UNPREDICTABILITY

- In applications such as reciprocal authentication and session key generation, the requirement is not so much that the sequence of numbers be statistically random but that the successive members of the sequence are unpredictable
- With "true" random sequences, each number is statistically independent of other numbers in the sequence and therefore unpredictable
- Care must be taken that an opponent not be able to predict future elements of the sequence on the basis of earlier elements

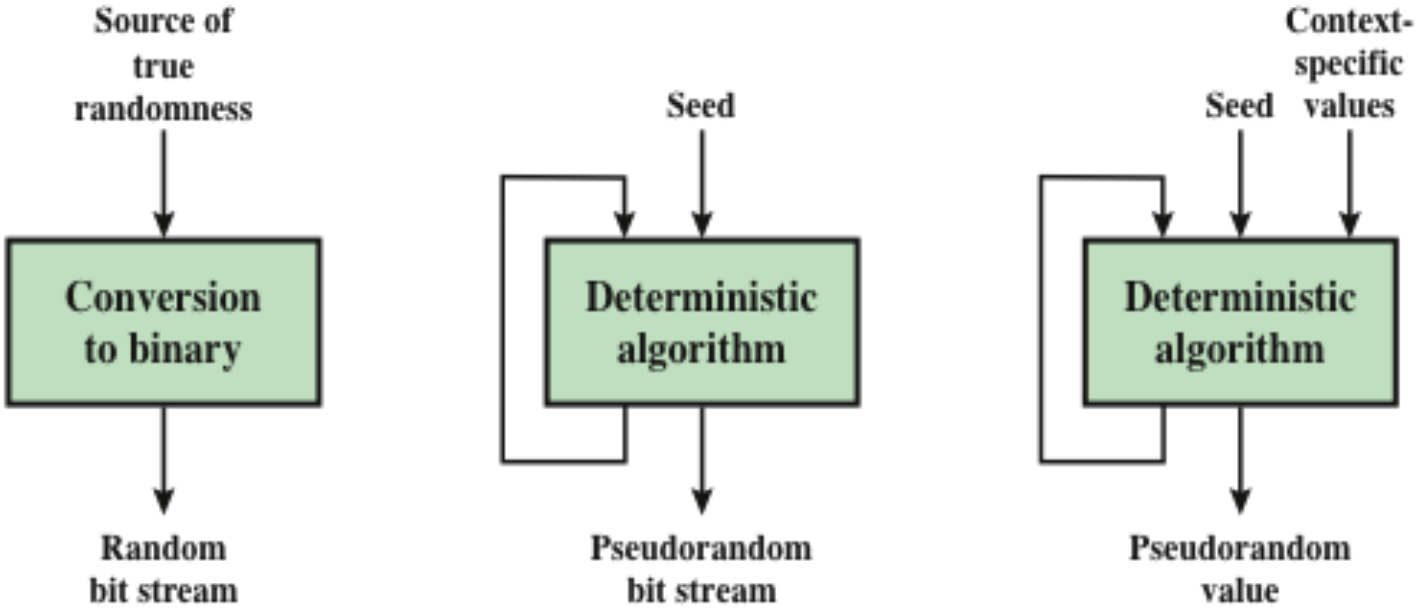


Figure 2.6 Random and Pseudorandom Number Generators

ALGORITHM DESIGN

Purpose-built algorithms	• Designed specifically and solely for the purpose of generating pseudorandom bit streams
Algorithms based on existing cryptographic algorithms	• Cryptographic algorithms have the effect of randomizing input • Can serve as the core of PRNGs
Three broad categories of cryptographic algorithms are commonly used to create PRNGs:	• Symmetric block ciphers • Asymmetric ciphers • Hash functions and message authentication codes

