EWD – Security part

Encryption algorithms

Symmetric Block Ciphers

XOR

- Modern techniques use bits rather than text letters
- Most transformations use eXclusive OR
- **Revsersibility** and **speed** are the main benefits of using XOR

XOR truth table:

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

XOR properties:

$A \oplus A = 0$

$A \oplus 0 = A$

$(A \oplus B) \oplus B = A$

Block Cipher

- A block cipher divides the plaintext into fixed-sixed blocks and transforms each block into a corresponding block of ciphertext
- Padding is required where the plaintext size is not an integer multiple of the block size
- Iterated block ciphers are based on a number of rounds where a round function is applied at each round.
- The round function usually takes a round key as one of its inputs.
  - Each round key based on bits extracted from the key

DES

- Data Encryption Standard (1976)
- Block size: 64 bits
- Key size: 56 bits
- No. of rounds: 16
- Based on design by Horst Feistel, IBM
  - Chosen by NBS (now called NIST), US national standards body
  - Influenced by NSA
- Very influential algorithm
- Now obsolete, but lives on in Triple DES (3DES)

AES

- Advanced Encryption Standard (2001)
- Chosen by design competition
  - Organised by NIST (US National Standards Inst.)
  - Winner: Rijndael (Belgium)
- Block size: 128 bits
- Key sizes: 128, 192, 256
- Relatively small memory requirement
- Suitable for variety of hardware and software architectures
- Royalty-free
- Considered secure
- Very widely used

AES

- You can find a nice AES animation here:

