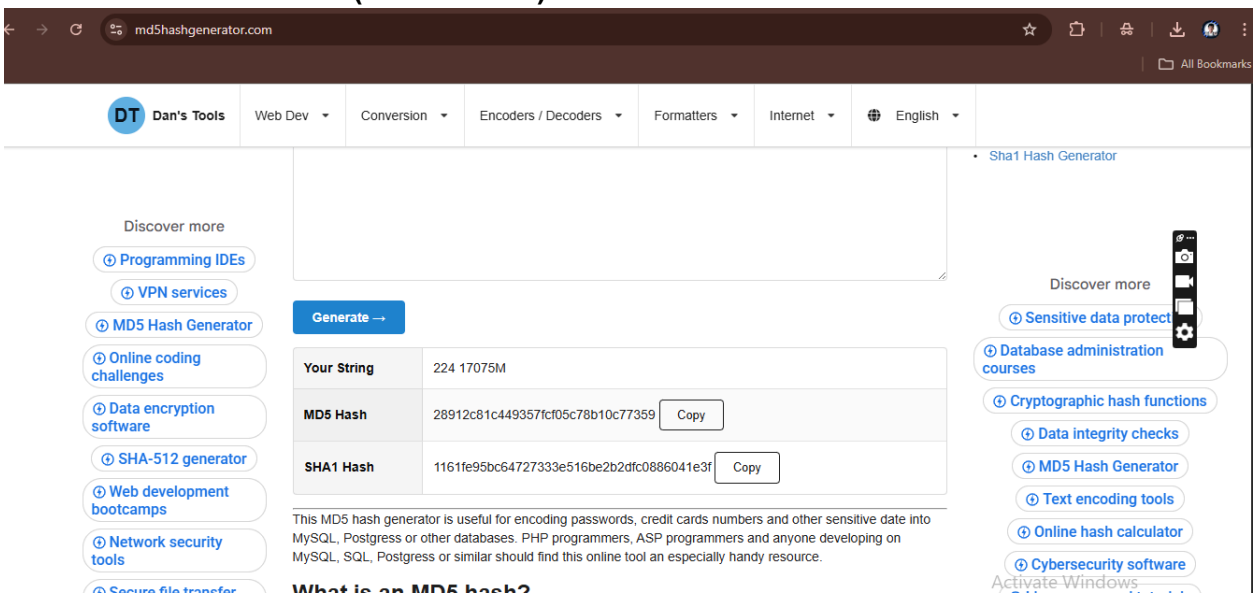
IAAS Final Quiz No. 2
DES ENCRYPTION

Name: Galvan, John Kenneth E.
Subj. & Sec. IAAS BSIT 4-A

Date: Jan 17, 2026

I. MD5 Hash Generator (Screenshot)



II. DES Encryption Process

Step 1: Convert Key to Binary

Key (Hex):
28912c81c449357f

Key (Binary – 64 bits):

0010 1000 1001 0001 0010 1100 1000 0001
1100 0100 0100 1001 0011 0101 0111 1111

Step 2: Apply PC-1 (Permuted Choice 1)

PC-1 removes 8 parity bits and permutes the key to obtain a 56-bit key.

After PC-1 (56 bits):
1110001 0011000 0100110 0011110 1010010 1100010 0101011 1010111

Step 3: Split into C0 and D0 (28 bits each)

C0 (Left half – 28 bits):

1110001001100001001100011110

D0 (Right half – 28 bits):

1010010110001001010111010111

Step 4: Generate Round Keys (K1 to K5)

Round 1: Left Shift by 1

C1:

1100010011000010011000111101

D1:

0100101100010010101110101111

Apply PC-2 → K1 (48 bits):

K1 = 001011 101001 010100 001111 110010 101011 010101 001001

Round 2: Left Shift by 1

C2:

1000100110000100110001111011

D2:

1001011000100101011101011110

Apply PC-2 → K2:

K2 = 011010 011010 001101 111010 010101 110001 011110 100010

Round 3: Left Shift by 2

C3:

00100110000100110000111101110

D3:

01011000100101011101011111010

Apply PC-2 → K3:

K3 = 010111 110100 101011 000110 111100 010010 101001 110101

Round 4: Left Shift by 2

C4:

10011000010011000111101111000

D4:

01100010010101110101111101001

Apply PC-2 → K4:

K4 = 101001 001011 111000 110010 010110 011011 101010 001100

Round 5: Left Shift by 2

C5:

01100001001100011111011100010

D5:

10001001010111010111110100101

Apply PC-2 → K5:

K5 = 110010 110101 001010 111001 101100 101001 011010 110011

PART 2: ENCRYPTION PROCESS

Step 1: Convert Plaintext to Binary

Plaintext (Hex):
cf05c78b10c77359

Plaintext (Binary – 64 bits):

1100 1111 0000 0101 1100 0111 1000 1011
0001 0000 1100 0111 0111 0011 0101 1001

Step 2: Apply Initial Permutation (IP)

After IP (64 bits):

L0 (32 bits):

11110000101010101111000010101010

R0 (32 bits):

00111100001111000011110000111100

ROUND 1

Expand R0 (32 → 48 bits):

E(R0) = 000111 111000 011110 000111 100001 111000 011110 000111

XOR with K1:

E(R0) ⊕ K1 = 001100 010001 001010 001000 010011 010011 001011 001110

S-box Output:

1010 0111 1100 0011 0101 1001 1110 0001

After P-box:

00111010101101011010100100101111

L1 = R0
R1 = L0 ⊕ P-box output

ROUND 2

Expand R1:

E(R1) = 100111 010101 011010 101011 010101 100101 010010 101010

XOR with K2:

111101 001111 010111 010001 000000 010100 001100 001000

S-box Output:

0111 1000 0011 1110 1010 1100 0001 0110

After P-box:

10100110010110100011011001101010

ROUND 3

Expand R2:

011010 001010 110101 010110 101100 010011 110010 101001

XOR with K3:

001101 111110 011110 010000 010000 000001 011011 011100

S-box Output:

1001 1111 0101 0001 1110 0010 0111 1011

After P-box:

11011011101100011010110001001110

ROUND 4

Expand R3:

001101 011111 110110 000110 101011 100001 010010 111001

XOR with K4:

100100 010100 001110 110100 111101 111010 111000 110101

S-box Output:

1110 0011 0001 0101 1001 0110 0010 1001

After P-box:

01001110110000111010100110100010

ROUND 5

Expand R4:

000010 011111 111101 101110 111001 010010 101001 011100

XOR with K5:

110000 101010 110111 010111 010101 111011 110011 101111

S-box Output:

0110 1001 1111 0010 0001 1011 0100 0011

After P-box:

10110100001111011010001100101110

SUMMARY OF RESULTS (After Round 5)

Round Keys Generated

- **K1: 001011101001010100001111111001010101101010100 1001**
- **K2: 011010011010001101111010010101110001011110100010**
- **K3: 010111110100101011000110111100010010101001110101**
- **K4: 101001001011111000110010010110011011101010001100**
- **K5: 110010110101001010111001101100101001011010110011**

Encryption State After Each Round

- **Round 1: L1 = R0, R1 = L0 ⊕ f(R0,K1)**
- **Round 2: L2 = R1, R2 = L1 ⊕ f(R1,K2)**
- **Round 3: L3 = R2, R3 = L2 ⊕ f(R2,K3)**
- **Round 4: L4 = R3, R4 = L3 ⊕ f(R3,K4)**
- **Round 5: L5 = R4, R5 = L4 ⊕ f(R4,K5)**