**Problem Session CMPE-455 “Security of Computer Systems and Networks” 04.04.2025**

[Information security requirements](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/Information%20Security%20Requirements%2028092016.docx)**,** [Access control models](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/Access%20control%20models%20%2027022019.docx), [DES](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/Ch3.DES%2005032023.doc), [RSA](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/RSA%20algorithm%2018032023.docx)**, and** [SHA-512](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMPE455/CMSE456%20CMPE455%20Spring%202025/SHA512%2018032025.pdf) (generation of words Wi on p. ​361 is not included)

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. *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. RSA settings, modulo value, Euler totient function, keys generation
7. RSA encryption/decryption
8. Use of RSA public key encryption
9. Use of RSA private key encryption
10. Find 5-1 mod 7, 5-1 mod 8, 6-1 mod 8
11. Calculate 2137 mod 25 manually
12. What is a prime number? How to check primality? Pseudocode?
13. What is GCD(a,b)? How to calculate it? Euclidean algorithm for GCD?
14. What is relative primality? How to decide that two numbers are relatively prime? Find GCD(123, 34)
15. Extended Euclidean algorithm (EEA). Find 34-1mod123 using EEA.
16. SHA-512 padding, buffer initialization, addition modulo 2^64, elementary function 80-round structure, use of words Wi and constants Ki in the rounds, round structure, functions used in it (Maj, Ch, Sum0, Sum1)