Session 9B

Cryptography - 2

Sheba Pari

Session 9B: Focus

- Types of Encryption
  - Stream Ciphers
  - Block Ciphers
- Cryptographic Techniques
  - Symmetric key Encipherment
  - Asymmetric key Encipherment
  - Hashing

Course page where the course materials will be posted as the course progresses:

Types of Encryption

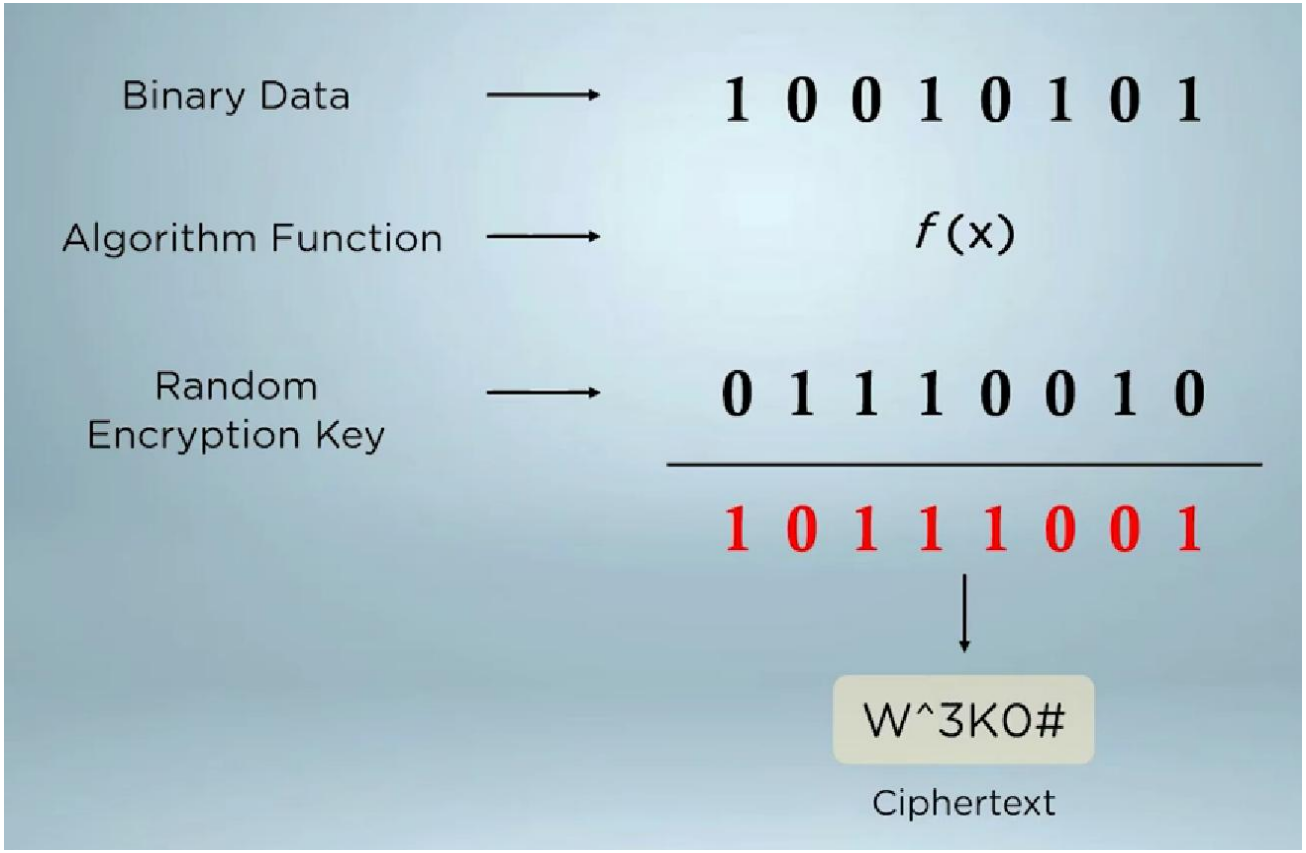
Types of Encryption

- Encryption can be done as either involves 3 distinct mechanisms
  - **Stream Ciphers**
  - **Block Ciphers**

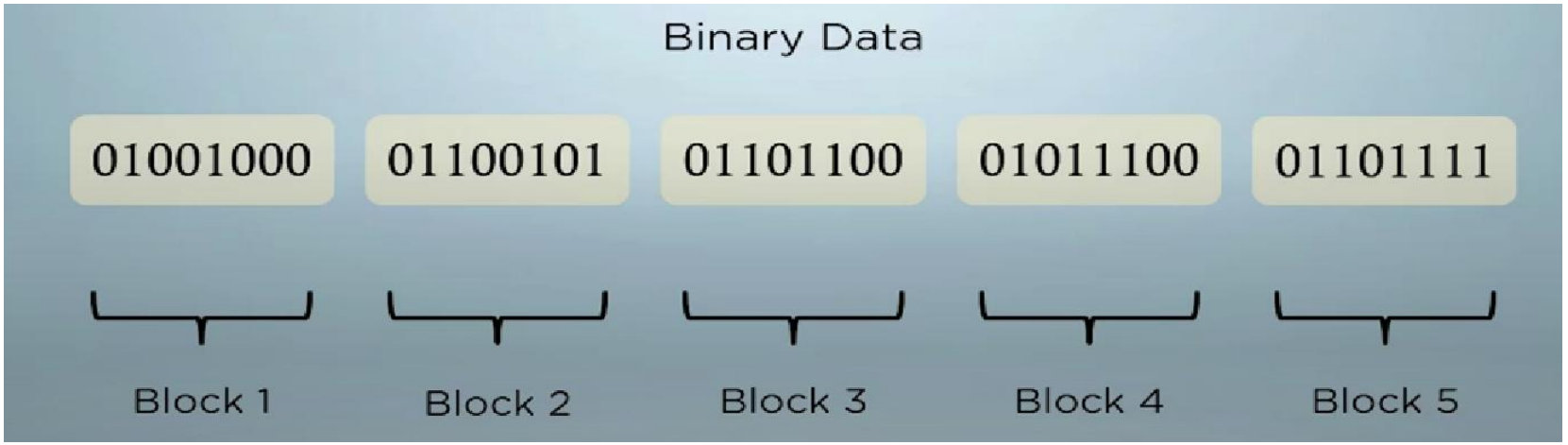
Stream Ciphers

- Encrypt information one bit/byte at a time
- Quicker Format of Encryption
- Data is converted to binary digits and encrypted sequentially
- Popular algorithms- RC4, Salsa20