  http://www.securityfit.cz/download/kib/rijndael_ingles2004.swf

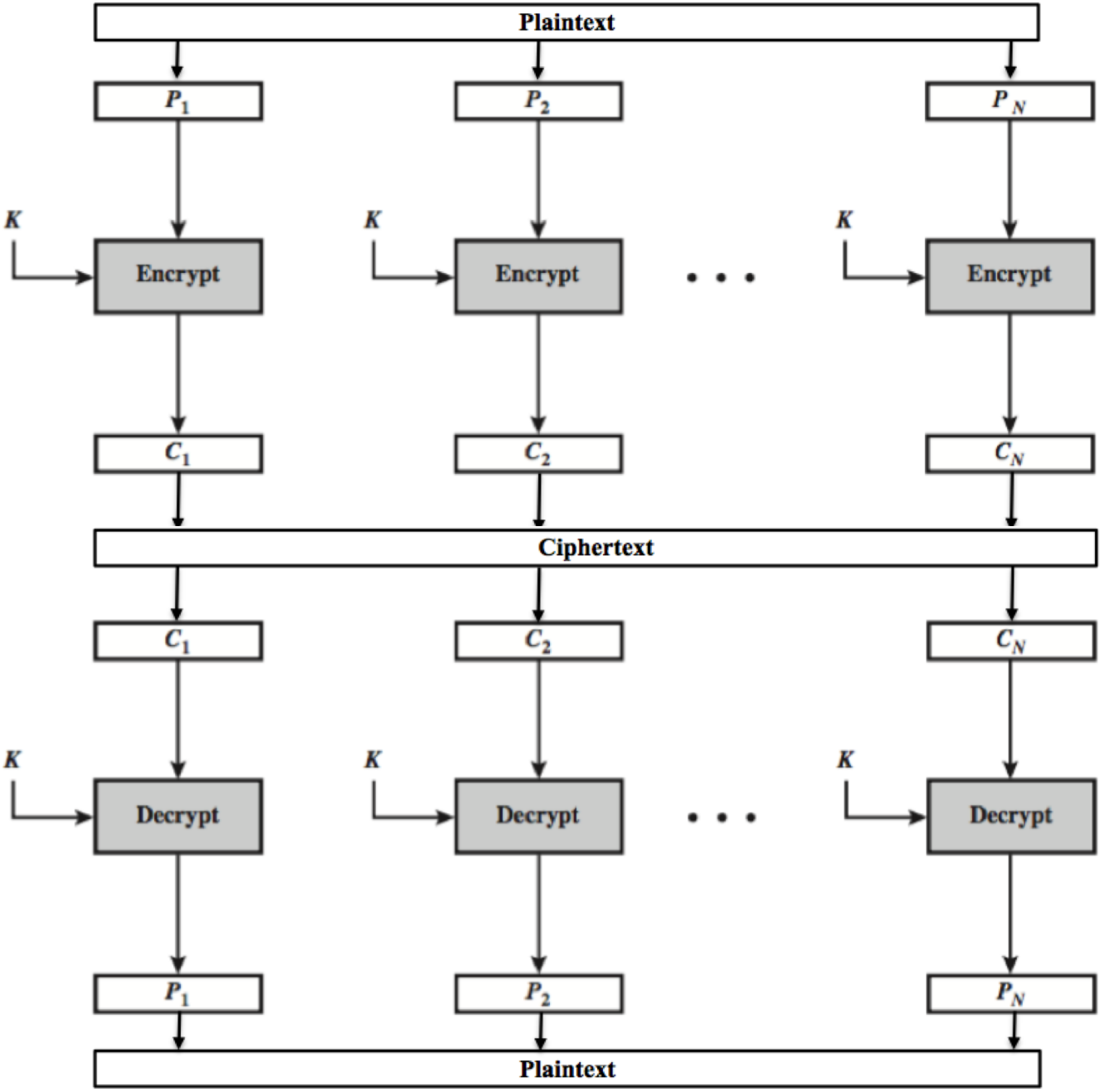
  or **http://tinyurl.com/aesflash**

Block Cipher – modes of operation

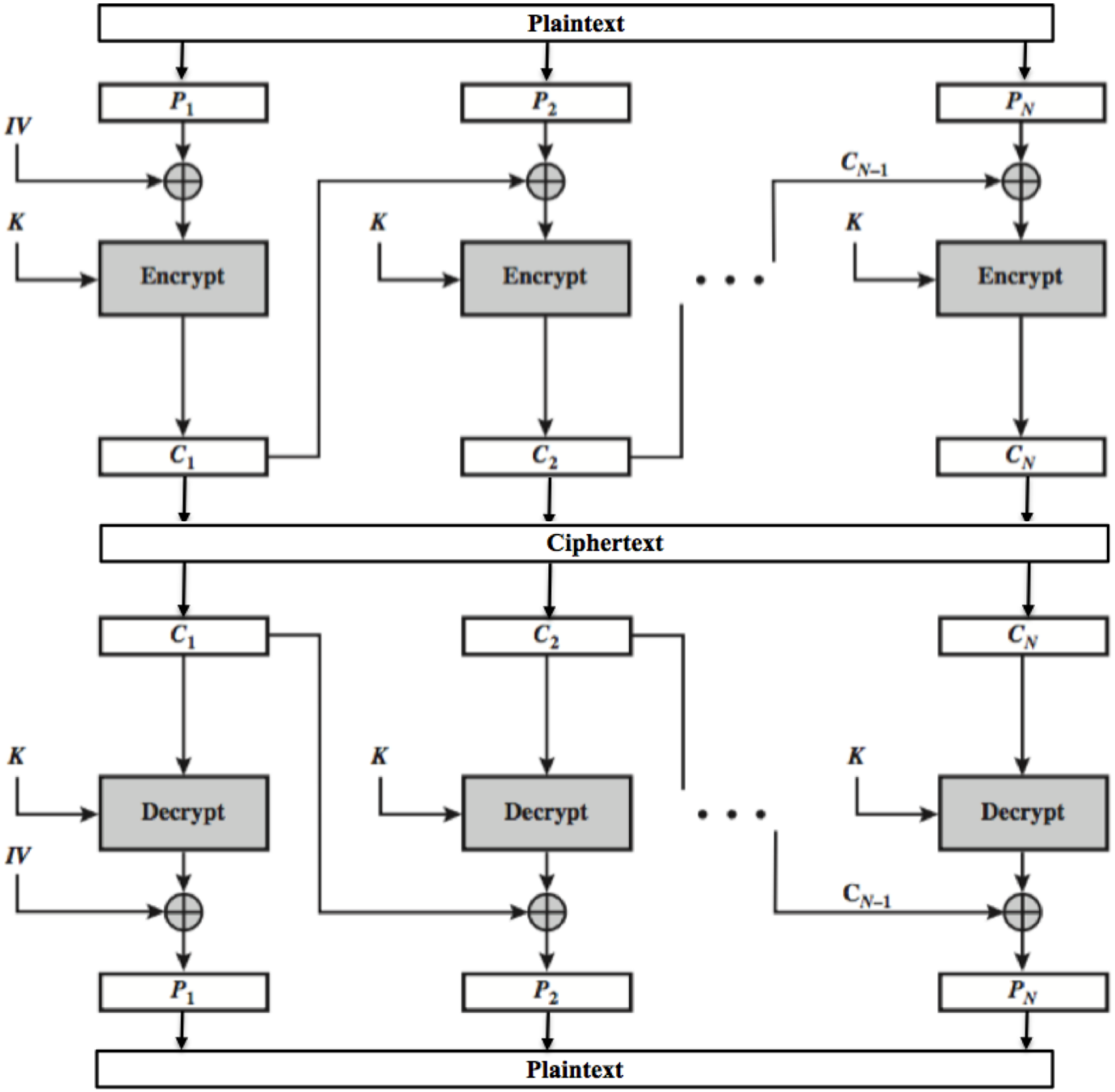
- Electronic Codebook (ECB) mode
  - Each block treated independently.
  - Insecure, as repeated plaintext blocks map to repeated ciphertext blocks
- Cipher Block Chaining (CBC) mode
  - Each plaintext block XORed with previous ciphertext block before encryption
- Counter (CTR) mode
  - For each plaintext block encrypt a counter and XOR the result with the plaintext block. Increment the counter for the next block

