■2 null bytes, 64 encoding?

AAA=

■Characteristics of Feistel Structure?

1. LD0 = RE16, LE16 = RD0, KE1 = KD16, regardless of Feistel function

$$LE_i = RE_{i-1}$$
$$RE_i = LE_{i-1} \oplus F(RE_{i-1}, K_i)$$

■constrain of Feistel function?

No

■Why permutation expension?

Let the 4-bit substitution be a function of previous and next segments

■what happen if replace all the values in the S-boxes with 0s?

because A OXR 0 = A, plaintext will be unchanged for every round and has no encryption

■round key generation of DES?

1. First 7 bits in each byte of the 8-byte key are extracted and permuted with key_permutation_1 table as a 56-bit encryption key.
2. 56-bit key is divided into 2 28-bit halves and each half is circularly shifted to the left by 1 or 2 bits depending on the round
3. Combined the 2 shifted halves as a 56-bit block, extract 48 bits and permute it with key_permutation_2 table as a 48-bit round key for a round.

■diffusion and confusion in DES? (avalanche effect)

1. Expansion permutation and substitution steps in DES enhance the diffusion in DES, so 1-bit change in the input plaintext block in average affect 34 bits of the output ciphertext block.
2. Round keys generated from the encryption key enhance the confusion in DES, so 1-bit change in the encryption key on average affect 35 bits of the ciphertext

■The property of Feistel structure?

Feistel function can be arbitrally defined and still working

■why expanded-permutation is “permutation”?

permutation is rearranged the origin plain text (same size in same size out). Because this operation changes the order of the bits as well as repeating certain bits.

■stepping stones to understand finite field?

Set, group, abailien group, ring, communitive ring, integral domain, field

■When does a set becoming a group?

A set of objects with a binary operator applying on the elements of set and satisfies 4 properties:

Closure: a∈ s, b ∈ s, a + b ∈ s,

Associativity: (a+b)+c = a+ (b+c)

existence of a unique identity element: for every a in the set, a○i= a

existence of an inverse element for each element: a○b= i

■example of infinite group and finite group?

Infinite group: The set of all integers with addition as operator

Finite group: a sequence with permutation operation. EX. $\mathbf{S_3} = <\mathbf{1,2,3}>$, $\mathbf{P_3} = \{<\mathbf{1,2,3}>,<\mathbf{1,3,2}>,<\mathbf{2,1,3}>,<\mathbf{2,3,1}>,<\mathbf{3,1,2}>,<\mathbf{3,2,1}>\}$

■how a group become ring?

Group operator is commutative: a○b = b○a

ring operator satisfies: closure, associativity, distributive over group operator

1. $a \times (b + c) = a \times b + a \times c$
2. $(a+b) \times \mathbf{c} = a \times c + a \times c$

■communitive ring become integral domain?

i. The communitive ring R include an identity element for the ring operation. a1 = 1a = a

ii. Let 0 denote the identity element for the group operation. If a ring operation of any two elements a and b of R results in 0, then either a or b must be 0.

■what a field has more than an integral domain

For every element a in F, except the element 0 (identity element of group operator), there must exist its multiplicative inverse in F.

$\mathbf{a \in F, a \neq 0, such\ that\ ab = ba = 1}$ (identity element for $\times$

■why are we interested in finding GCD?

To make sure the two numbers are relatively prime and every element has multiplicative inverse

■proof of Euclic;s revursion?

a>b, a=mb+r, common divisor of a and b is the common divisor of a, b, r

So gcd(a, b) = gcd(b, r).

■Bezout' s identity?

gcd(a, n)=xa+yn, a>0, n >0

x and y do not have to be unique for given a and n and x and y may be positive or negative or zero

I. S = {am + bn | am + bn > 0, m, n∈Z }
II. let d denote the smallest element of S. a=qd+ r, 0 . r < d
III. If r is a non-zero integer less than d that would violate the fact that d is the smallest positive linear sum of a and b
IV. Since r is zero, it must be the case that a = qd for some integer q. Similarly, we can prove that b is sd for some integer s. This proves that d is a common divisor of a and b.

