Cybersecurity

Block Ciphers and Lightweight Cryptography

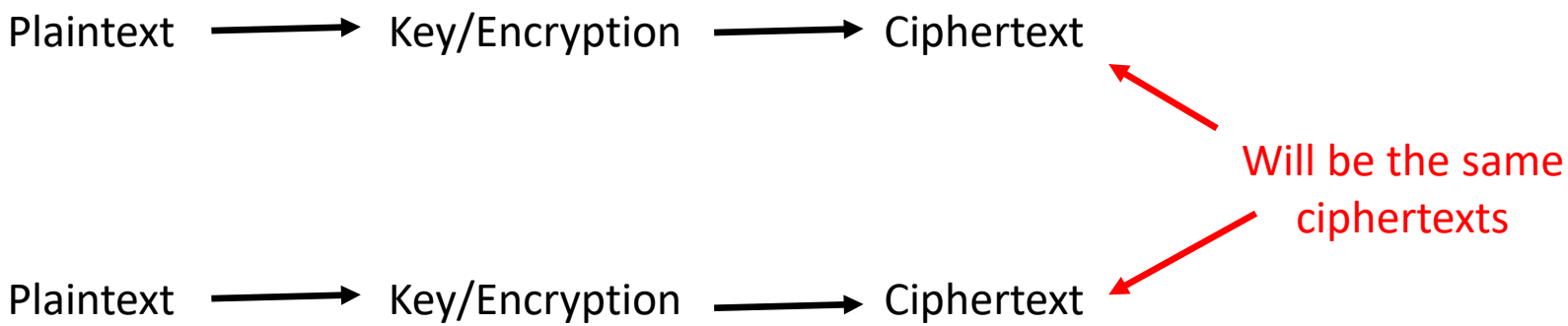
CYBER.ORG

Block cipher

- Break data into fixed-length groups known as blocks
- Process each block sequentially
- Mode of operation
  - Defines method
  - Provides authentication
- Block size does not change
  - Data may not evenly divide into blocks
  - May require padding before encryption
    - Padding = adding “filler” data
      - All zeros or some known, repeating pattern

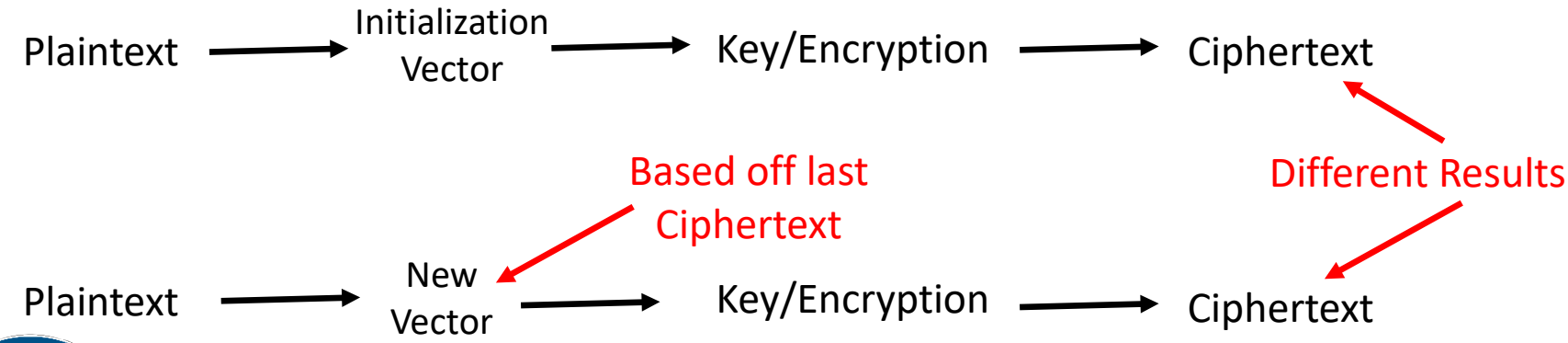
Electronic Codebook (ECB)

- Most simple encryption mode
- Each block encrypted with same key
  - Identical plaintext creates identical ciphertext



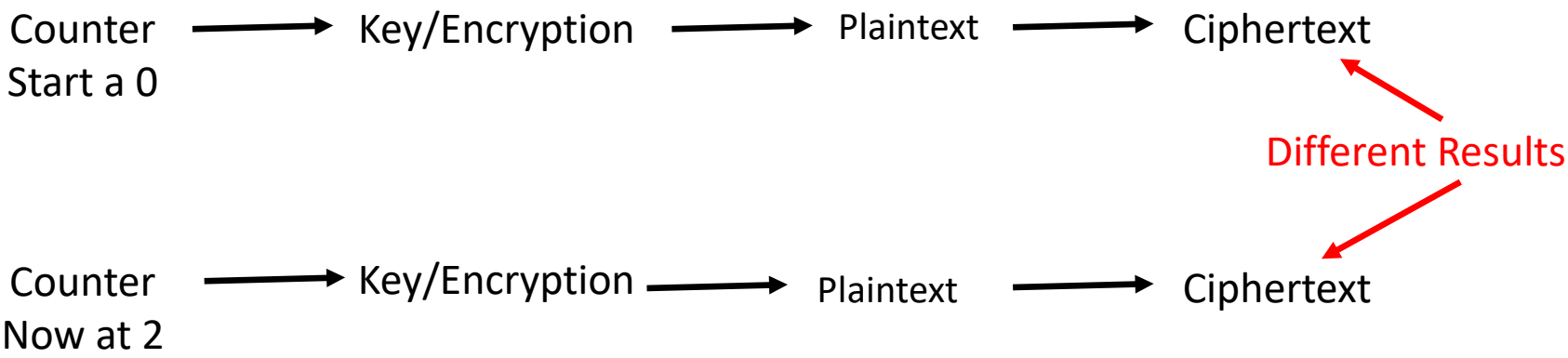
Cipher Block Chaining (CBC)

- Easy to implement, Popular
- Each block is XORed with *previous* ciphertext block
  - Adds additional obfuscation
  - First block does not have previous ciphertext so uses IV (Initialization Vector) as starting value



Counter (CTR)

- Block cipher but acts as stream cipher
  - Encrypts “counter” iterations
- Plaintext can vary in size since it’s part of the XOR operation
  - e.g. 16 bits at a time (stream) instead of a 128-bit block



Galois/Counter Mode (GCM)

- Encryption with authentication
  - Authentication (integrity of data) is part of algorithm
  - Combines Counter Mode with authentication
  - Like CTR, block encryption that acts like a stream cipher
- Very efficient
- Commonly used on data packets
  - Network traffic security (wireless, IPSec)
  - SSH, TLS
- Variant known as GMAC
  - Galois Message Authentication Code

Lightweight Cryptography

- Requires low computational complexity
- Not useful on high powered devices
- Useful with international guidelines