CS101 (Discrete Mathematics)
Guided by :- Dr. Sudarshan Iyengar

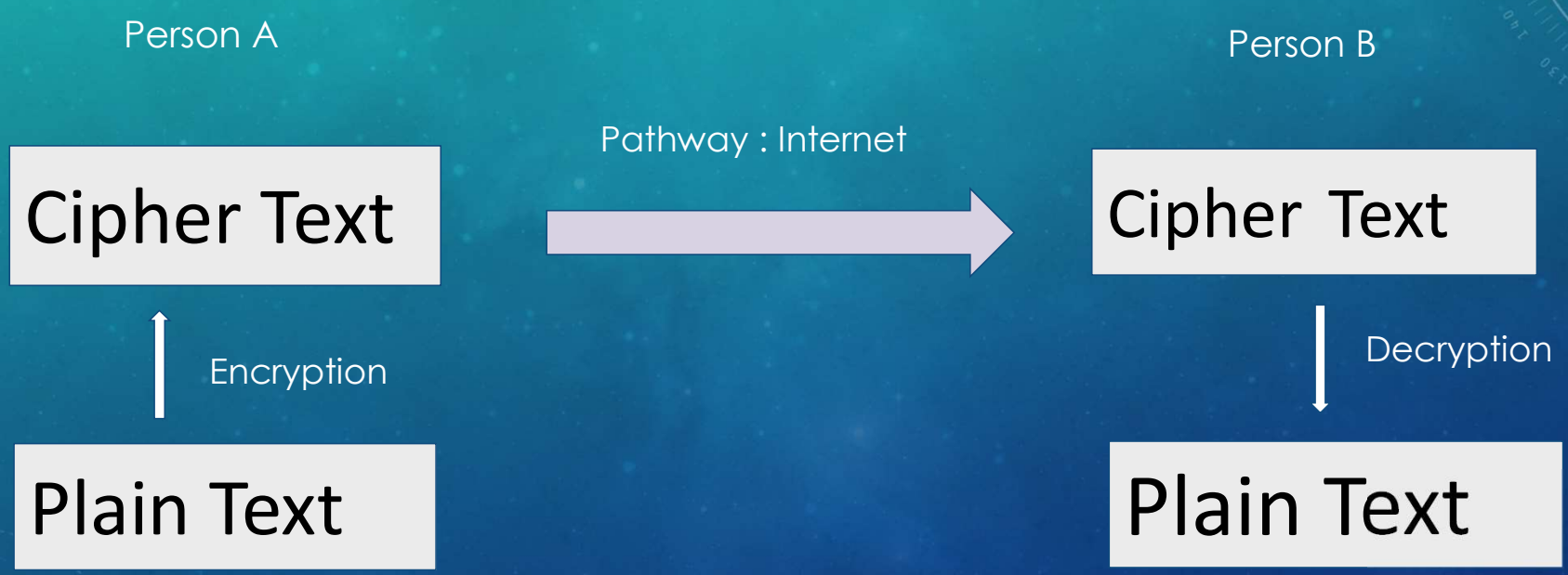
RSA ENCRYPTION AND ITS APPLICATIONS IN PRIVACY PROTECTION

MADE BY – 1. HARSH PATIDAR (2022MCB1265)
2. SHWETA MAURYA (2022MCB1281)
3. KESHAV BANSAL (2022MCB1268)
4. JIGISHA ARORA (2022MCB1267)

MOTIVATION FOR CRYPTOGRAPHY!!

- Why Cryptography ??
- How encrypting text is of our interest?
- How will we be doing it so ?

HOW CRYPTOGRAPHY WORKS?



SYMMETRIC KEY CRYPTOGRAPHY,

This uses a secret key for both encryption and decryption. Data is translated to a format that cannot be interpreted or inspected by someone who does not have the secret key used to encrypt it during this phase.

The strength of the random number generator used to generate the secret key determines the effectiveness of this method. Symmetric Key Cryptography, commonly used on the Internet today, comprises two kinds of algorithms: Block and Stream. The Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) are two common encryption algorithms. This type of encryption is typically much faster than Asymmetric Encryption, but it allows the secret key to be held by both the sender and the data receiver.

