**Problem Session CMSE-353 “Security of Software Systems” 15.01.2021**

AES, Hill cipher, RSA, Digital signatures, Certificates, SSL, Microsoft Password

1. RSA: key generation, Euclid GCD algorithm, Extended Euclidean algorithm, finding multiplicative inverse, Euler totient function, encryption/decryption, exponentiation by squaring with in-line reducing
2. RSA uses: data hiding, key exchange, digital signature, hash function
3. Certificates, Certificate authority (CA), Subject, Public key, version, serial number, issuer, validity period, CA web-site, revocation list
4. Secure sockets layer and Microsoft password authentication protocols. Relation between them
5. AES: Encryption/Decryption schemes, rounds, plaintext, state array, forward and inverse state transformations, add round key, substitute byte, shift row, mix column, GF(2^8) elements, irreducible polynomial, addition/subtraction, multiplication/division, remainder after division. Key expansion procedure, initialization, recursive procedure, RotWord, SubByte, round constant
6. Hill cipher, vector-matrix multiplication, encryption/decryption, matrix inversion, determinant
7. *Matrix inversion (for Hill ciphers*)

 - ? 

 n=10

detA=45+84+96-105-48-72=225-225=0

It means that inverse of the matrix does not exist

1. *Matrix inversion*

-? n=10



 (1)

where - is a determinant of sub matrix of A, obtained by deletion of i-th row and j-th column, det(A) – determinant of A. Taking into account that we work with integers on modulo n, we rewrite (1):

 (2)

det(A) =40+84+96-105-64-48=220-217=3

From (2):



















Thus, we get



and

