CSE 484/M584: Computer Security (and Privacy)

Spring 2025

David Kohlbrenner
dkohlbre@cs

UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner, Nirvan Tyagi. Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials

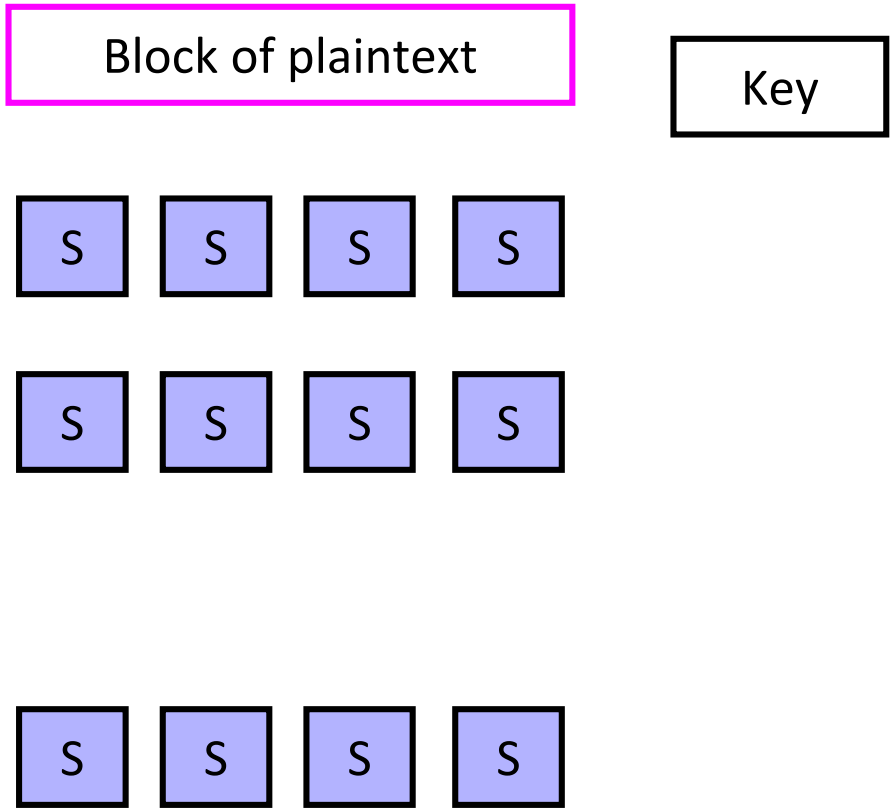
Admin

- Lab1a Grades are out
  - File regrades BEFORE May 7
- HW1 due next wednesday
- Lab 2 (Cryptolab) is out

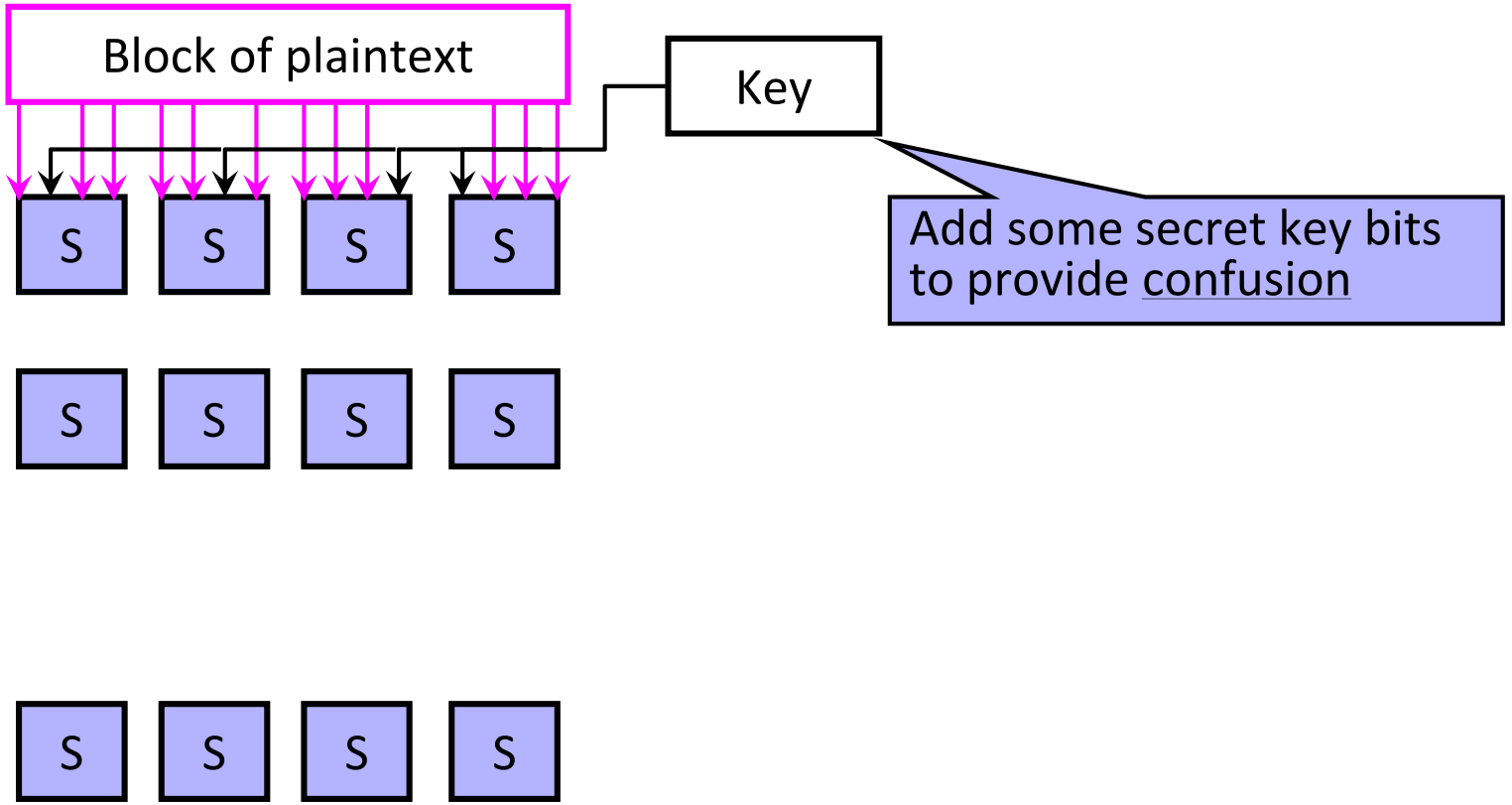
Crosswalk ‘hack’

