CSE 484 / CSE M 584: Computer Security and Privacy

Cryptography: Symmetric Encryption [continued]

Fall 2016

Ada (Adam) Lerner
lerner@cs.washington.edu

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Announcements

- Homework 2 (on crypto) will be out early next week.

Participatory Security Mindset Anecdote

- Cyberwarfare class gave an unfair exam on short notice:

Participatory Security Mindset Anecdote

- Cyberwarfare class gave an unfair exam on short notice:

- "For this exam, you will be required to write down the first 100 digits of pi."

Participatory Security Mindset Anecdote

- Cyberwarfare class gave an unfair exam on short notice:

- "For this exam, you will be required to write down the first 100 digits of pi."

- "You may cheat on this exam."

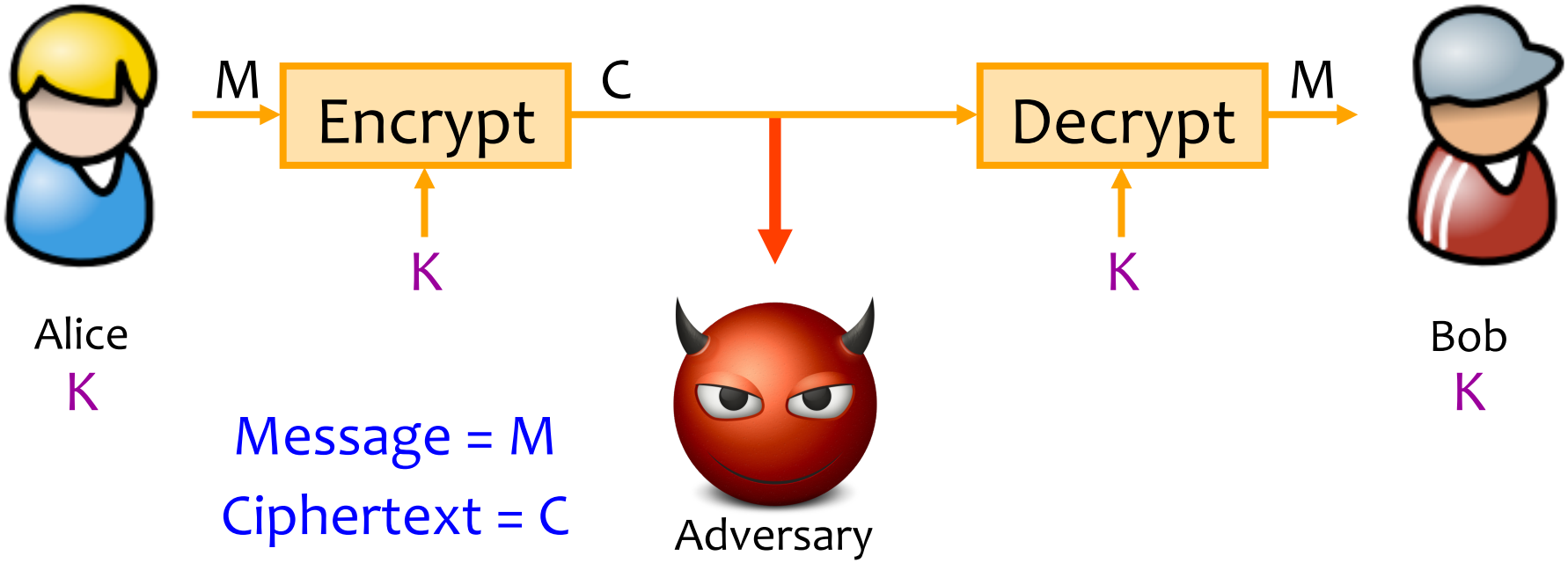
My favorites

- Write 100 digits of pi on a piece of paper *before the exam.* Turn it in.

- Write 3.1415926535 followed by 90 random digits. Turn it in, assuming graders too lazy to check past the first 10 digits

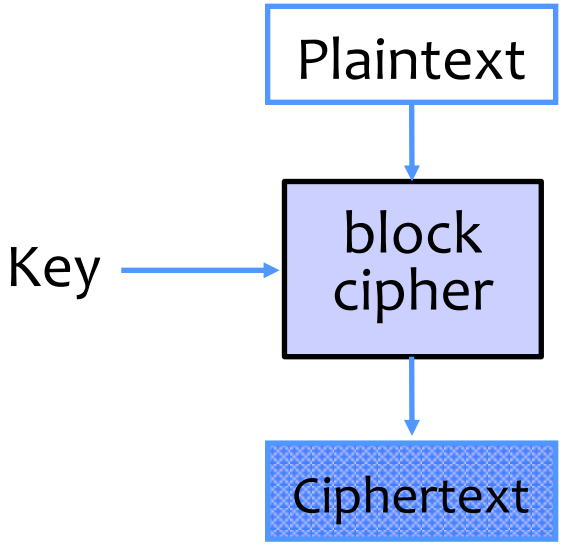
Achieving Privacy (Symmetric)

Encryption schemes: A tool for protecting privacy.

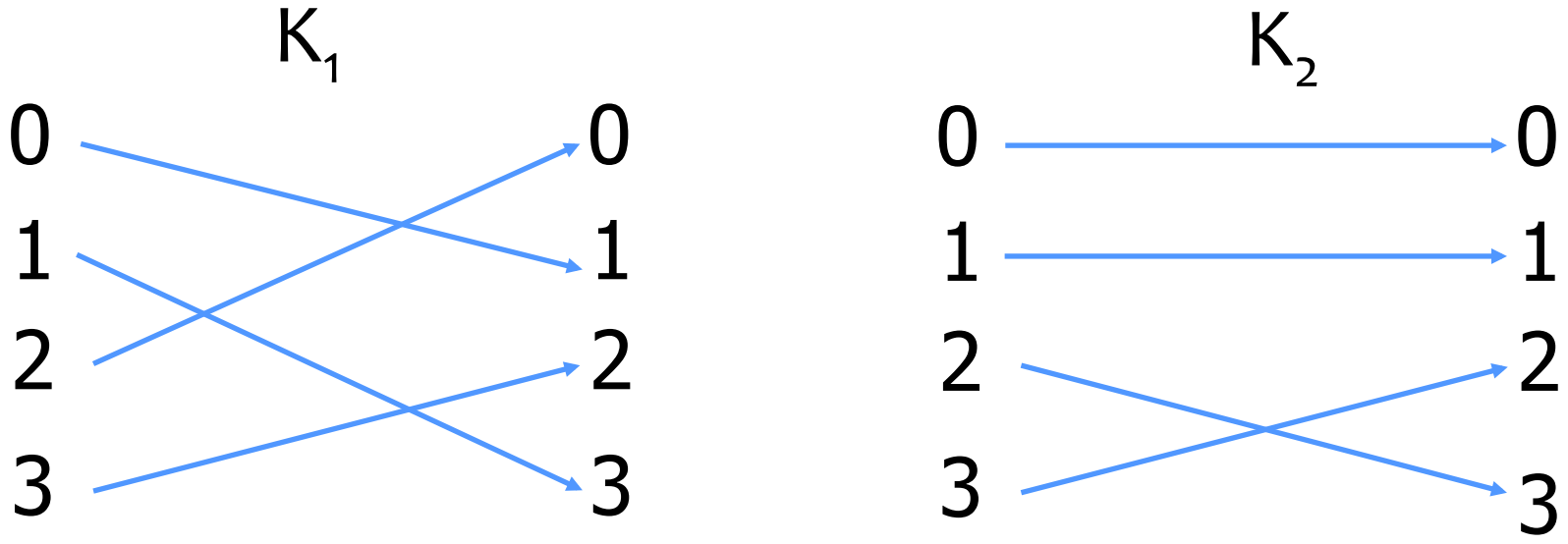


Block Ciphers

- Operates on a single chunk ("block") of plaintext
  - For example, 64 bits for DES, 128 bits for AES
  - Each key defines a different permutation
  - Same key is reused for each block (can use short keys)