Electronic Codebook Mode (ECB) Encryption

ECB Decryption



Cipher Block Chaining (CBC) Encryption

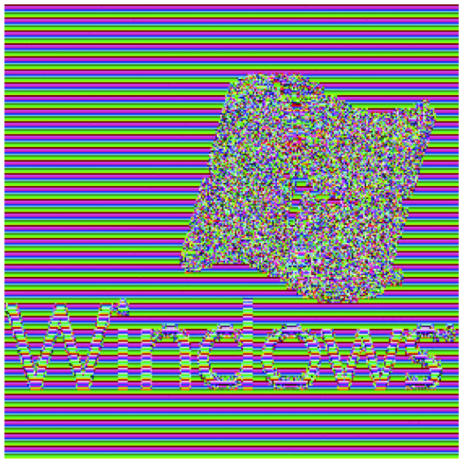


CBC Decryption

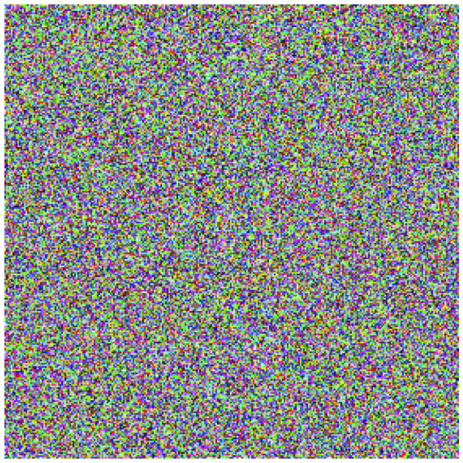
Comparing CBC with ECB

- Codebooks are a problem as patterns in the plaintext may remain in the ciphertext

Plaintext



Ciphertext (ECB)

