CS326 – Systems Security

Lecture 7

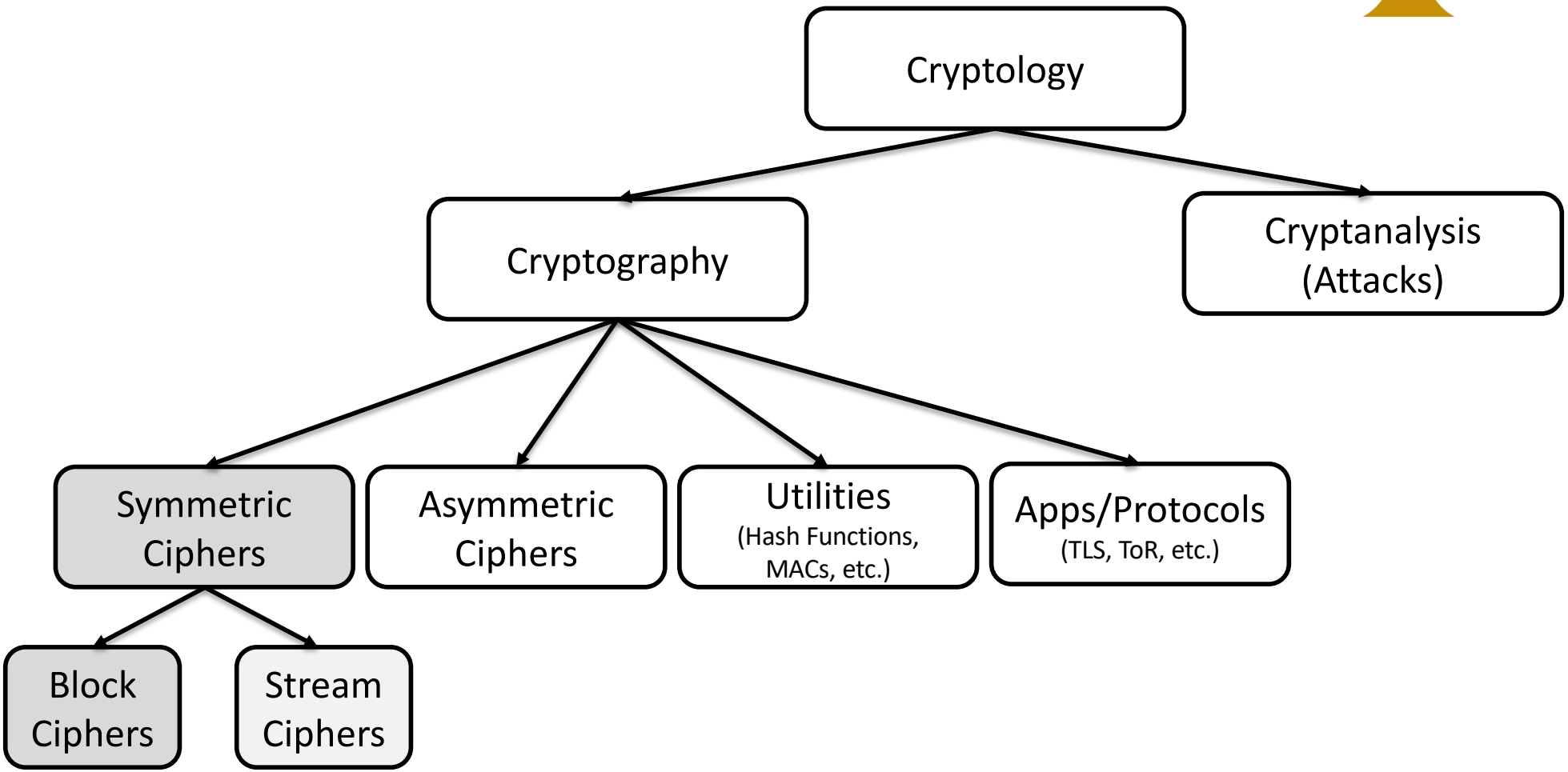
Modes of Operation in Block Ciphers

Elias Athanasopoulos
athanasopoulos.elias@ucy.ac.cy

Sections of this Lecture

- More on Block Ciphers
- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Counter Mode (CTR)