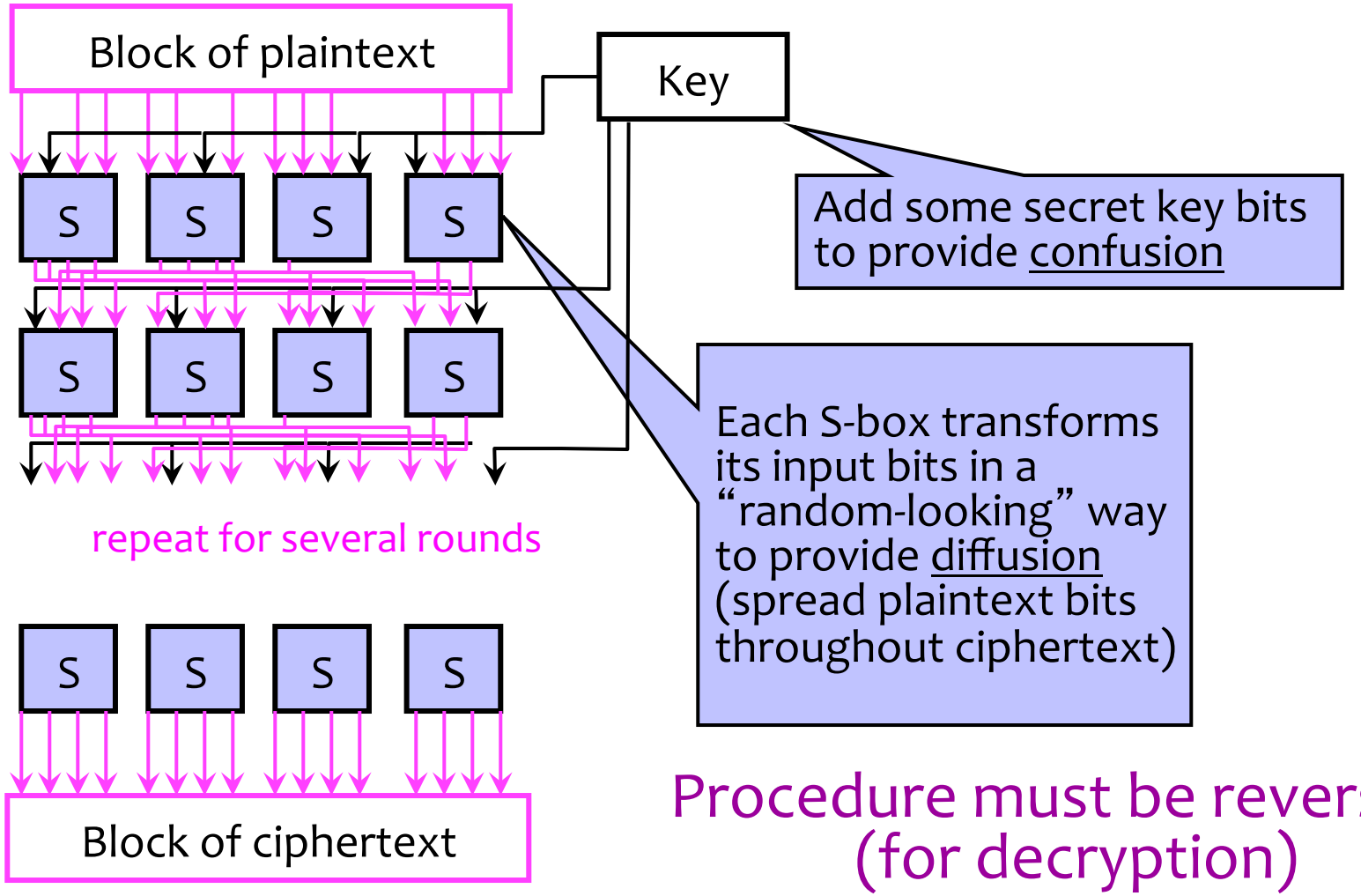


Permutations



- For N-bit input, $2^N!$ possible permutations
- Time and cost of breaking the cipher exceed the value and/or useful lifetime of protected information

Block Cipher Operation (Simplified)



Procedure must be reversible (for decryption)