ADVANTAGES OF SYMMETRIC KEY CRYPTOGRAPHY,

Encrypted data can be transmitted over a network in Symmetric Cryptosystems even though it is certain that the data would be intercepted. Since no key is sent with the files, the chances of data decryption are zero.

A message can only be decrypted by a device that has a hidden key.

This type of encryption is simple to implement. All users need to do is specify and exchange the secret key until they can begin encrypting and decrypting messages.

Symmetric key encryption is much faster than asymmetric key encryption.

Uses fewer computer resources. As opposed to public-key encryption, single-key encryption needs fewer computing resources.

DISADVANTAGES OF SYMMETRIC KEY CRYPTOGRAPHY,

Key transportation is a concern in symmetric cryptosystems. The secret key must be sent to the receiving device before the final message is sent. Electronic communication is unreliable, and no one can guarantee the communication networks will not be tapped. As a result, the only safe method of sharing keys will be to do it in person.

The message's origin and validity cannot be assured. Messages cannot be proven to have originated from a specific person since both sender and recipient use the same key. If there is a disagreement, this may be a challenge.

For communication between each different party, a new shared key must be created. This poses a challenge with handling and securing both of these keys.

ASYMMETRIC KEY CRYPTOGRAPHY,

Asymmetric cryptography is a second form of cryptography. It is called a Public-key cryptography. There are two different keys including one key is used for encryption and only the other corresponding key should be used for decryption. There is no other key can decrypt the message and not even the initial key used for encryption. The style of the design is that every communicating party needs only a key pair for communicating with any number of other communicating parties.

ADVANTAGES OF ASYMMETRIC KEY CRYPTOGRAPHY,

There is no need to exchange keys in asymmetric or public key cryptography, eliminating the key distribution issue.

The main benefit of public-key cryptography is improved security: private keys are never exchanged or exposed to others.

Message verification is provided by public-key cryptography, which requires the use of digital signatures, which allows the receiver of a message to check that the message is actually from a specific sender.

The usage of digital signatures in public-key cryptography helps the recipient to determine whether or not the message was altered during transit. A digitally signed message cannot be altered without rendering the signature null.

DISADVANTAGES OF ASYMMETRIC KEY CRYPTOGRAPHY,

- It consumes more computer resources. It necessitates much more computing resources than single-key encryption.
- Authentication of public keys is recommended/required. No one can be certain that a public key corresponds to the individual it identifies, so everybody must verify that their public keys are theirs.
- A widespread security breach is likely if an intruder obtains a person's private key and reads his or her entire message.
- The loss of a private key can be irreversible. When a private key is lost, all incoming messages cannot be decrypted.

RSA ALGORITHM

RSA stands for Rivest Shamir Adleman . These are the scientist who had created this algorithm.

1. It is a asymmetric algorithm which works on two keys one is public and other is private key
2. Public key of receiver is used to encrypt the data
3. Private key of receiver is used to decrypt the data
4. It has mainly two components -

- Key generation
- Encryption and decryption function

LET US UNDERSTAND HOW THIS ALGORITHM ACTUALLY WORKS

1 . **Key Generation -**

1. Choose two large prime number p and q
2. Now compute n = p*q
3. Choose a number e where e is less than the (p-1)*(q-1) which is same as saying that choose a number which is less than the ϕ(n)
4. A number d is selected so that e*d mod n = 1

NOW WHAT WE GOT !

1. Public key (n,e) - for encryption
2. Private key (n,d) - for decryption

2 . ENCRYPTION AND DECRYPTION

Let us consider that our plaintext is g and then our encrypted cyphertext is c

1. c = g^e (mod n)
2. To decrypt the ciphertext c, we compute the plaintext g as
3. g = c^d (mod n)

we can use modular exponentiation algorithms to do this computation efficiently.