Cryptography Roadmap

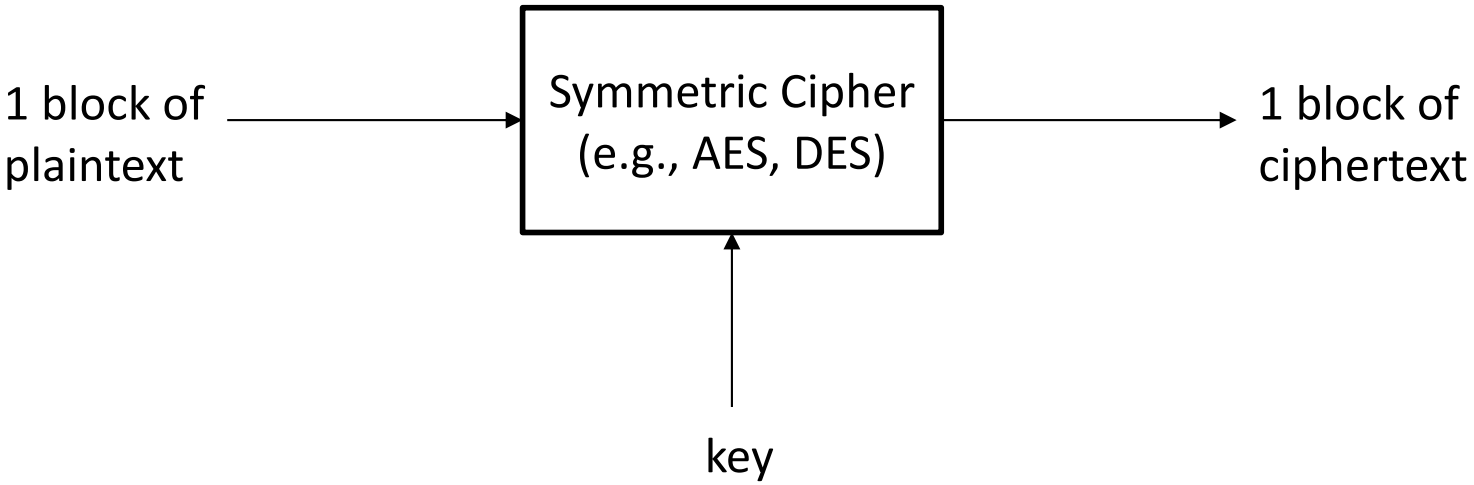


MORE ON BLOCK CIPHERS

Block Ciphers Usage

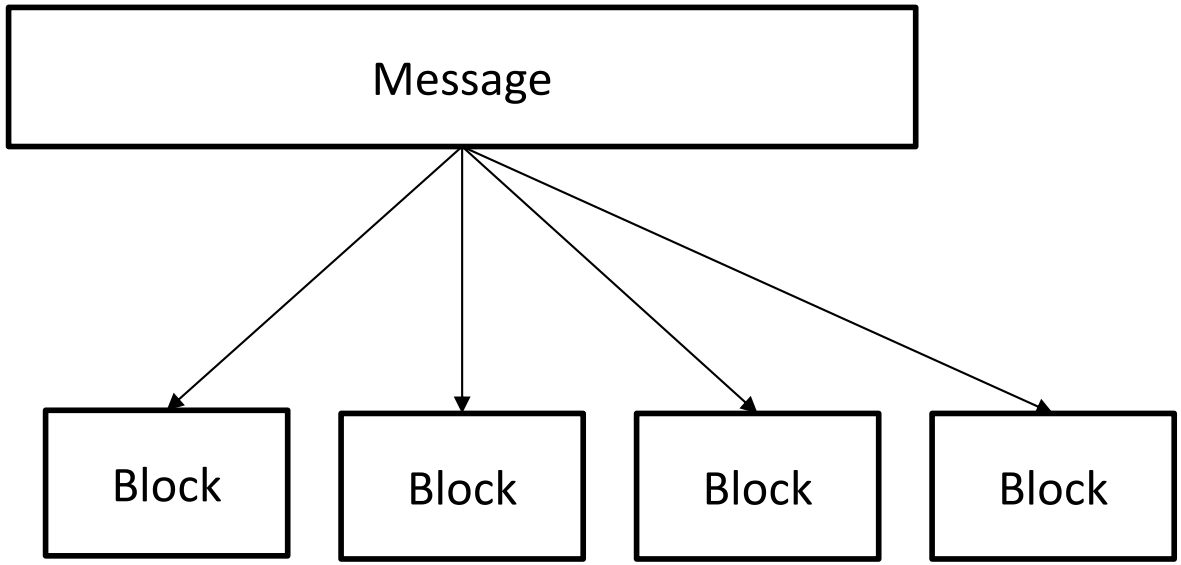
- Build different types of block-based encryption schemes
- Realize stream ciphers
- Construct cryptographic hash functions
- Make message authentication codes (MACs)
- Build key establishment protocols
- Make a pseudo-random number generator