■main focus of studying polynomial arithmetic?

in adding, subtracting, multiplying, and dividing the polynomials and figuring out how to characterize a given set of polynomials with respect to such operations.

■polynomial over a field?

coefficient is drawn from that field

■$3x^2 + 4x + 1$ *divided by* $5x + 6$ *over* Z_7?

2x+4

■GF(2)

$(x^4 + x^2 + x + 1) + (x^3 + 1)$

$(x^4 + x^2 + x + 1) - (x^3 + 1) = (x^4 + x^2 + x + 1) + (x^3 + 1)$

$(x^4 + x^2 + x + 1) * (x^3 + 1)$

$(x^4 + x^2 + x + 1)/(x^3 + 1)$

■how many polynomial are there in GF(2^3)? 8

■what is 010*101 in GF(2^3) given irreducible polynomial is x^3+x+1? 001

X^3 mod /(x^3+x+1) = x+1

If irreducible polynomial is x^3+x^2+1?111

■what is the key schedule in AES?

i. arranges the 16 bytes of the encryption key in the form of a 4*4 array
ii. expands the words [w0,w1,w2,w3] into a 44-word key

$$w_{i+4} = w_i \otimes g(w_{i+3})$$

■DES each component purpose?

1. Round key generation and key mixing: ensure that each bit of the original encryption key is used in roughly 14 of the 16 rounds, introduce confusion
2. Expansion permutation: The input to the function is a 32-bit word, but the round-key is a 48-bit word. The expansion permutation is needed to increase the number of bits in the input word to 48.
3. S-box substitution: introduce diffusion in the generation of the output from the input. the row lookup for each of the eight S-boxes becomes a function of the input bits for the previous S-box and next S-box. Enhance the resistance of DES to differential cryptanalysis-attack
4. P-box permutation: a single sbox have effect on many sboxes in the next round.

■why use base64?

Base64 encoding encodes binary data as printable characters, and is free of any special characters or control characters, so that computer can communicate without error.

■5 modes problems with image

I. Show whether or not the set of remainders Z_{12} forms a group with either one of the modulo addition or modulo multiplication operations.

$$Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$$

i. Z_{12} forms a group with modulo addition

1. Closure: a = x mod 12, b = y mod 12, a+b = (x mod 12) + (y mod 12) = (x+y) mod 12. x+y is an integer and any integer divided by 12 must has a remainder $\in Z_{12}$. $\therefore$ Z_{12} is closed.
2. Associativity:
   w = 12a + r_a, x = 12b + r_b, y = 12c + r_c
   w+x = 12a + r_a + 12b + r_b
   (w+x)+y = 12a + r_a + 12b + r_b + 12c + r_c
   x+y = 12b + r_b + 12c + r_c
   w+(x+y) = 12a + r_a + 12b + r_b + 12c + r_c
   (w+x)+y = w+(x+y)
   $\therefore$[(w+x)+y] mod 12 = [w+(x+y)] mod 12
3. existence of a unique identity element:
   For each w$\in Z_{12}$, 0+w = w+0 = w
   (0+w) mod n = (w+0) mod n = w mod n
4. existence of an inverse element for each element:
   For each w$\in Z_{12}$, there exists a z$\in Z_{12}$ such that (w+z)mod12 = 0.
   0+0=0, [1+(12-1)] mod 12 =0, [2+(12-2)] mod 12 =0…
   [5+(12-5)] mod 12 =0, [6+(12-6)] mod 12 = 0

ii. Z_{12} does not form a group with modulo multiplication
Existence of an inverse element is not for each element. Zero doesn't have multiplicative inverse.

II. Compute gcd(29495, 16983) using Euclid's algorithm. Show all the steps.

gcd(29495, 16983) = gcd(16983, 29495%16983)= gcd(16983, 12512)
= gcd(12512, 16983%12512) = gcd(12512, 4471)
= gcd(4471, 12512%4471)= gcd(4471, 3570)
= gcd(3570, 4471%3570)= gcd(3570, 901)
= gcd(901,3570%901)= gcd(901,867)
= gcd(867,901%867)= gcd(867,34)
= gcd(34,867%34)= gcd(34,17)
= gcd(17,34%17)= gcd(17,0)=17

