# CSC429 – Computer Security

LECTURE 2
MODERN CRYPTOGRAPHY

**Mohammed H. Almeshekah, PhD**
**meshekah@ksu.edu.sa**

# Modern Cryptography

- One thread of defeating frequency analysis
  - Use different keys in different locations
  - Example: one-time pad, stream ciphers
- Another way to defeat frequency analysis
  - Make the unit of transformation larger, rather than encrypting letter by letter, encrypting block by block
  - Example: block cipher

# Stream Ciphers

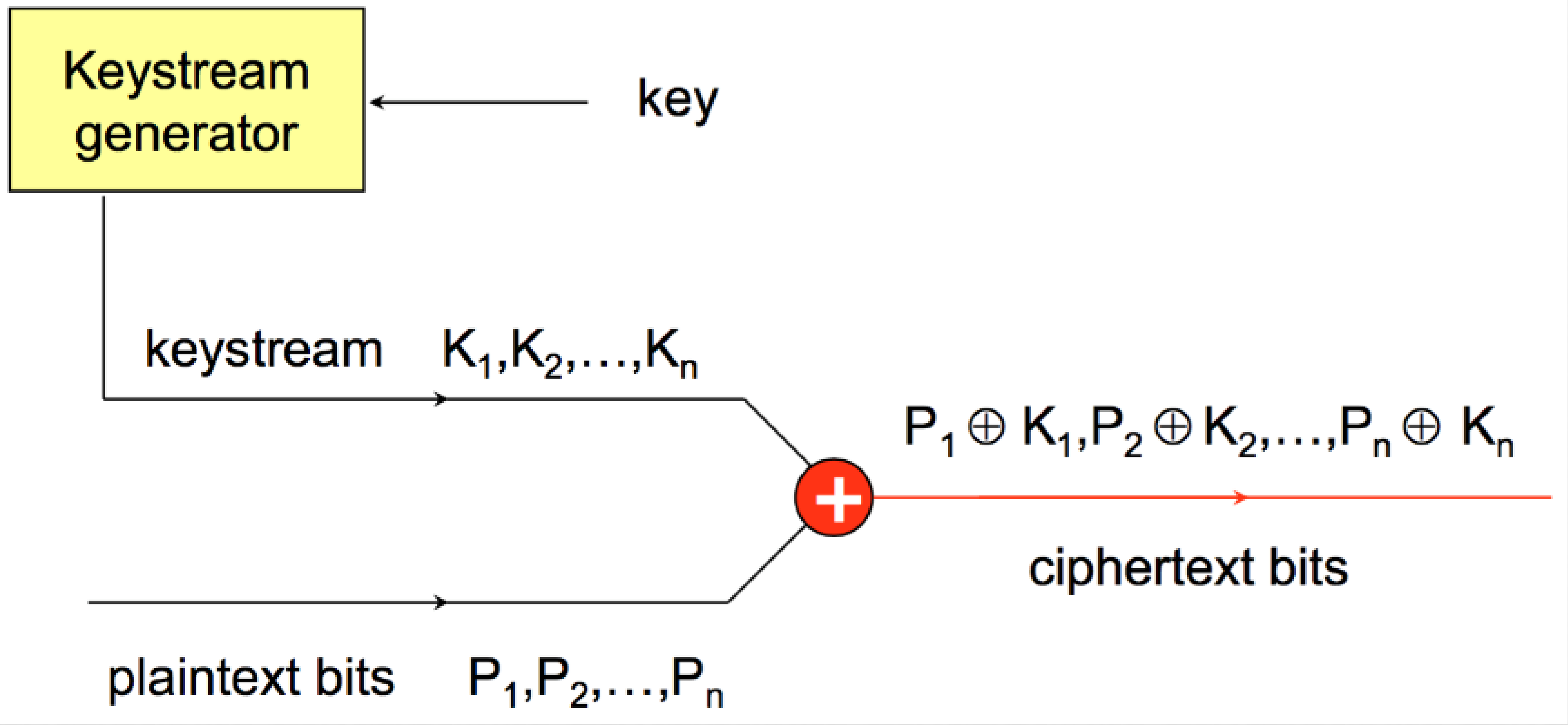
- In One-Time Pad, a key is a random string of length at least the same as the message.
  - Is this practical?

- Stream ciphers:
  - Idea: replace "rand" by "pseudo rand".
  - Use Pseudo Random Number Generator:
    - PRNG: $\{0,1\}^s \rightarrow \{0,1\}^n$
    - expand a short (e.g., 128-bit) random seed into a long (e.g., $10^6$ bit) string that "looks random".
  - Secret key is the seed
  - $E_{key}[M] = M \oplus PRNG(key)$

# Pseudo Random Number Generator (PRNG)

- Useful for cryptography and for simulation.
- The same seed gives the same output stream:
  - why is this necessary for stream ciphers?
- **Cryptographically secure pseudo-random number generator** requires unpredictable sequences
  - satisfies the "next-bit test“: given consecutive sequence of bits output (but not seed), next bit must be hard to predict
  - withstands “state compromise extensions” : given sequences from bits k+1 on, should be difficult to predict earlier bits
- Also useful for generating temporary keys, etc.

# Stream Cipher – Illustrated



# Properties of Stream Ciphers

- Typical stream ciphers are very fast.
- If the same stream is used twice ever, then easy to break.
- Highly malleable
  - Easy to change ciphertext so that plaintext changes in predictable, e.g., flip bits
  - which of the three properties (confidentiality, integrity, availability) is violated here?