Modes of Operation



In practice, someone needs to transmit a message that contains several blocks (e.g., a PDF document, or an e-mail)

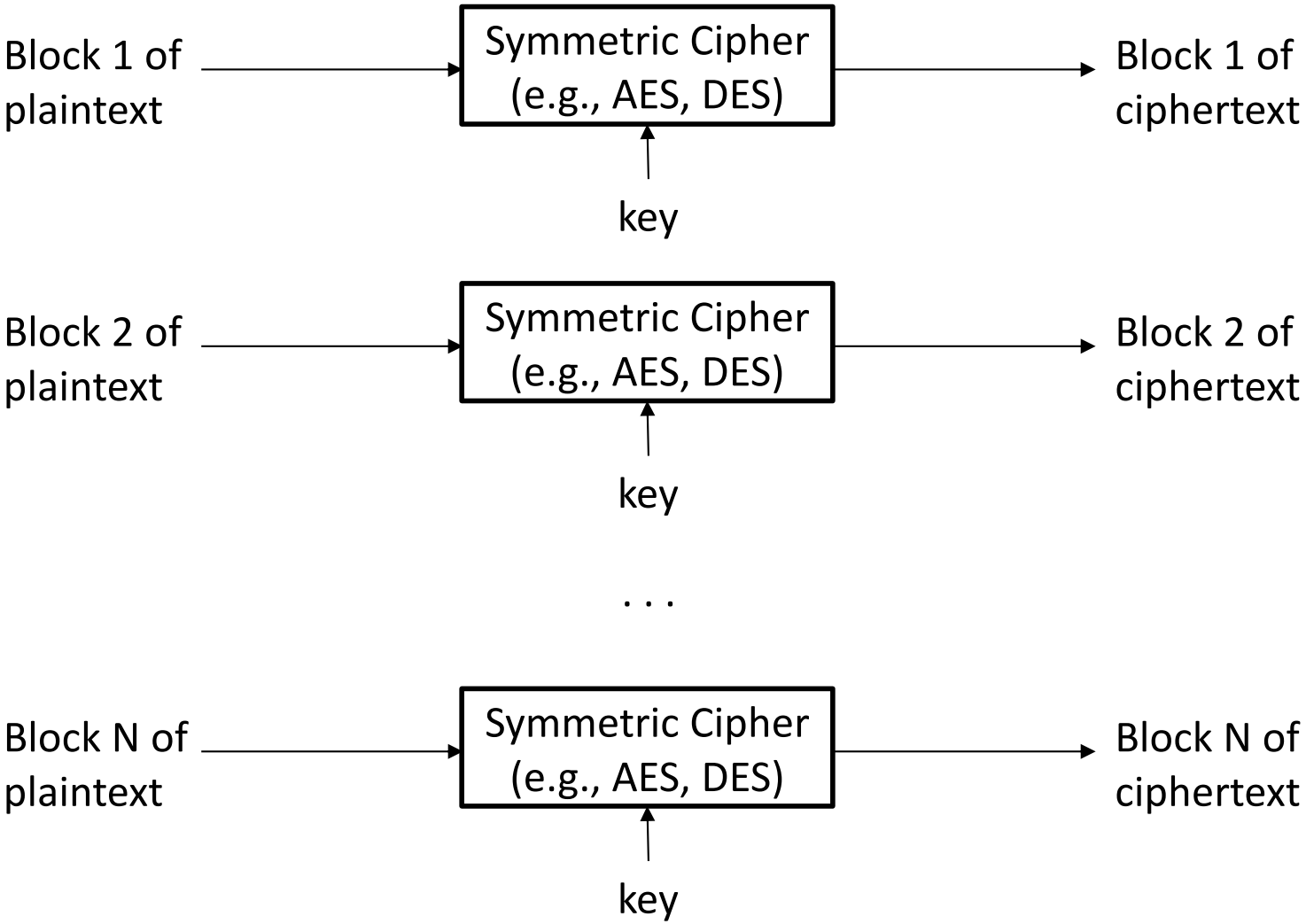
Problem



Assume that we cut the message in blocks, how the blocks are then encrypted?