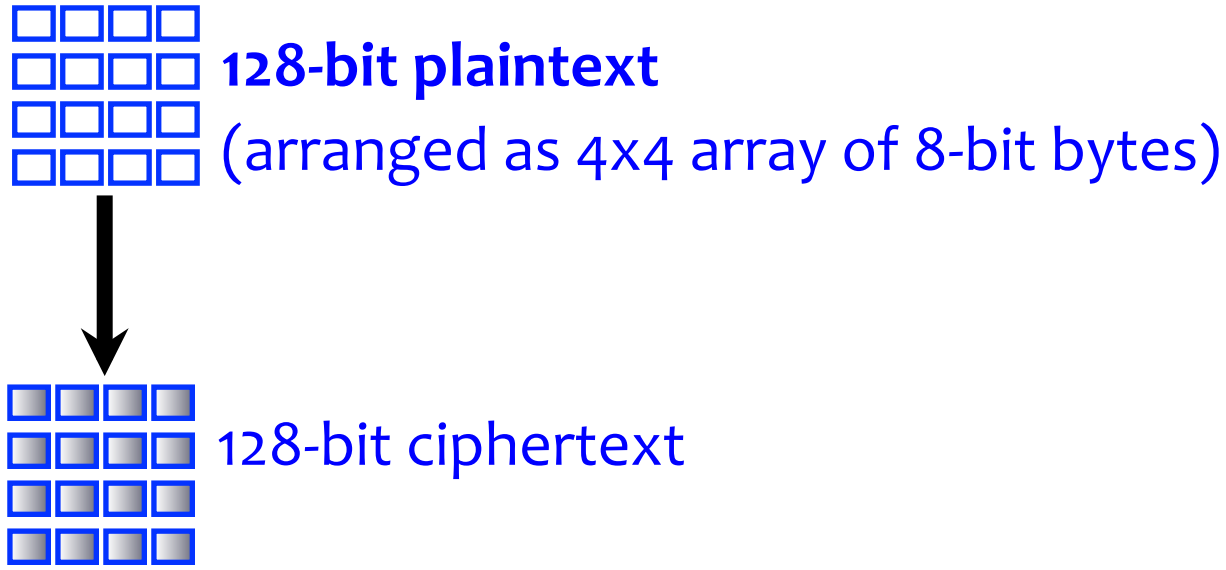
Standard Block Ciphers

- **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

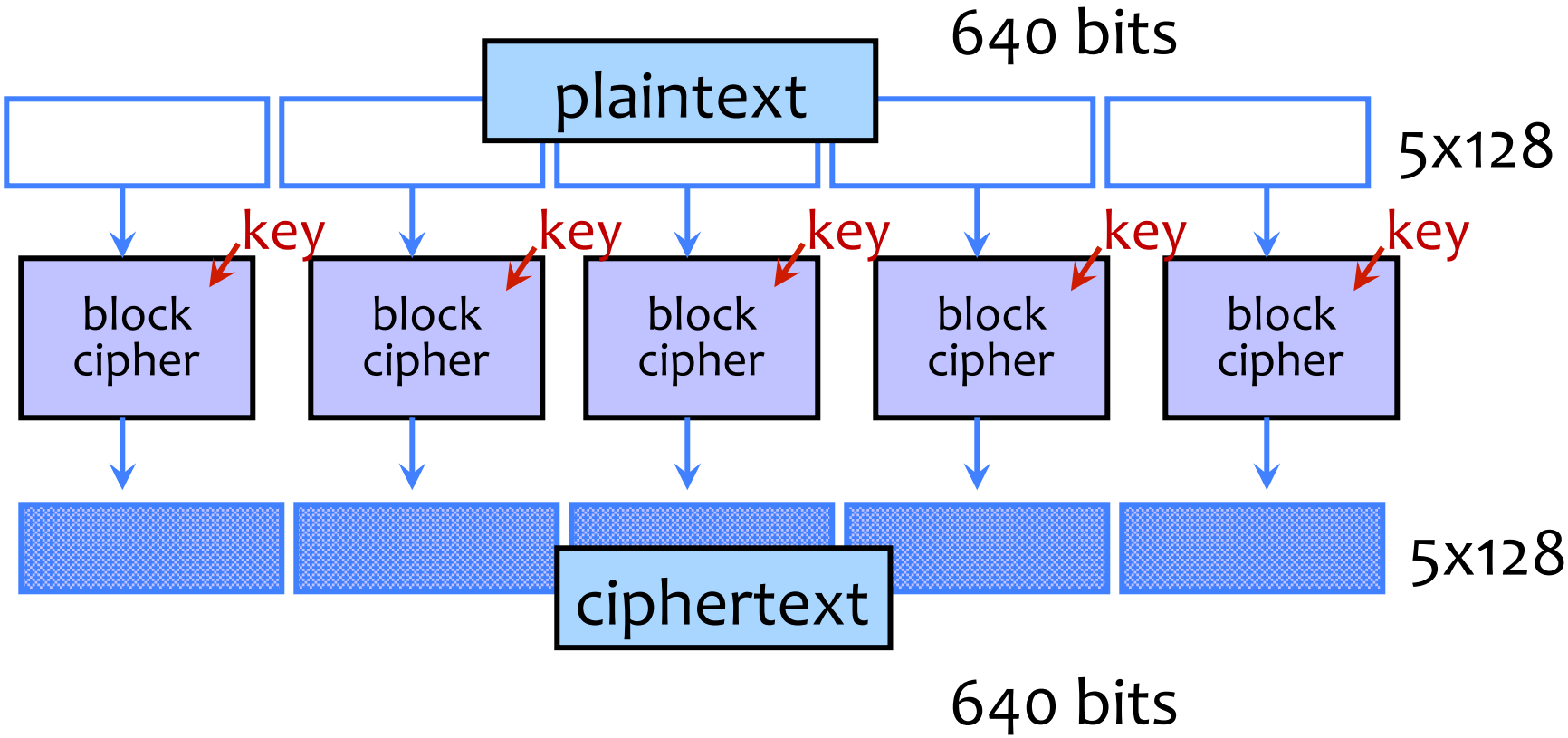
Encrypting a Large Message with AES

- 128-bit block size, but plaintext is longer.

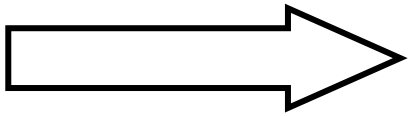


- What should we do?