Stream Ciphers

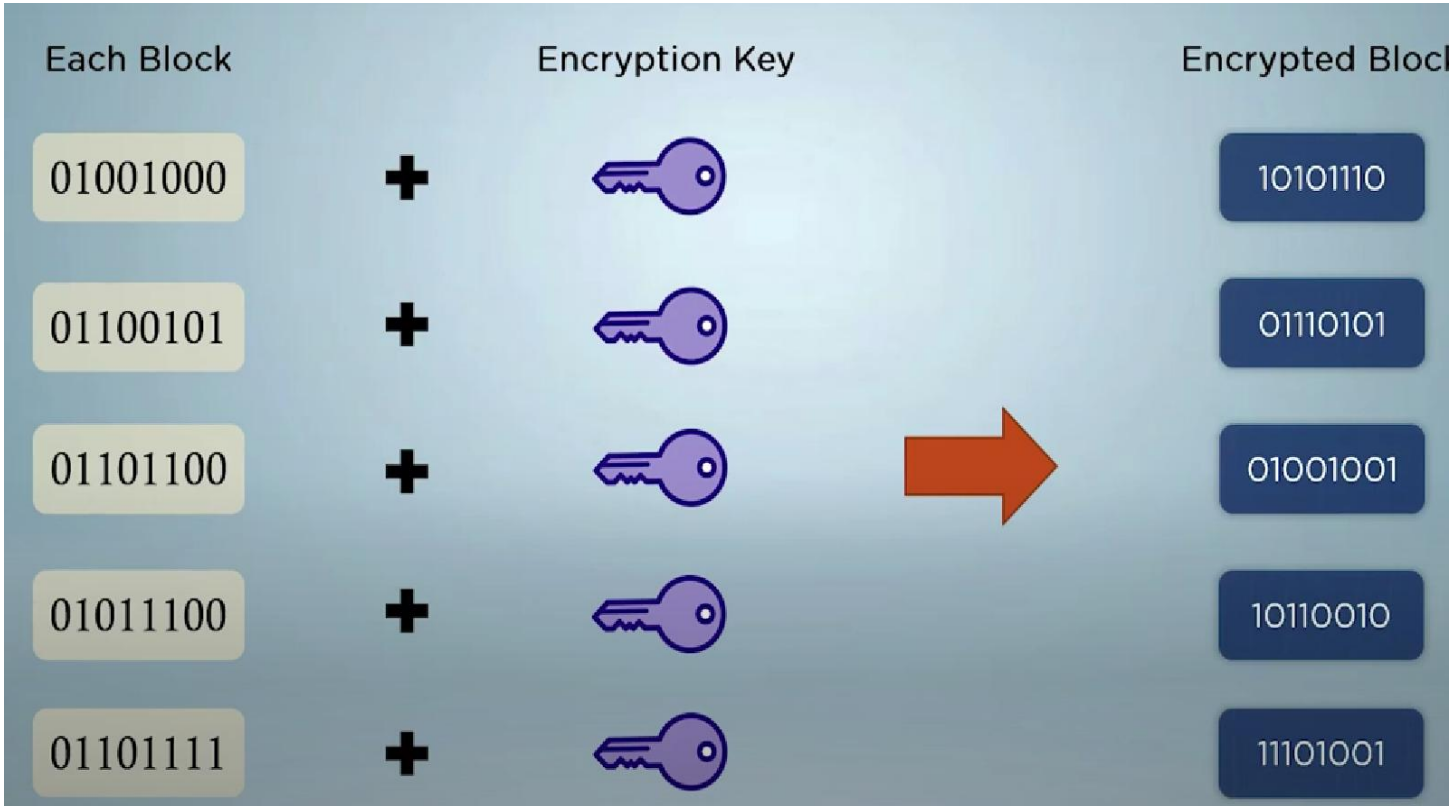


Block Ciphers

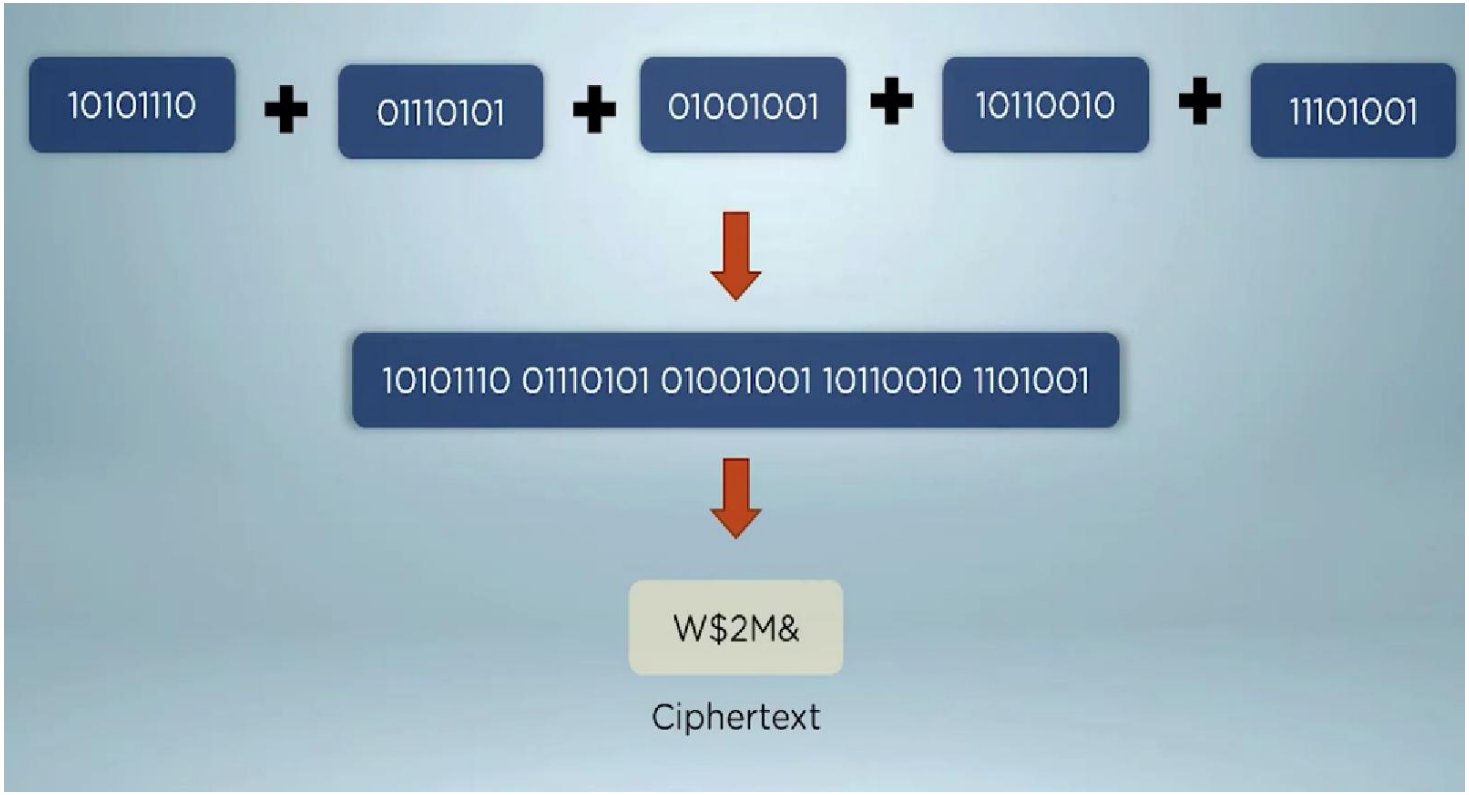


- Information broken down to chunks/blocks of fixed size
- Size of block depends on key size
- The chunks are encrypted and later chained together
- Popular algorithms- AES, DES, 3DES