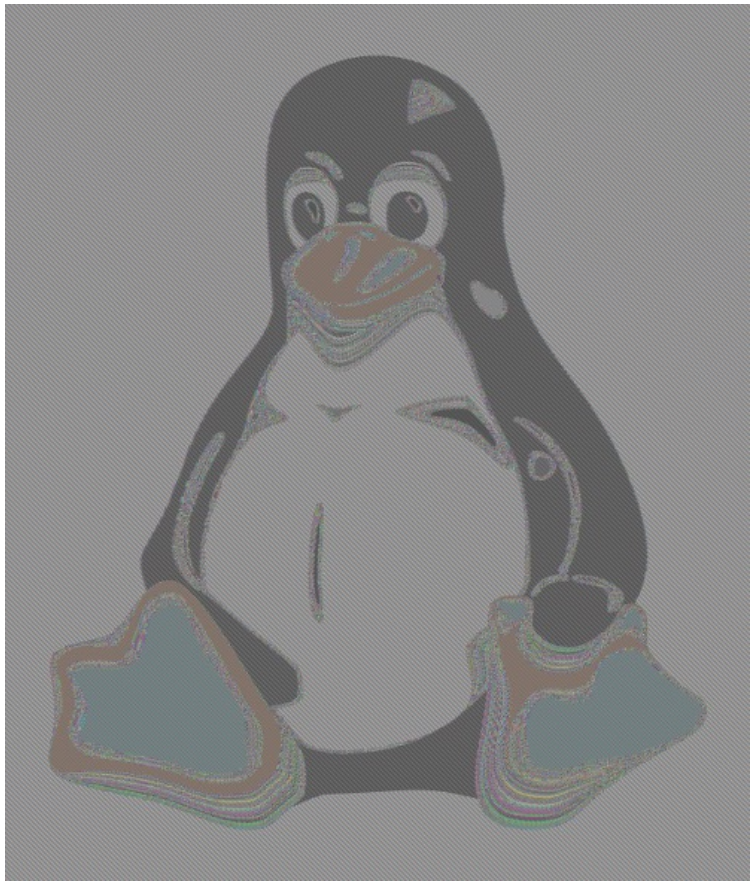
ELECTRONIC CODE BOOK (ECB)

ECB Overview



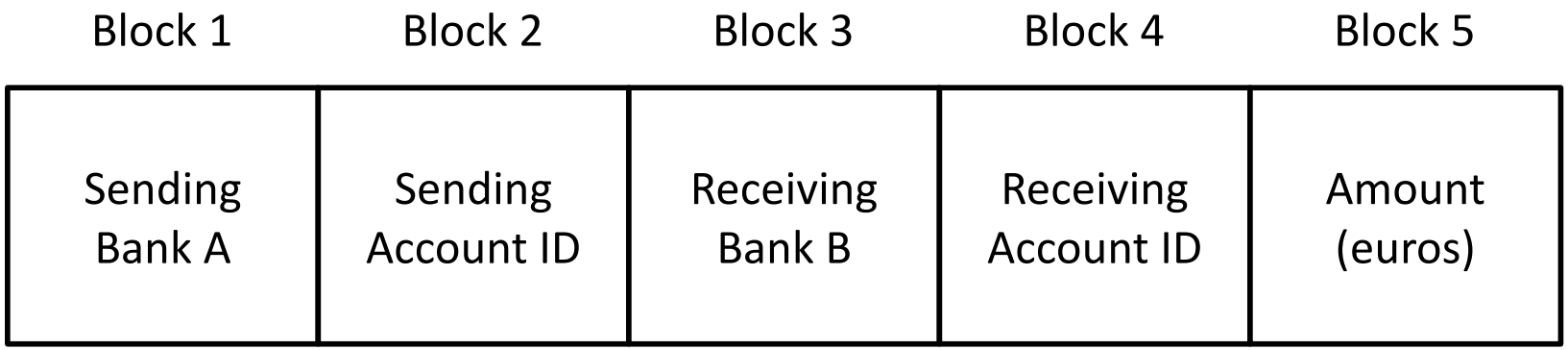
ECB Description

- ECB serves as a gigantic codebook
- For a fixed key, every block of plaintext maps to a particular block of ciphertext
- Vulnerable to attacks



Substitution Attack

- Suppose an electronic bank transfer
  - The encryption key between the two banks does not change too frequently