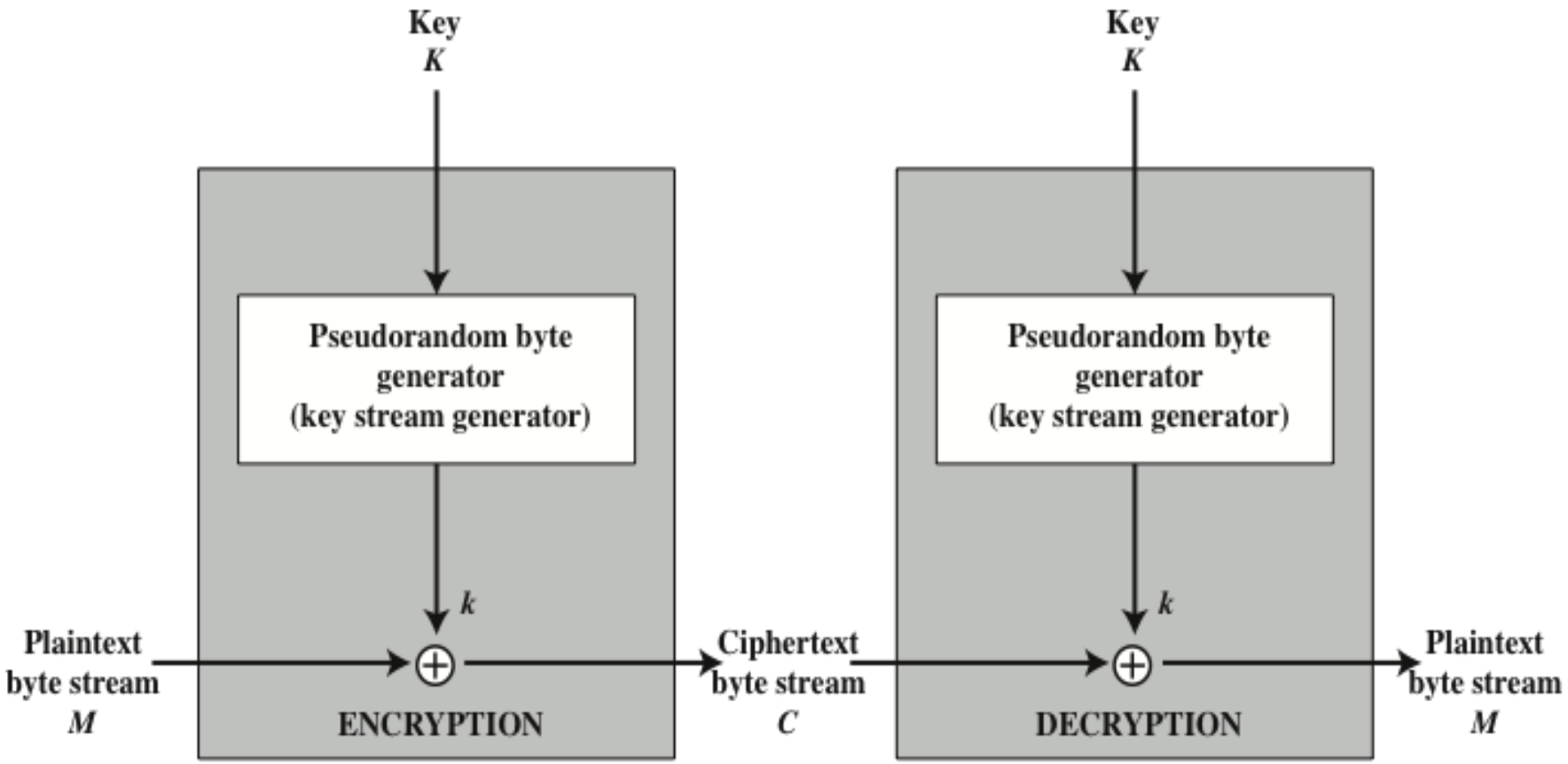


Figure 2.7 Stream Cipher Diagram

Stream Cipher Design Considerations

- The encryption sequence should have a large period
  - The longer the period of repeat, the more difficult it will be to do cryptanalysis
- The keystream should approximate the properties of a true random number stream as close as possible
  - The more random-appearing the keystream is, the more randomized the ciphertext is, making cryptanalysis more difficult
- The pseudorandom number generator is conditioned on the value of the input key
  - To guard against brute-force attacks, the key needs to be sufficiently long
  - With current technology, a key length of at least 128 bits is desirable

RC4 ALGORITHM

- A stream cipher designed in 1987 by Ron Rivest for RSA Security
- It is a variable key-size stream cipher with byte-oriented operations
- The algorithm is based on the use of a random permutation
- Is used in the Secure Sockets Layer/Transport Layer Security (SSL/TLS) standards that have been defined for communication between Web browsers and servers
- Also used in the Wired Equivalent Privacy (WEP) protocol and the newer WiFi Protected Access (WPA) protocol that are part of the IEEE 802.11 wireless LAN standard