Block Ciphers



Block Ciphers



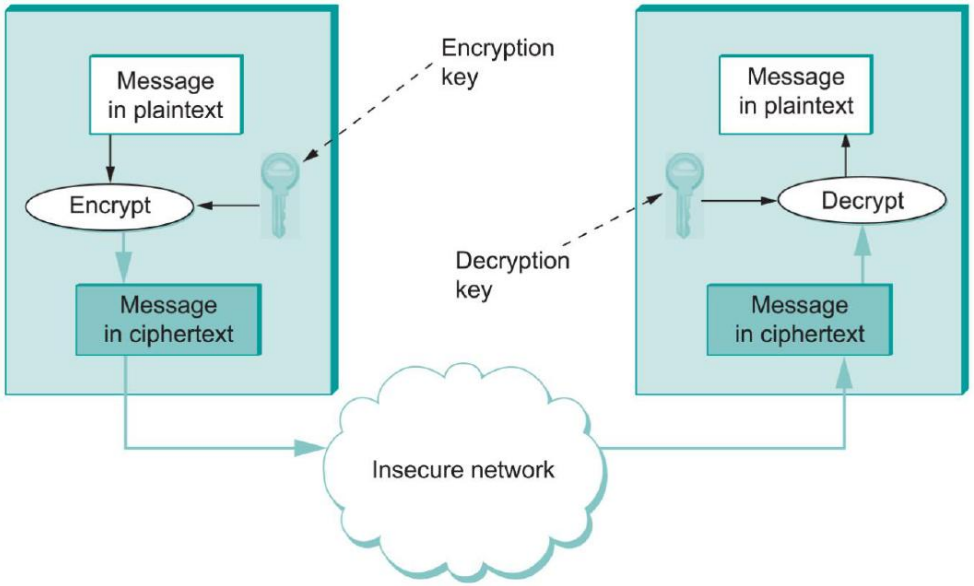
Cryptographic Techniques

Cryptographic Techniques

- Cryptography involves 3 distinct mechanisms
  - **Symmetric key Encipherment**
  - **Asymmetric key Encipherment**
  - **Hashing**

Symmetric Key Ciphers
(secret-key)

Secret-key Encryption and Decryption



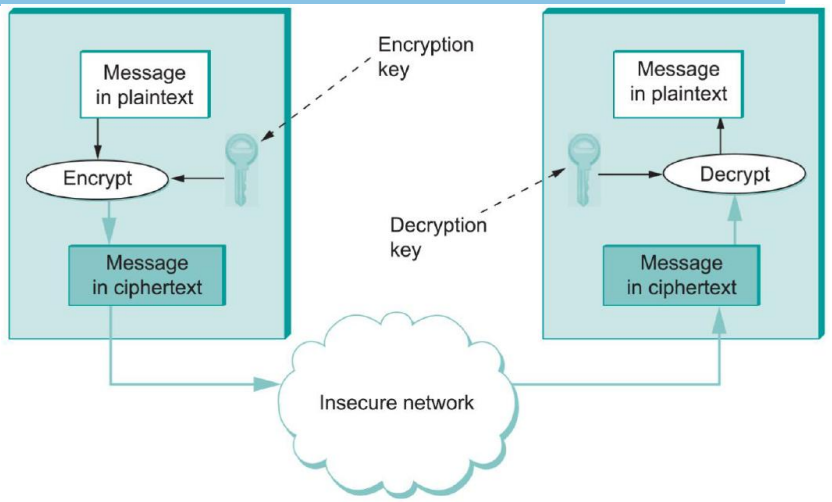
Plain text is the original, unencrypted information or data.

Cipher text is the result of applying an encryption algorithm to the plain text; it appears scrambled or unreadable without the appropriate decryption key.

- The **transformation** represented by an **encryption** function and its corresponding **decryption** function is called a **cipher**.
- Encryption and decryption functions have to be parameterized by a key and the functions are considered to be public knowledge—only the key needs to be secret.
- The **ciphertext** produced for a given **plaintext** message depends on both the **encryption function** and the **key**.

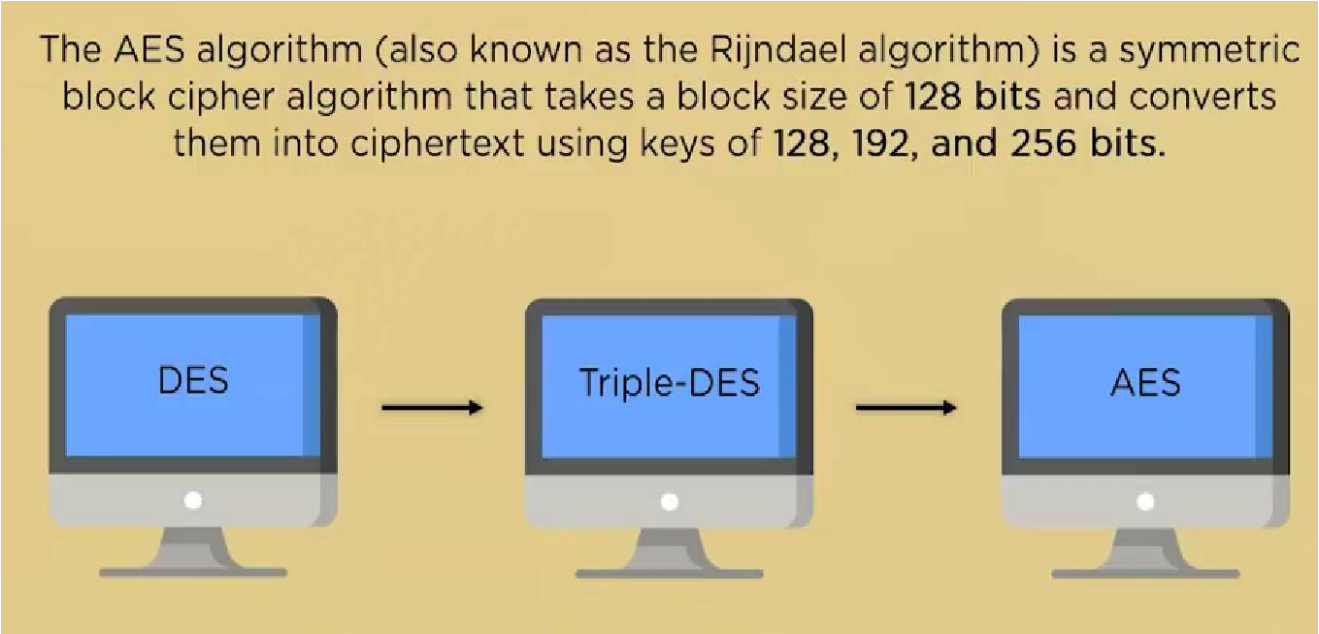
Secret-key Encryption and Decryption

- Here, **both participants** in a communication **share** the **same key**.
- **Secret-key** ciphers are also known as **symmetric-key** ciphers.
- Advanced Encryption Standard (**AES**) standard issued by NIST.



