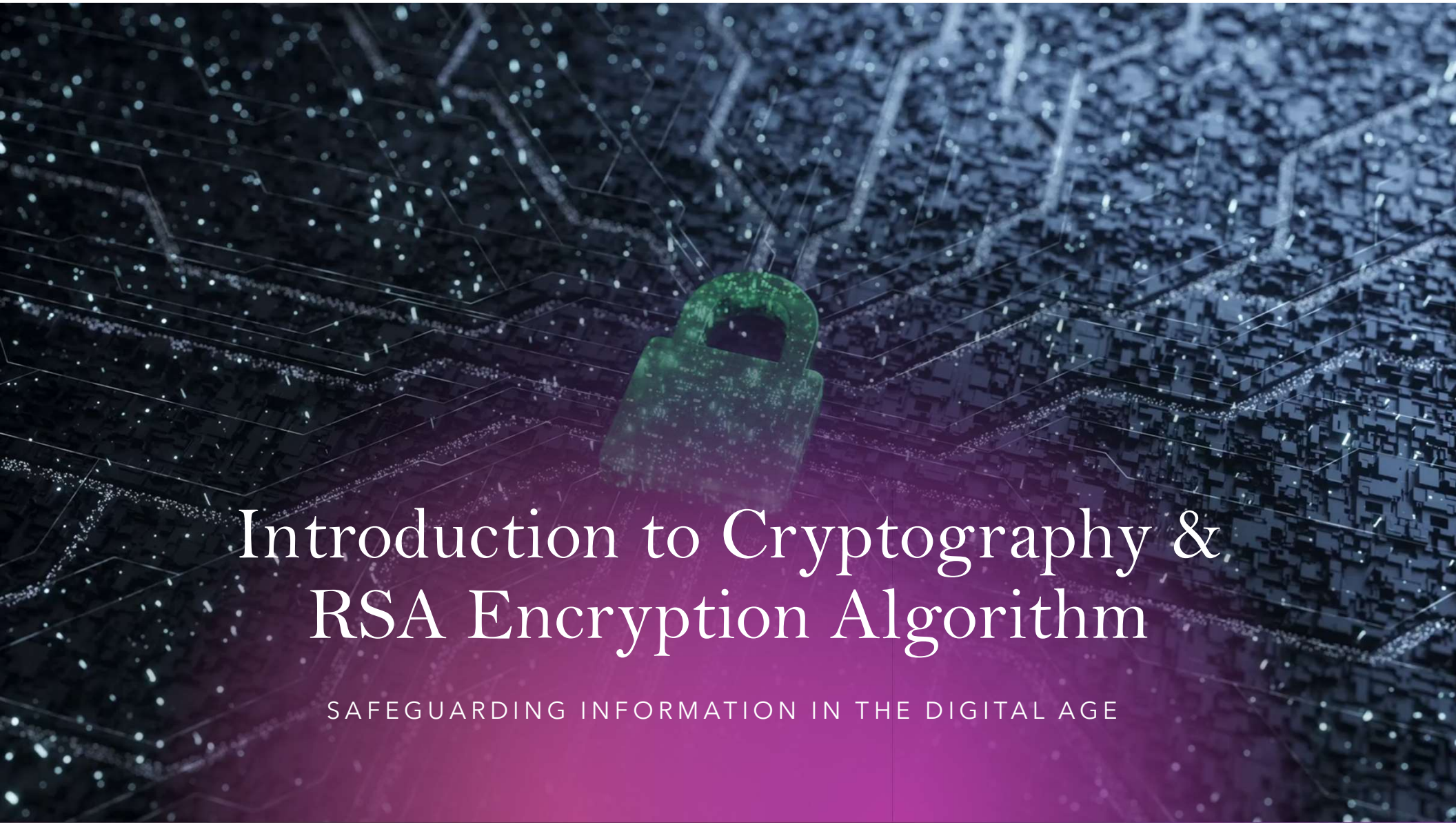


Introduction to Cryptography & RSA Encryption Algorithm

SAFEGUARDING INFORMATION IN THE DIGITAL AGE

What is Cryptography?