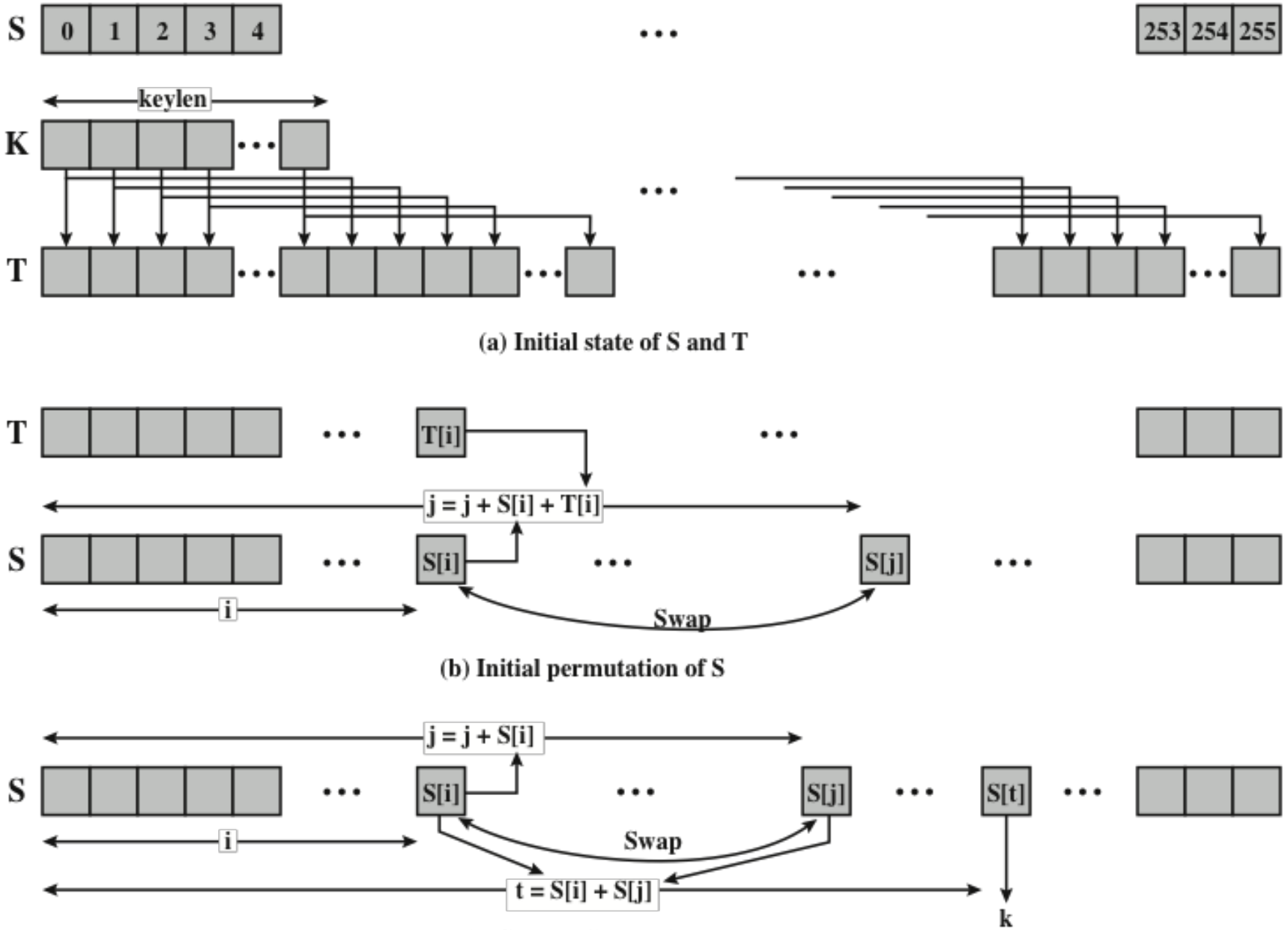


Figure 2.8 RC4

CIPHER BLOCK MODES OF OPERATION

- A symmetric block cipher processes one block of data at a time
  - In the case of DES and 3DES, the block length is b=64 bits
  - For AES, the block length is b=128
  - For longer amounts of plaintext, it is necessary to break the plaintext into b-bit blocks, padding the last block if necessary
- Five modes of operation have been defined by NIST
  - Intended to cover virtually all of the possible applications of encryption for which a block cipher could be used
  - Intended for use with any symmetric block cipher, including triple DES and AES

ELECTRONIC CODEBOOK MODE (ECB)