# Stream Ciphers vs. OTP

- Length of keys: – keys are shorter

- Randomness of keys:
  - keys are pseudo-randomly generated

- One-time use of keys:
  - keys can be used once since they are “cheap”
  - can derive one-time keys from the initial key

# Example of Real Stream Ciphers

- RC4
  - Simple, fast stream cipher, with relatively low level of security
  - Most widely implemented stream cipher in software
  - Widely supported (for example in SSL/TLS, WEP and Microsoft Office)
- A5/1
  - Used in GSM to secure the radio link
- E0
  - Used in Bluetooth

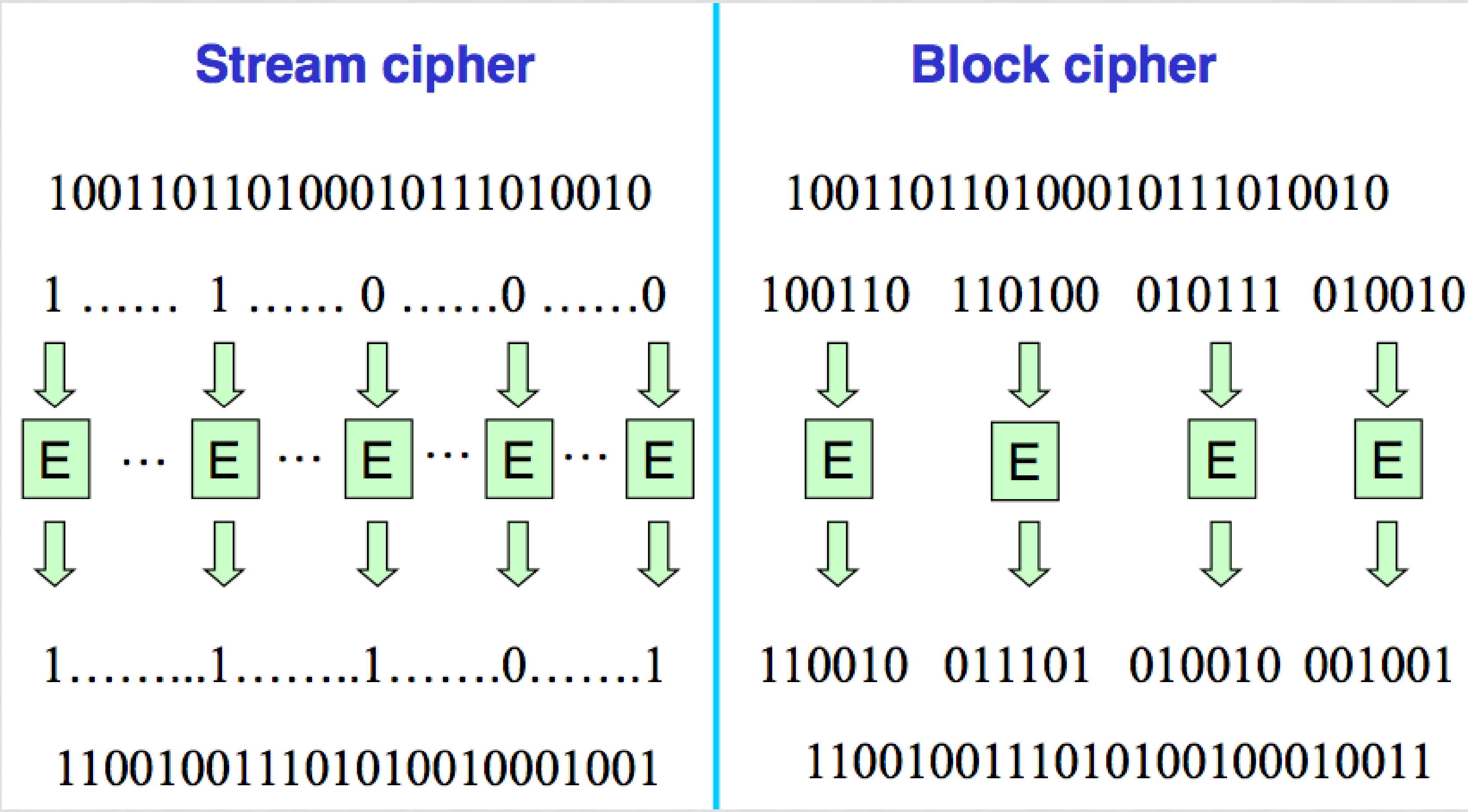
# Modern Cryptography

Block Ciphers

# Modern Cryptography – Revisit

- One thread of defeating frequency analysis
  - Use different keys in different locations
  - Example: one-time pad, stream ciphers
- Another way to defeat frequency analysis
  - Make the unit of transformation larger, rather than encrypting letter by letter, encrypting block by block
  - Example: block cipher

# Block vs. Stream Ciphers



# Block Ciphers

- An ideal block cipher is a substitution cipher from $\{0,1\}^n$ to $\{0,1\}^n$
  - Also known as a random permutation
  - Each key determines one permutation on the plaintext space

- Is this practical?
  - What is the total number of keys?
  - What is the length of a key?

# Practical Block Ciphers

- The best block cipher should be a pseudo-random permutation (PRP)

- For n-bit plaintext and ciphertext blocks and a fixed key, the encryption function is a bijection; $E : P_n \times K \rightarrow C_n$ s.t. for all key $k \in K$, $E(x, k)$ is an invertible mapping written $E_k(x)$.

- The inverse mapping is the decryption function, $y = D_k(x)$ denotes the decryption of plaintext x under k.

# Block Ciphers – Terminology

- Block size: in general larger block sizes mean greater security.
- Key size: in general  larger key size means greater security (larger key space).
- Encryption modes: define how messages larger than the block size are encrypted, very important for the security of the encrypted message.

# Next Lecture

- Modern Cryptography:
  - Block ciphers.
  - Hash Functions.
  - Message Authentication Codes.

- Readings for next lecture:
  - Anderson's book - sections (5.5), (5.3.1) and (5.6.2).