Explain about RSA? 2100031921

RSA is a type of asymmetric encryption, which uses two different but linked keys. In RSA cryptography, both the public and the private keys can encrypt a message.
The opposite key from the one used to encrypt a message is used to decrypt it. The primary function of RNA is to create proteins via translation.

RNA carries genetic information that is translated by ribosomes into various proteins necessary for cellular processes. mRNA, rRNA, and tRNA are the three main types of RNA involved in protein synthesis.
RSA private and public keys. An RSA key pair includes a private and a public key. The RSA private key is used to generate digital signatures,

and the RSA public key is used to verify digital signatures. The RSA public key is also used for key encryption of DES or AES DATA keys and

Explain about RSA? 2100031921

theRSA private key for key recovery.

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and the Private key is kept private.

An example of asymmetric cryptography:

A client (for example browser) sends its public key to the server and requests some data.
The server encrypts the data using the client's public key and sends the encrypted data.
The client receives this data and decrypts it.
Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the public key of the browser.

The ideal The idea of RSA is based on the fact that it is

Explain about RSA? 2100031921

key consists of two numbers where one number is a multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasible task.