CONFUSED ! LET US TAKE AN EXAMPLE FOR BETTER UNDERSTANDING

For simplicity , let us take an example considering the small prime number

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < phi(n) . Let e = 7
- Compute a value for d such that (d * e) mod φ(n) = 1. One solution is d = 3

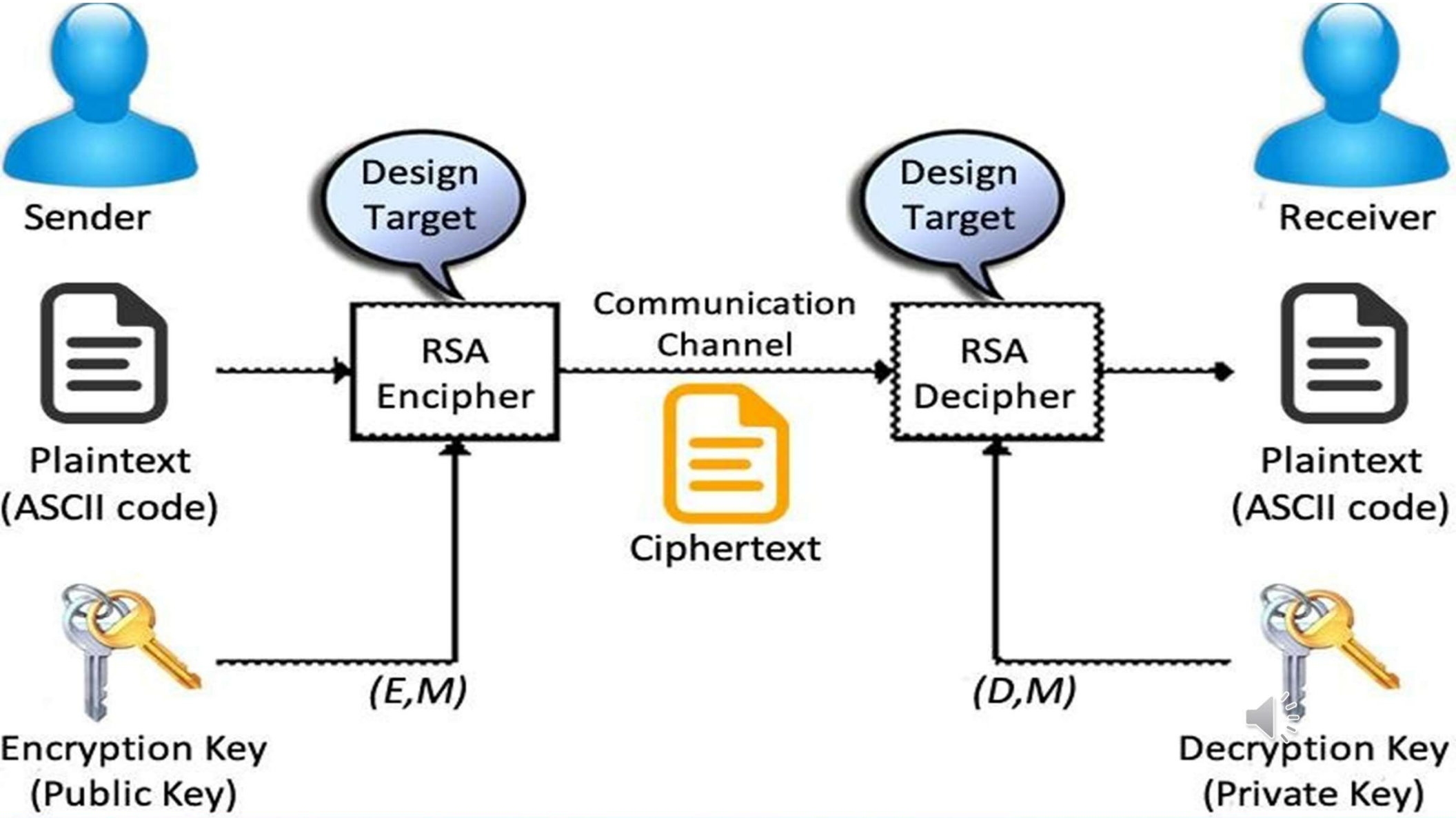
[(3 * 7) mod 20 = 1]

- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $g = 2$ is $c = 2^7 \bmod 33 = 29$
- The decryption of $c = 29$ is $g = 29^3 \bmod 33 = 2$
- So we are getting g which is our message which we need to encrypt

WHAT MAKES RSA A USEFUL ALGORITHM

1. The idea of RSA is based on the fact that it is difficult to factorize a large integer.
2. IT becomes more difficult when we have n which is the multiplication of two large prime number
3. p*q -> n { easy}
4. n -> p*q {difficult}

The crux of the security of RSA is that the attacker needs to first find out p and q by factorization of n which takes place in exponential time. Research shows that this can take more than 70 years if N is a 100 digit number. Due to this complexity, the attacker is unable to find the decryption key d because d depends on p, q and encryption key e. So even if n and e are known to the attacker, d cannot be computed.