Electronic Code Book (ECB) Mode



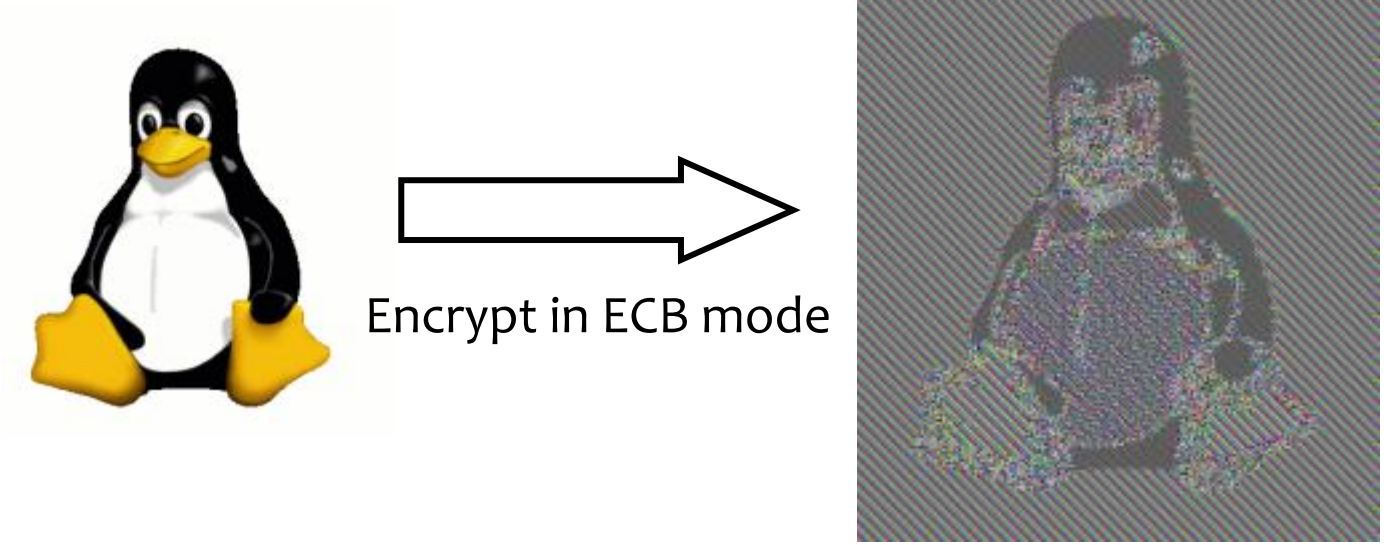
Information Leakage in ECB Mode



Encrypt in ECB mode

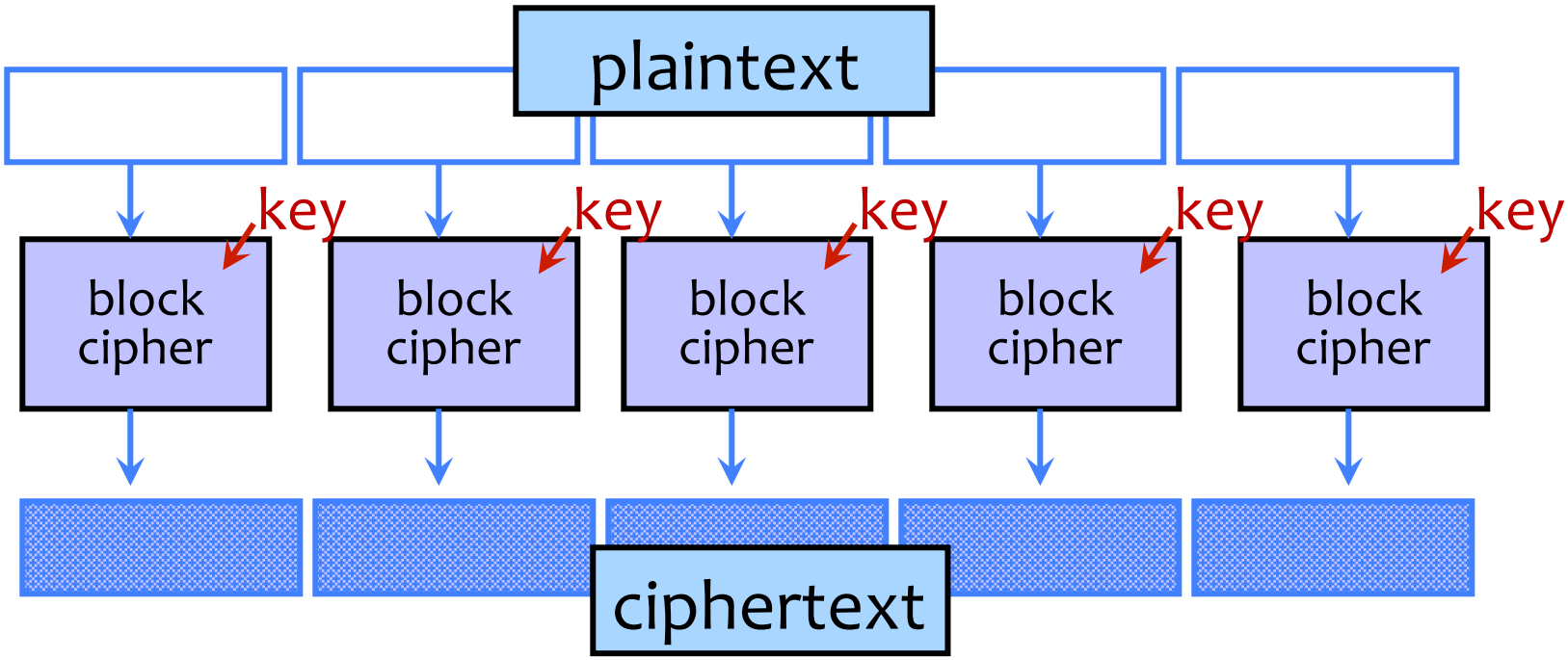
[Wikipedia]

Information Leakage in ECB Mode



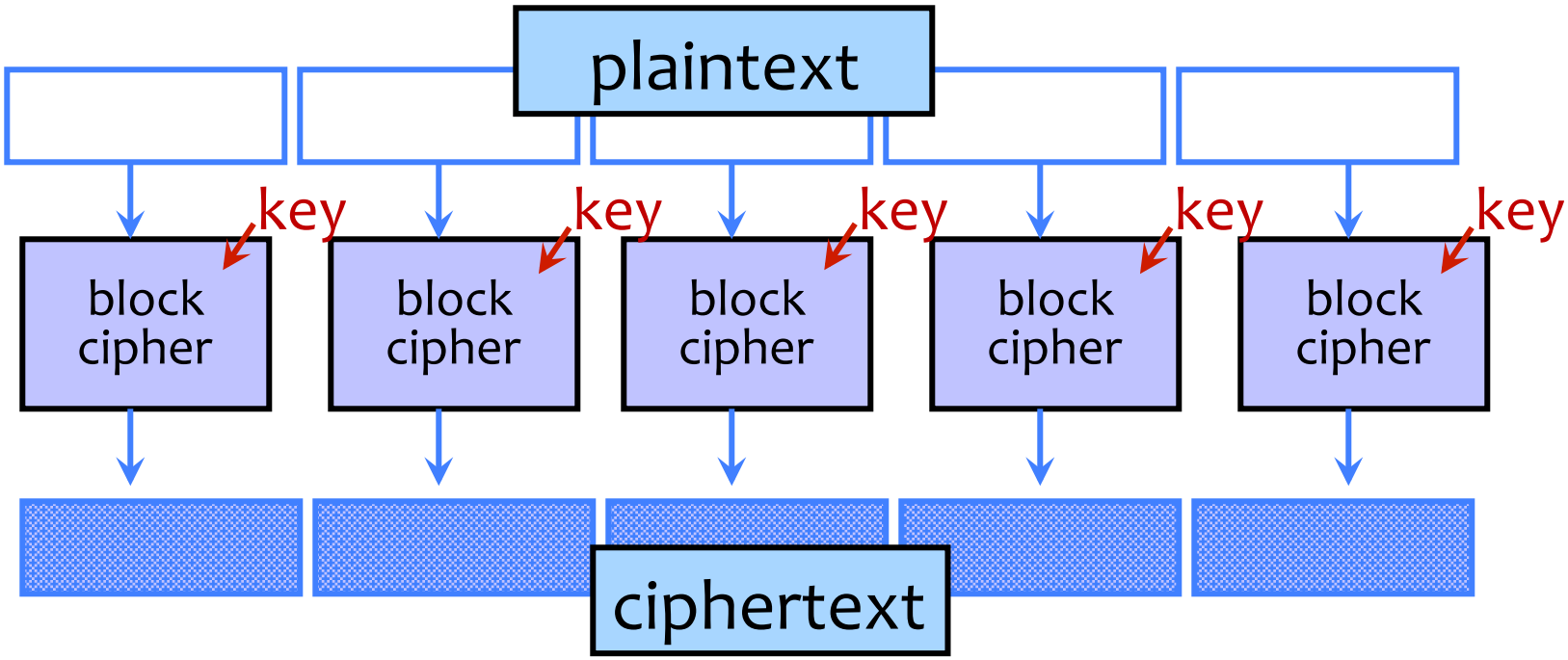
[Wikipedia]