Symmetric Encryption

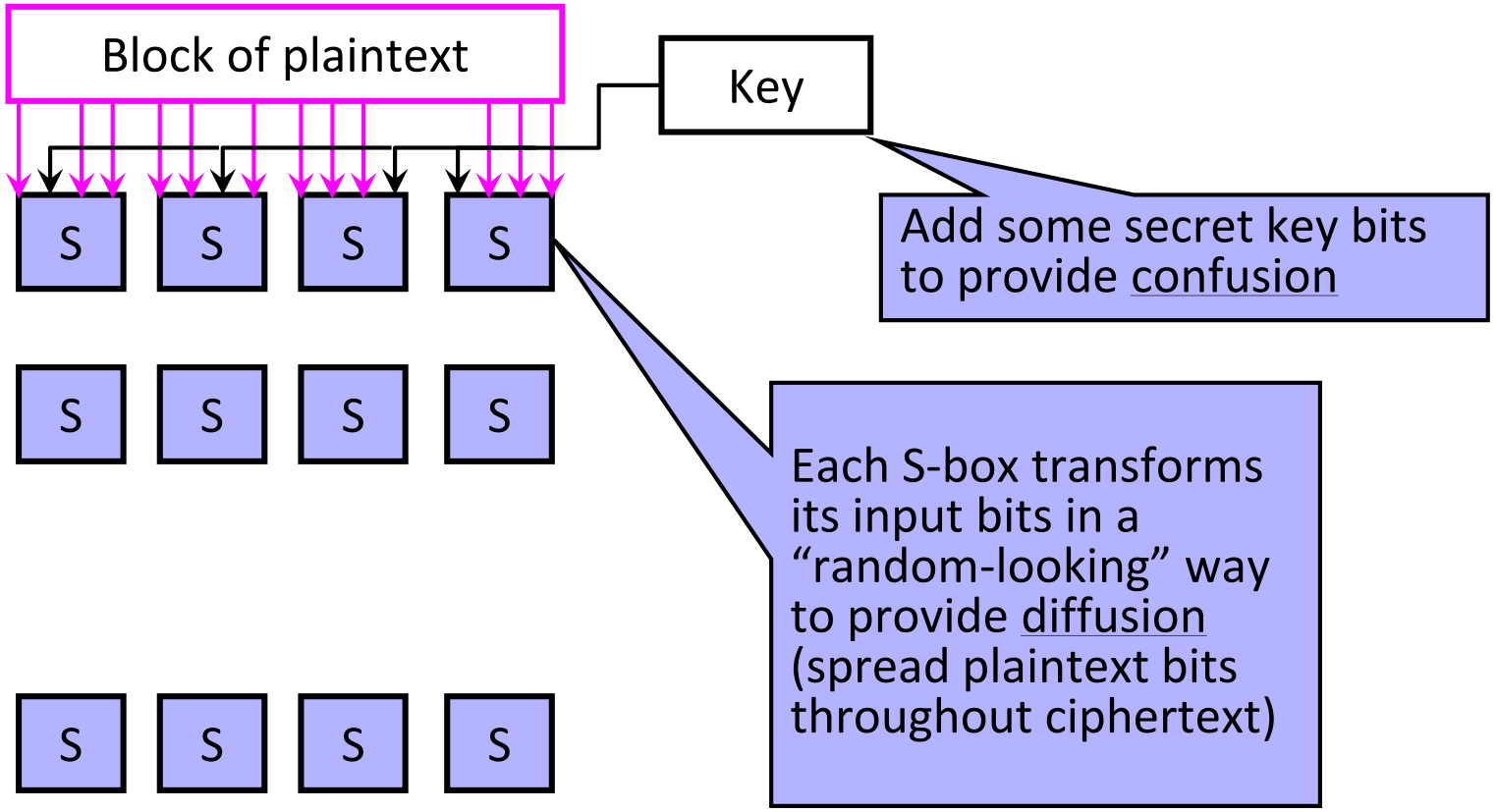
Block Cipher Operation (Simplified)



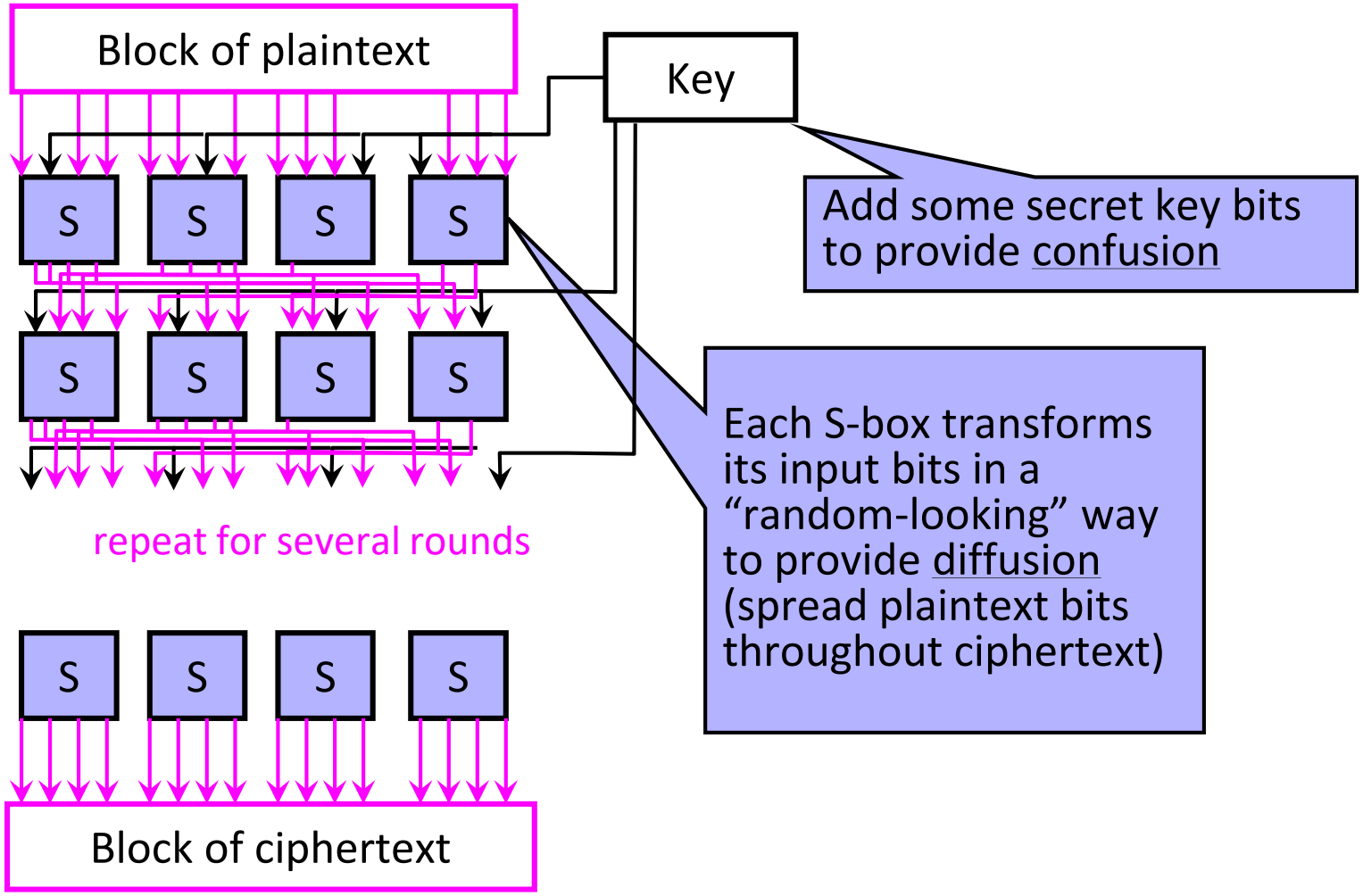
Block Cipher Operation (Simplified)