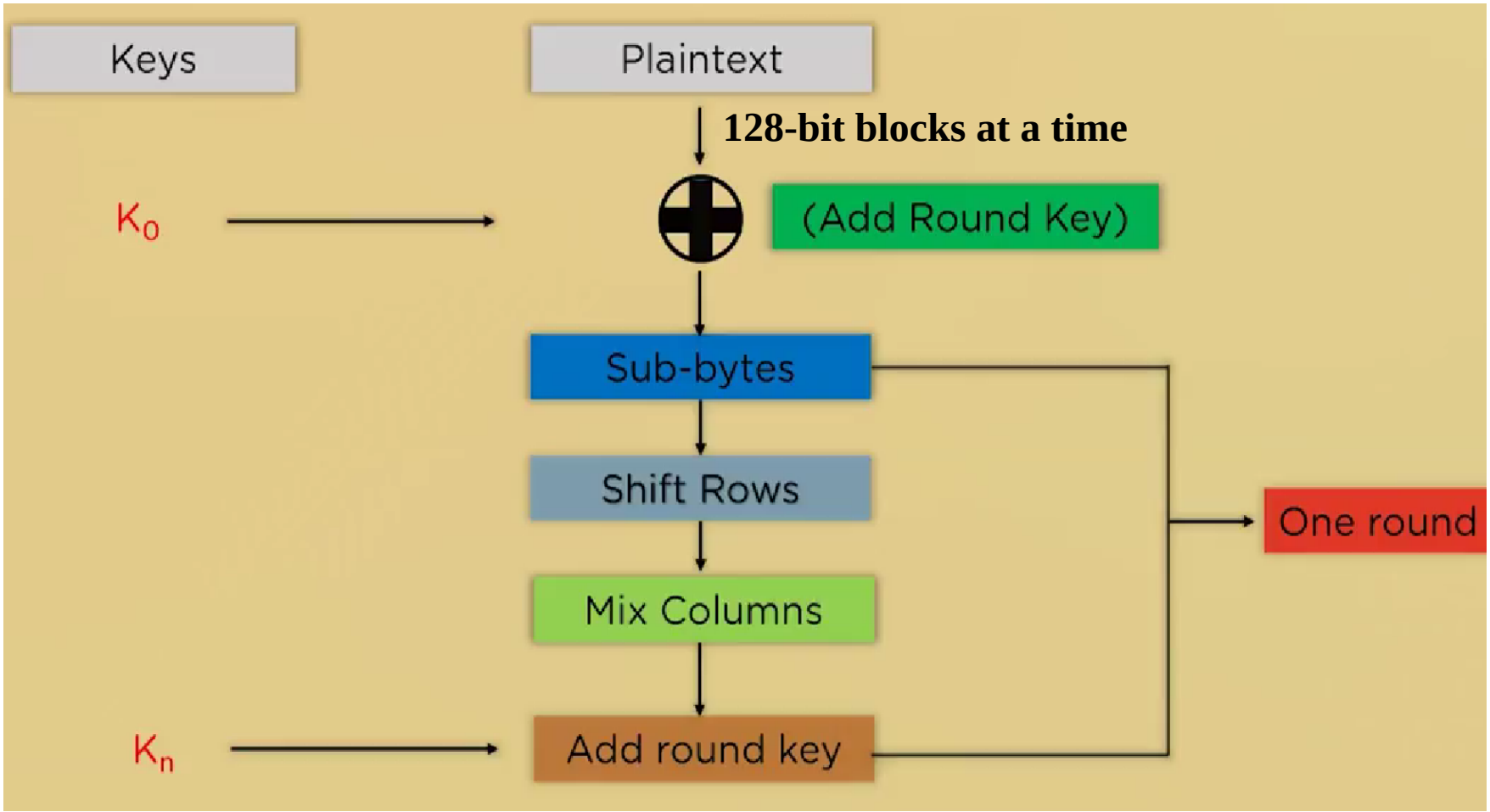
- AES supports key lengths of 128, 192, or 256 bits, and the block length is 128 bits. AES permits fast implementations in both software and hardware.
- It does not require much memory, which makes it suitable for small mobile devices.
- It is used to securely encrypt data in fixed-size blocks (often 128 bits).
- AES has some mathematically proven security properties and, has not suffered from any significant successful attacks.

AES (Advanced Encryption Standard)



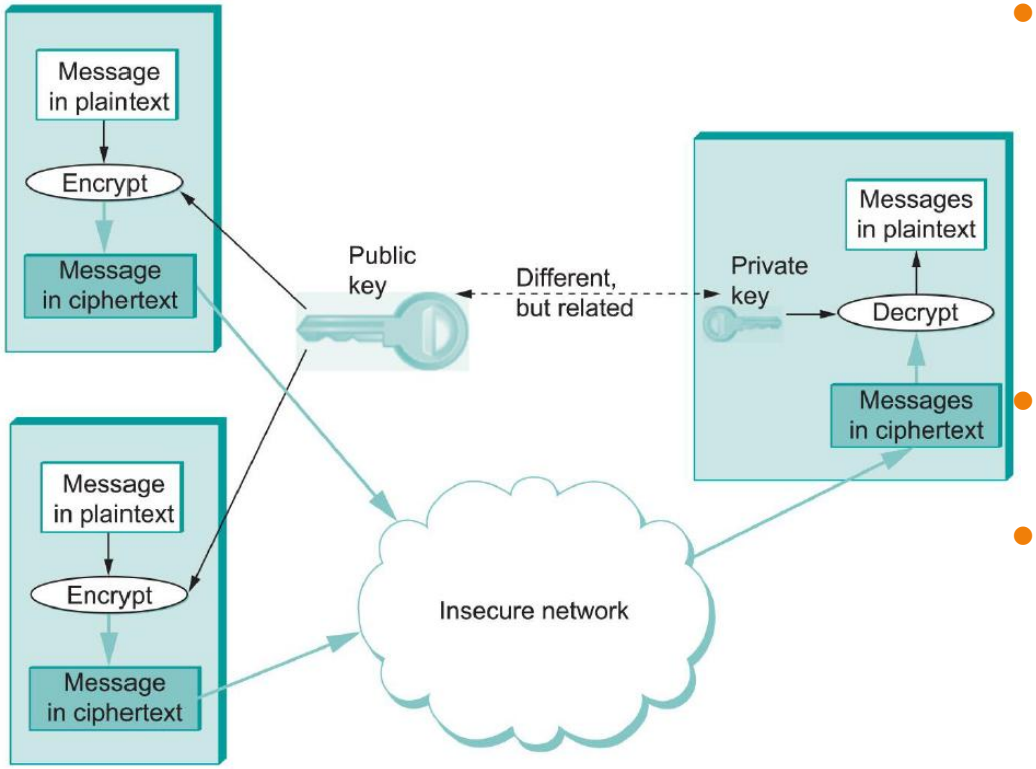
AES encrypts data by processing it in **128-bit blocks** using a **secret key**, employing **multiple rounds of operations** like byte **substitution**, **row shifting**, **column mixing**, and **adding the round key.**

