▓2 null bytes, 64 encoding? AAA=

▓Characteristics of Feistel Structure?

1. Divide input into two halves
2. Substitution+permutation
3. LE0 = RD16, RE0 = LD16, KE0 = KD16, reguardless of Feistel function

▓constrain of Feistel function? No

▓Why permutation expension? Let the 4-bit substitution be a function of previous and next segements

▓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 decryption

▓round key generation of DES?

▓diffusion and confusion in DES?

▓The property of Feistel structure? Feistel function can be arbitrly defined and still working

▓why expanded-permutation is “permutation”? permutation is rearranged the origin plain text (same size in same size out)

▓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 with operator has 4 properties: closure, associativity, identity, inverse

▓example of infinite group and finite group? All integer with addition as operator, a sequence with permutation operation

▓how a group become ring? second operator with closure, associative, sidtributive on first operator

▓communitive ring become integral domain? Identity element with respect of ring operator and ab = 0 implies that at leat either a or b is 0

▓what a fiels has more than an integral domain

▓divisor notation a|b

▓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

▓Bezout’s identity? gcd(a, n)=xa+yn

▓main focus of studying polynomial arithmetic? Adding,

▓polynomial over a field? coefficient is drawn from that field

▓divide 2x+4

▓GF(2)

)

) = )

)

) =x+