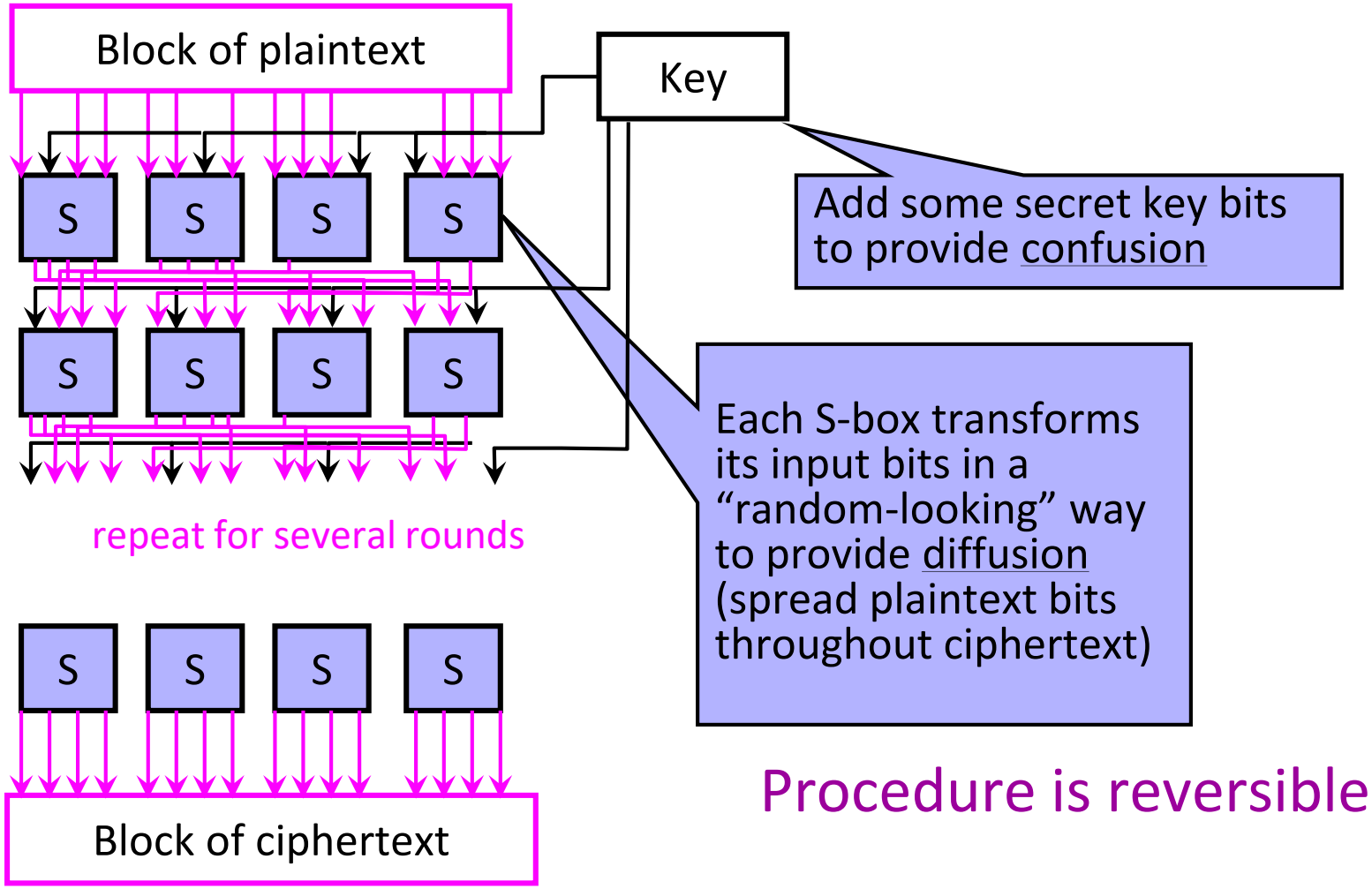
Block Cipher Operation (Simplified)



Block Cipher Operation (Simplified)



Block Cipher Operation (Simplified)



Procedure is reversible!

Block Cipher Security

- Security: For a randomly selected key: Computationally hard to distinguish outputs of the block cipher from outputs of a truly random permutation

- Popular block ciphers (e.g., AES) do not have proofs of security!
  - Design is open and standard is created through public competition
  - Current best attacks against AES-128 take 2^{126} time
  - Block ciphers with proofs of security exist but are less efficient

Standard Block Ciphers

- **DES: Data Encryption Standard**
  - Feistel structure: builds invertible function using non-invertible ones
  - Invented by IBM, issued as federal standard in 1977
  - 64-bit blocks, 56-bit key + 8 bits for parity

DES and 56 bit keys

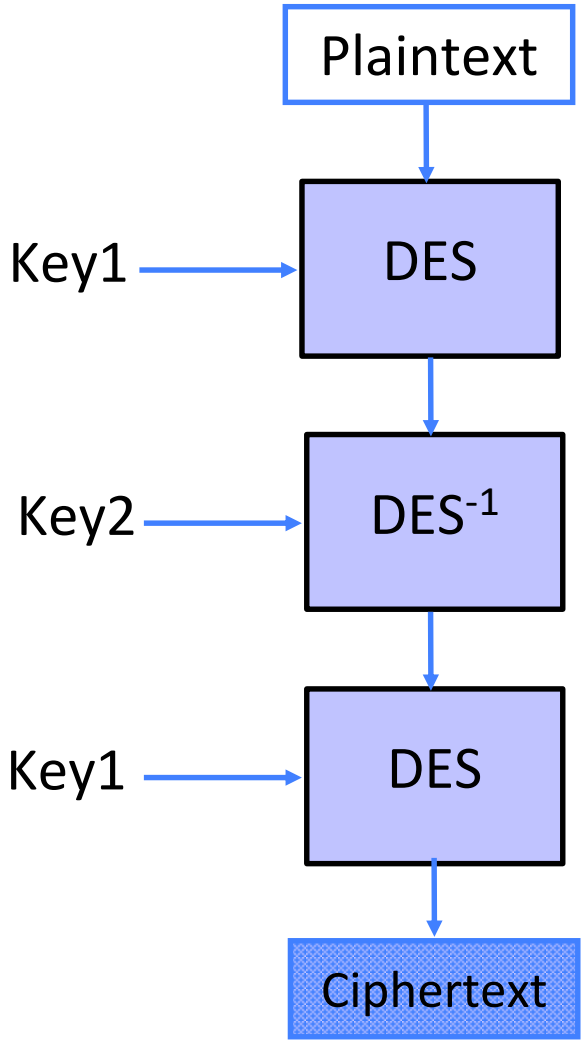
- 56 bit keys are quite short

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^{6} years

- 1999: EFF DES Crack + distributed machines
  - < 24 hours to find DES key
- DES ---> 3DES
  - 3DES: DES + inverse DES + DES (with 2 or 3 diff keys)

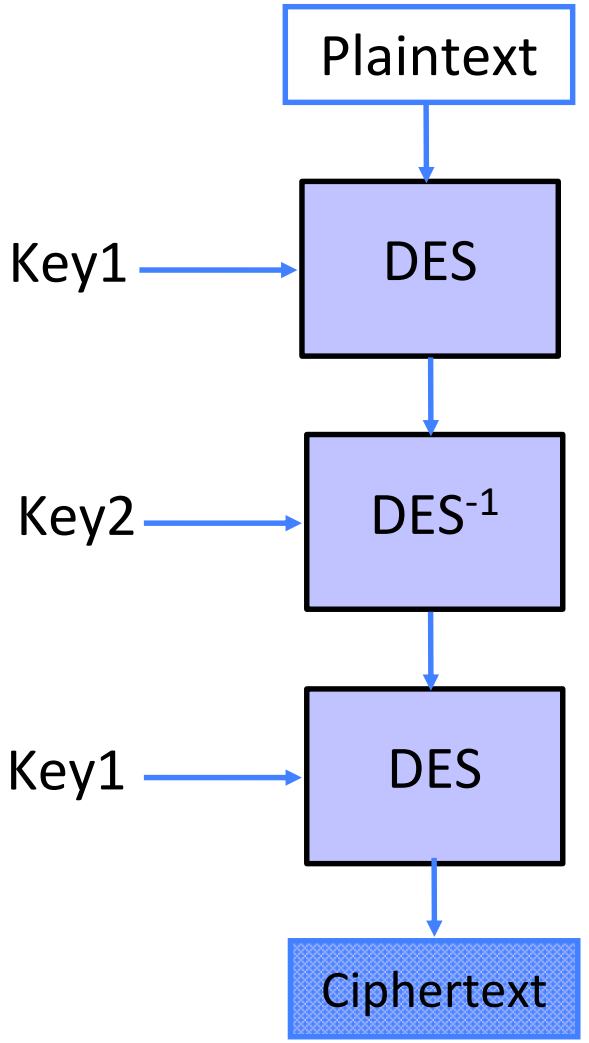
3DES

- Two-key 3DES increases security of DES by doubling the key length
- Why 3DES and not cool-new-scheme?