III. With the help of Bezout's identity, show that if c is a common divisor of two integers a, b > 0, then c | gcd(a,b) (i.e. c is a divisor of gcd(a,b)).
A>b, a=mb+r, common divisor of a and b is the common divisor of a, b, r

IV. Use the Extended Euclid's Algorithm to compute by hand the multiplicative inverse of 25 inZ_{28}. List all of the steps.

gcd(28,25)= gcd(25,3) residue 3=1× $28 - 1 \times 25$

= gcd(3,1) residue 1=1× $25 - 8 \times 3$

=1× $25 - 8 \times (1 \times 28 - 1 \times 25)$

=9× $25 - 8 \times 28$

So the multiplicative inverse of 25 in Z_{28} is 9.

V. In the following, find the smallest possible integer x. Briefly explain (i.e. you don't need to list out all of the steps) how you found the answer to each. You should solve them without using brute-force methods:

(a) 8x $\equiv$ 11 (mod 13)

$8^{-1} \times 8x \equiv 8^{-1} \times 11 \pmod{13}$

gcd(13,8) = gcd(8,5) residue 5 = 1× $13 - 1 \times 8$

= gcd(5,3) residue 3 = 1× $8 - 1 \times 5 = 2 \times 8 - 1 \times 13$

= gcd(3,2) residue 2 = 1× $5 - 1 \times 3 = 2 \times 13 - 3 \times 8$

= gcd(2,1) residue 1 = 1× $3 - 1 \times 2 = 5 \times 8 - 3 \times 13$

X = $8^{-1} \times 11 \bmod 13 = 5 \times 11 \bmod 13 = 3$

(b) 5x $\equiv$ 3 (mod 21)

21+1-5=17

X = $5^{-1} \times 3 \bmod 21 = 17 \times 3 \bmod 21 = 9$

(c) 8x $\equiv$ 9 (mod 7)

Gcd(8,7) = gcd(7,1) residue 1 = 1× $8 - 1 \times 7$

X = $8^{-1} \times 9 \bmod 7 = 1 \times 9 \bmod 7 = 2$

I. Determine the following in GF(11), please show your work:

i. $(3x^4 + 5x^2 + 10)$-$(8x^4 + 5x^2 + 2x + 1)$

= -5x^4-2x-9

ii. $(5x^2 + 2x + 7) \times (5x^3 + 3x^2 + 3x + 2)$

= 25x^5+15x^4 + 15x^3 + 10x^2+10x^4+6x^3 +

6x^2+4x+35x^3+21x^2+21x+14

=25x^5+25x^4 + 56x^3 + 37x^2+25x+14

=3x^5+3x^4 + x^3 + 4x^2+3x+3

iii. $\frac{x^5+8x^4+x^3+4x^2+8x}{6x^3+3x^2+2}$

1/6 = 1× $6^{-1} = 1 \times 2 = 2\ mod\ 11 = 2$

Product of $2x^2$ and $6x^3 + 3x^2 + 2$ is $x^5 + 6x^4 + 4x^2$, subtract it from the dividend $x^5 + 8x^4 + x^3 + 4x^2 + 8x$, result is $2x^4 + x^3 + 8x$.

2/6 = 2× $6^{-1} = 2 \times 2 = 4\ mod\ 11 = 4$

Product of 4x and $6x^3 + 3x^2 + 2$ is $2x^4 + x^3 + 8x$, subtract it from the dividend $2x^4 + x^3 + 8x$, result is 0.

Therefore, $\frac{x^5+8x^4+x^3+4x^2+8x}{6x^3+3x^2+2} = 2x^2 + 4x$

II. For the finite field GF(2^3), calculate the following for the modulus polynomial$x^3 + x^2 + 1$

i. $(x^2 + x + 1) \times (x + 1)$
$=(x^2 + x + 1) \times (x + 1)\ mod\ (x^3 + x^2 + 1)$
$=(x^3 + 2x^2 + 2x + 1)\ mod\ (x^3 + x^2 + 1)$
$=x^2 + 2x$

ii. $(x^2 + 1) - (x^2 + x + 1)$
=-x mod$(x^3 + x^2 + 1)$ = x

iii. $\frac{x^2+x+1}{x^2+1}$ = 1 + $\frac{x}{x^2+1}$

■construct a Base64 encoded version of the string "hello\njello" Your answer should be "aGVsbG8KamVsbG8=". What do you think the character = at the end of the Base64 representation is for? padding

■text file contains "hello" has the following bytes (in hex) "68 65 6C 6C 6F 0A" Looks like there are six bytes in the file whereas the word hello has only five characters. What do you think is going on? Do you know why your editor might want to place that extra byte in the file and how to prevent that from happening?