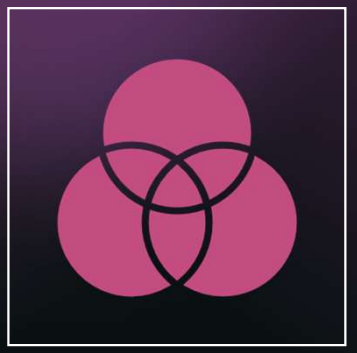
- Cryptography derives from the Greek word "kryptós", and it means hiding. Cryptography is like the art and science of securing information and communication, by converting it to meaningless(unreadable) information, to prevent unauthorized people (third parties) from accessing this data.

Historical Background

- Throughout history the practise of trying to encrypting and decrypting information backs old civilizations it starts from simple substitution ciphers (Caesar cipher) to sophisticated encryption techniques designed (TripleDES, Towfish algoBlowfish algoAdvanced Encryption Standard (AES)) which is a very advanced ways of encryption.

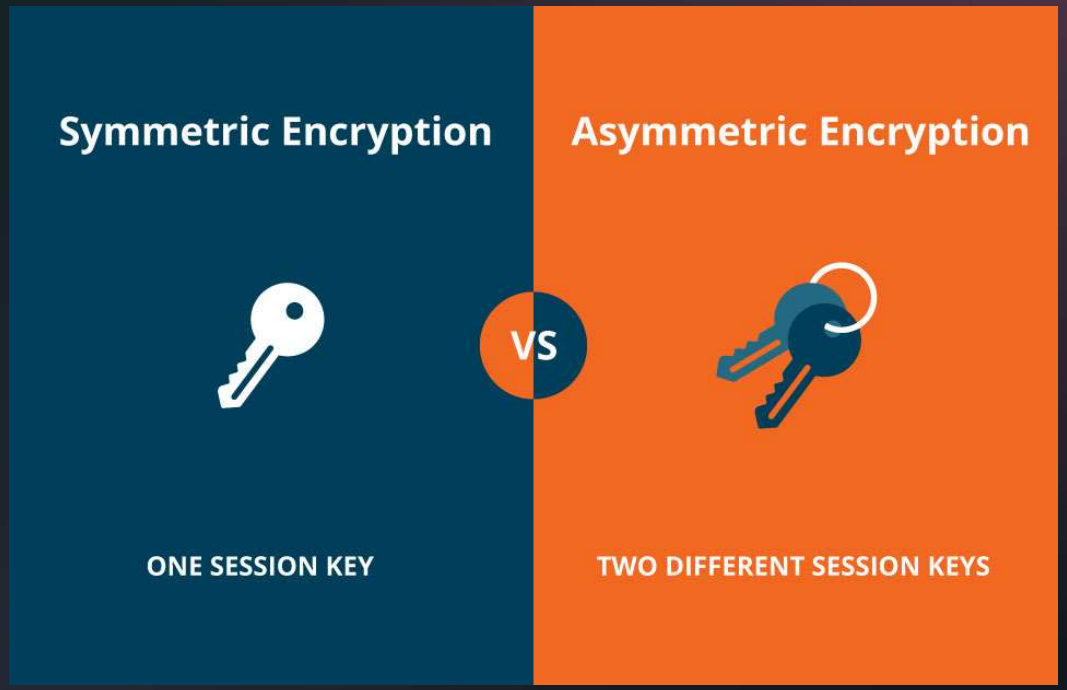
Fundamentals of Cryptography

Confidentiality: Ensuring that the information remains accessible by only the authorized people and prevents any other pyring eyes.



Integrity: Ensuring that the information remains unchanged during transmission and description.

Types of Encryption



- Symmetric-key Cryptography: The symmetric-key encryption was built on the usage of single for both encryption and decryption where the same secret key is shared between the sender and receiver, like Caesar cipher and DES (Data Encryption Standard)
- Asymmetric-key Cryptography (Public-key Cryptography): This algorithm was built based on a pair of distinct keys, a public key for encryption and private key for decryption. This way provides enhanced encryption and security. The RSA algorithm is one of the most popular algorithm in public-key cryptography

Introduction to RSA (Rivest-Shamir-Adleman) Encryption Algorithm

- RSA is a public key cryptosystem, the algorithm named after Rivest–Shamir–Adleman the scientist who described the algorithm in 1977 but recently it was known that in 1973 there was an English mathematician Clifford Cocks who had developed an equivalent system for Government Communications Headquarters (GCHQ). In a public key cryptosystem the encryption is public and differs from the private key which is kept secret. The public key generated based on 2 large prime numbers will be explained in the math section. The security of the RSA algorithm relies on the difficulty of how to factorize the product of the 2 large prime numbers (that's why it should be large).The encryption process includes transforming plaintext (eg. message) into ciphertext using the public key (any one can encrypt the message but not every can decrypt it)