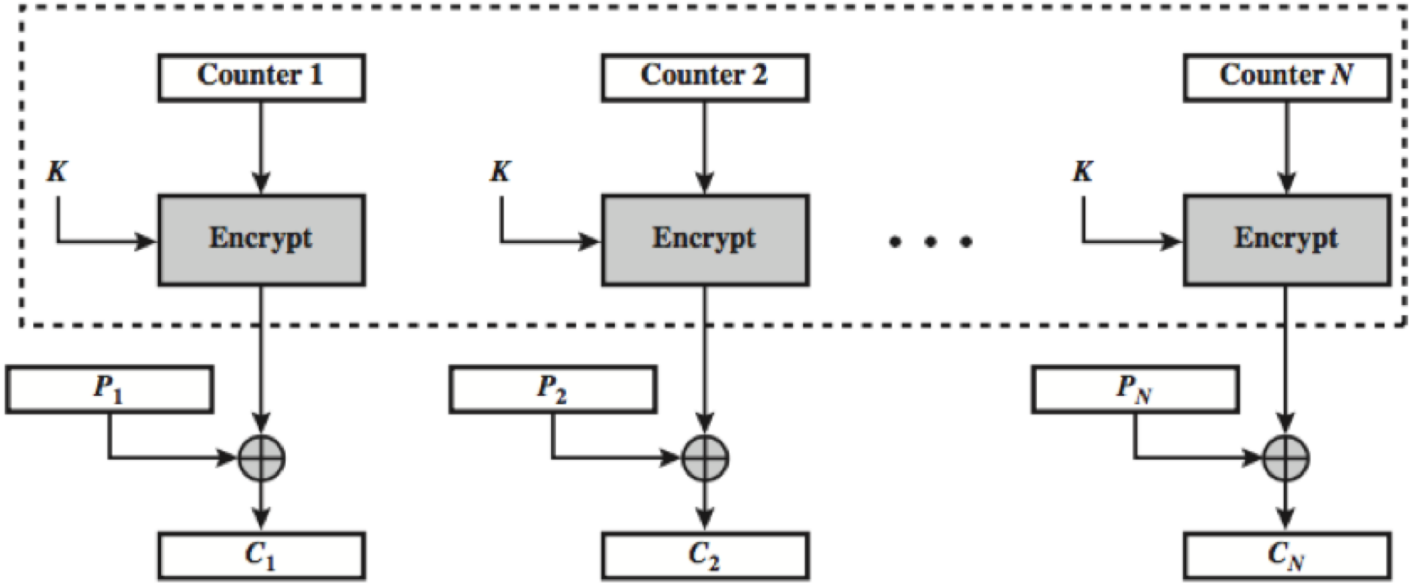


Ciphertext (CBC)

