

# 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

©2017 Avinash Kak, Purdue University



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

	<i>Section Title</i>	<i>Page</i>
<b>3.1</b>	<b>Ideal Block Cipher</b>	3
3.1.1	Size of the Encryption Key for the Ideal Block Cipher	6
<b>3.2</b>	<b>The Feistel Structure for Block Ciphers</b>	7
3.2.1	Mathematical Description of Each Round in the Feistel Structure	10
3.2.2	Decryption in Ciphers Based on the Feistel Structure	12
<b>3.3</b>	<b>DES: The Data Encryption Standard</b>	16
3.3.1	One Round of Processing in DES	18
3.3.2	The S-Box for the Substitution Step in Each Round	22
3.3.3	The Substitution Tables	26
3.3.4	The P-Box Permutation in the Feistel Function	30
3.3.5	The DES Key Schedule: Generating the Round Keys	32
3.3.6	Initial Permutation of the Encryption Key	35
3.3.7	Contraction-Permutation that Generates the 48-Bit Round Key from the 56-Bit Key	38
<b>3.4</b>	<b>What Makes DES a Strong Cipher (to the Extent It is a Strong Cipher)</b>	41
<b>3.5</b>	<b>Homework Problems</b>	43

## 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* correspond-

ing 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.

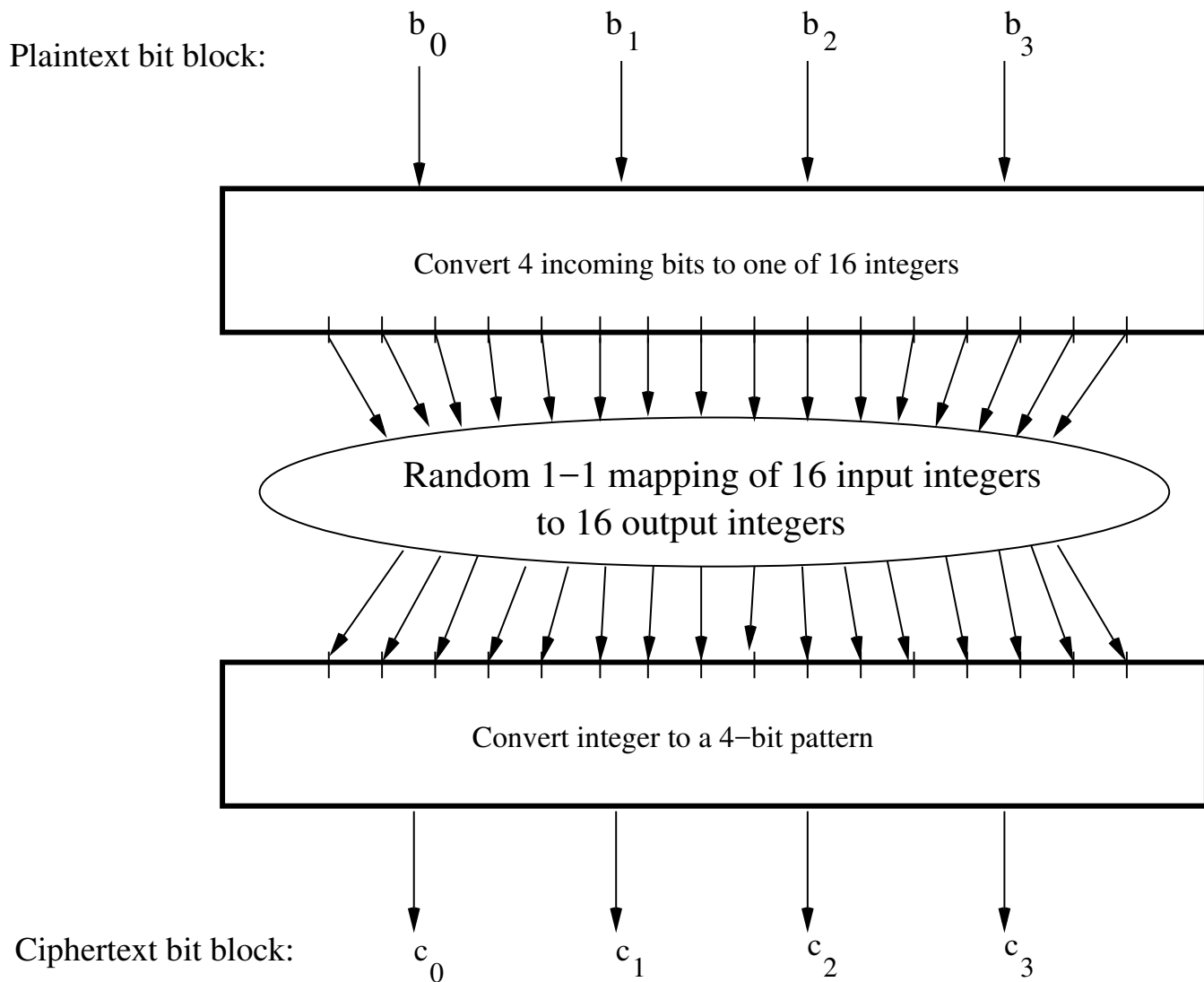


Figure 1: *The ideal block cipher when the block size equals 4 bits.* (This figure is from Lecture 3 of “Lecture Notes on Computer and Network Security” by Avi Kak)

[Click here to download full PDF material](#)