The mechanism behind the RSA algorithm

Key Generation:

- Selection of two large prime numbers, denoted as 'p' and 'q'.
- Computation of 'n' as the product of 'p' and 'q'.
- Selection of 'e', a value relative prime with '(n)', typically small, and less than '(n)'.
- Calculation of ' Φ(n)' being equal to '(p-1)(q-1)'.
- Then our public key is made from (n, e).
- Generating the private key d= (k*Φ(n) + 1) / e for some integer k.
- Then the private key is d

Strengths of RSA

Security Based on Mathematical Complexity:

- RSA's security relies on the difficulty of factoring the product of two large prime numbers into their original primes.

Secure Exchange of Information:

- RSA is a powerful tool for encrypting messages and files to ensure that only intended recipients can access the information.
- Achieved through the use of a public key to encrypt the data.

Standardization and Adoption:

- RSA has become an industry standard widely adopted in various applications.
- Used in secure email, digital signatures, and SSL/TLS for securing web communications.

RSA Encryption Challenges

- As RSA faces challenges in the evolving cybersecurity landscape, adapting to the Internet of Things (IoT) and quantum computing becomes crucial. The resource constraints of IoT devices pose hurdles, and the threat of quantum algorithms poses a potential risk to traditional RSA encryption. The evolving use cases include RSA's integration into cloud computing environments for secure data transmission, and ongoing research explores post-quantum cryptography solutions. Despite challenges, RSA continues to be a key player in ensuring secure communications, emphasizing the need for continuous adaptation in the era of advanced technologies.

Real-world Applications of RSA

Online Banking Transactions

RSA is extensively used to secure online banking transactions and protect customer financial data.

Secure Communications (SSL/TLS)

RSA is a fundamental component of SSL/TLS protocols, ensuring secure web communications.