- Plaintext is handled *b* bits at a time and each block of plaintext is encrypted using the same key
- The term "codebook" is used because, for a given key, there is a unique ciphertext for every *b*-bit block of plaintext
  - One can imagine a gigantic codebook in which there is an entry for every possible *b*-bit plaintext pattern showing its corresponding ciphertext
- With ECB, if the same *b*-bit block of plaintext appears more than once in the message, it always produces the same ciphertext
  - Because of this, for lengthy messages, the ECB mode may not be secure
  - If the message is highly structured, it may be possible for a cryptanalyst to exploit these regularities

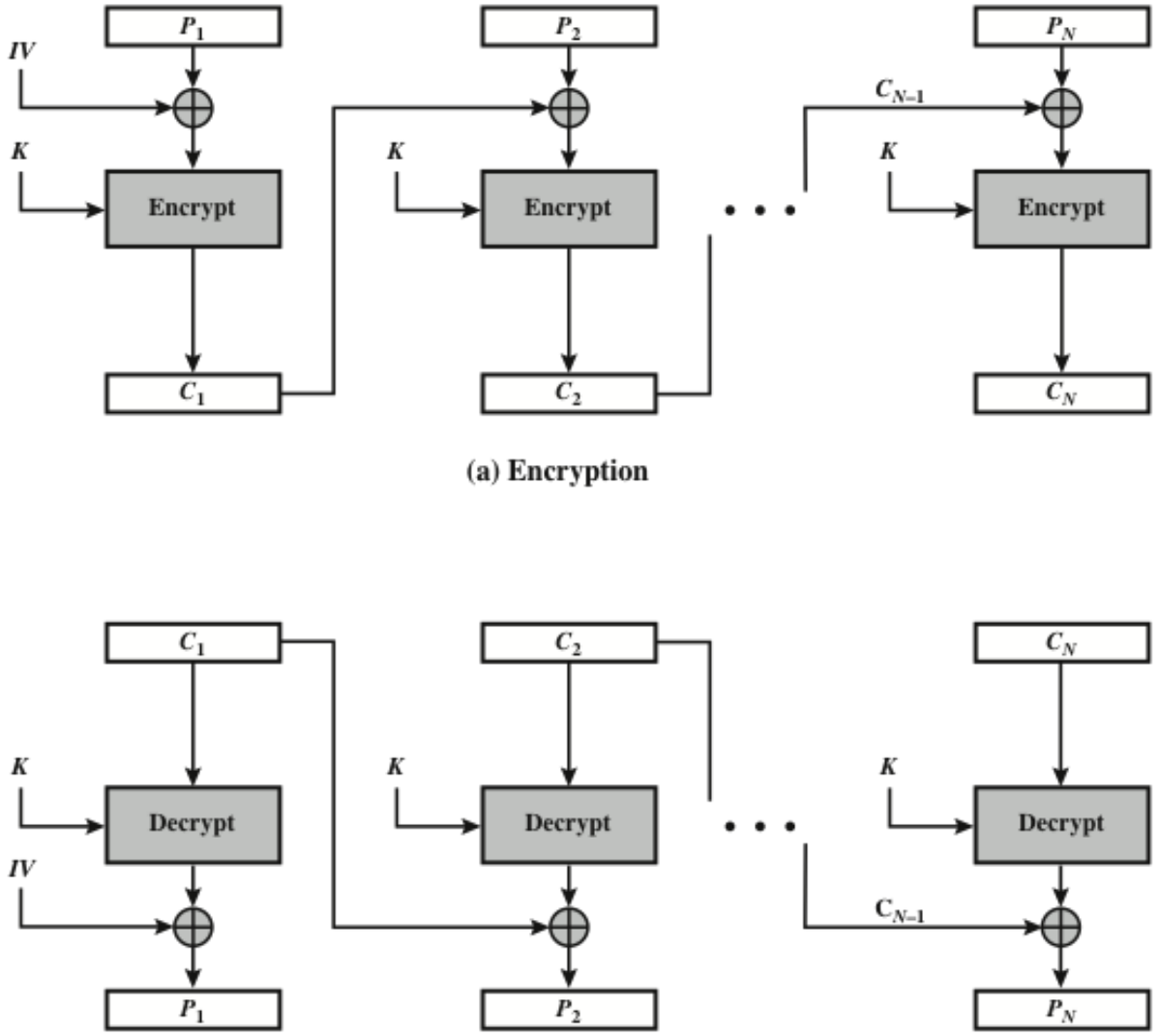
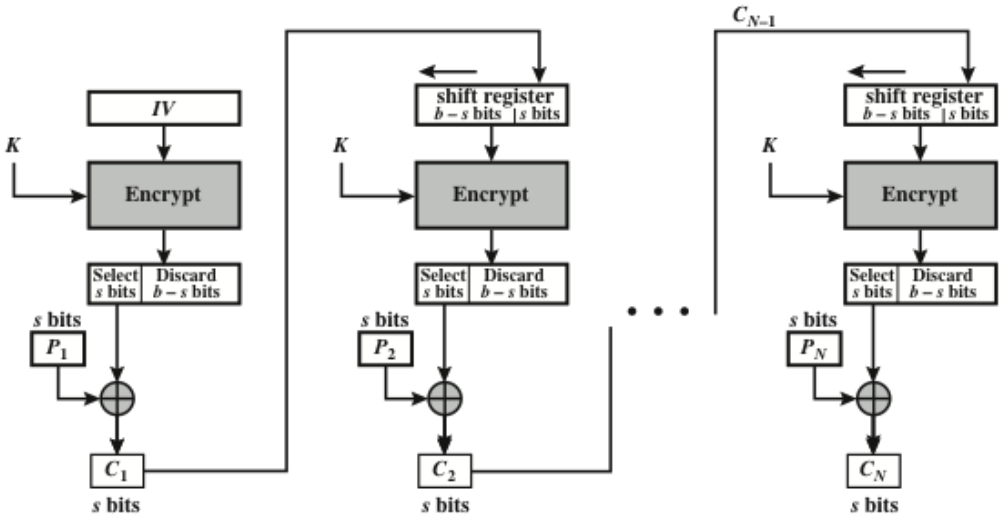
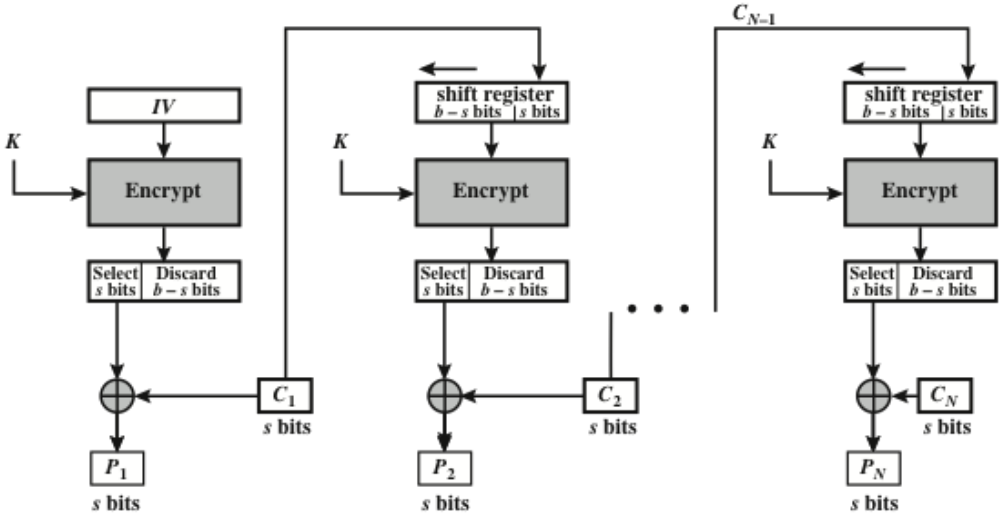


