# RİVEST-SHAMİR-ADLEMAN

Group 1

2025

1
2
3
4
5
6
7
8
9

# Brief History

Rivest-Shamir-Adleman (RSA) is a well-known public-key or asymmetric cryptographic algorithm named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, who published it in 1977.234+1 RSA uses a pair of keys for encryption and decryption: a public key for encryption and a private key for decryption.236 The security of RSA is based on the difficulty of factoring large integers, specifically the product of two large prime numbers.

1
2
3
4
5
6
7
8
9

# Key Concepts & Formulas

## Prime Factorization

RSA security is based on the difficulty of factoring the product of two large prime numbers.

## Key Generation:

1. Choose two distinct large prime numbers, p and q.
2. Compute $n = p \times q$ (modulus).
3. Compute Euler's totient function: $\phi(n) = (p - 1)(q - 1)$.
4. Choose an integer e (public key) such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.
5. Compute d (private key) such that $d \equiv e^{-1} \bmod \phi(n)$.

1
2
3
4
5
6
7
8
9

# Encryption & Decryption

## Encryption

- *Ciphertext* $c \equiv m^e \bmod n$, *where* $m$ *is the plaintext message.*

## Decryption

- *Plaintext* $m \equiv c^d \bmod n$.

1
2
3
4
5
6
7
8
9

# Examples of Real-World Applications

- ***Secure Web Traffic:*** *RSA is used in HTTPS to encrypt data between web browsers and servers.*
- ***Email Encryption:*** *RSA is used in PGP (Pretty Good Privacy) for secure email communication.*
- ***VPNs:*** *RSA is used in Virtual Private Networks to establish secure connections.*
- ***Digital Signatures:*** *RSA is used to verify the authenticity of digital documents and software.*

1
2
3
4
5
6
7
8
9

# Advantages:

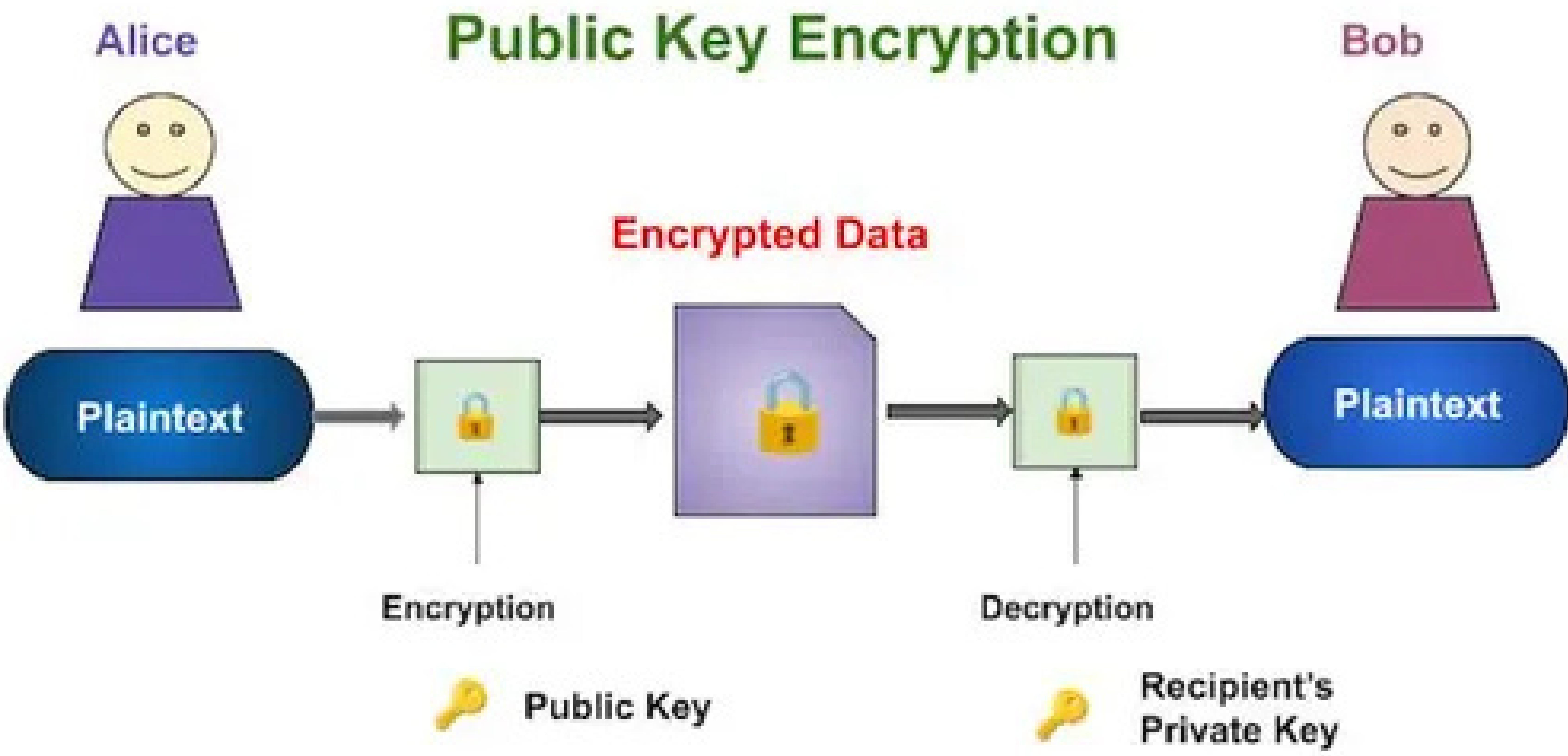
- ***Wide Adoption:*** *RSA is well-established and widely supported in cryptographic libraries and protocols.*
- ***Versatility:*** *Can be used for both encryption and digital signatures.*
- ***Proven Security:*** *RSA has been extensively studied and remains secure when implemented correctly with sufficiently large key sizes (e.g., 2048 or 4096 bits).*

1
2
3
4
5
6
7
8
9

# Disadvantages

- ***Computational Overhead:*** *RSA is slower than symmetric-key algorithms like AES, especially for large data volumes.*
- ***Key Size:*** *RSA requires larger key sizes compared to ECC for equivalent security, leading to increased computational and storage costs.*
- ***Quantum Threat****: RSA is vulnerable to attacks by quantum computers using Shor’s algorithm.*

1
2
3
4
5
6
7
8
9


Alice
Public Key Encryption
Bob
Encrypted Data
Plaintext
Plaintext
Encryption
Decryption
Public Key
Recipient's
Private Key

1
2
3
4
5
6
7
8
9

# Questions?

# Thank you