Electronic Code Book (ECB) Mode

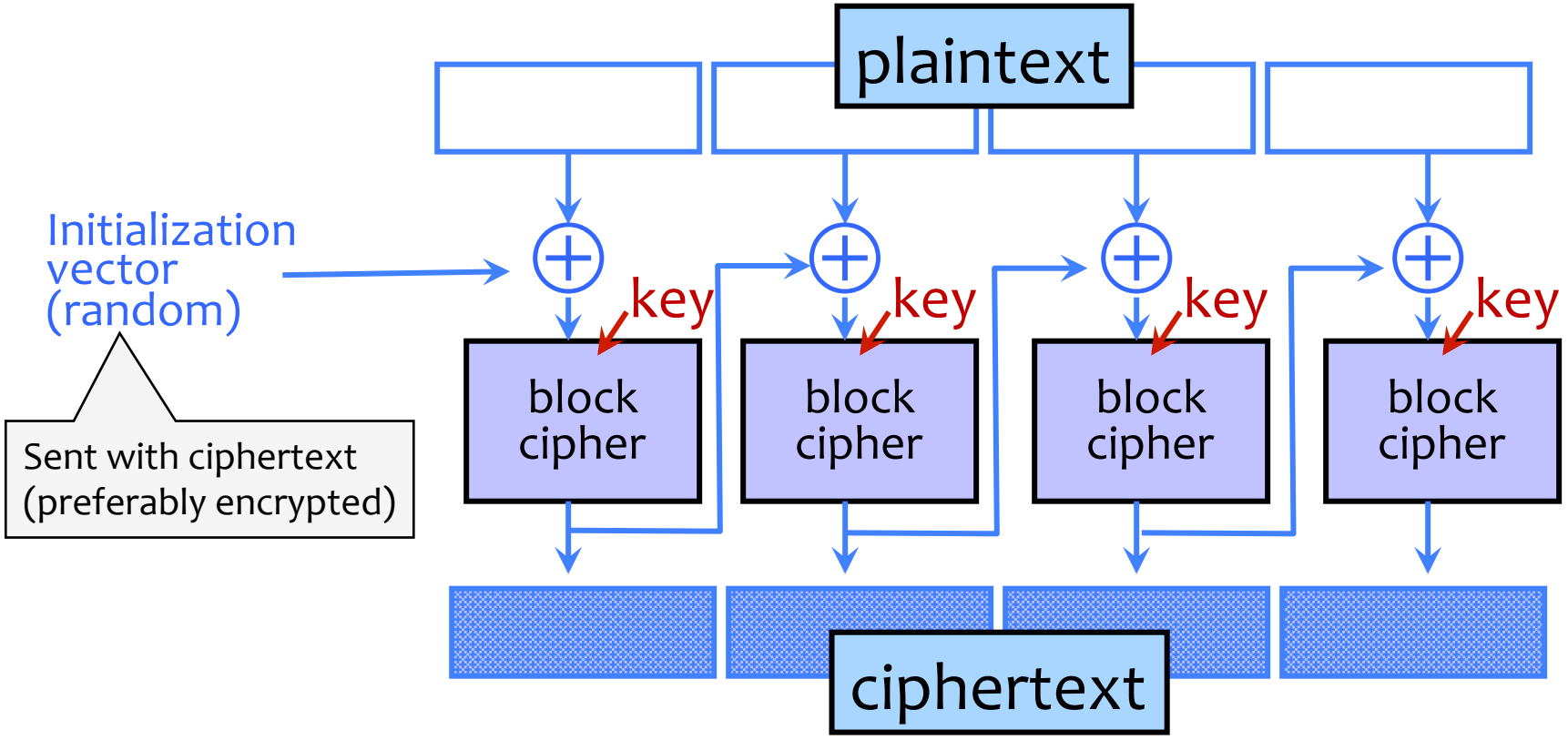


- Identical blocks of plaintext produce identical blocks of ciphertext
- No integrity checks: can mix and match blocks

