



SNS COLLEGE OF TECHNOLOGY
Coimbatore-35
An Autonomous Institution



Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University,
Chennai

19ECT301-COMMUNICATION NETWORKS III YEAR/ V SEMESTER

UNIT 4- NETWORK & DATA SECURITY

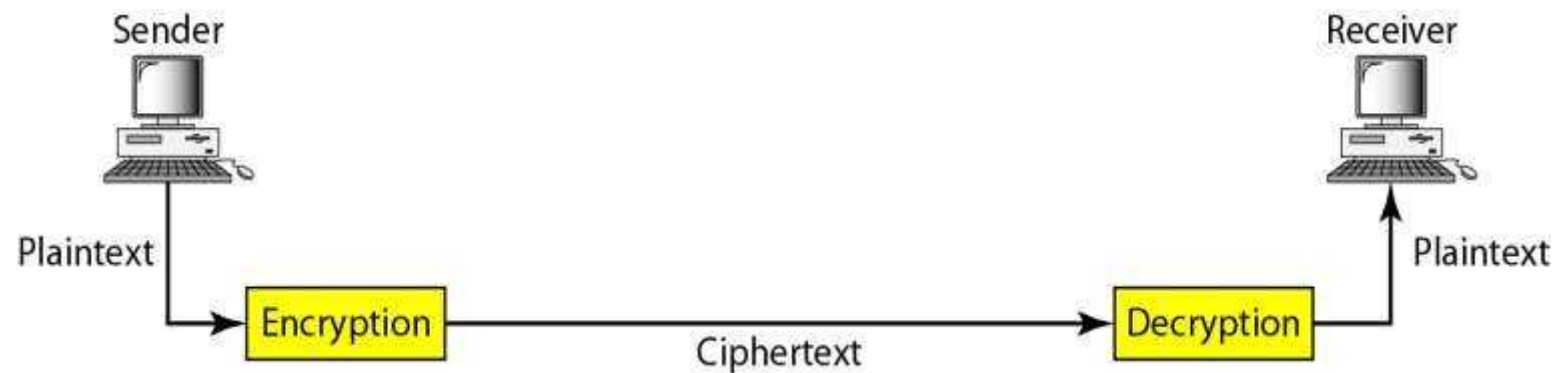
TOPIC –Cryptography Techniques



Cryptography components



- encryption and decryption algorithms as ciphers
- cipher is also used to refer to different categories of algorithms in cryptography



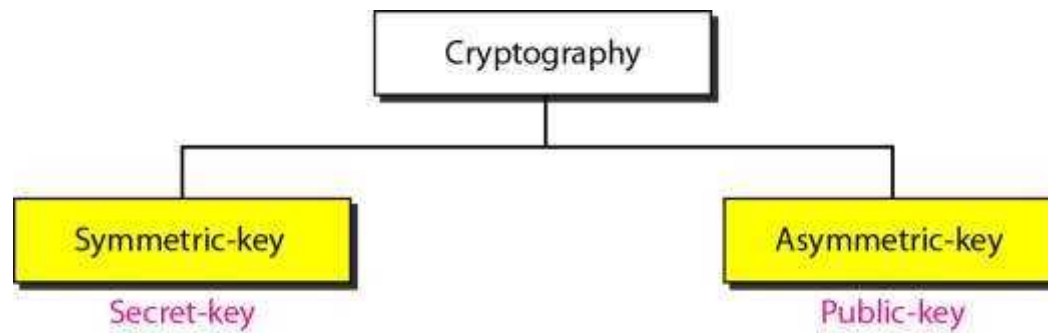


Key

- A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on.
- To encrypt a message, we need an encryption algorithm, an encryption key, and the plaintext.
- These create the ciphertext.
- To decrypt a message, we need a decryption algorithm, a decryption key, and the ciphertext.
- These reveal the original plaintext.

