Question 1:

Initial Permutation (IP):
Apply the initial permutation to the 64-bit input data.

bit #	58	50	42	34	26	18	10	2
bit	1	0	0	1	0	0	1	0
bit #	60	52	44	36	28	20	12	4
bit	0	0	0	0	0	0	1	0
bit #	62	54	46	38	30	22	14	6
bit	0	1	0	0	0	1	1	0
bit #	64	56	48	40	32	24	16	8
bit	1	1	1	1	0	0	1	0
bit #	57	49	41	33	25	17	9	1
bit	0	1	0	0	1	0	1	1
bit #	59	51	43	35	27	19	11	3
bit	0	0	0	1	0	0	0	0
bit #	61	53	45	37	29	21	13	5
bit	1	0	0	1	0	0	1	0
bit #	63	55	47	39	31	23	15	7
bit	0	1	1	0	0	0	0	1

Round 1:
1. L0 = 01001011001011000100100001100100
   R0 = 11110110010101101000011111011010
2. E(R0) = 1111000000110011011110110100100101100001001000
3. E(R0) XOR Subkey1 = E(R0) XOR K1

Perform S-box substitution

For S1, S2, S5, and S6, we have:

S1: 1101 -> 5
S2: 1010 -> A
S5: 1010 -> A
S6: 1010 -> A

For S3, S4, S7, and S8, we have:

S3: 1000 -> 8
S4: 1000 -> 8

S7: 0001 -> 1
S8: 1001 -> 9
Concatenate the results from the S-boxes:

S1 S2 S5 S6 S3 S4 S7 S8
5 A A A 8 8 1 9

Now, let's calculate the XOR of these results with L0:
L0 XOR P4(S1, S2, S5, S6, S3, S4, S7, S8)
L0 = 01001011001011000100100001100100
P4(S1, S2, S5, S6, S3, S4, S7, S8) = 0110111011101100
L1 = L0 XOR P4(S1, S2, S5, S6, S3, S4, S7, S8) = 0010010111000000

Now, for R0, we have:
R0 = 11110110010101101000011111011010

Now, swap the positions of L0 and R0 to prepare for the next round:

L1 = 0010010111000000
R1 = 11110110010101101000011111011010
Now, we'll calculate the values for the second round:

Round 2:
Sure, let's continue with the calculations for the second round (Round 2) of the reduced DES:

Round 2:
Expand R1 to 48 bits:

E(R1) = 111100001010101010001011001010111010010101110

XOR the expanded R1 with the 48-bit subkey for round 2 (derived from the 56-bit key):

For the second round, we need to derive the subkey from the original 56-bit key. Here's how we generate Subkey 2:

Original 56-bit key:
11010100010000101100111111001100101011001000101100000

After a left circular shift by one:
10101000100001011001111110011001010110010001011000001

Discard the first and last bits in both halves:
Left half:
01010001000010110011111100110010101100100010110000
Right half:
01010001000010110011111100110010101100100010110000

Perform a permutation choice 2 (PC-2) to obtain the 48-bit subkey for the second round:

PC-2(Subkey 2) = 1000001111100001101001110001010010000110010000

Now, XOR the expanded R1 with the derived Subkey 2:
E(R1) XOR Subkey2 = 111100001010101010001011001010111010010101110
XOR 1000001111100001101001110001010010000110010000

Perform this XOR operation bit by bit:

XOR Result: 0111001101001011001011000011111100100011001100
Apply the S-boxes to the result:

S1: 1100 -> C
S2: 1101 -> D
S5: 1011 -> B
S6: 0001 -> 1
S3: 1000 -> 8
S4: 1111 -> F
S7: 0011 -> 3
S8: 1000 -> 8
Concatenate the results from the S-boxes:
S1 S2 S5 S6 S3 S4 S7 S8
C D B 1 8 F 3 8

Perform a permutation (P4) on the output of the S-boxes:
P4(CDB18F38) = 1010101100011000

XOR the result of the previous step with L1 (left half from round 1):
L1 = 0010010111000000
P4(CDB18F38) = 1010101100011000
L2 = L1 XOR P4(CDB18F38) = 1000111011011000

Now, for R1, we have:
R1 = 0111001101001011001011000011111100100011001100

Now, swap the positions of L1 and R1 to prepare for the final permutation (FP):
L2 = 1000111011011000
R2 = 0111001101001011001011000011111100100011001100
Finally, perform the final permutation (FP) by reversing the initial permutation (IP) to obtain the ciphertext:

bit #	58	50	42	34	26	18	10	2
bit	1	0	0	1	0	0	1	0
bit #	60	52	44	36	28	20	12	4
bit	0	0	0	0	0	0	1	0
bit #	62	54	46	38	30	22	14	6
bit	0	1	0	0	0	1	1	0
bit #	64	56	48	40	32	24	16	8
bit	1	1	1	1	0	0	1	0
bit #	57	49	41	33	25	17	9	1
bit	0	1	0	0	1	0	1	1
bit #	59	51	43	35	27	19	11	3
bit	0	0	0	1	0	0	0	0
bit #	61	53	45	37	29	21	13	5
bit	1	0	0	1	0	0	1	0
bit #	63	55	47	39	31	23	15	7
bit	0	1	1	0	0	0	0	1