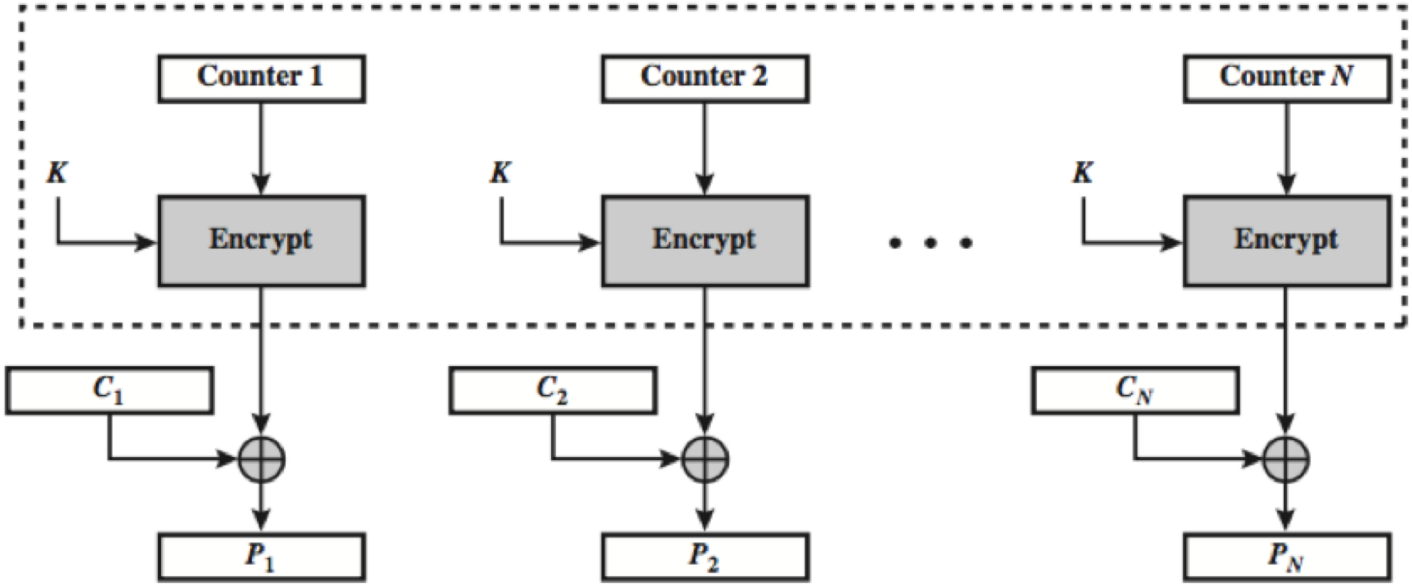
Source: msdn.microsoft.com

Counter Mode (CTR)

Most popular implementation is slightly more elaborate version than this, known as Galois/Counter Mode (GCM)