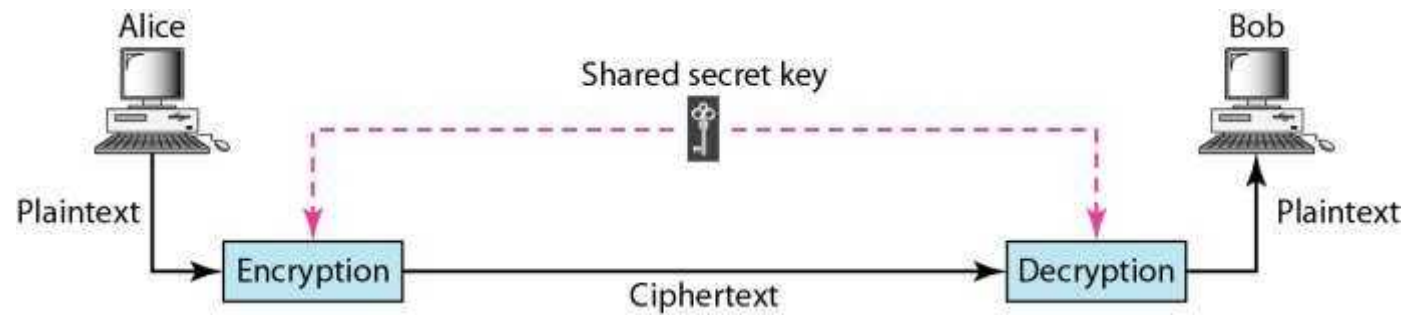


Categories of cryptography





Symmetric-key cryptography



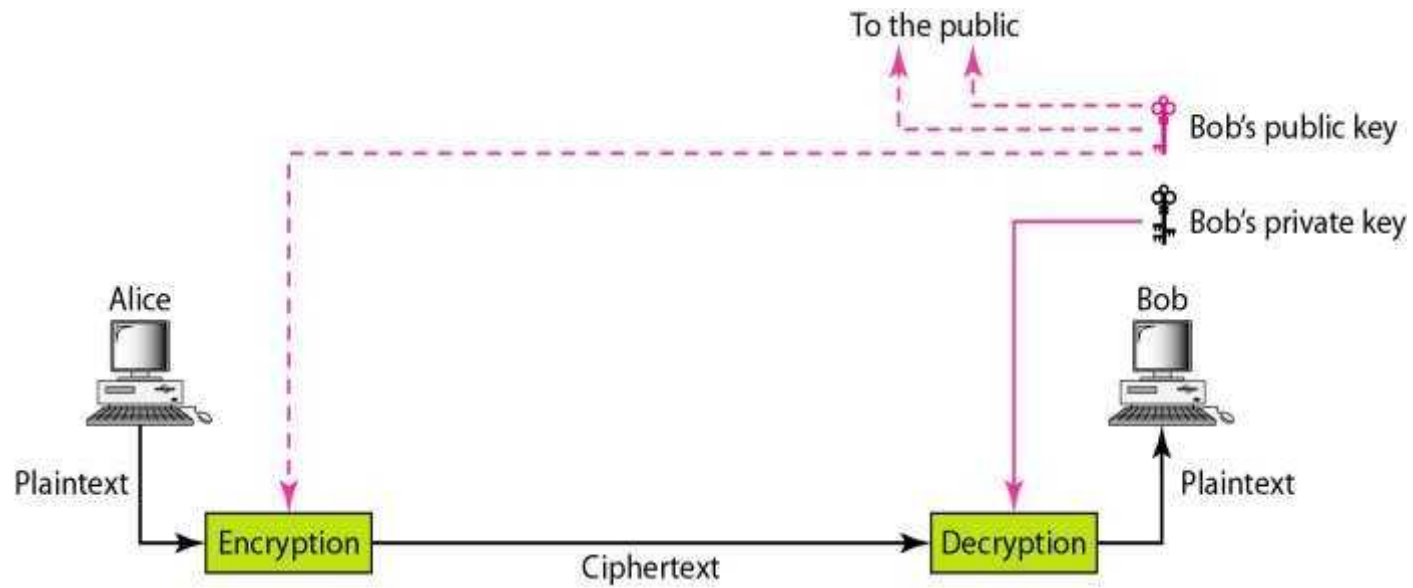


Note

In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.