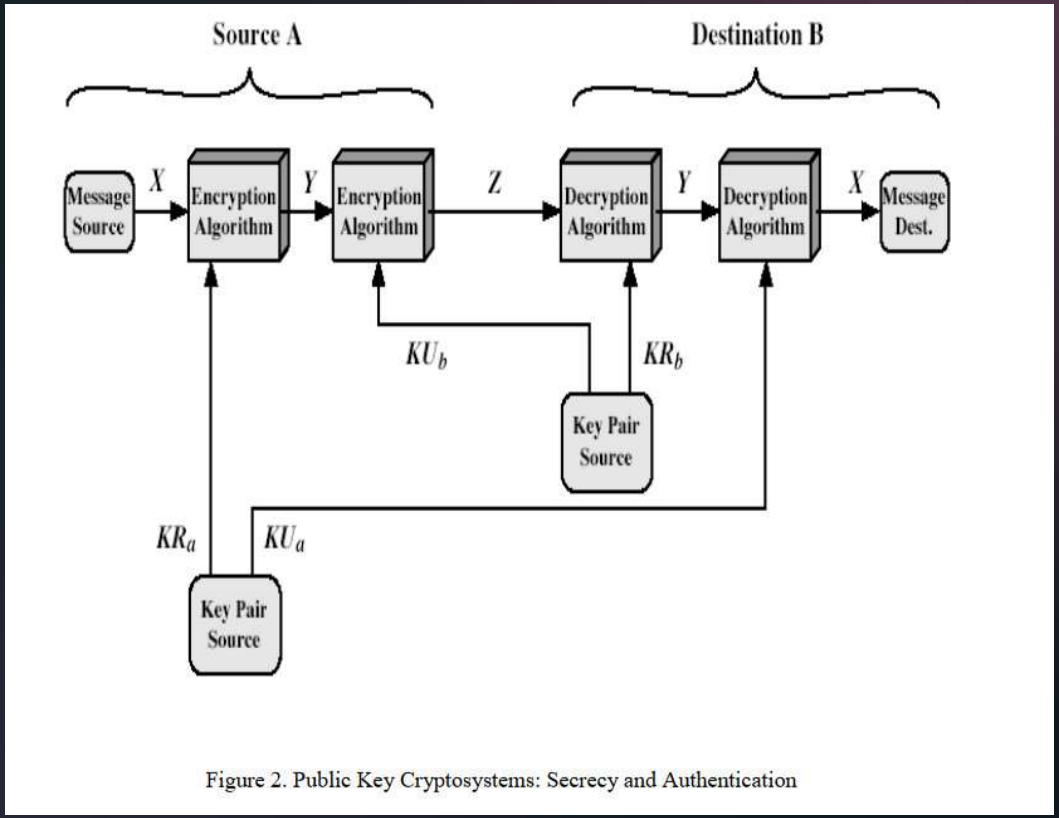
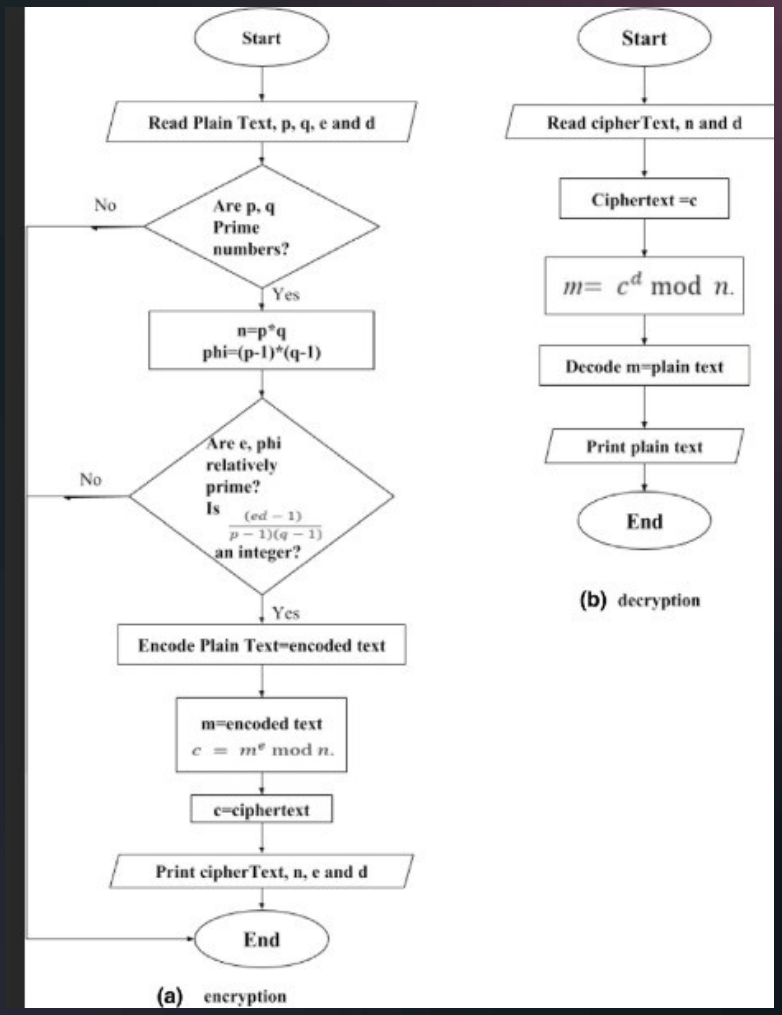


Figure 2. Public Key Cryptosystems: Secrecy and Authentication

Case Study: RSA Encryption in Online Banking

- Implementation:
- A leading bank implements RSA encryption for securing online banking transactions. Each customer has a unique public-private key pair for secure communication.
- Benefits: Enhances security in online transactions and protects sensitive customer information.
- Relevance: Highlights the real-world application of RSA in the financial sector for securing digital transactions.



