Lecture 3: Block Ciphers and the Data Encryption Standard

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

January 21, 2017
6:49pm

Goals:

- To introduce the notion of a block cipher in the modern context.
- To talk about the infeasibility of **ideal block ciphers**
- To introduce the notion of the **Feistel Cipher Structure**
- To go over **DES**, the Data Encryption Standard
- **To illustrate some of the DES steps with Python code**

CONTENTS

3.1: IDEAL BLOCK CIPHER

- In a modern block cipher (but still using a classical encryption method), we replace a block of N bits from the plaintext with a block of N bits from the ciphertext. This general idea is illustrated in Figure 1 for the case of $N = 4$. (In general, though, N is set to 64 or multiples thereof.)

- To understand Figure 1, note that there are 16 different possible 4-bit patterns. We can represent each pattern by an integer between 0 and 15. So the bit pattern 0000 could be represented by the integer 0, the bit pattern 0001 by integer 1, and so on. The bit pattern 1111 would be represented by the integer 15.

- In an ideal block cipher, the relationship between the input blocks and the output block is completely random. But it must be invertible for decryption to work. Therefore, it has to be one-to-one, meaning that each input block is mapped to a unique output block.

- The mapping from the input bit blocks to the output bit blocks can also be construed as a mapping from the *integers* corresponding to the input bit blocks to the *integers* corresponding to the output bit blocks.

- The encryption key for the ideal block cipher is the codebook itself, meaning the table that shows the relationship between the input blocks and the output blocks.

- Figure 1 depicts an ideal block cipher that uses blocks of size 4. Each block of 4 bits in the plaintext is transformed into a block of 4 ciphertext bits.

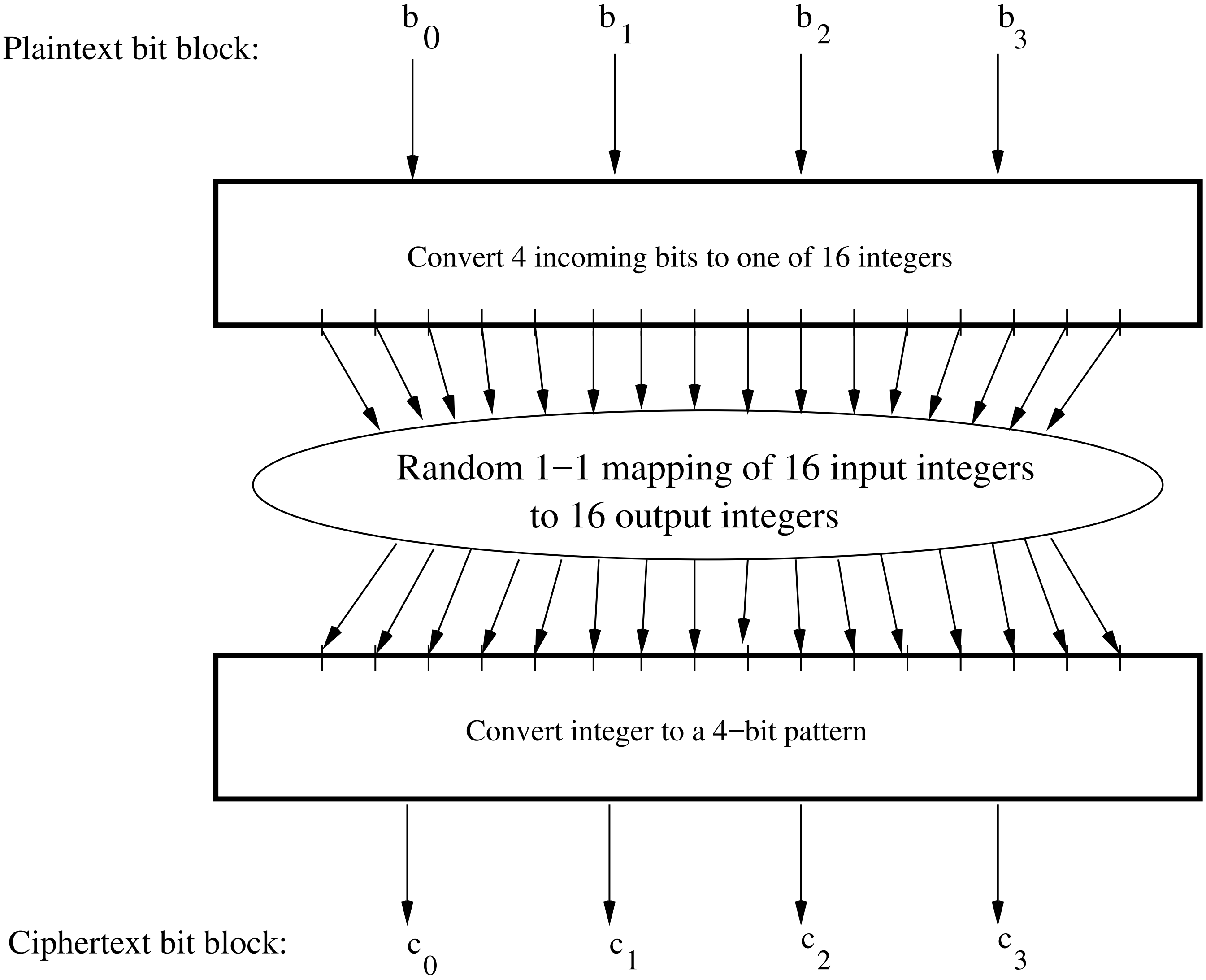
Plaintext bit block:
b_0
b_1
b_2
b_3
Convert 4 incoming bits to one of 16 integers
Random 1−1 mapping of 16 input integers to 16 output integers
Convert integer to a 4−bit pattern
Ciphertext bit block:
c_0
c_1
c_2
c_3

Figure 1: *The ideal block cipher when the block size equals 4 bits.* (*This figure is from Lecture 3 of "Lecture Notes on Computer and Network Security" by Avi Kak*)