Asymmetric-key cryptography





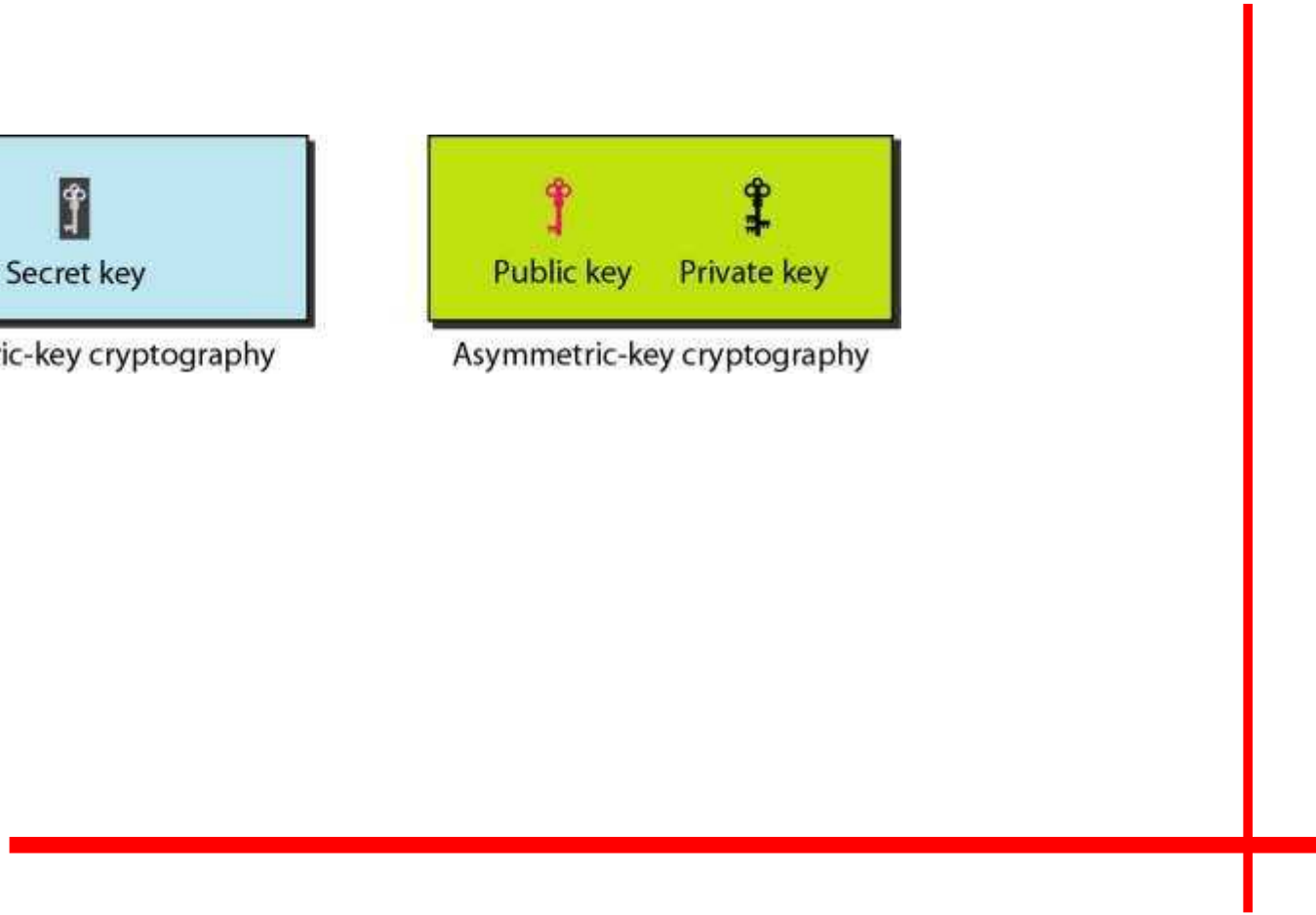
Keys used in cryptography



Symmetric-key cryptography

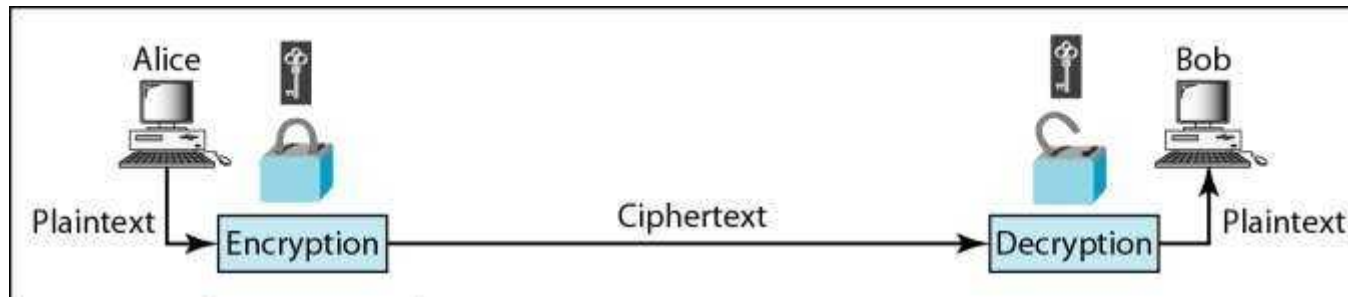


Asymmetric-key cryptography

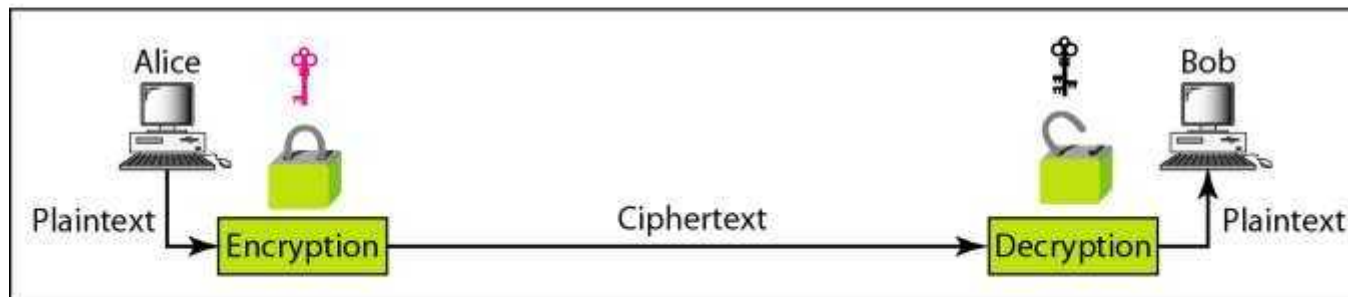




Comparison between two categories of cryptography