AES


Keys
Plaintext
128-bit blocks at a time
K_0
(Add Round Key)
Sub-bytes
Shift Rows
Mix Columns
Add round key
K_n
One round

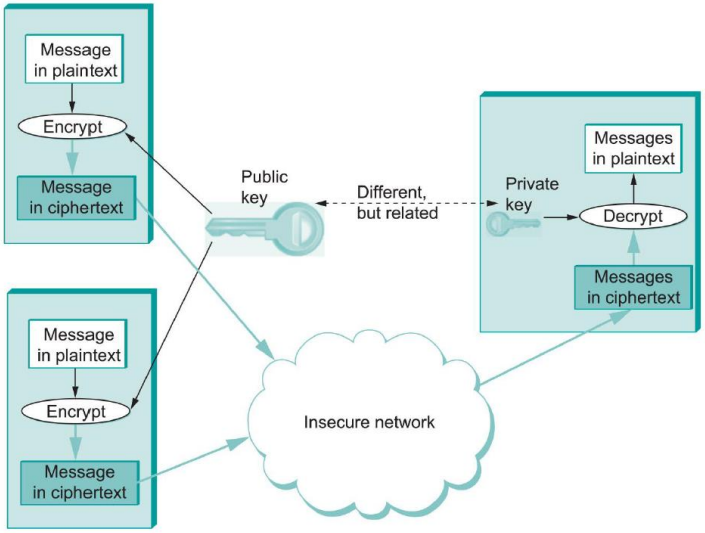
Asymmetric Key Ciphers
(private and public keys)

Public-key Encryption and Private-key Decryption



- Instead of a single key shared by two participants, a **public-key cipher** uses a **pair of related keys**, one for encryption and a different one for decryption.
- The pair of keys is "owned" by just one participant.
- The **owner** keeps the **decryption key secret** so that only the owner can decrypt messages; that key is called the **private key**.
- The **owner** makes the **encryption key public** so that anyone can **encrypt messages** for the owner; that key is called the **public key**.
- Obviously, for such a scheme to work, it must not be possible to deduce the private key from the public key.

Public key Encryption and Private key Decryption



- Any participant can get the public key and send an encrypted message to the owner of the key, and only the owner has the private key necessary to decrypt it.
- If we think of keys as defining a communication channel between participants, secret-key cipher provides a channel that is two-way between two participants.
- In secret-key, each participant holds the same (symmetric) key that either one can use to encrypt or decrypt messages in either direction.
- A public/private key pair, in contrast, provides a channel that is one-way and many-to-one: from everyone who has the public key to the unique owner of the private key.
- In public-key, for two-way confidentiality between two participants, each participant needs its own pair of keys, and each encrypts messages using the other's public key.

RSA- Key Generation - Info

1. Two large prime numbers are chosen (p and q)

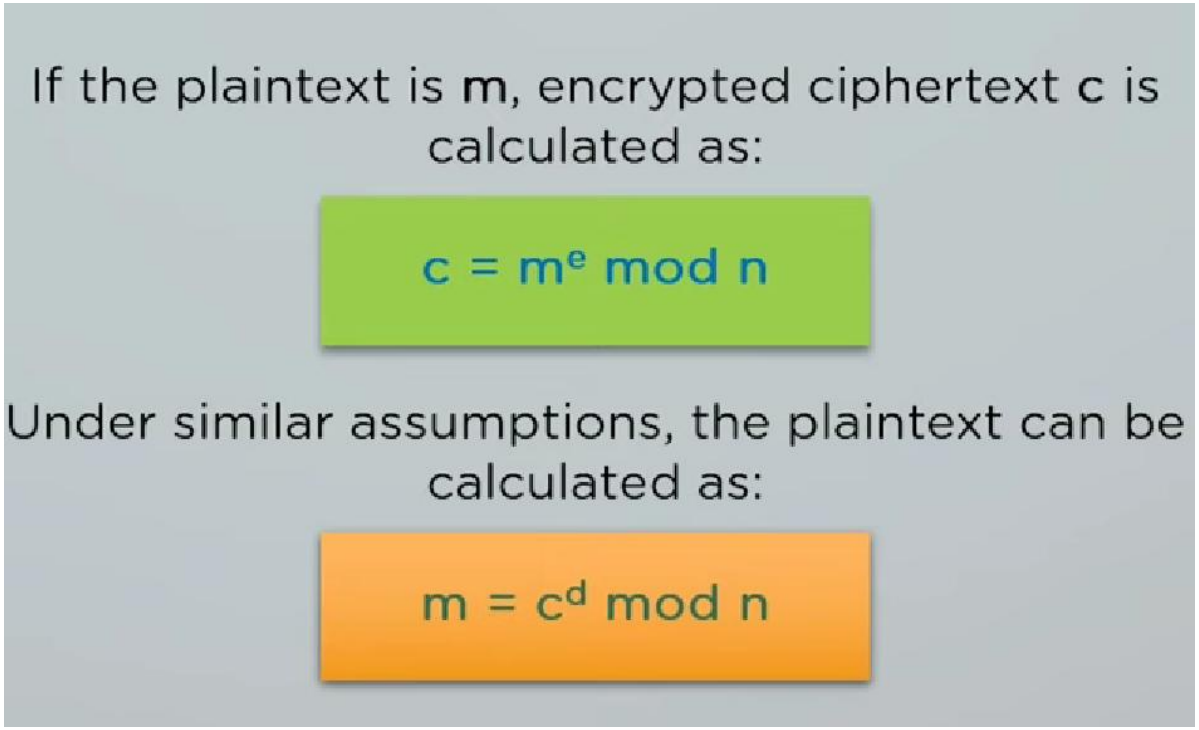
2. Compute $n = p * q$ and $z = (p-1)(q-1)$