Figure 2.9 Cipher Block Chaining (CBC) Mode



(a) Encryption



(b) Decryption

Figure 2.10 *s*-bit Cipher Feedback (CFB) Mode

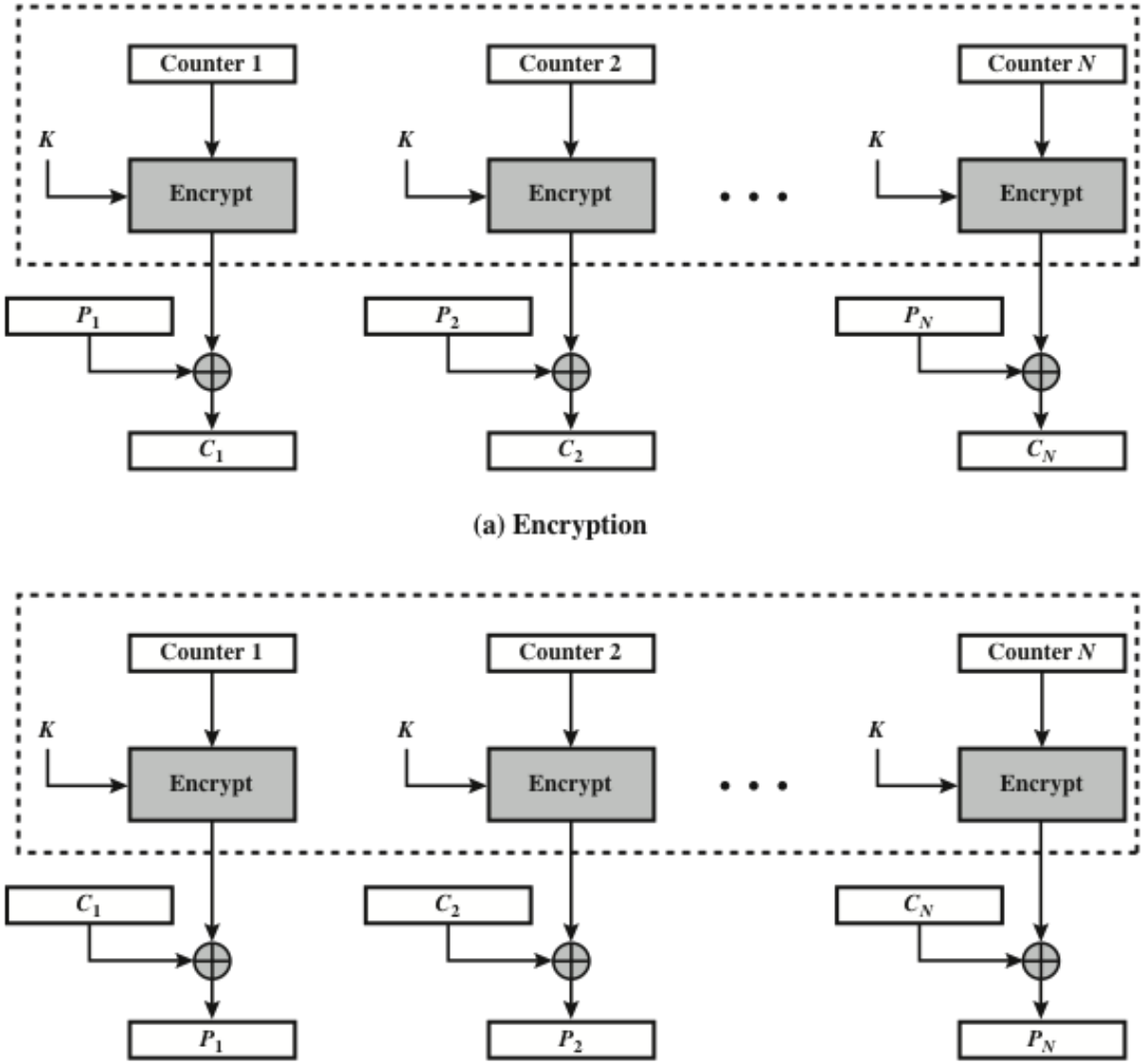


Figure 2.11 Counter (CTR) Mode

ADVANTAGES OF CTR MODE

- Hardware efficiency
  - Encryption/decryption can be done in parallel on multiple blocks of plaintext or ciphertext
  - Throughput is only limited by the amount of parallelism that is achieved
- Software efficiency
  - Because of the opportunities for parallel execution, processors that support parallel features can be effectively utilized
- Preprocessing
  - The execution of the underlying encryption algorithm does not depend on input of the plaintext or ciphertext --- when the plaintext or ciphertext input is presented, the only computation is a series of XORs, greatly enhancing throughput
- Random access
  - The *i*th block of plaintext or ciphertext can be processed in random-access fashion
- Provable security
  - It can be shown that CTR is at least as secure as the other modes discussed in this section
- Simplicity
  - Requires only the implementation of the encryption algorithm and not the decryption algorithm

SUMMARY

- Symmetric encryption principles
  - Cryptography
  - Cryptanalysis
  - Feistel cipher structure
- Symmetric block encryption algorithms
  - Data encryption standard
  - Triple DES
  - Advanced encryption standard
- Random and pseudorandom numbers
  - The use of random numbers
  - TRNGs, PRNGs, PRFs
  - Algorithm design
- Stream ciphers and RC4
  - Stream cipher structure
  - RC4 algorithm
- Cipher block modes of operation
  - ECB
  - CBC
  - CFB
  - CTR