RSA Encryption

Slide 3:

- Hi everyone, Today, I'm going to explain how the RSA keeps our information safe.
- RSA stands for Rivest-Shamir-Adleman, the inventors of this public-key cryptosystem. Developed in 1977, it's one of the oldest and most widely used encryption methods around.
- Public-key cryptography is like having a special lock. You give out the public key, like a keyhole, to anyone. But only you have the private key, like the right key, to unlock the message.

Slide 4:

- Let’s talk about how secure RSA is. As we saw, it relies on two keys: a public key and a private key.
- The security of the entire system depends on the difficulty of cracking the private key.
- A larger key size makes it much harder to crack the code. For instance, it can take trillions of years to crack a 2048-bit key.

Slide 5:

Encryption is like a secret code that keeps your important stuff safe from snoops. It's like putting your message in a locked box before sending it, so only the intended recipient with the right key can open it. This makes sure that nobody else can peek at your personal or business information when it's being sent over the internet. It works on all kinds of devices and makes communication between them super secure. So, encryption basically protects your data from eavesdroppers.

Slide 6:

Let's explore how RSA works.

Key Generation is the first step, where a pair of keys—one public and one private—are created. These keys are mathematically linked and essential for the encryption and decryption processes.

During the **Encryption Process**, the sender uses the recipient's public key to encrypt the message, ensuring that only the intended recipient can decrypt it.

Finally, in **Decryption Process** the recipient uses their private key to decrypt the message, making it readable. This ensures that communication remains secure and private.

Slide 7:

Let's break down the key generation process in RSA encryption into the following simple steps:

1.Prime Number Selection:

First, we choose two distinct prime numbers, p and q. These primes form the backbone of our encryption keys. For example, let's pick p = 61 and q = 53.

2. Modulus Calculation:

Next, we calculate the modulus n by multiplying our two primes:

$n=p\times q$ we get

$n=61\times53=3233$. This modulus n is a critical part of both the public and private keys.

3. Euler's Totient Function:

Now we calculate Euler's totient function,

$\phi(n)$, which helps in generating the keys. The formula is

$\phi(n)=(p-1)\times(q-1)$ this becomes

$\phi(3233)=(61-1)\times(53-1)=60\times52=3120$

Slide 8:

4. Public Key Exponent Selection: We need to choose a public exponent e. This number should be greater than 1 and less than $\phi(n)$, and it must be co-prime to $\phi(n)$. In other words, the greatest common divisor (GCD) of e and $\phi(n)$ should be 1. For our example, we select e=17, which is co-prime to 3120.

5. Private Key Exponent Calculation: Now, we need to calculate the private exponent d. This number is derived from the equation $e\times d\equiv1 \bmod \phi(n)$.

For our example: ……

So, we find that d=2753d=2753 is our private key exponent

Slide 11:

RSA encryption works by using prime numbers. It’s based on the idea of Prime Number Factorization, which means breaking a number down into the prime numbers that multiply together to make it.

The security of RSA comes from how hard it is to factorize a large number n back into its original primes, p and q. While multiplying the primes is easy, figuring out what primes were used to get n is extremely tough. This makes RSA a strong and secure method for encrypting data.

Slide 12:

Data Transmission: RSA keeps important information like bank details and private messages safe when you send them online.

Digital Signatures: RSA is also employed to create digital signatures, which verify the authenticity and integrity of messages and documents. By signing with their private key, senders authenticate the message's origin, while recipients use the sender's public key to verify the signature.

Secure Email: RSA plays a vital role in secure email communication. Protocols like PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extensions) use RSA to encrypt email content and verify digital signatures, ensuring both confidentiality and authenticity.

SSL/TLS Protocols: RSA helps make websites safe so you can browse and shop without worries.

Slide 13:

RSA encryption uses asymmetric keys to securely transmit data and verify digital signatures, making it fundamental to modern digital security. Its widespread adoption and compliance with regulatory standards highlight its critical role in safeguarding sensitive information across various platforms.

Or

RSA encryption stands as a cornerstone in modern cryptography, offering strong security for data transmission, digital signatures, and communications. Its math-based approach ensures confidentiality, integrity, and authenticity across industries, making it indispensable for safeguarding digital information in today's digital age.