3. Choose a number e where $1 < e < (p-1)(q-1)$

4. A number d is selected so that $ed \bmod z = 1$ and calculated as $d = e^{-1} \bmod (p-1)(q-1)$

5. Public key is (n,e) and private key is (n,d)

RSA- Encryption & Decryption - Info



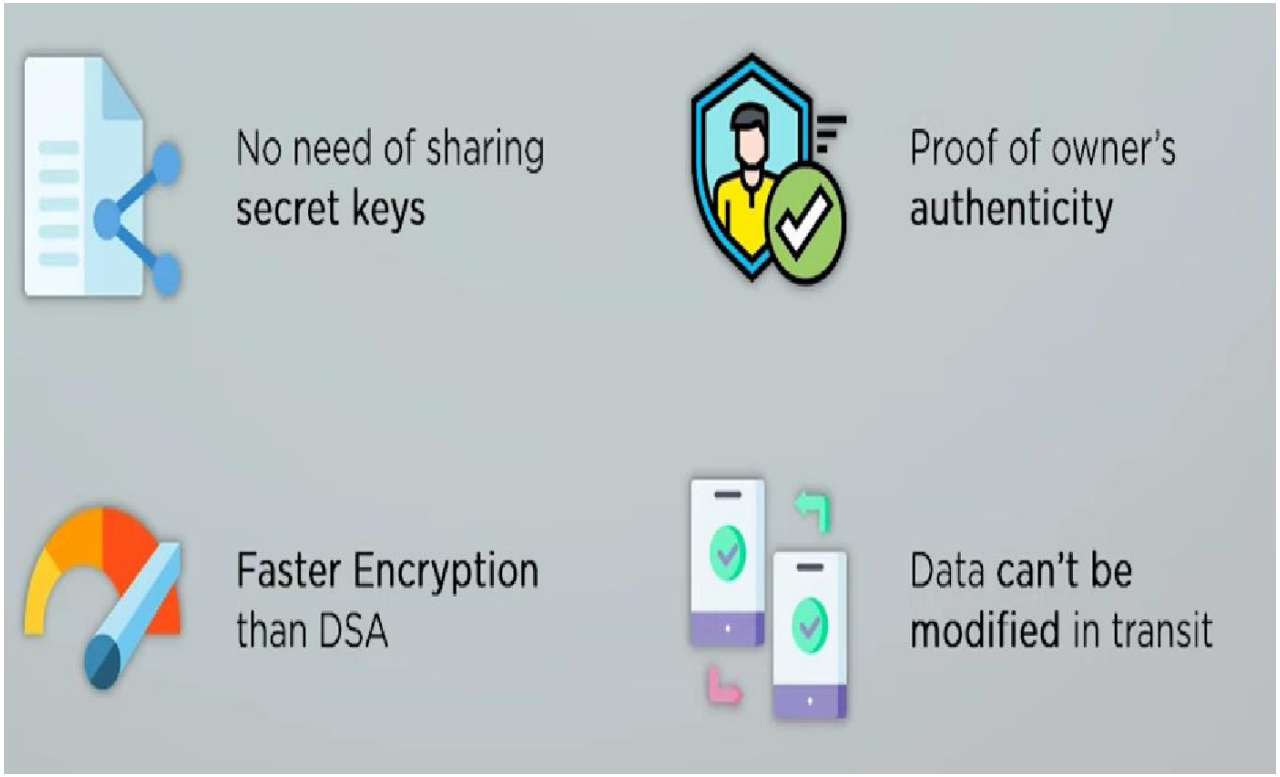
Note:
Calculate **Euler's totient** function:
$\varphi(n) = (p-1)\times(q-1)$

1. Pick two **large prime numbers**, say **p** and q.
2. Compute their product: $n = p \times q$

Note: This **n** is part of both the **public** and private **keys**.

3. e is **co-prime**
4. **d** as the **modular multiplicative inverse** of e mod $\varphi(n)$

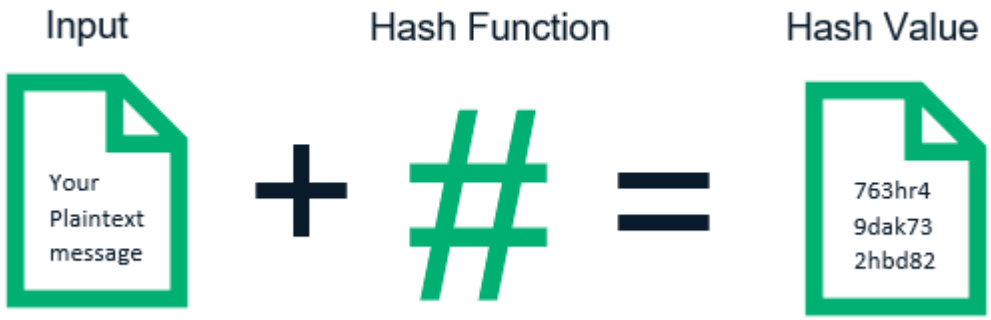
RSA- Advantages



DSA: Digital Signature Algorithm

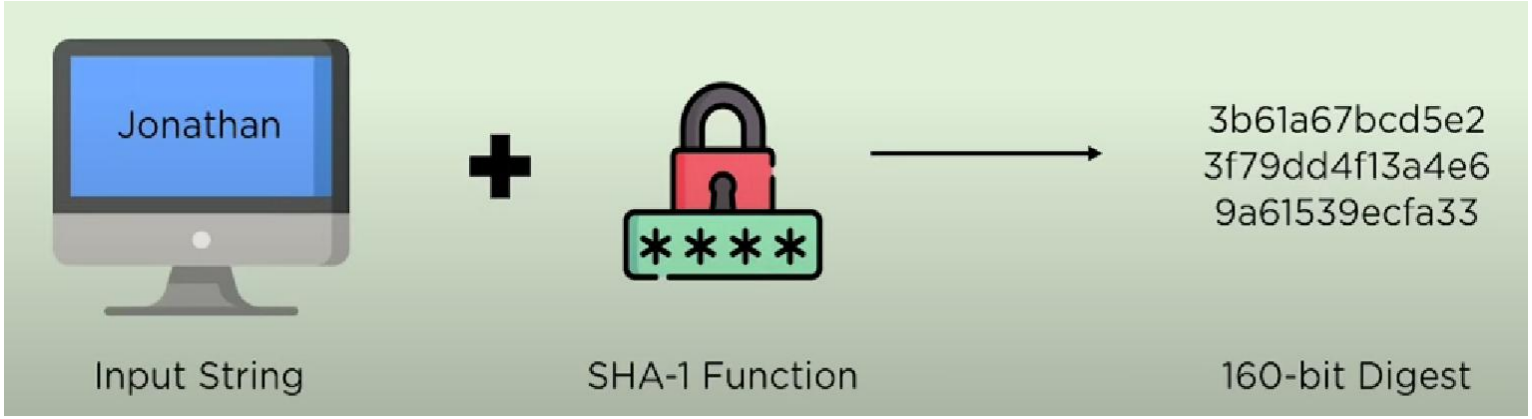
Hashing

Hashing



- In hashing, a **fixed length message digest** is created out of a variable length message.
- The digit is normally **much smaller** than the message.
- Hashing is used to provide **check values.**

Hashing-SHA



- Secure Hash Algorithm
- Has Multiple families such as SHA-0, SHA-1, SHA-2, SHA-3