The feature exists because as defined by POSIX, a text file consists of lines, and by definition, a line terminates with a newline character.

Lets now try to encrypt the contents of this text file with a 4-bit block cipher whose codebook contains the following entries:
6, 0, 13, 4, 3, 1, 14, 8, 7, 12, 9, 15, 5, 2, 11, 10
Lets say that I write the encrypted output into a different file and then examine this new file with the hexdump -C command.What will I see in the encrypted file?

6 ->1

8->7

key space: 4*(2**4)

■relationship between the input and the output is completely random and mapping between the input blocks and the output blocks must be one-to-one for an ideal block cipher to be invertible for decryption to work. If we had to express this mapping in the form of a table lookup, what will be the size of the table?
2^blocksize

■What would be the encryption key for an ideal block cipher?

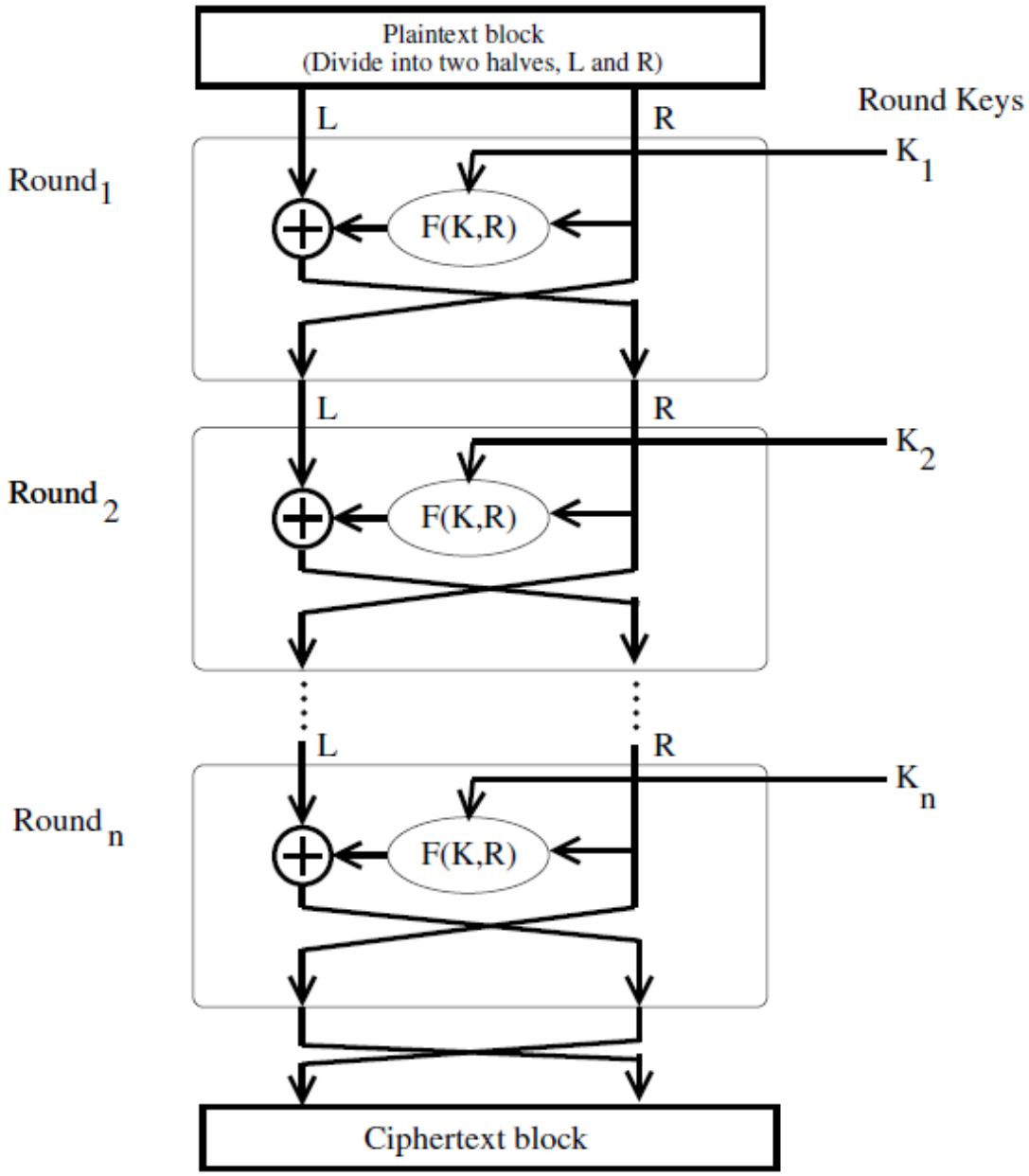
the codebook itself, meaning the table that shows the relationship between the input **blocks** and the output **blocks**.