Sender
Design Target
Design Target
Receiver
Plaintext (ASCII code)
RSA Encipher
Communication Channel
RSA Decipher
Plaintext (ASCII code)
Ciphertext
(E,M)
(D,M)
Encryption Key (Public Key)
Decryption Key (Private Key)

SOME IMPORTANT APPLICATIONS OF RSA ARE :

Digital signatures: RSA facilitates the creation of digital signatures, which are used to verify the authenticity and integrity of a message.

Secure email: RSA can be used for sending and receiving encrypted emails, which can prevent eavesdropping, spoofing, or phishing. RSA can also be used for signing emails, which can prove the sender's identity and prevent repudiation .

RSA APPLICATIONS (CONTD.)

Secure file transfer: RSA encryption can be employed to safeguard files being transferred between parties, ensuring that only the intended recipient can decrypt and access the files.

Software protection: RSA encryption can be used to make software tamper-proof. The publisher of the software encrypts the software using their private key, which is a secret key that only the publisher knows. This means that anyone who tries to copy or use the software without authorization will not be able to decrypt it.

SHORTCOMINGS OF RSA

1.Computational Complexity: RSA encryption and decryption operations require intensive computational calculations, especially for large key sizes. As a result, RSA can be slower compared to symmetric encryption algorithms, affecting performance in resource-constrained environments.

2.Key Management: RSA relies on the secure generation, storage, and exchange of key pairs. Managing and protecting these keys can be challenging, especially in large-scale systems or distributed environments. Key distribution can be particularly difficult, requiring secure channels for key exchange.

3.Key Size and Payload Limitation: The security of RSA is dependent on the size of the keys used. As computational power advances, larger key sizes are required to maintain the same level of security. This leads to larger ciphertexts and longer processing times. Transmitting and storing larger keys can be cumbersome and resource-intensive.

4.Lack of Perfect Forward Secrecy: RSA does not provide perfect forward secrecy. If an attacker compromises the private key, they can decrypt all past encrypted communications. This is in contrast to symmetric encryption algorithms like Diffie-Hellman or elliptic curve cryptography (ECC), which provide perfect forward secrecy.
5.Vulnerability to Certain Attacks: RSA can be vulnerable to specific attacks if not implemented correctly. These include chosen ciphertext attacks, padding oracle attacks, and side-channel attacks. Proper implementation, adherence to security guidelines, and employing suitable padding schemes are essential to mitigate these vulnerabilities.

6.Patent Issues (historical): In the past, RSA was subject to patent restrictions, limiting its usage and implementation. However, these patents have expired, and RSA can now be used freely.

7.Limited Use for Large Data: RSA is not well-suited for encrypting large amounts of data directly due to its payload limitation. To encrypt larger data sets, hybrid encryption schemes combining RSA with symmetric encryption algorithms are commonly used, which adds complexity and overhead.

While RSA remains widely used, it is important to consider these limitations and explore alternative cryptographic algorithms that may better align with specific requirements and security considerations.

CONCLUSION

In conclusion, the RSA encryption algorithm is a fundamental and widely used method for secure communication. It relies on the computational difficulty of factoring large prime numbers to provide robust encryption and decryption processes. RSA's key management and padding schemes enhance its security. However, the emergence of quantum computing poses a potential threat to RSA's security, necessitating ongoing research in post-quantum cryptography. Overall, RSA has played a vital role in ensuring secure communications, but it is crucial to adapt to emerging threats and embrace new cryptographic techniques for future security.

REFERENCES

1. ChatGpt
2. GeeksforGeeks
3. Wikipedia