**Problem Session CMSE-353 “Security of Software Systems” 24.11.2020**

**Classical Ciphers, RSA, DES**

1. What CIA concepts are?
2. What Authenticity, Assurance, Anonymity are?
3. What are the classes of intruders? What insider is? External intruder?
4. How intrusion can be detected?
5. What are the types of malware?
6. What are the methods of password cracking?
7. What are the requirements to strong passwords?
8. What social engineering is? What are the methods of SE?
9. What is Access Control Matrix? List? Capability list?
10. What is Mandatory Access Model? What rules are used in it?
11. What RSA method is? How many keys RSA has? How RSA keys are defined? How a private RSA key is defined? Public? How in RSA a message is encrypted? Decrypted?
12. Can RSA be used for secret data transmission? How it can be done?
13. What digital signature is? How RSA digital signature can be constructed? What hash function is? Why hashing is used in RSA signature?
14. What certificate is? What for certificates are issued? Who issues certificates? What is the main information in a certificate? How a certificate is verified?
15. How certificates are used in SSL protocol? How SSL protocol works for establishing secure connection between a client and a server? Who creates a secret key in SSL protocol? How the secret key is delivered to the other party?
16. *~~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



1. *Invert permutation:*

P=(159742638)

=(168527493)

P(578632149)=(539167284)

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

P(P-1)=I=(123456789)

(159742638) (1,6,8,5,2.7493)=(1, 2,3,..)

1. *Consider the following message:*

S IDKHKDM AF HCRKIABIE SHIMC KD LFEAILA

Dkombmov

Basilisk to

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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ciphetext | 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 |
| plaintext | t | h | e | s | n | o | w | l | a | y | i | c | k | p | d | f | r | v | b | g | j | m | q | u | x | z |

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 DES is related to Feistel cipher? What part of an input is encrypted in each round? Why swaps are used?
3. What Initial permutation is? How Inverse initial permutation is constructed?
4. What is a round key? What is the bit-size of a round key? What is the source for round keys generation?
5. How a right half is expanded by Expansion-Permutation transformation?
6. How S-boxes work?
7. What is a middle bit?
8. What is an end bit?
9. How outputs of S-boxes are transformed?
10. How to decide what S-boxes are affected by a given S-box?
11. How round keys are generated? What is the aim of Permuted choice 1? How shifts are used for key generation? What is the aim of Permuted choice 2?