Substitution Attack

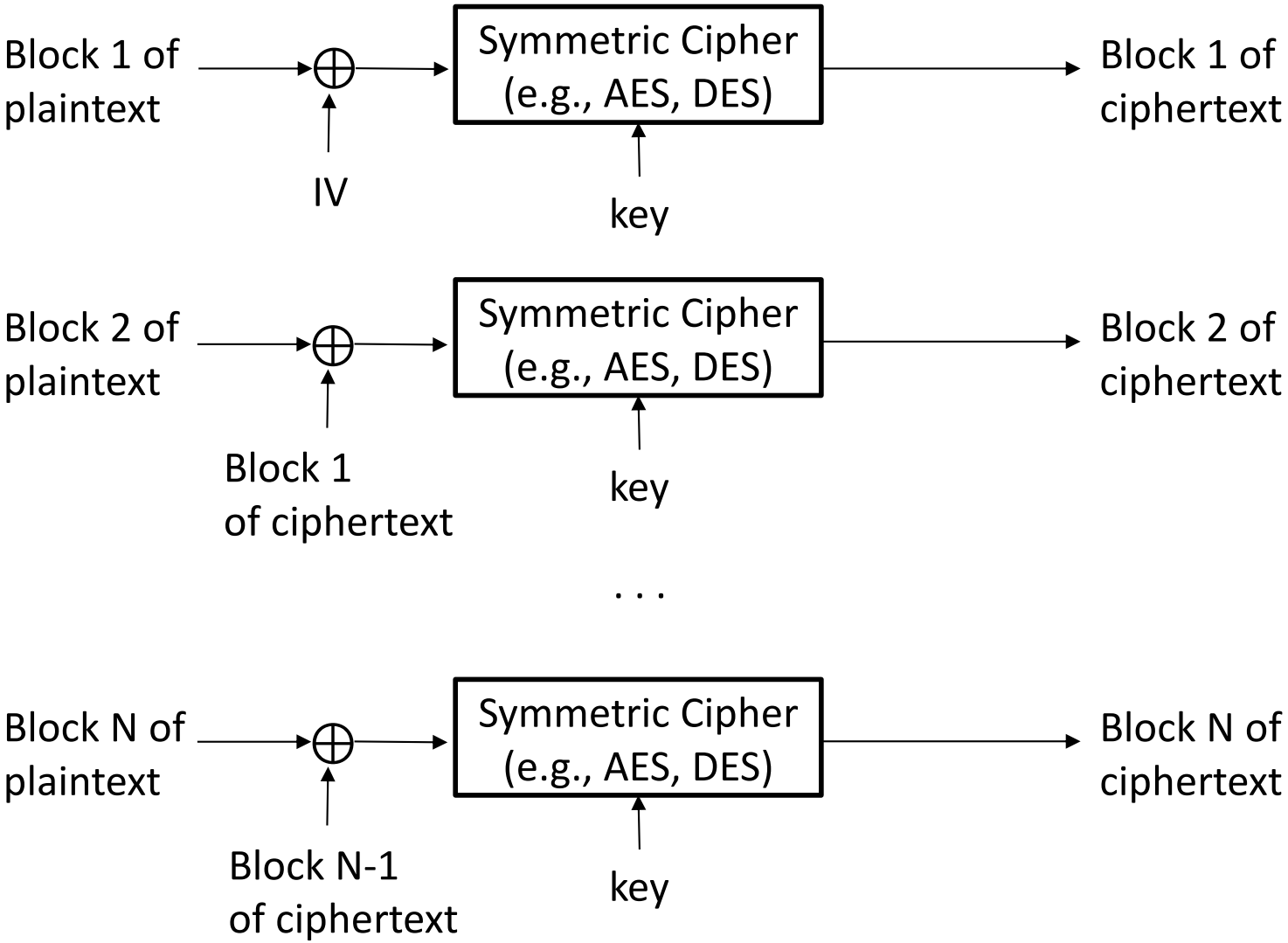
- The attacker sends 1-euro transfers from their account at bank A to their account at bank B repeatedly
- They can check for ciphertext blocks that repeat, and they store blocks 1, 3 and 4 of these transfers
- They now simply replace block 4 of other transfers with the block 4 that they stored before
  - All transfers from some account of bank A to some account of bank B are redirected to go into the attacker's B account!