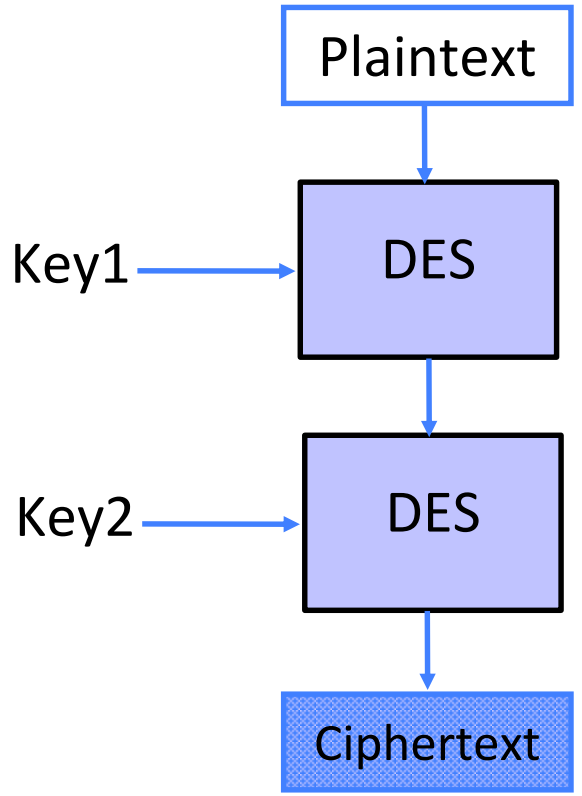


3DES

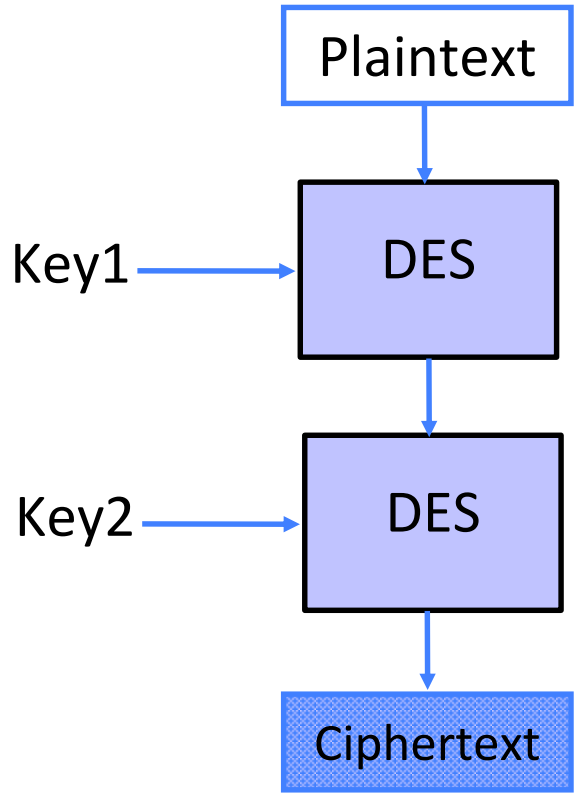
- Two-key 3DES increases security of DES by doubling the key length
- Why 3DES and not cool-new-scheme?
- Why not 2DES?



Meet-in-the-middle

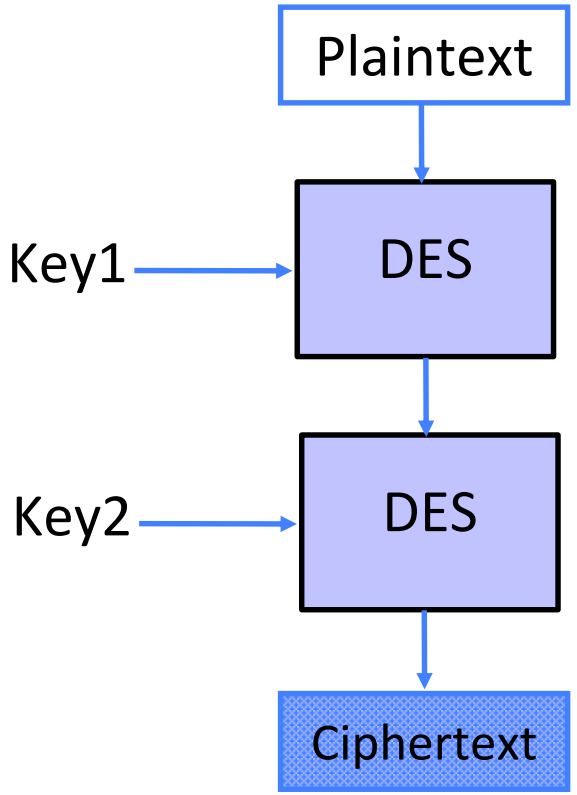


Meet-in-the-middle



Meet-in-the-Middle Attack

- Guess 2^{56} values for Key1, and create a table from P1 to a middle value M1 for each key guess ($M1^{G1}$, $M1^{G2}$, $M1^{G3}$, …)
- Guess 2^{56} values for Key2, and create a table from C1 to a middle value M'1 for each key guess ($M'1^{G1}$, $M'1^{G2}$, $M'1^{G3}$, …)
- Look for collision in the middle values → if only one collision, found Key1 and Key2; otherwise repeat for (P2,C2), …



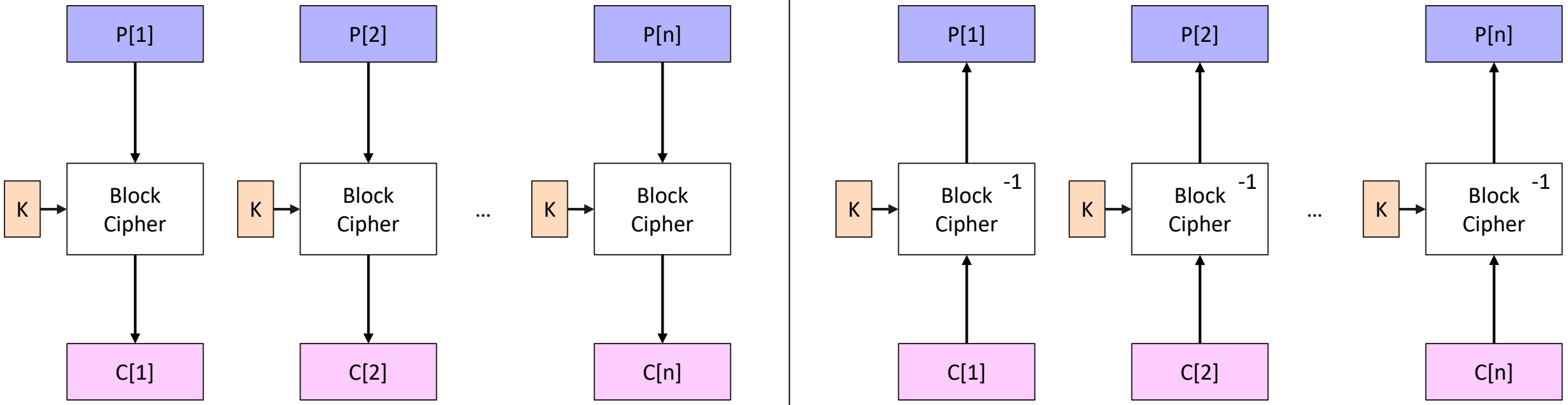
Standard Block Ciphers

- **DES: Data Encryption Standard**
  - Feistel structure: builds invertible function using non-invertible ones
  - Invented by IBM, issued as federal standard in 1977
  - 64-bit blocks, 56-bit key + 8 bits for parity