Code Overview

RSA Algorithm:

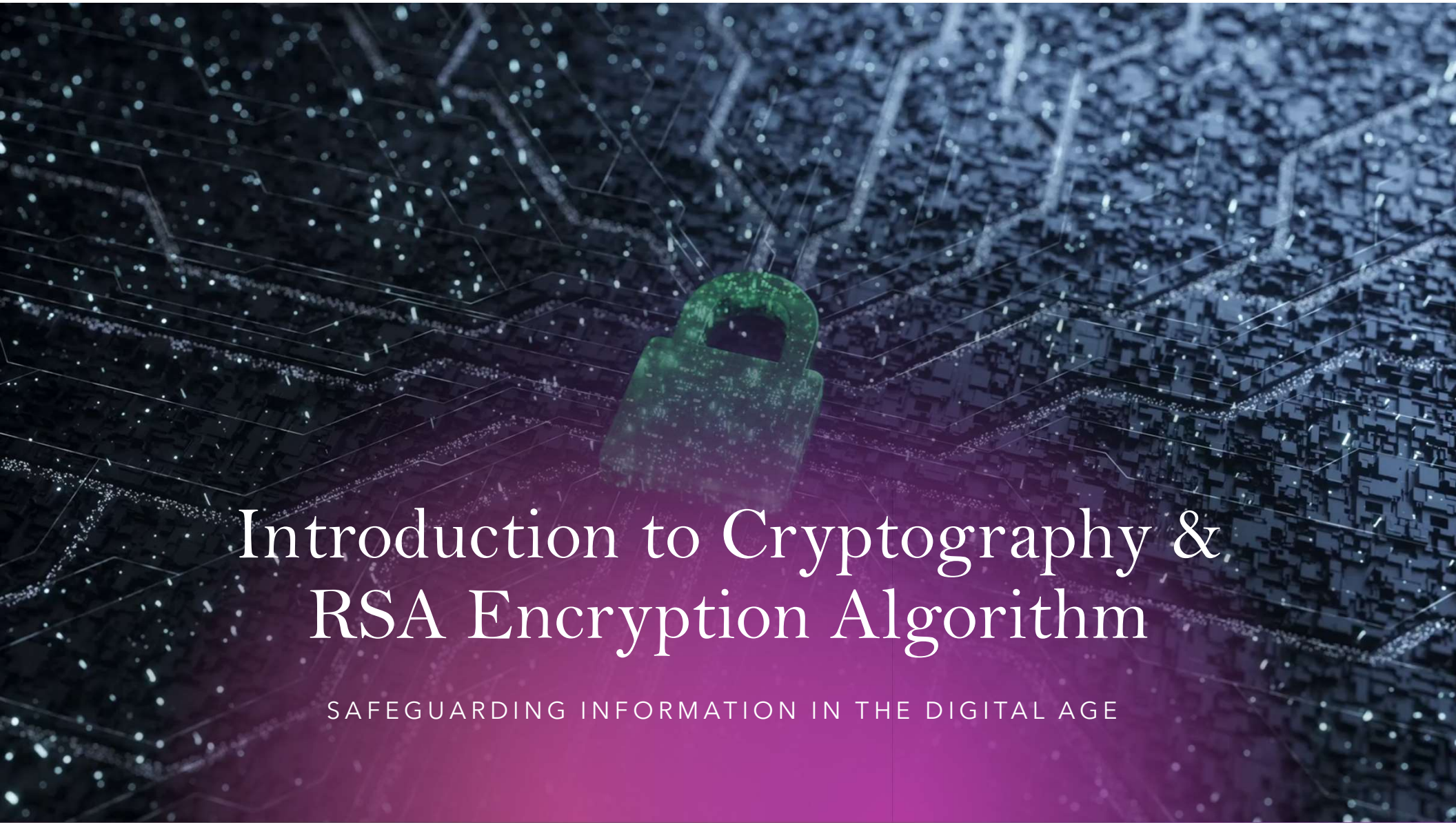
- Key Generation
- Encryption
- Decryption

Conclusion

- Today’s presentation has provided a comprehensive overview of cryptography and delved into the intricacies of the RSA encryption algorithm. We explored the fundamental principles behind cryptography, emphasizing its crucial role in securing sensitive information in our digitally interconnected world.
- As we navigate the complexities of modern communication and transactions, understanding the principles of cryptography becomes impotant. The RSA algorithm, with its elegant blend of security and efficiency, exemplifies the power of cryptographic techniques in ensuring confidentiality, integrity, and authenticity.

Thank You

”



Introduction to Cryptography & RSA Encryption Algorithm

SAFEGUARDING INFORMATION IN THE DIGITAL AGE

What is Cryptography?