Cipher Block Chaining (CBC) Mode

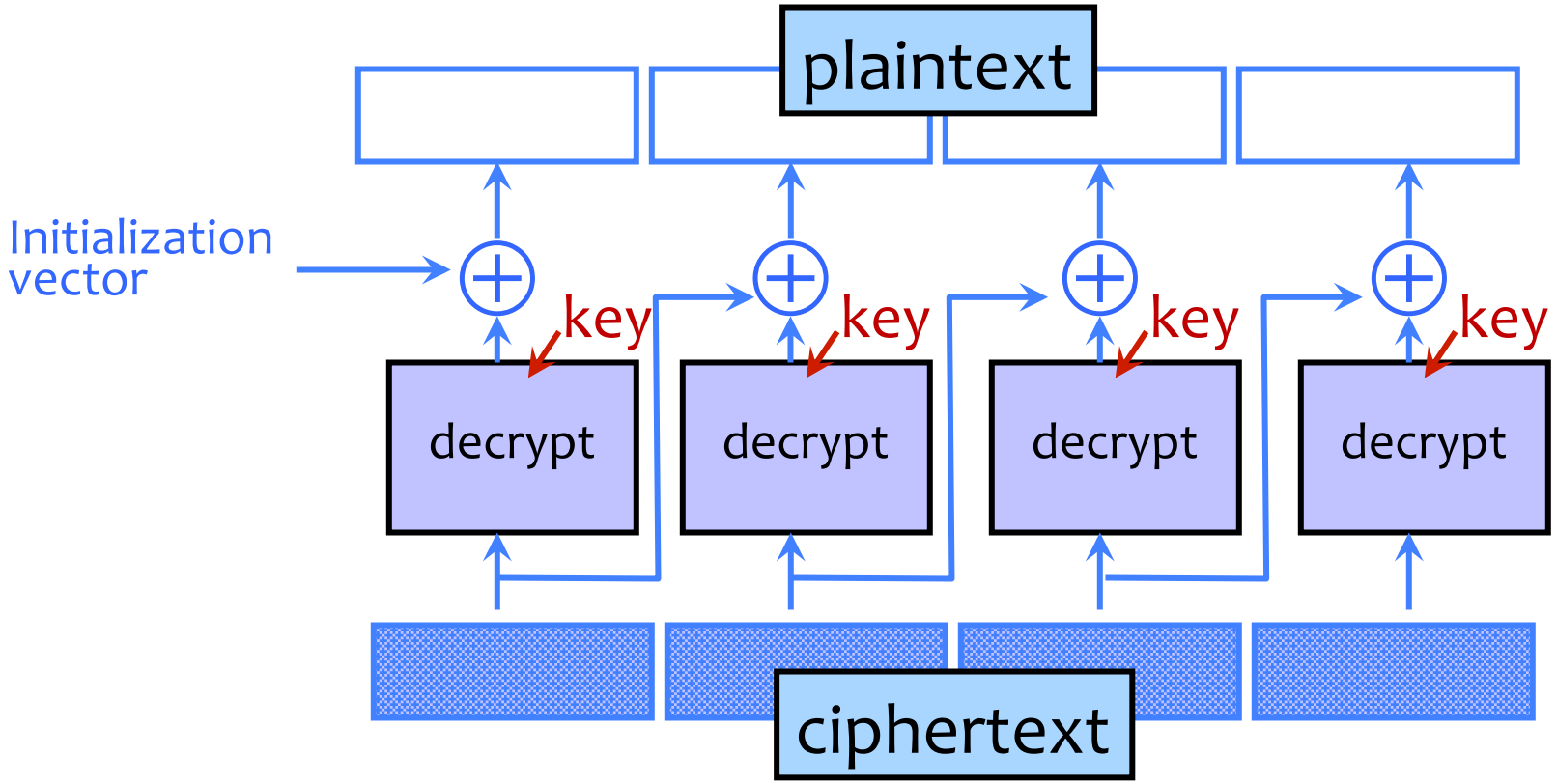


Cipher Block Chaining (CBC) Mode: Encryption

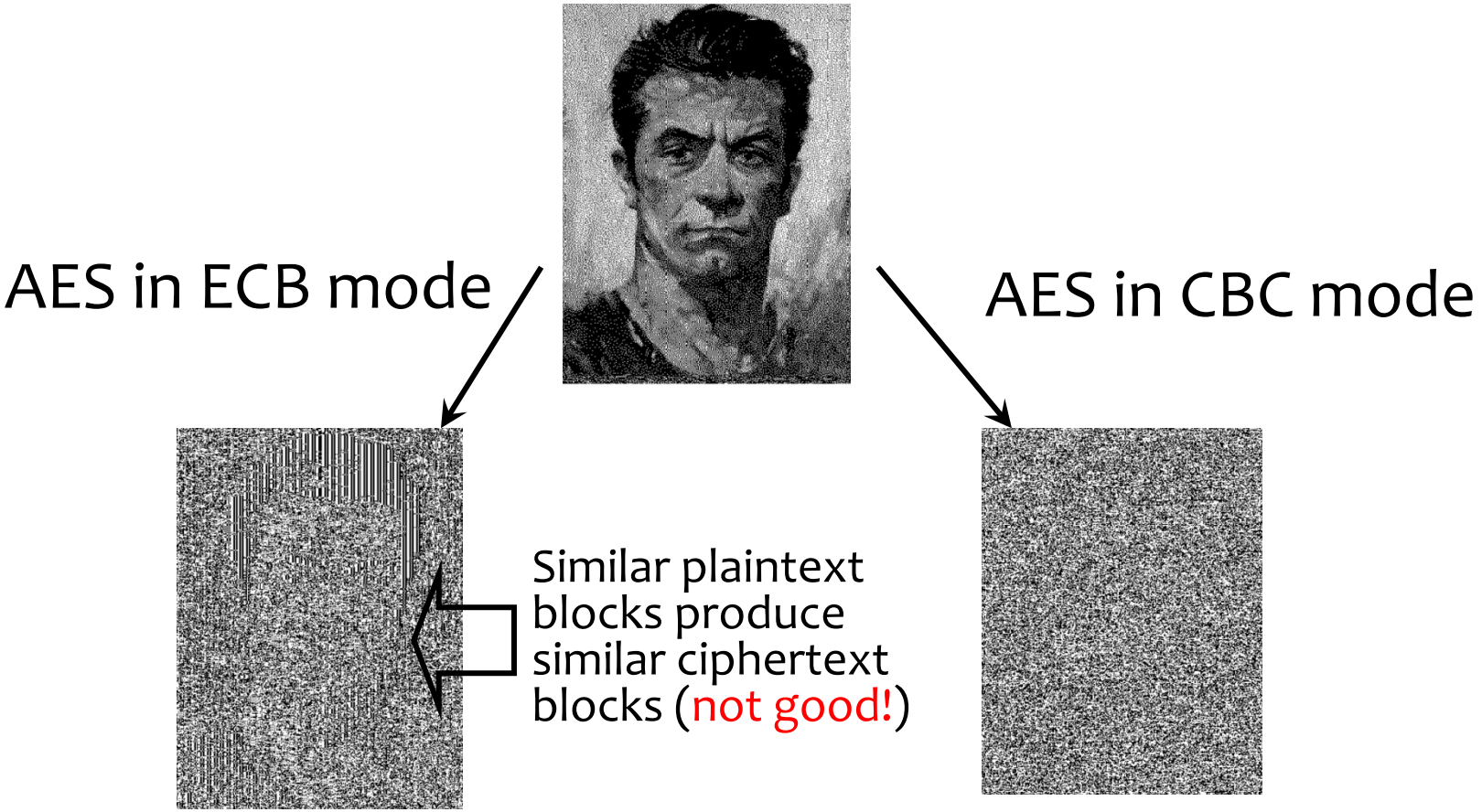


- Identical blocks of plaintext encrypted differently
- Last cipherblock depends on entire plaintext
  - Still does not guarantee integrity