■What makes ideal block ciphers impractical?

The size of the encryption key would make the ideal block cipher an impractical idea.

■What do we mean by a Feistel Structure for Block Ciphers?

Feistel cipher partitions input block into two halves, the left half and the right half, which are processed through multiple rounds.



■DES encryption was broken in 1999.Why do you think that happened?

in the age of parallel computing, breaking DES has become easy with the help of brute force attack.

■Since DES was cracked, does that make this an unimportant cipher?
DES instances can be applied many times to a plaintext.(2DES/3DES).
■What is the 0 element for the permutation group defined over N objects? Note that the 0 element is the identity element for the group operator, usually denoted +.
<1,2,…n>
■If the group operator is referred to as addition, then the group also allows for subtraction. What do we mean by that?
A – b = a + (-b)
■What is the most elementary reason for the fact that the set of all possible permutations over N objects along with the permutation operator is not a ring?

■For a given N, the set of all square N*N matrices of real numbers is a ring, the group operator being matrix addition and the additional ring operator being matrix multiplication. Why can this ring not be an integral domain?

■What is a good notation for a field? Explain your notation.

$$\{\mathbf{F}, +, \times\}$$

■Does a field contain a multiplicative inverse for every element of the field?
Not for the identity element with respect to the group operator
■What do we get from the following mod operations:

$$\begin{aligned} 2 \bmod 7 &= ? \\ 8 \bmod 7 &= ? \\ -1 \bmod 8 &= ? \\ -19 \bmod 17 &= ? \end{aligned}$$

■What is the difference between "a mod n" and "a ≡ b (mod n)"
the remainder between 0 and n-1
if a mod n = b mod n, a and b is congruent modulo n, expressed as a ≡ b (mod n) or a = b (mod n) or a = b mod n
■

$$(p + q) \bmod n = [(p \bmod n) + (q \bmod n)] \bmod n$$

Choose numbers for p, q, and n that show that the following version of the above is NOT correct:

$$(p + q) \bmod n = (p \bmod n) + (q \bmod n)$$

■Zn stands for the set of residues. What does that mean?

Zn is the set of remainders in arithmetic modulo n. Zn = {0,1, 2, .., n−1}

■How would you explain that Zn is a commutative ring?

I. Zn is a group: group operator is modulo n addition
II. Zn is an abelian group: modulo n addition community
(3+ 4)mod3 = (4+ 3) mod 3
III. Zn is a ring: ring operator is modulo n multiplication, closure, associativity, distribute over addition
IV. Zn is a commutative ring: modulo n multiplication community
V. Zn is more than a commutative ring, but not quite an integral domain: Zn possesses a multiplicative identity, but it does NOT satisfy the other condition of integral domains which says that if ab = 0 then either a or b must be zero. Consider modulo 8 arithmetic. 2*4 = 0, which is a clear violation of the second rule for integral domains
VI. Zn is not a field:
i. For every element of Zn, there exists an additive inverse in Zn. But there does not exist a multiplicative inverse for every non-zero element of Zn.

