**Problem Session CMPE-455 “Security of Computer Systems and Networks” 14.04.2023**

**Information security requirements, Access control, RSA, DES, Digital signature, Certificates, SSL, Diffie-Hellman key exchange, DSA, SHA-512, Authentication procedures, AES**

1. What are the requirements of confidentiality, integrity, and availability?
2. What are the requirements of assurance, authenticity, and anonymity?
3. *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. What is Access Control Matrix? Access control list? Capability list?
2. What is Mandatory Access Model? What rules are used in it?
3. RSA settings, modulo value, Euler totient function, keys generation
4. RSA encryption/decryption
5. Use of RSA public key encryption
6. Use of RSA private key encryption
7. Find 5-1 mod 7, 5-1 mod 8, 6-1 mod 8
8. Calculate 2137 mod 25 manually
9. What is a prime number? How to check primality? Pseudocode?
10. What is GCD(a,b)? How to calculate it? Euclidean algorithm for GCD?
11. What is relative primality? How to decide that two numbers are relatively prime? Find GCD(123, 34)
12. Extended Euclidean algorithm (EEA). Find 34-1mod123 using EEA.
13. *Invert permutation:*

P=(159742638)

=(168527493)

P(578632149)=(539167284)

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

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. What is RSA digital signature? How calculated? How verified? Why hash function is used? Give example of hash function with 8-bit output
7. What certificate is? What for it is used? What three conditions are used to verify a certificate? Who issues a certificate? What is CA? How public key of CA is delivered to a verifier?
8. What for SSL is used? How certificate is used in SSL? How session key is defined in SSL? How client authenticates a server in SSL? How server authenticates a client in SSL?
9. How TLS extends SSL? What is Diffie-Hellman key exchange? How it works? Give an example
10. What is DSA? What for it is used in TLS? How it works? Give an example
11. SHA-512 general schema, message padding, message block size, hash size, initial value and its calculation, elementary function structure, use of constants Kt, derived words Wt, constants Kt calculation, round structure, functions Ch, Maj, Sum0, Sum1, calculation of Wt
12. Simple protected authentications procedures, one-, two-, and three-way authentication procedures using certificates, one-time password
13. AES structure, encryption, decryption, add round key, substitute byte, shift rows, mix columns, polynomials arithmetic, monic polynomial, find (x2+3x+1)(x4-2x3+2) mod (x5+2x+1) over Z6.