- **AES: Advanced Encryption Standard**
  - New federal standard as of 2001
    - NIST: National Institute of Standards & Technology
  - Based on the Rijndael algorithm
    - Selected via an open process
  - 128-bit blocks, keys can be 128, 192 or 256 bits

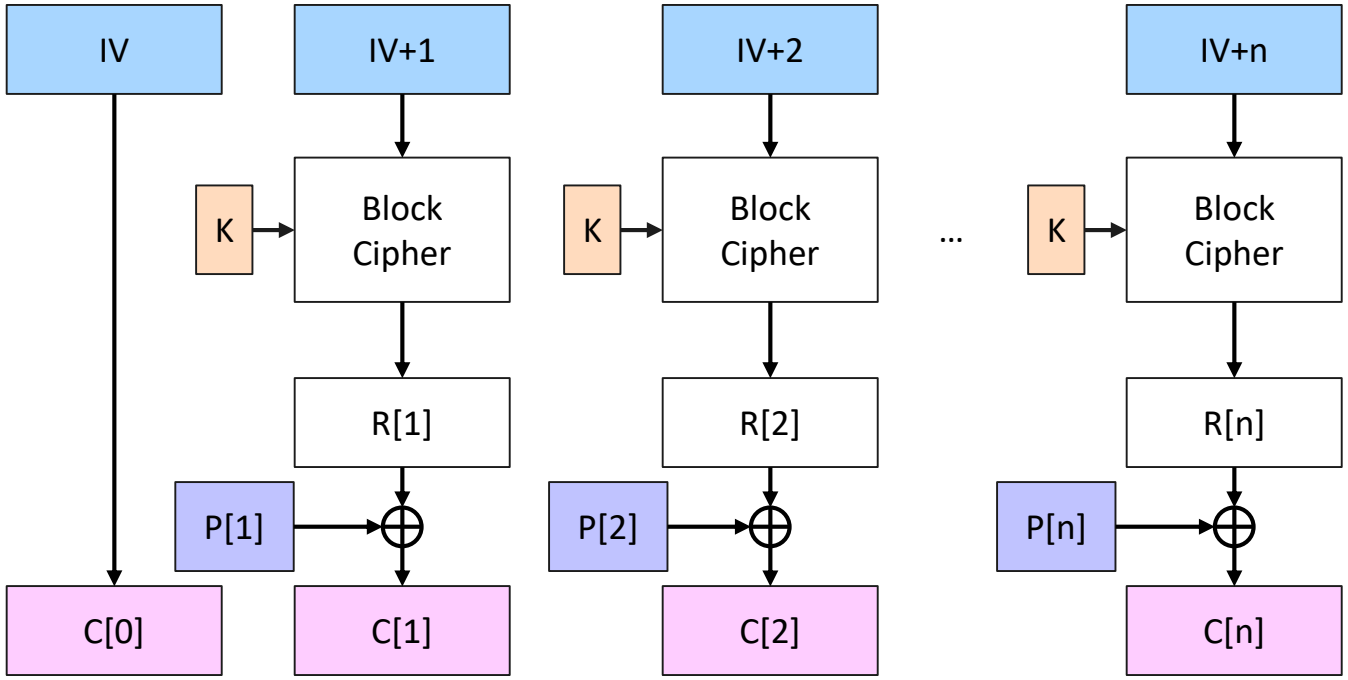
Electronic Code Book (ECB) Mode

- Idea: Simply split up the plaintext into block-sized chunks!

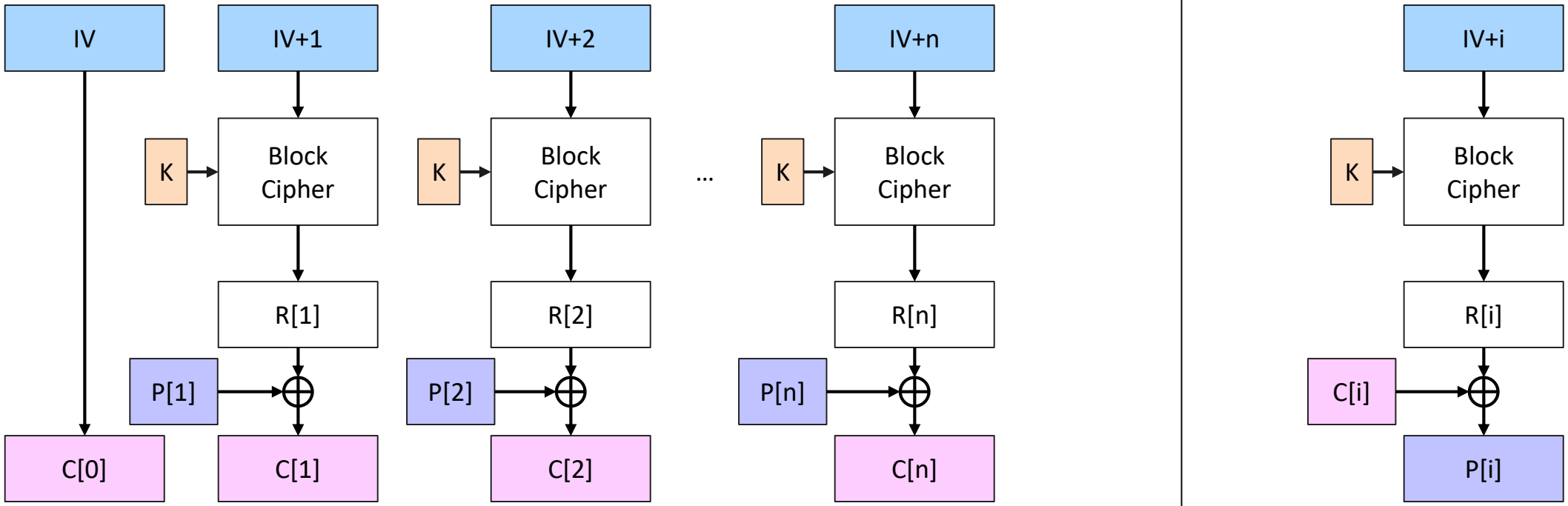


- Identical blocks of plaintext produce identical blocks of ciphertext
- No integrity checks: can mix and match blocks