CIPHER BLOCK CHAINING (CBC)

Cipher Block Chaining (CBC)

- Chain all blocks together
- For decrypting the *Nth* block, you need to decrypt *all* previous blocks
- For just the first block, generate a random number (nonce), usually called Initialization Vector (IV)
  - Apply XOR with IV and the first block of plaintext before encryption
- For all other blocks
  - Apply XOR with the previous block of ciphertext and the current block of plaintext before encryption

CBC Overview



Initialization Vector (IV)

- If the IV is kept the same for several encryptions, the attacker can infer cipher blocks
- If we choose a new IV every time we encrypt, the CBC mode becomes a probabilistic encryption scheme
  - Two encryptions of the same plaintext look entirely different
- It is not needed to keep the IV secret!
- Typically, the IV should be a non-secret nonce (value used only once)

CBC Encryption/Decryption

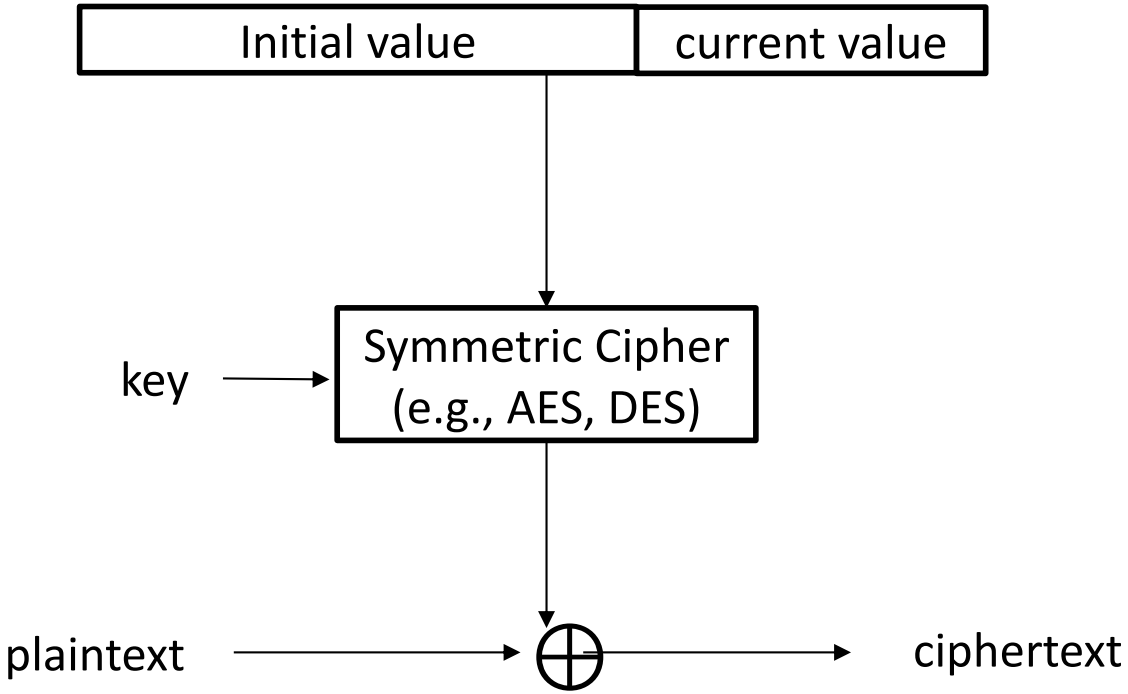
- Encryption
  - First block: $c_1 = \mathbf{e_k}(p_1 \oplus IV)$
  - General block: $c_i = \mathbf{e_k}(p_i \oplus c_{i-1})$, $i \geq 2$
- Decryption
  - First block: $p_1 = \mathbf{d_k}(c_1) \oplus IV$
  - General block : $p_i = \mathbf{d_k}(c_i) \oplus c_{i-1}$, $i \geq 2$

COUNTER MODE (CTR)

Counter Mode (CTR)

- Transforms a block cipher to a stream cipher
- The key stream is computed in a blockwise fashion
- The input to the block cipher is a counter which assumes a different value every time the block cipher computes a new key stream block
- Can be parallelized

CTR Overview



CTR Encryption/Decryption

- Encryption

  $c_i = e_k (IV \,||\, CTR_i) \oplus p_i,\ i \geq 1$

- Decryption

  $p_i = e_k (IV \,||\, CTR_i) \oplus c_i,\ i \geq 1$

- Notice we do not use the decryption part of the symmetric cipher!

Resources

- This lecture was built using material that can be found at
  - Chapter 5, Understanding Cryptography, http://www.crypto-textbook.com
  - Chapter 7, Handbook of Applied Cryptography, http://cacr.uwaterloo.ca/hac/
  - Chapter 4, Serious Cryptography, https://nostarch.com/seriouscrypto