Z_8	:	0	1	2	3	4	5	6	7
additive inverse	:	0	7	6	5	4	3	2	1
multiplicative inverse	:	-	1	-	3	-	5	-	7

ii. multiplicative inverses exist for only those elements of Zn that are relatively prime to n.
iii. two integers a and b are relatively prime to each other if Greatest Common Divisor. gcd(a, b) = 1

VII. Zn has 5 properties:
i. Commutativity

$$(w + x) \bmod n = (x + w) \bmod n$$
$$(w \times x) \bmod n = (x \times w) \bmod n$$

ii. Associativity

$$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$$
$$[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$$

iii. Distributivity of Multiplication over Addition

$$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$$

iv. Existence of Identity Elements

$$(0 + w) \bmod n = (w + 0) \bmod n$$
$$(1 \times w) \bmod n = (w \times 1) \bmod n$$

v. Existence of Additive Inverses

For each $w \in Z_n$, there exists a $z \in Z_n$ such that

$$w + z = 0 \bmod n$$

■If I say that a number b in Zn is the additive inverse of a number a in the same set, what does that say about (a + b) mod n? 0

■If I say that a number b in Zn is the multiplicative inverse of a number a in the same set, what does that say about (a ×b) mod n? 1

■Is it possible for a number in Zn to be its own additive inverse? Give an example.

Z2, 1+1=0

■Is it possible for a number in Zn to be its own multiplicative inverse? Give an example.

Z2, 1*1=1

■What are the asymmmetries between the modulo n addition and modulo n multiplication over Zn?

i. For every element of Zn, there exists an additive inverse in Zn. But there does not exist a multiplicative inverse for every non-zero element of Zn.
ii. multiplicative inverses exist for only those elements of Zn that are relatively prime to n.

Is it true that there exists an additive inverse for every number in Zn regardless of the value of n?Is it true that there exists a multiplicative inverse for every number in Zn regardless of the value of n?For any given n, what special property is satisfied by those numbers in Zn that possess multiplicative inverses?

■Find the multiplicative inverse of each nonzero element in Z11.

■When is polynomial division permitted in general?

Polynomial division is obviously not allowed for polynomials that are not defined over fields. You cannot divide $4x^2 + 5$ by the polynomial 5x. If you tried, the first term of the quotient would be (4/5)x where the coefficient of x is not an integer.

■When the coefficients of polynomials are drawn from a finite field, the set of polynomials constitutes a?

1. POLYNOMIALS OVER A FIELD CONSTITUTE A RING
   I. The group operator is polynomial addition,

II. The polynomial 0 is obviously the identity element with respect to polynomial addition.
III. Polynomial addition is associative and commutative.
IV. The set of all polynomials over a given field is closed under polynomial addition.
V. Polynomial multiplication distributes over polynomial addition.
VI. polynomial multiplication is associative.
VII. the set of all polynomials over a field constitutes a polynomial ring.
VIII. polynomial multiplication is commutative, the set of polynomials over a field is actually a commutative ring.
IX. it does not make sense to talk about multiplicative inverses of polynomials in the set of all possible polynomials that can be defined over a finite field. (Recall that our polynomials do not contain negative powers of x.)
X. it is possible for a finite set of polynomials, whose coefficients are drawn from a finite field, to constitute a finite field.

■What is an irreducible polynomial?

A polynomial f(x) over a field F, if f(x) cannot be expressed as a product of two polynomials, both over F and both of degree lower than that of f(x).

■there exist two different irreducible polynomials of degree 3 over GF(2): "x^3+x+1" and "x^3+ x^2+ 1". whether the MI of 010 will be different when GF(23) is based on x3 + x2 + 1?

■When the set of all integers is divided by a prime, we obtain a set of remainders whose elements obey a certain special property with regard to the modulo multiplication operator over the set. What is that property?

■When the set of all polynomials over GF(p) for a prime p is divided by an irreducible polynomial, we obtain a set of remainders with some very special properties. What is so special about this set? How is such a set denoted?

■How do we get a finite field of the form GF(2n)?

■If GF(p) gives us a finite field (with p elements), why is that not good enough for us? Why do we need finite fields of the form GF(2n)?