Applications of SHA

Digital Signature Verification

Password Hashing

SSL Handshake in browsing

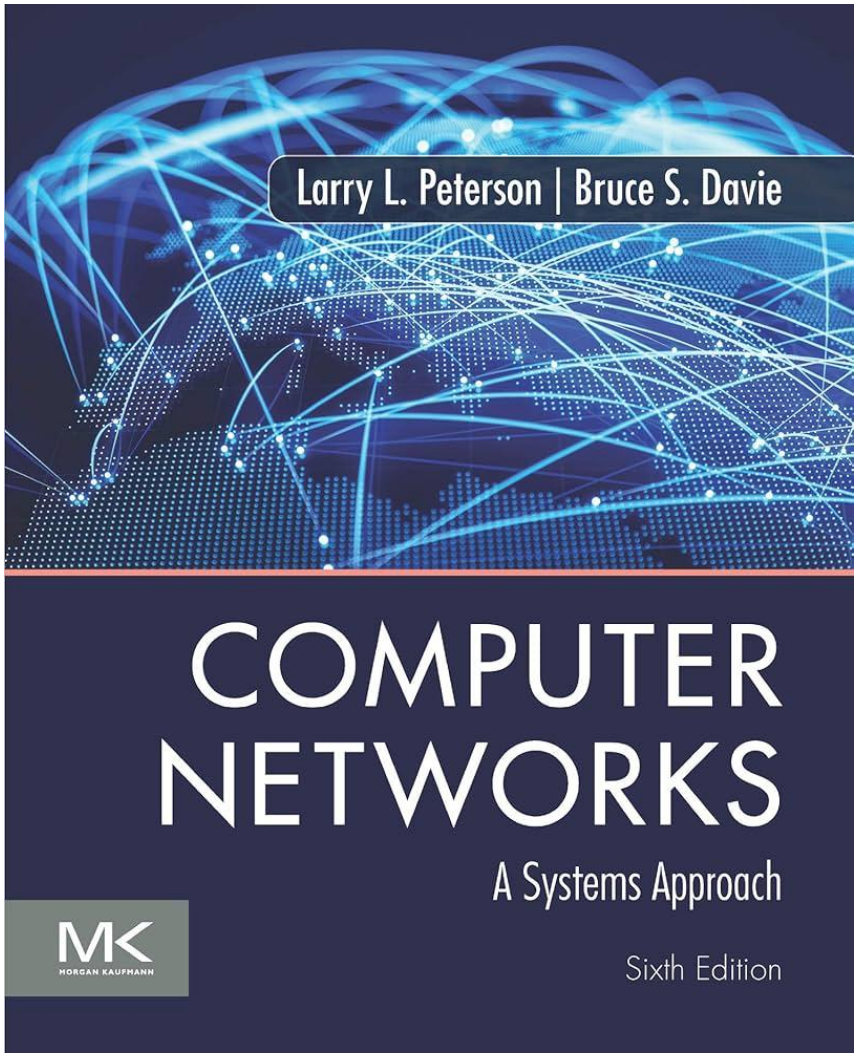
Integrity checks

Session 9B: Summary

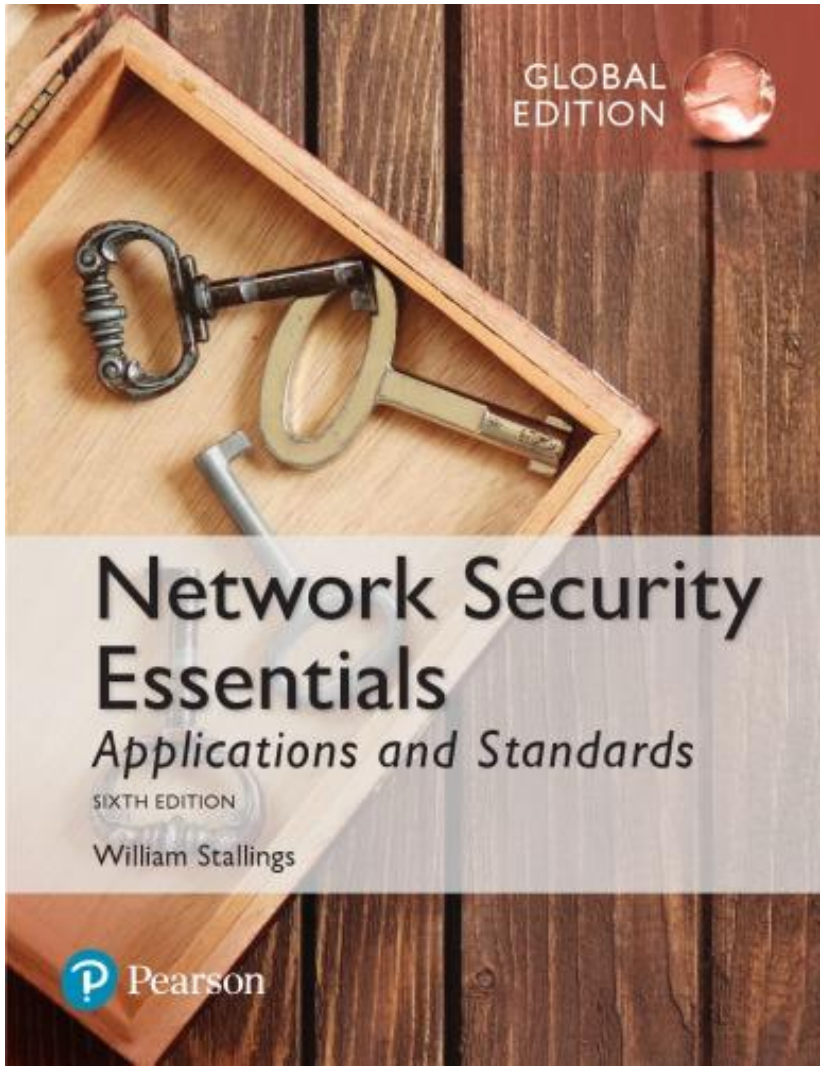
- Types of Encryption
  - Stream Ciphers
  - Block Ciphers
- Cryptographic Techniques
  - Symmetric key Encipherment
  - Asymmetric key Encipherment
  - Hashing

