**Problem Session CMPE-455 “Security of Computer Systems and Networks” 04.04.2019**

**Classical Ciphers, DES, Modular arithmetic, AES**

1. What is Access Control Matrix? List? Capability list?
2. What is Mandatory Access Model? What rules are used in it?
3. *Invert permutation:*

P=(159742638)

=(168527493)

P(578632149)=(539167284)

(P(578632149))= (539167284)=(57863249)

1. *Consider the following message:*

SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA

The ciphertext was produced using the 1st sentence of The Other Side of Silence (a book about the spy Kim Philby):

The snow lay thick on the steps and the snowflakes driven by the wind looked black in the highlights of the cars.

A simple substitution cipher was used.

English letters are:

*Plain: a b c d e f g h i j k l m n o p q r s t u v w x y z*

Decipher this message

basalisk to leviathan blake is contact

1. How DES encryption is organized? Why DES decryption is possible without nonlinear round function F(Ri-1, Ki) inverting?
2. How S-boxes work?
3. What is a middle bit?
4. What is an end bit?
5. How round keys are generated?
6. Find 5-1mod7, 5-1mod8, 6-1mod8
7. Calculate 2137mod25 manually
8. What is a prime number? How to check primality? Pseudocode?
9. What is GCD(a,b)? How to calculate it? Euclidean algorithm for GCD?
10. What is relative primality? How to decide that two numbers are relatively prime? Find GCD(123, 34)
11. Extended Euclidean algorithm (EEA). Find 34-1mod123 using EEA.
12. Polynomials arithmetic. Monic polynomial. Find (x2+3x+1)(x4-2x3+2)mod(x5+2x+1) over Z6.
13. What reducible polynomial is? What irreducible polynomial is? Check reducibility of x2+2x+1 over Z3. Of x2+2x+2?
14. What is GF(p)? GF(pn)? Show that 2\*5=1 in GF(23) with irreducible polynomial x3+x+1. Use EEA to find multiplicative inverse of 5 in GF(23) with irreducible polynomial x3+x+1.
15. How many rounds are used in AES? What GF is used AES? What irreducible polynomial is used in AES? What are the key sizes of AES? How plaintext and key are arranged for AES with 10 rounds, 128 bit block size, and 128 bit key size? What is state array? How ciphertext is obtained? How many round keys are constructed and how are they arranged?
16. What transformations are used in a round of AES? What transformation mixes state with secret information? What is shift row transformation? What is mix column transformation? What is a substitution transformation?
17. How S-box is used for substitution transformation? How inverse S-box is used? Find S({AB}). Find S-1({AB}).