Engineering Task force (IETF) standards suits of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key enchange and key management are defined in it.

Uses of IP Security

- To encrypt application layer data
- To provide security for routers sending routing data across the public Internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual private Network (VPN) connection.



7 Describe the DNS security in detail

The DNS is the protocol that makes the Internet usable by allowing the use of domain names. DNS is widely trusted by organizations, and DNS traffic is tipically allowed to pass freely through firewalls As a result, the security of the DNS is a critical component of network security.

Working of DNS Security.

The DNS turns domain names, or website names, into internet protocol (IP) address

These are unique identifiers that help computers around the world access the information quickly.

DNS security adds a set of extensions for increased protection.

These security extensions include-

(a) Origin authentication of DNS data:- This ensures that the reciepient of the data can verify the source.

(b) Authenticated denial of existence- This tells a resolver.

Data Integrity:- This assures the data recipient that the data has not been changed in transit.