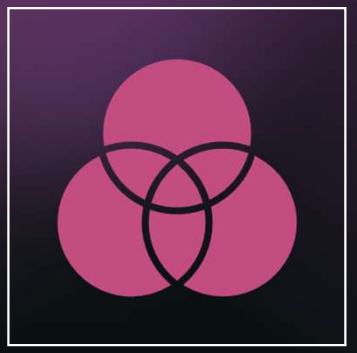
- Cryptography derives from the Greek word "kryptós", and it means hiding. Cryptography is like the art and science of securing information and communication, by converting it to meaningless(unreadable) information, to prevent unauthorized people (third parties) from accessing this data.

Historical Background

- Throughout history the practise of trying to encrypting and decrypting information backs old civilizations it starts from simple substitution ciphers (Caesar cipher) to sophisticated encryption techniques designed (TripleDES, Towfish algoBlowfish algoAdvanced Encryption Standard (AES)) which is a very advanced ways of encryption.

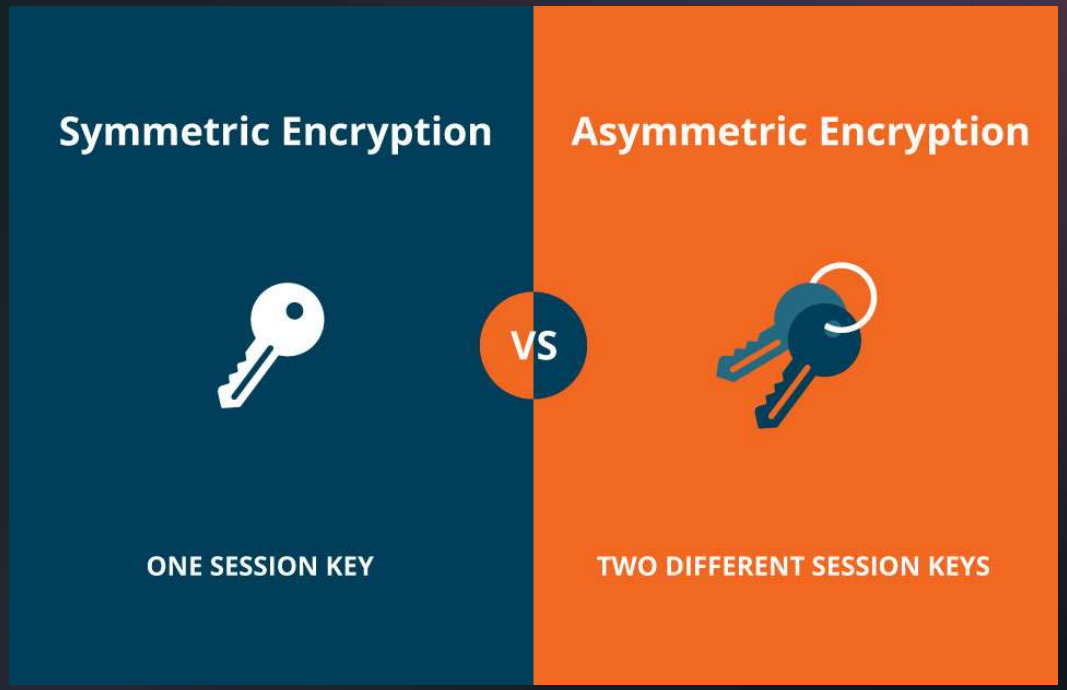
Fundamentals of Cryptography

Confidentiality: Ensuring that the information remains accessible by only the authorized people and prevents any other pyring eyes.



Integrity: Ensuring that the information remains unchanged during transmission and description.

Types of Encryption



- Symmetric-key Cryptography: The symmetric-key encryption was built on the usage of single for both encryption and decryption where the same secret key is shared between the sender and receiver, like Caesar cipher and DES (Data Encryption Standard)
- Asymmetric-key Cryptography (Public-key Cryptography): This algorithm was built based on a pair of distinct keys, a public key for encryption and private key for decryption. This way provides enhanced encryption and security. The RSA algorithm is one of the most popular algorithm in public-key cryptography

Introduction to RSA (Rivest-Shamir-Adleman) Encryption Algorithm

- RSA is a public key cryptosystem, the algorithm named after Rivest–Shamir–Adleman the scientist who described the algorithm in 1977 but recently it was known that in 1973 there was an English mathematician Clifford Cocks who had developed an equivalent system for Government Communications Headquarters (GCHQ). In a public key cryptosystem the encryption is public and differs from the private key which is kept secret. The public key generated based on 2 large prime numbers will be explained in the math section. The security of the RSA algorithm relies on the difficulty of how to factorize the product of the 2 large prime numbers (that's why it should be large).The encryption process includes transforming plaintext (eg. message) into ciphertext using the public key (any one can encrypt the message but not every can decrypt it)