■How will you prove that GF(23) is at least an integral domain? How will you prove it is a finite field?

■Lets say that our irreducible polynomial is x3+x+1. Obviously, each polynomial in GF(2^3) will be of degree 2 or less. Drawing a parallel between the polynomials and the bit patterns, how many polynomials are there in GF(2^3) ?

■With polynomial coefficients drawn from GF(2), lets use the irreducible polynomial x3 + x + 1 to construct the finite field GF(23). Now calculate

$$(x^2 + x + 1) + (x^2 + 1) \quad = \quad ?$$
$$(x^2 + x + 1) - (x^2 + 1) \quad = \quad ?$$
$$(x^2 + x + 1) \times (x^2 + 1) \quad = \quad ?$$
$$(x^2 + x + 1) \; / \; (x^2 + 1) \quad = \quad ?$$

■Given the following two 3-bit binary code words from GF(2^3) with the modulus polynomial x3 + x + 1: B1 = 111, B2 = 101

$$B_1 + B_2 \quad = \quad ?$$
$$B_1 - B_2 \quad = \quad ?$$
$$B_1 \times B_2 \quad = \quad ?$$
$$B_1 \; / \; B2 \quad = \quad ?$$

What would happen to the results in this question if we changed the modulus polynomial to x3 + x2 + 1 ?

■With regard to the first step of processing in each round of AES on the encryption side: How does one look up the 16*16 S-box table for byte-by-byte substitutions? In other

words, assuming I want a substitute byte for the byte b7b6b5b4b3b2b1b0, how do I use these bits to find the replacement byte in the S-box table?
The byte stored in the cell (9, 5) of the above table is the multiplicative inverse (MI) of 0x95, which is 0x8A

■What are the steps that go into the construction of the 16**16 S-box lookup table?
entries in the lookup table are created by using the notions of multiplicative inverses in GF(2^8) and bit scrambling

■What is rationale for the bit scrambling step that is used for finding the replacement byte that goes into each cell of the S-box table?
to destroy the bit-level correlations inside each byte.

■The second step in each round permutes the bytes in each row of the state array. What is the permutation formula that is used?

(i) not shifting the first row of the state array; (ii) circularly shifting the second row by one byte to the left; (iii) circularly shifting the third row by two bytes to the left; and (iv) circularly shifting the last row by three bytes to the left.

$$\begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2.0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3.0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} \Longrightarrow \begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.1} & s_{1,2} & s_{1,3} & s_{1,0} \\ s_{2.2} & s_{2,3} & s_{2,0} & s_{2,1} \\ s_{3.3} & s_{3,0} & s_{3,1} & s_{3,2} \end{bmatrix}$$

■Describe the mix columns transformation that constitutes the third step in each round of AES.

i. Each byte in a column is replaced by two times that byte, plus three times the next byte, plus the byte that comes next, plus the byte that follows. For the bytes in 1st, 2nd,3rd,4th row

$$s'_{0,j} = (0x02 \times s_{0,j}) \otimes (0x03 \times s_{1,j}) \otimes s_{2,j} \otimes s_{3,j}$$

$$s'_{1,j} = s_{0,j} \otimes (0x02 \times s_{1,j}) \otimes (0x03 \times s_{2,j}) \otimes s_{3,j}$$

$$s'_{2,j} = s_{0,j} \otimes s_{1,j} \otimes (0x02 \times s_{2,j}) \otimes (0x03 \times s_{3,j})$$

$$s'_{3,j} = (0x03 \times s_{0,j}) \otimes s_{1,j} \otimes s_{2,j} \otimes (0x02 \times s_{3,j})$$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2.0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3.0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0.0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1.0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2.0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3.0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

■What goes into computing g()?

I. Perform a one-byte left circular rotation on the argument 4-byte word.
II. Perform a byte substitution for each byte of the word returned by the previous step
III. XOR the bytes obtained from the previous step with a round constant

$$RC[1] = 0x01$$
$$RC[j] = 0x02 \times RC[j-1]$$

■A block cipher algorithm in its basic form is almost never used for encrypting long messages. Why? How are block ciphers deployed in practice if you want to encrypt long messages?