COURSE TECHNOLOGY
CENGAGE Learning™

BẢO MẬT THÔNG TIN

ThS Đàm Quang Viễn

COURSE TECHNOLOGY
CENGAGE Learning™

Chương 3

MÃ HÓA ĐỐI XỨNG HIỆN ĐẠI

Summary

- 1. Lập sơ đồ khối mã hoá DES. Nêu các đặc trưng của DES.
- 2. Lập sơ đồ khối mã hoá AES. Nêu các đặc trưng của AES.
- 3.. Mô tả các đặc trưng mã khối, chuẩn mã DES, chuẩn mã nâng cao

BÀI TẬP SINH VIÊN

1. Cho khóa k = **133457799bbcdff1** , lập khóa con K1 sinh từ K
2. Một bản rõ nội dung ***0123456789ABCDEF***
   mã hóa theo Des tìm E(R0)và tìm E(R0)⊕K1
3. Tính thay thế S-Box tương ứng với câu 2
4. Tìm đầu ra của S-box
5. Tìm hoán vị P của đầu ra ở câu 4
6. Tìm R1 và L1

BÀI TẬP SINH VIÊN

$E(R_0)$	=	011110100001010101010101011110100001010101010101
K_1	=	000110110000001011101111111110001110000011100 10
$E(R_0) \oplus K_1$	=	011000010001011110111010100001100110010100100111
Đầu ra S-Box	=	010111001000001010110101100 10111
$f(R_0,K_1)$	=	00100011010010101010100110111011
$L_2=R_1$	=	11101111010010100110010101000100