CBC Mode: Decryption

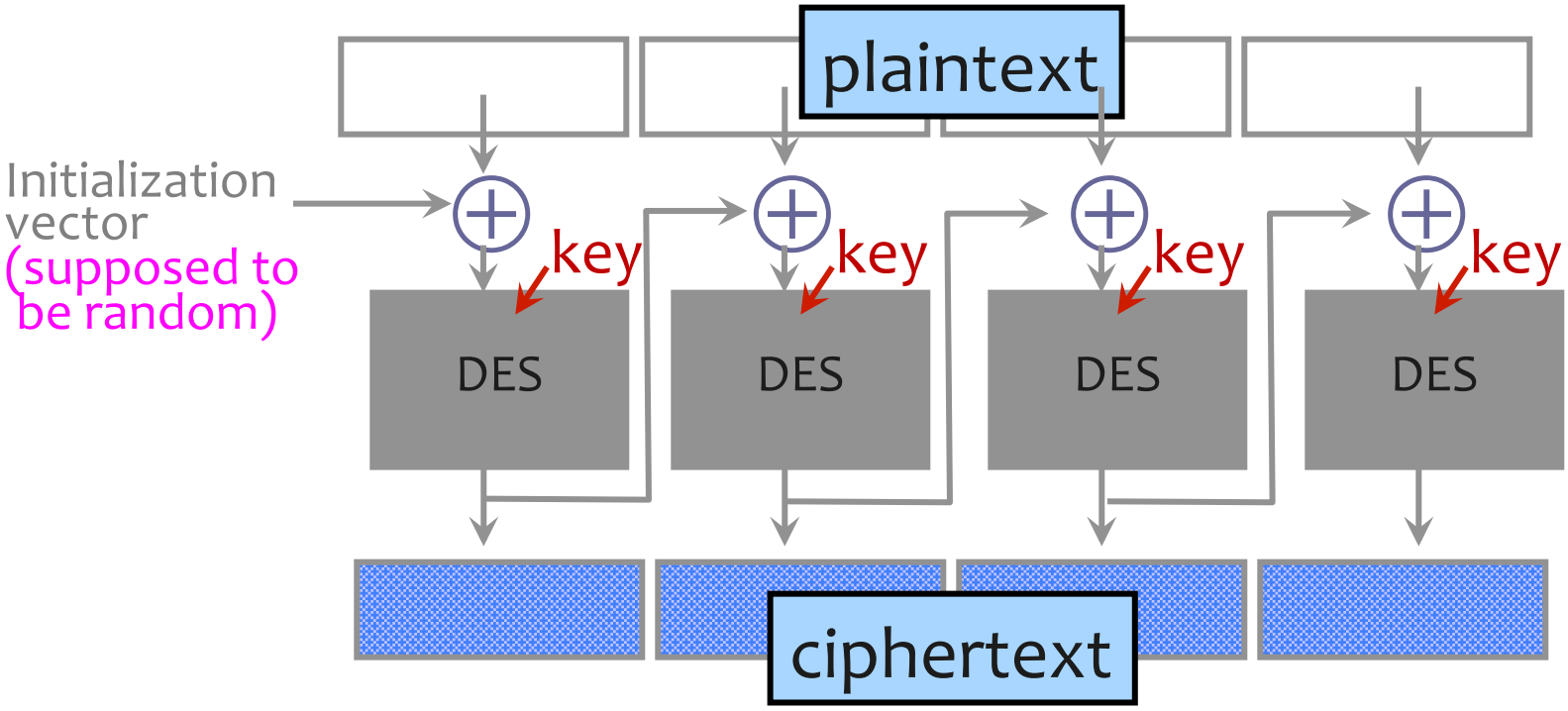


ECB vs. CBC



[Picture due to Bart Preneel]

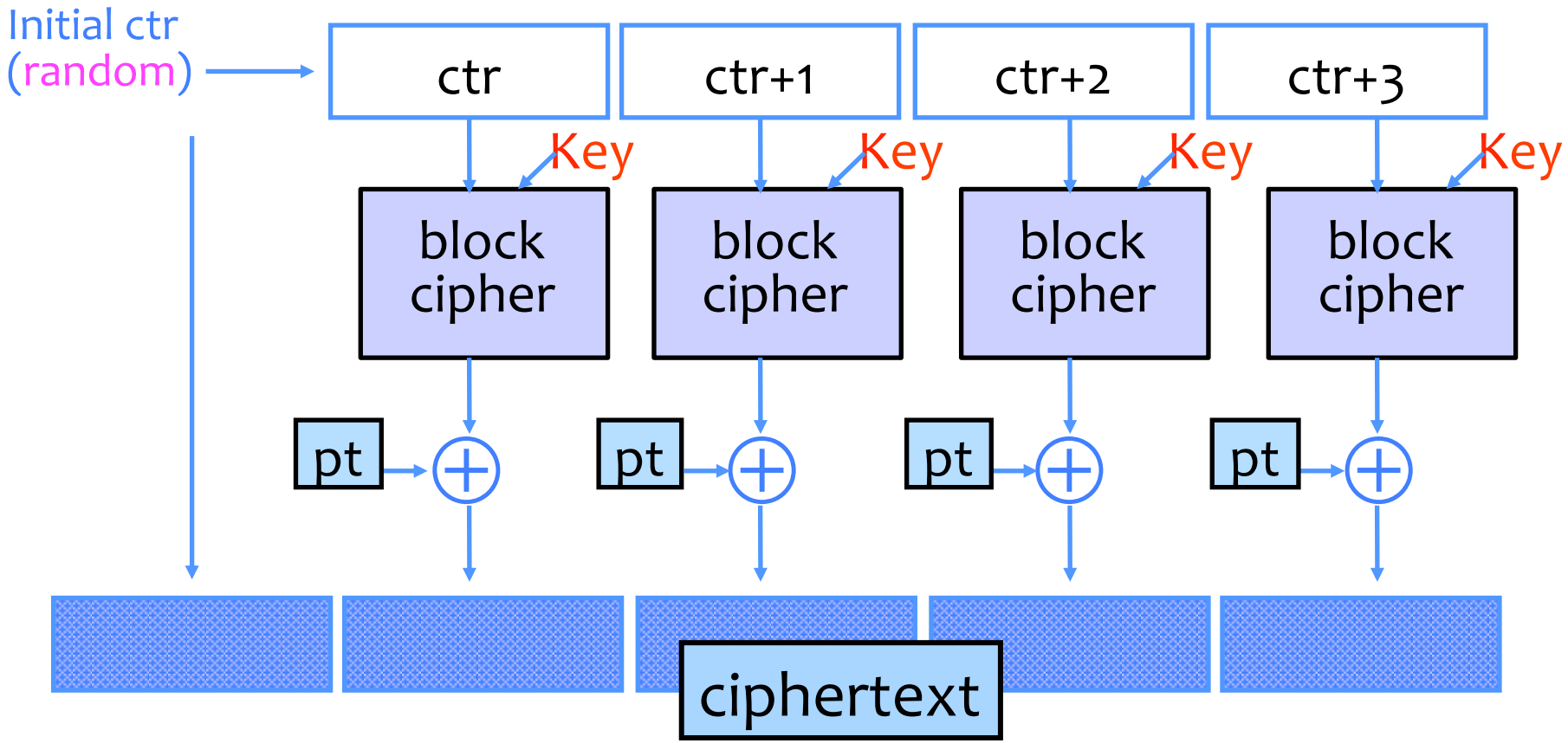
CBC and Electronic Voting



Found in the source code for Diebold voting machines:

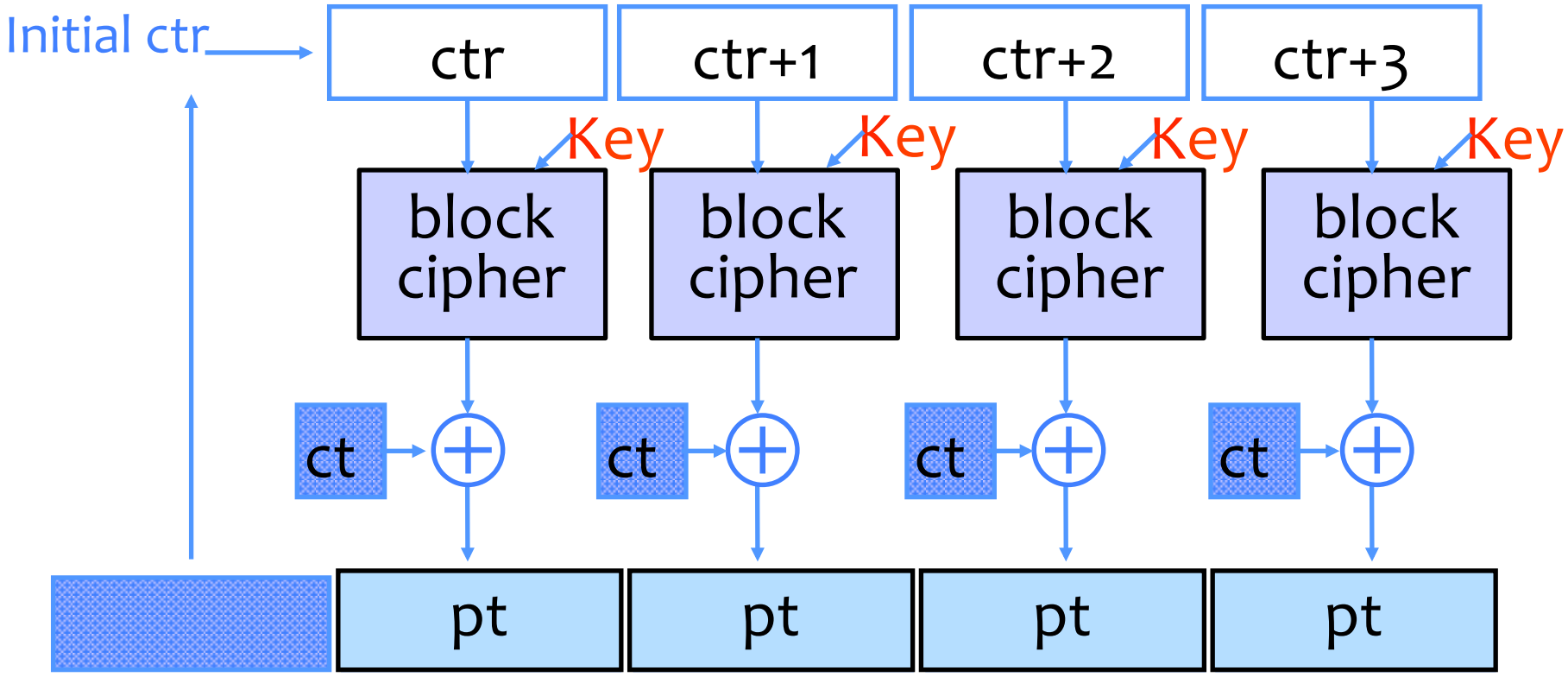
```
DesCBCEncrypt((des_c_block*)tmp, (des_c_block*)record.m_Data,
        totalSize, DESKEY, NULL, DES_ENCRYPT)
```

Counter Mode (CTR): Encryption



- Identical blocks of plaintext encrypted differently
- Can compute in parallel (unlike CBC)
- Still does not guarantee integrity; Fragile if ctr repeats

Counter Mode (CTR): Decryption



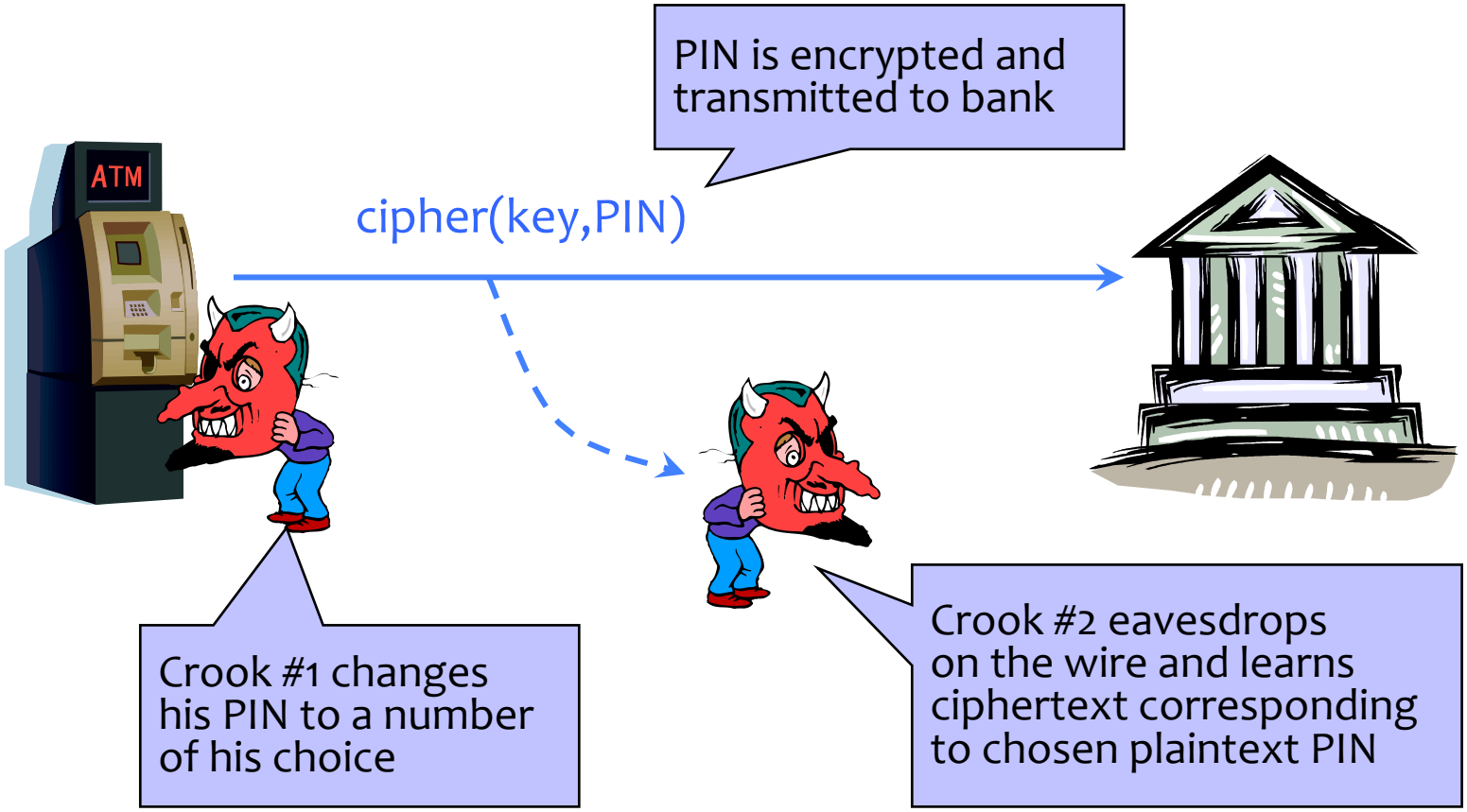
When is an Encryption Scheme "Secure"?

- 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?
- Fixed mapping from plaintexts to ciphertexts?
  - What if attacker sees two identical ciphertexts and infers that the corresponding plaintexts are identical?
  - Implication: encryption must be randomized or stateful

How Can a Cipher Be Attacked?

- Attackers knows ciphertext and encryption algthm
  - 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

Chosen Plaintext Attack



… repeat for any PIN value

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, he cannot verify his guess
  - Every ciphertext is unique, encrypting same message twice produces completely different ciphertexts
- Security against chosen-ciphertext attack (CCA)
  - Integrity protection – it is not possible to change the plaintext by modifying the ciphertext