Textbooks

Textbook 1

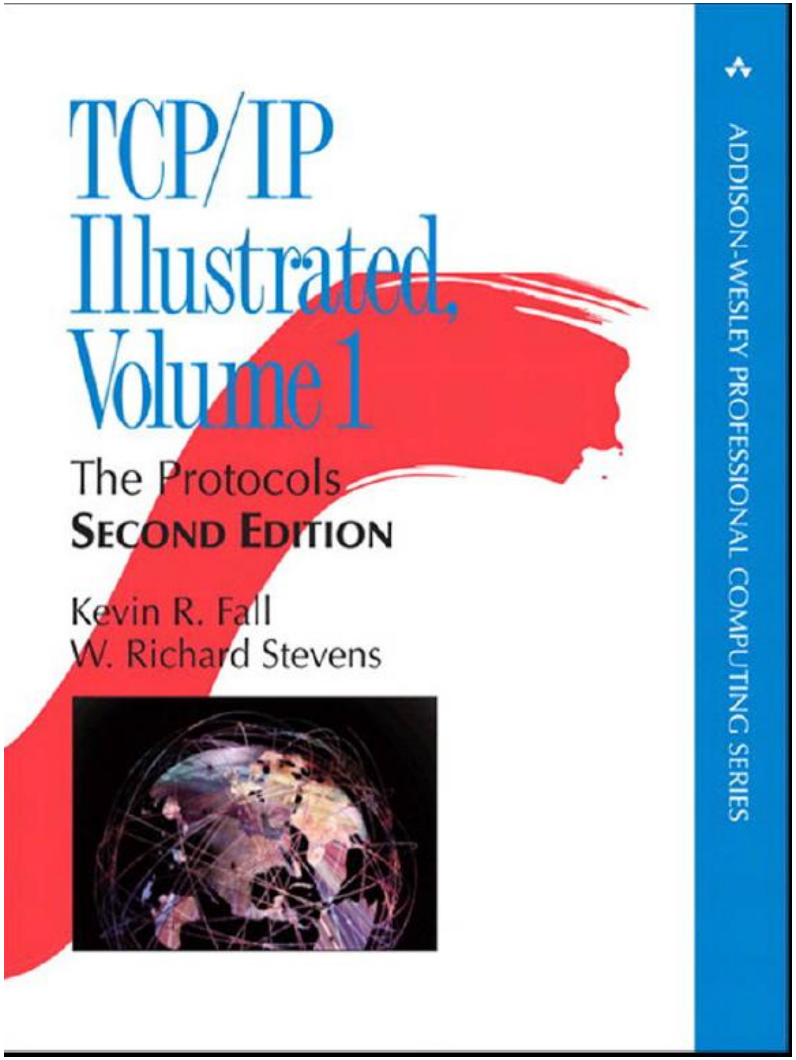


Textbook 2



References

Ref 1



Ref 2

TCP Congestion Control: A Systems Approach

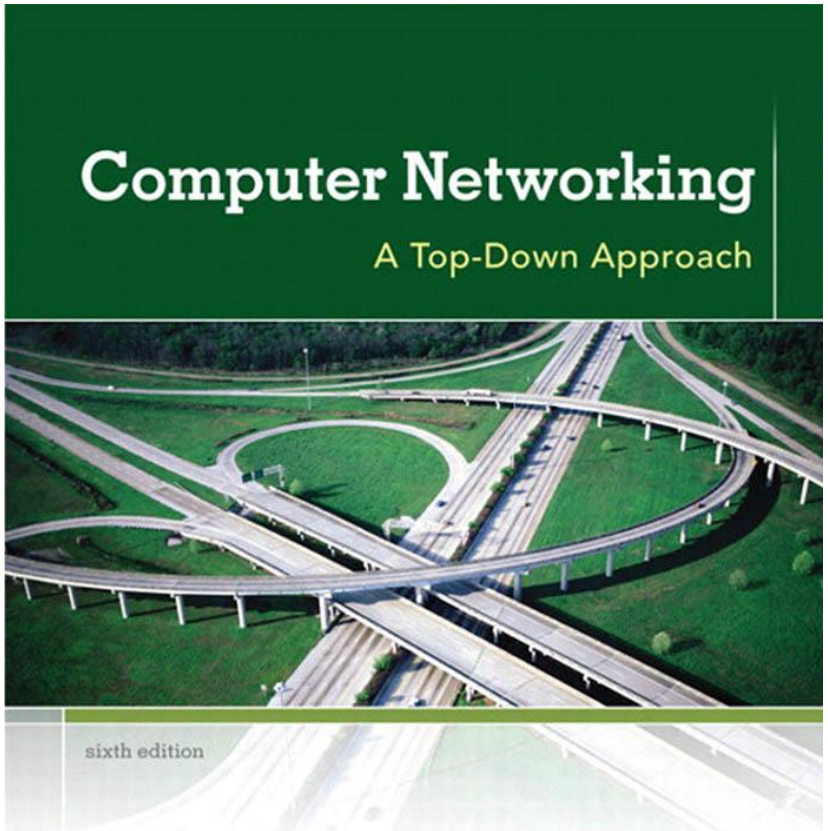
HTTPS://SYSTEMSAPPROACH.ORG

TCP Congestion Control: A Systems Approach

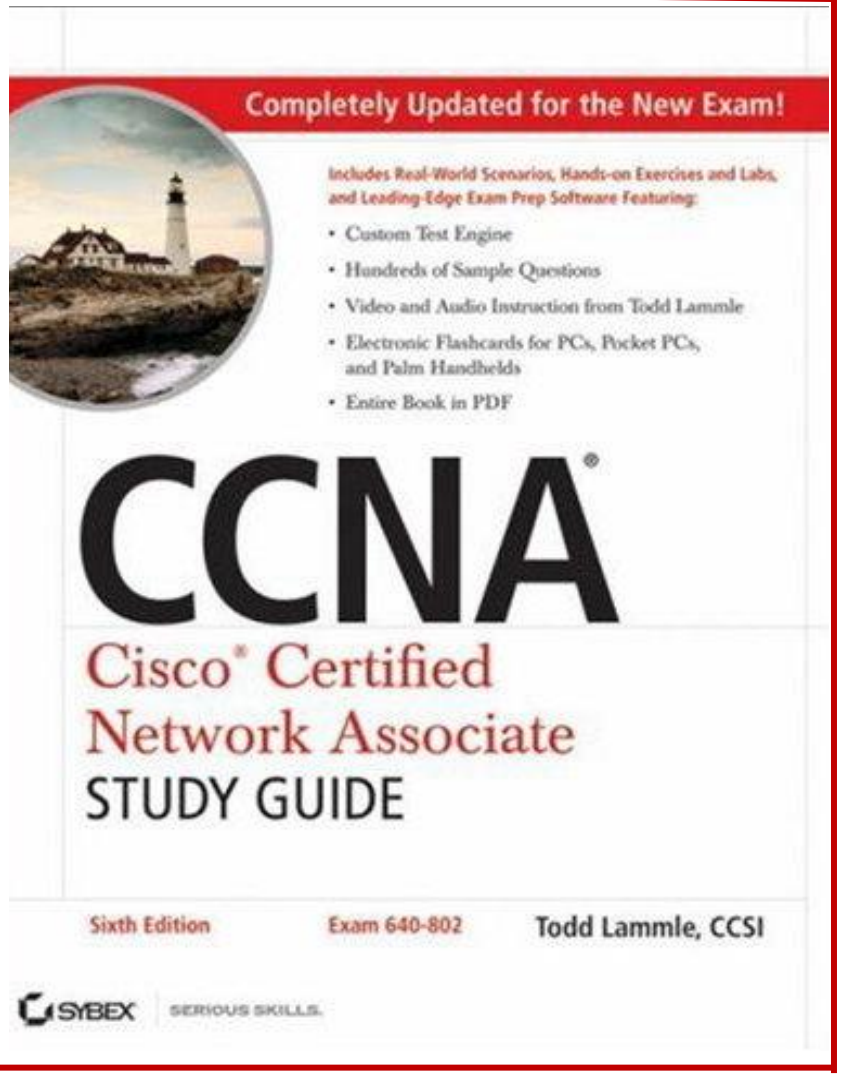
Peterson, Brakmo, and Davie

References

Ref 3



Ref 4



References

Ref 5