The mechanism behind the RSA algorithm

Key Generation:

- Selection of two large prime numbers, denoted as 'p' and 'q'.
- Computation of 'n' as the product of 'p' and 'q'.
- Selection of 'e', a value relative prime with '(n)', typically small, and less than '(n)'.
- Calculation of ' Φ(n)' being equal to '(p-1)(q-1)'.
- Then our public key is made from (n, e).
- Generating the private key d= (k*Φ(n) + 1) / e for some integer k.
- Then the private key is d

Strengths of RSA

Security Based on Mathematical Complexity:

- RSA's security relies on the difficulty of factoring the product of two large prime numbers into their original primes.

Secure Exchange of Information:

- RSA is a powerful tool for encrypting messages and files to ensure that only intended recipients can access the information.
- Achieved through the use of a public key to encrypt the data.

Standardization and Adoption:

- RSA has become an industry standard widely adopted in various applications.
- Used in secure email, digital signatures, and SSL/TLS for securing web communications.

RSA Encryption Challenges

- As RSA faces challenges in the evolving cybersecurity landscape, adapting to the Internet of Things (IoT) and quantum computing becomes crucial. The resource constraints of IoT devices pose hurdles, and the threat of quantum algorithms poses a potential risk to traditional RSA encryption. The evolving use cases include RSA's integration into cloud computing environments for secure data transmission, and ongoing research explores post-quantum cryptography solutions. Despite challenges, RSA continues to be a key player in ensuring secure communications, emphasizing the need for continuous adaptation in the era of advanced technologies.

Real-world Applications of RSA

Online Banking Transactions

RSA is extensively used to secure online banking transactions and protect customer financial data.

Secure Communications (SSL/TLS)

RSA is a fundamental component of SSL/TLS protocols, ensuring secure web communications.