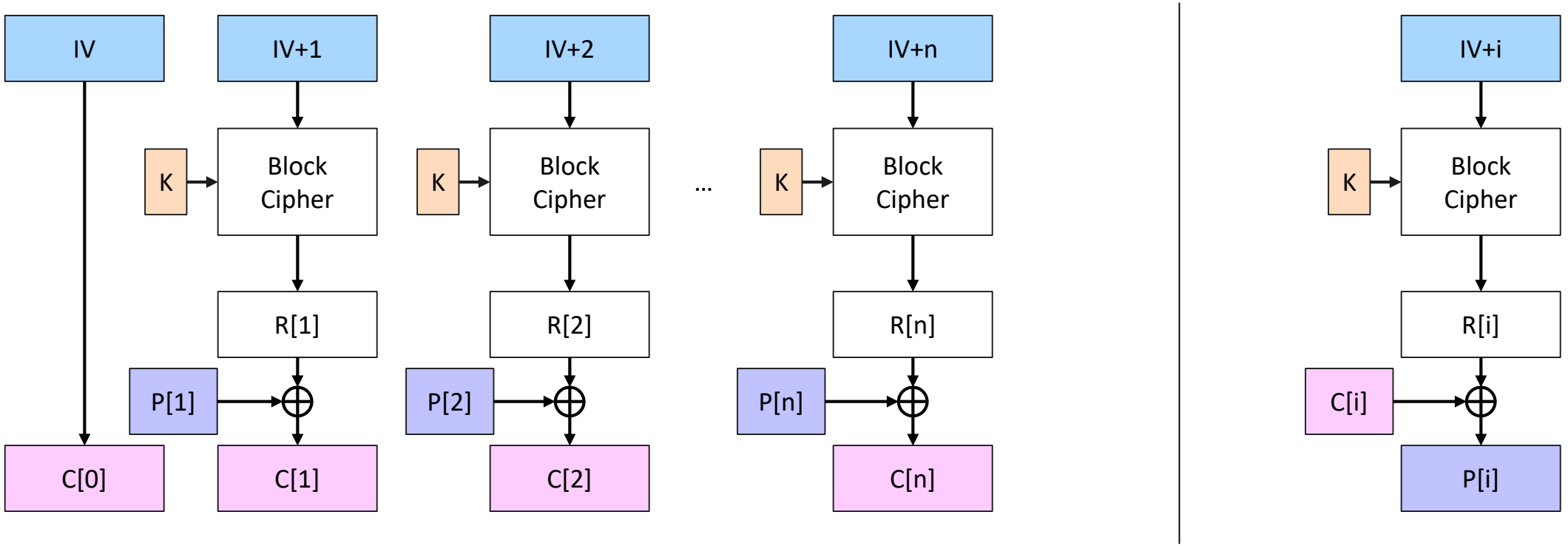
Counter (CTR) Mode



Counter (CTR) Mode

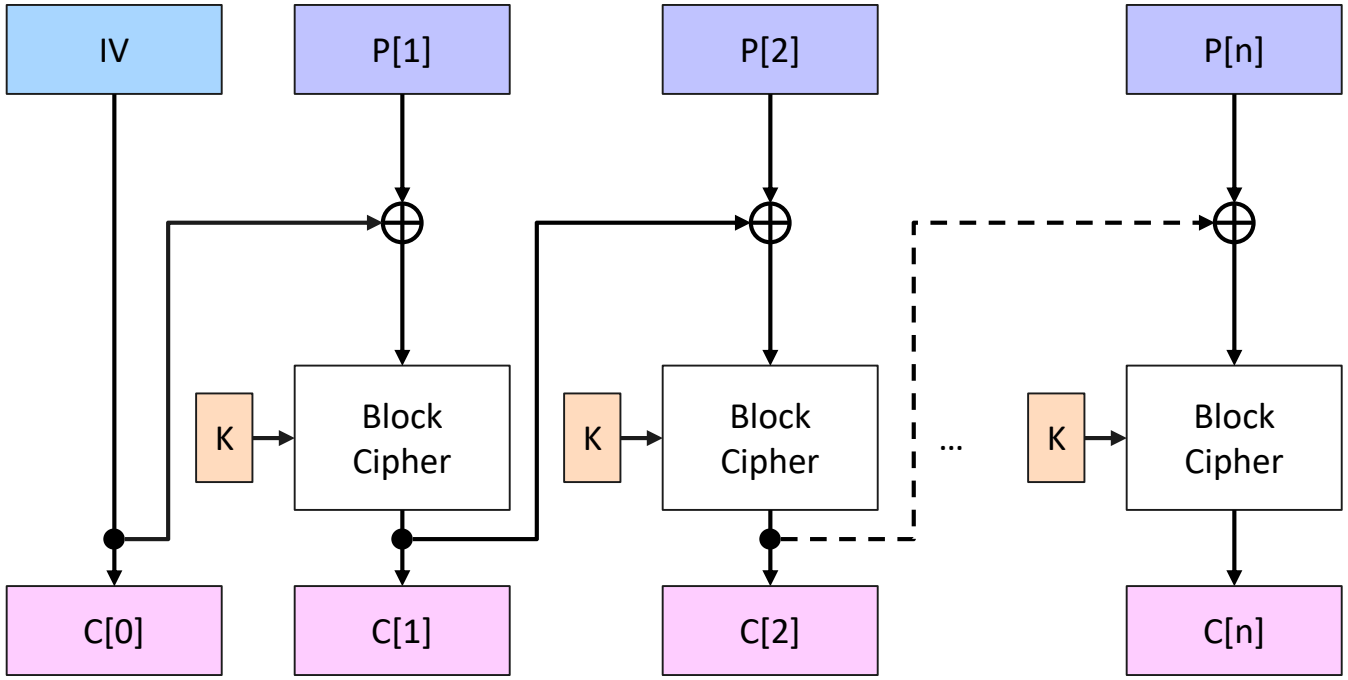


Counter (CTR) Mode

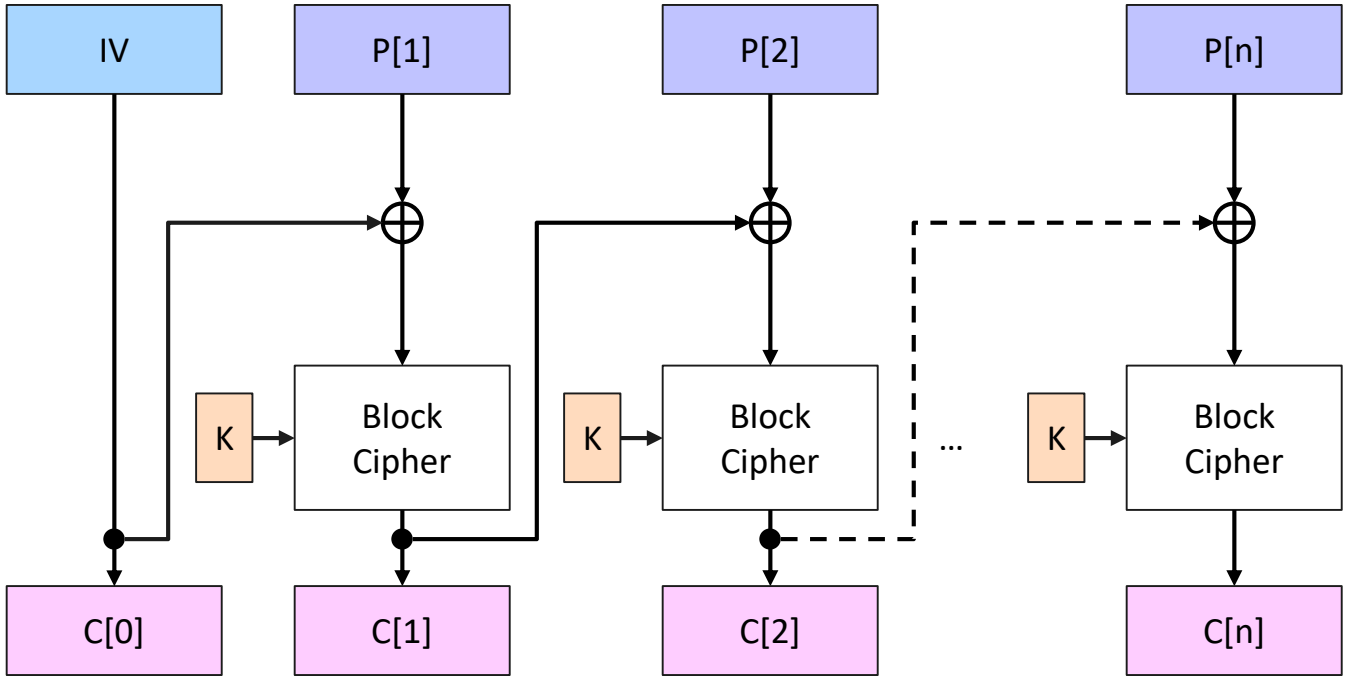


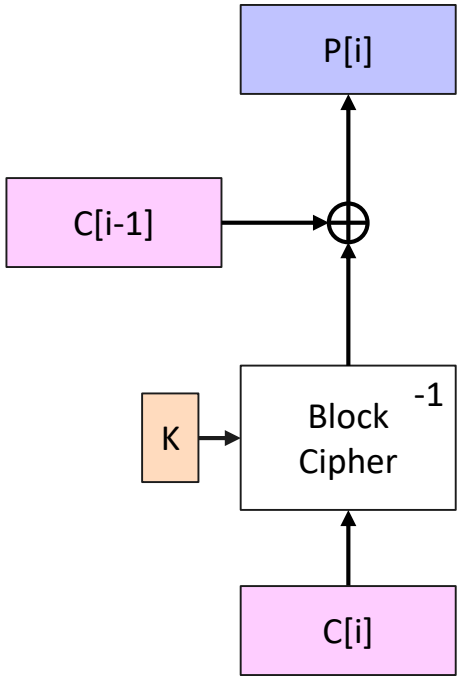
- Security intuition: Outputs of block cipher look like a “random” one-time-pad!
  - As long as initialization vector (IV) is never reused then one-time-pad is never reused
- Parallelizable
- Decryption doesn’t require block cipher inverse (connection to stream cipher and PRNGs)

Cipher Block Chaining (CBC) Mode

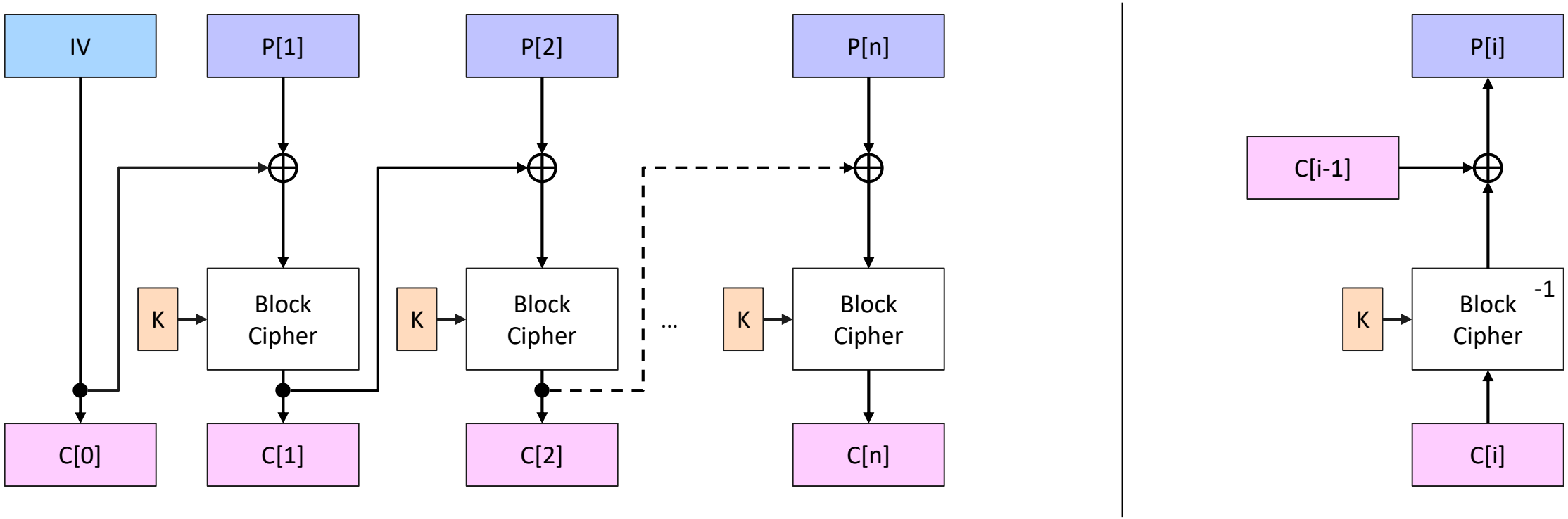


Cipher Block Chaining (CBC) Mode



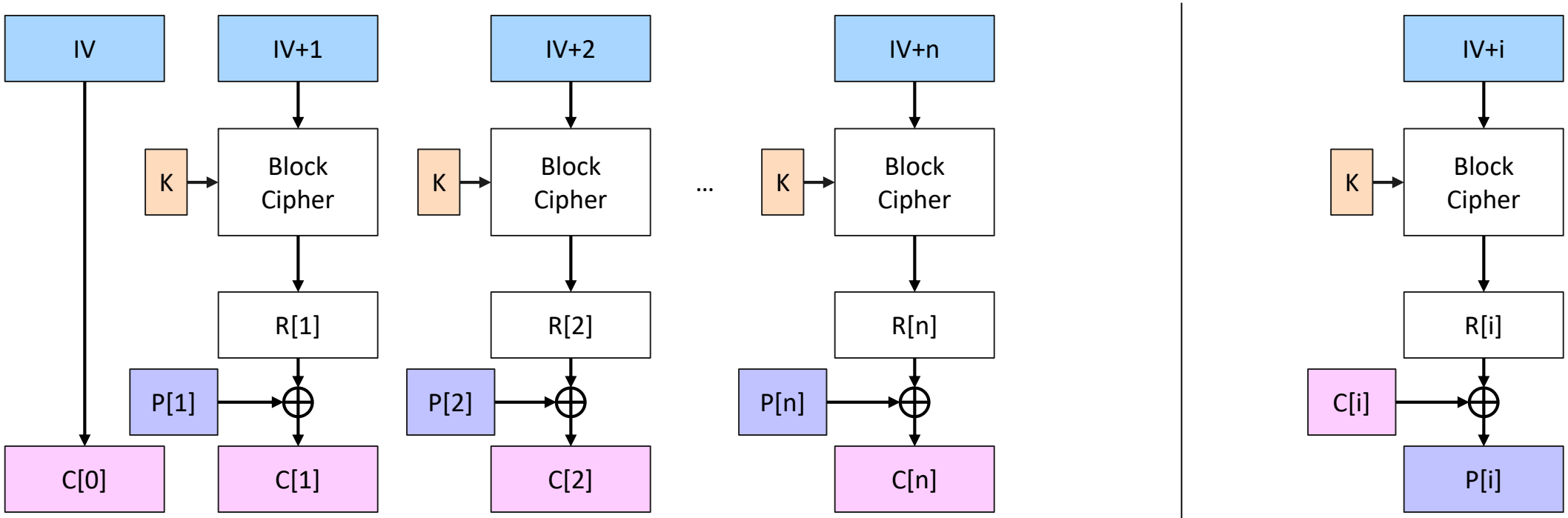


Cipher Block Chaining (CBC) Mode



- Security intuition: Ciphertext blocks appear random, and thus produce unpredictable inputs to block cipher
  - Also requires IV to not be reused
- Encryption is serial
- Decryption requires block cipher inverse

IV Reuse?


IV
IV+1
IV+2
IV+n
K
Block Cipher
K
Block Cipher
...
K
Block Cipher
R[1]
R[2]
R[n]
P[1]
P[2]
P[n]
C[0]
C[1]
C[2]
C[n]
IV+i
K
Block Cipher
R[i]
C[i]
P[i]

When is an Encryption Scheme “Secure”?

- Hard to recover the key?
  - What if attacker can learn plaintext without learning the key?
- Hard to recover plaintext from ciphertext?
  - What if attacker learns some bits or some function of bits?