a. Symmetric-key cryptography



b. Asymmetric-key cryptography



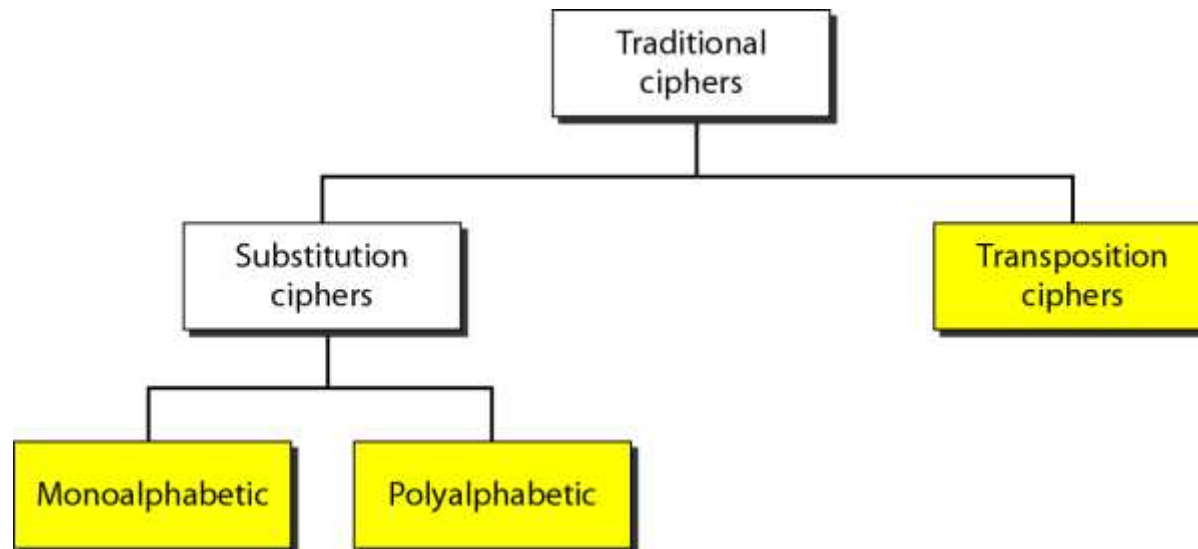
SYMMETRIC-KEY CRYPTOGRAPHY



Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war). We still mainly use symmetric-key cryptography in our network security.



Traditional ciphers





Thank You!