So, the ciphertext after the second round of reduced DES is:
0100110000111101 0010001101010101

Question 2:

a- Convert the given 128-bit input to Hexadecimal form:

Input:
0110101000110101010100110010000101101000100111111101110000101010

Hexadecimal representation: 6A35A426FD0A

b- Write the input in a state diagram (4 by 4 matrix):

State Matrix:
6A 35 A4 26
FD 0A BC 01

c- Apply SubBytes Step:

Substitute each byte in the state matrix using the AES S-box:

Substituted State Matrix:
8D E1 D2 71
53 F4 E7 F0

d- Apply ShiftRows Step:

Shift the rows of the state matrix:

Shifted State Matrix:
8D E1 D2 71
F4 E7 F0 53

e- Apply MixColumns Step:

Apply the MixColumns operation using the irreducible polynomial $P(x) = x^8 + x^4 + x^3 + x + 1$:

Mixed State Matrix:

1A 58 29 9F
2F E1 05 33

f- Apply AddRoundKey Step:

Use the given round key to perform the XOR operation with the state matrix:

Round Key:
0A 5A 6E 1E
2F D2 1B 7E
01 0D 06 14
25 E6 12 7F

Result after AddRoundKey:
10 02 44 4F
00 33 1D 4D
These are the results at each step of the AES encryption process. The final state matrix, after applying all steps, is `10 02 44 4F 00 33 1D 4D`.

Question 3:

A)

i. $37 \cdot 3 \; mod \; 23$

$37 \cdot 3 = 111$
111 mod 23 = 19

ii. $19 \cdot 13$ mod 23

$19 \cdot 13 = 247$
(247\mod 23 = 6

iii. $18 \cdot 15$ mod 12

$18 \cdot 15 = 270$
(270\ mod 12 = 6

iv. $15 \cdot 29 + 11 \cdot 15$ mod 23

$15 \cdot \; 29 = 435$
$11 \cdot 15 = 165$
435 + 165 = 600
(600\ mod 23 = 5

B)

i.GCD of 8 and 17:

$17 = 2 \cdot 8 + 1$
$8 = 8 \cdot 1$

The remainder is 1, so the GCD of 8 and 17 is 1.

ii. GCD of 5 and 17:

$17 = 3 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$
$2 = 2 \cdot 1$

The remainder is 1, so the GCD of 5 and 17 is 1.

iii. GCD of 5 and 37:

$37 = 7 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$
$2 = 2 \cdot 1$

The remainder is 1, so the GCD of 5 and 37 is 1.

iv. GCD of 10 and 15:

$15 = 1 \cdot 10 + 5$
$10 = 2 \cdot 5$

The remainder is 5, so the GCD of 10 and 15 is 5.

C)

i. 8^(-1) mod 17:

$17 = 2 \cdot 8 + 1$
$8 = 8 \cdot 1$

$1 = 17 - 2 \cdot 8$
$1 = 17 - 2(17 - 2 \cdot 8)$
$1 = 3 \cdot 17 - 2 \cdot 8$

$-2 + 17 = 15$

So, 8^(-1) mod 17 = 15

ii. 5^(-1) mod 17:

$17 = 3 \cdot 5 + 2$
$5 = 2 \cdot + 1$
$2 = 2 \cdot 1$

$1 = 5 - 2$
$1 = 5 - (17 - 3 \cdot 5)$
$1 = 4 \cdot 5 - 17$

$4 + 17 = 21$

So, 5^(-1) mod 17 = 4

iii. 5^(-1) mod 37:

$37 = 7 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$
$2 = 2 \cdot 1$

$1 = 5 - 2$
$1 = 5 - (37 - 7 \cdot 5)$
$1 = 8 \cdot 5 - 37$

$8 + 37 = 45$

So, 5^(-1) mod 37 = 45

iv. 10^(-1) mod 15:

15 = 1· 10 + 5
10 = 2·5 + 0

5 = 15 - 10
5 = 15 - (15 - 10)
5 = 2·15 - 15

2 + 15 = 17

So, 10^(-1) mod 15 = 17
D)

To find all elements in modulo 216 with no multiplicative inverse, we need to identify elements that are not coprime to 216.

216 can be factored as (2^3 · 3^3).

Elements that have common factors with 216 (other than 1) are multiples of 2 or 3. So, the elements in modulo 216 with no multiplicative inverses are:

- All even numbers (multiples of 2).
- All multiples of 3 that are not multiples of 2.

In other words, all elements of the form (2k) (where (k) is an integer) and all elements of the form (3m) (where (m) is an integer and (3m) is not a multiple of 2) have no multiplicative inverses modulo 216.