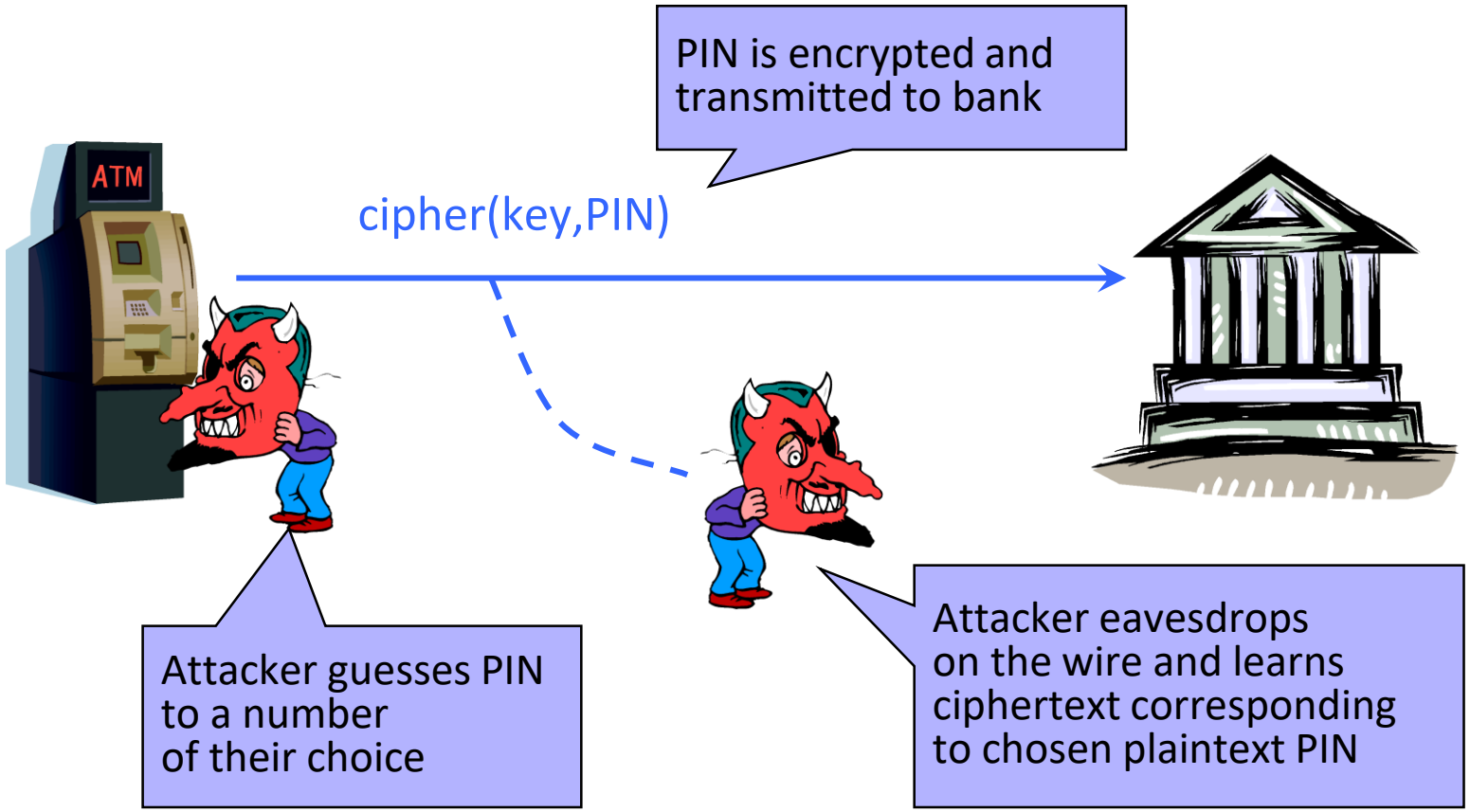
When is an Encryption Scheme “Secure”?

Gradescope!

How Can a Cipher Be Attacked?

- Attackers knows ciphertext and encryption algorithm
  - What else does the attacker know? Depends on the application in which the cipher is used!
- Ciphertext-only attack
- KPA: Known-plaintext attack (stronger)
  - Knows some plaintext-ciphertext pairs
- CPA: Chosen-plaintext attack (even stronger)
  - Can obtain ciphertext for any plaintext of his choice

Chosen Plaintext Attack



… repeat for any PIN value

How Can a Cipher Be Attacked?

- Attackers knows ciphertext and encryption algorithm
  - What else does the attacker know? Depends on the application in which the cipher is used!
- Ciphertext-only attack
- KPA: Known-plaintext attack (stronger)
  - Knows some plaintext-ciphertext pairs
- CPA: Chosen-plaintext attack (even stronger)
  - Can obtain ciphertext for any plaintext of his choice
- CCA: Chosen-ciphertext attack (very strong)
  - Can decrypt any ciphertext except the target

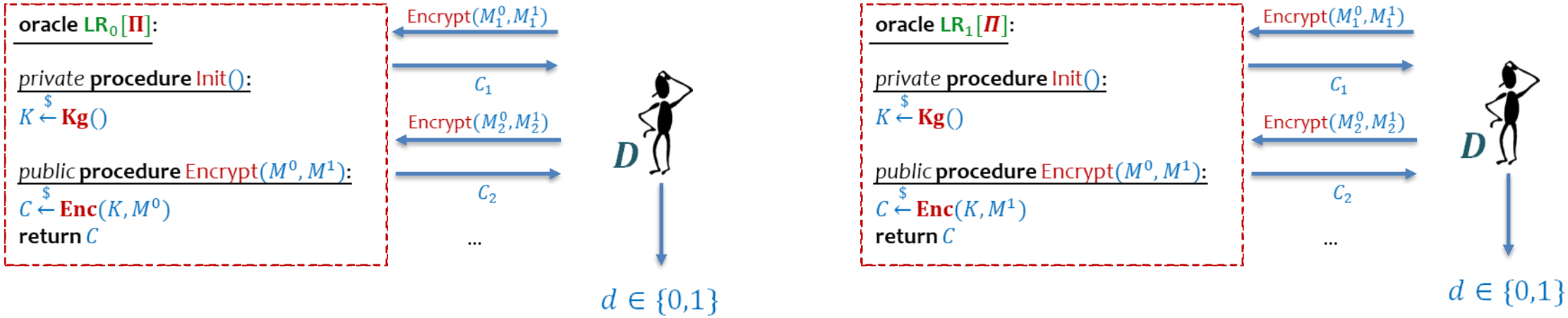
Very Informal Intuition

Minimum security requirement for a modern encryption scheme

- Security against chosen-plaintext attack (CPA)
  - Ciphertext leaks no information about the plaintext
  - Even if the attacker correctly guesses the plaintext, they cannot verify their guess
  - Every ciphertext is unique, encrypting same message twice produces completely different ciphertexts
    - Implication: encryption must be randomized or stateful

The Shape of the Formal Approach

- INDistinguishability under Chosen Plaintext Attack ("IND-CPA")
- Formalized cryptographic game
  - Adversary submits pairs of plaintexts (M_0, M_1)
  - Gets back ONE of the ciphertexts (C_b)
  - Adversary must **guess** which ciphertext this is (C_0 or C_1)
  - If they can do better than 50/50, they win



Very Informal Intuition

Minimum security requirement for a modern encryption scheme

- Security against chosen-plaintext attack (CPA)
  - Ciphertext leaks no information about the plaintext
  - Even if the attacker correctly guesses the plaintext, they cannot verify their guess
  - Every ciphertext is unique, encrypting same message twice produces completely different ciphertexts
    - Implication: encryption must be randomized or stateful
- Security against chosen-ciphertext attack (CCA)
  - Integrity protection – it is not possible to change the plaintext by modifying the ciphertext