(a) Encryption



(b) Decryption

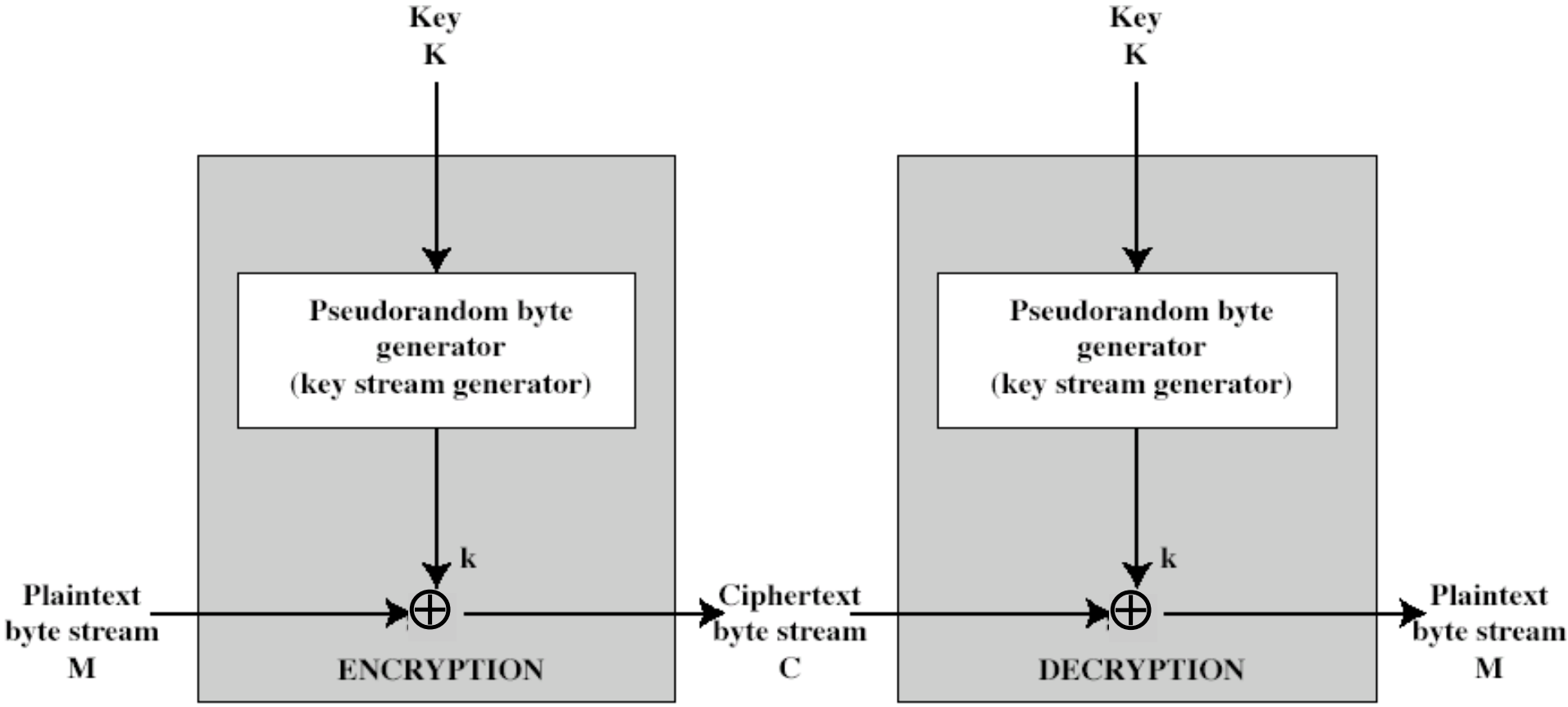
Stream Ciphers

Stream Ciphers

- Process message “continuously”
  - Optimised for real-time and two-way comms
  - Usually one byte at a time
  - As distinct from a block cipher

- Typically simple XOR of each plaintext bit with the output of a pseudo-random number generator (PRNG)

Stream Cipher Structure



$C_i = M_i \oplus k_i$

$M_i = C_i \oplus k_i$

Danger with Stream Cipher

- If plaintext-ciphertext pairs can be gathered, then it is easy to record the keystream:
  - as $M_i \oplus C_i = k_i$

- Thus the cipher is broken if any way to predict key stream for next ciphertext
- Key streams should never be re-used (or re-started with the same seed)

Public-key Algorithms

Trapdoor functions

- Public-key cryptography relies on functions that are computationally easy in one direction and computationally infeasible in the other
- Examples:

"Easy" problem	"Hard" problem	Technique
Multiplying prime numbers, $n = pq$	Factoring n	RSA
Modular exponentiation, $g^x \pmod{n}$	Calculating discrete log; solving for x in $a = g^x \pmod{n}$	Diffie-Hellmann
Elliptic curve point multiplication, $R = kP$	Finding elliptic curve multiplicand, k	Elliptic curve cryptography

RSA

- Rivest, Shamir & Adleman, MIT, 1977
- Very well known versatile public-key scheme
- Uses large integers as keys (>1000 bits)
- Security due to extreme difficulty of factoring large “semiprime” integers
  - i.e. factoring product of two prime numbers

RSA

- Based on three related integers: e, d, n
- RSA function ("encryption"):
  - Input: $M < n$
  - Output: $C = M^e \pmod{n}$
- Inverse RSA ("decryption"):
  - Input: C
  - Output: $M = C^d \pmod{n}$

d and e are mathematically related: e is chosen and d is calculated from e and the **factors** of n

Diffie-Hellman

- Public-key Technique for exchanging secret keys
  - First public-key technique (1976)
- The secret key is calculated by both parties
- Requires some global public parameters
- Based on difficulty in solving for x:

$$a = g^x \pmod{n}$$

a, g, n known

Elliptic Curve Cryptography

- Majority of public-key crypto (RSA, D-H) use either integer or polynomial arithmetic with very large numbers/polynomials
- Imposes a significant load in storing and processing keys and messages
- An alternative is to use elliptic curves
- Offers same security as RSA with smaller bit sizes and lower processing and memory overhead
- Recent growth in use