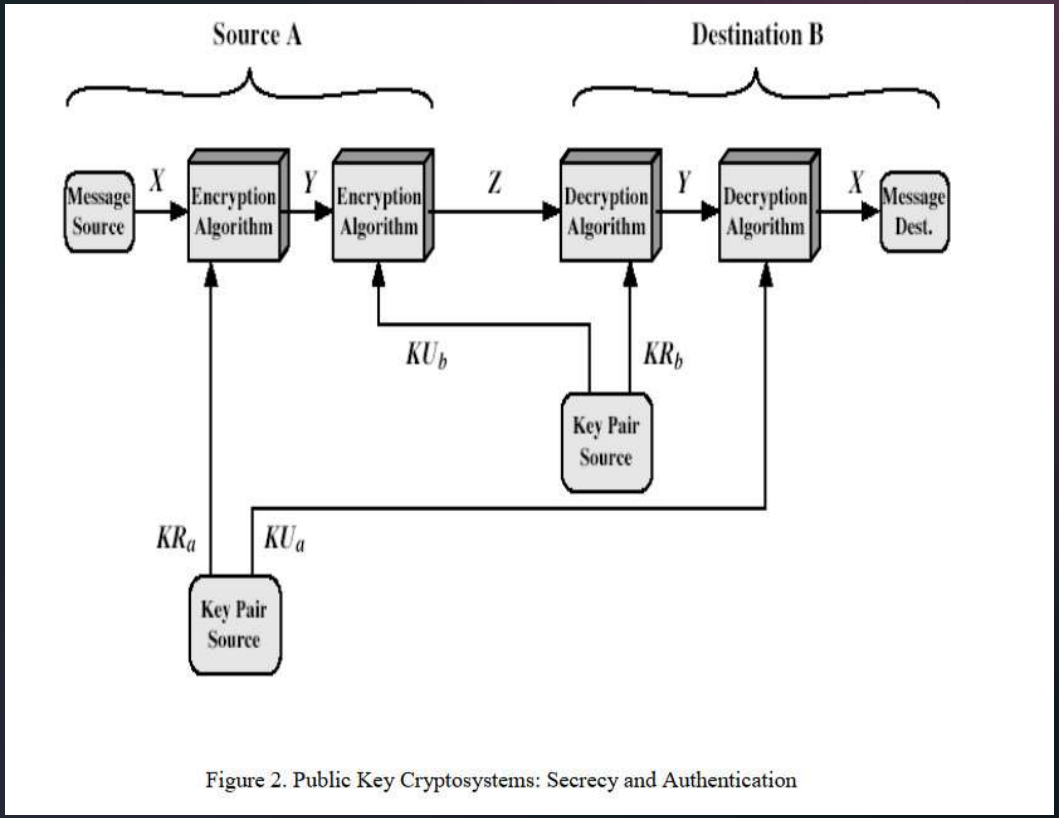
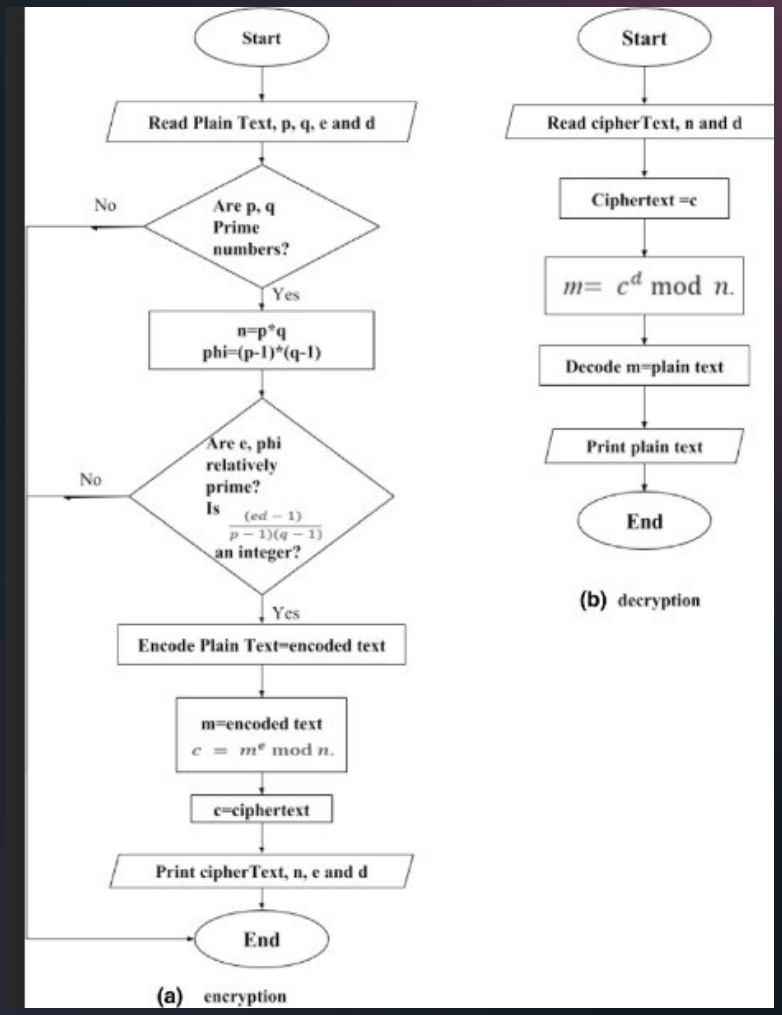


Figure 2. Public Key Cryptosystems: Secrecy and Authentication

Case Study: RSA Encryption in Online Banking

- Implementation:
- A leading bank implements RSA encryption for securing online banking transactions. Each customer has a unique public-private key pair for secure communication.
- Benefits: Enhances security in online transactions and protects sensitive customer information.
- Relevance: Highlights the real-world application of RSA in the financial sector for securing digital transactions.



Code Overview

RSA Algorithm:

- Key Generation
- Encryption
- Decryption

Conclusion

- Today’s presentation has provided a comprehensive overview of cryptography and delved into the intricacies of the RSA encryption algorithm. We explored the fundamental principles behind cryptography, emphasizing its crucial role in securing sensitive information in our digitally interconnected world.
- As we navigate the complexities of modern communication and transactions, understanding the principles of cryptography becomes impotant. The RSA algorithm, with its elegant blend of security and efficiency, exemplifies the power of cryptographic techniques in ensuring confidentiality, integrity, and authenticity.

Thank You

”