**Problem Session CMPE-553 “Cryptography and Network Security” 16.11.2022**

**Classical Ciphers, DES, AES**

1. AES: 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 is it related to the plaintext? What is column-major order of storing multi-dimensional arrays? Row-major? How ciphertext is obtained? How many round keys are constructed and how are they arranged?
2. AES: 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?
3. AES: How S-box is used for substitution transformation? How inverse S-box is used? Find S(AB). Find S-1(AB).
4. AES: How S-box is constructed? What are the steps of its construction?
5. AES: Calculate Shift row transformation for

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12 | 34 | 56 | 78 |  |  |  |  |  |
| 9a | bc | de | Ef | => |  |  |  |  |
| 4A | 4b | 4c | 4d |  |  |  |  |  |
| 8C | De | bd | 3f |  |  |  |  |  |

1. AES: For the mix column transformation,

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 87 | F2 | 4D | 97 |  | 47 | 40 | A3 | 4C |
| 6E | 4C | 90 | EC | => | 37 | D4 | 70 | 9F |
| 46 | E7 | 4A | C3 |  | 94 | E4 | 3A | 42 |
| A6 | 8C | D8 | 95 |  | ED | A5 | A6 | BC |

show that actually 40 is obtained in the State(0,1). Mix column transformation is as follows

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 02 | 03 | 01 | 01 |  | S00 | S01 | S02 | S03 |  | S00’ | S01’ | S02’ | S03’ |  |
| 01 | 02 | 03 | 01 | \* | S10 | S11 | S12 | S13 | = | S10’ | S11’ | S12’ | S13’ | (5.3) |
| 01 | 01 | 02 | 03 |  | S20 | S21 | S22 | S23 |  | S20’ | S21’ | S22’ | S23’ |  |
| 03 | 01 | 01 | 02 |  | S30 | S31 | S32 | S33 |  | S30’ | S31’ | S32’ | S33’ |  |

1. DES: How DES encryption is organized? Why DES decryption is possible without nonlinear round function F(Ri-1, Ki) inverting?
2. DES: How DES is related to Feistel cipher? What part of an input is encrypted in each round? Why swaps are used?
3. DES: What Initial permutation is? How Inverse initial permutation is constructed?
4. DES: What is a round key? What is the bit-size of a round key? What is the source for round keys generation?
5. DES: How a right half is expanded by Expansion-Permutation transformation?
6. DES: How S-boxes work?
7. DES: What is a middle bit?
8. DES: What is an end bit?
9. DES: How outputs of S-boxes are transformed?
10. DES: How to decide what S-boxes are affected by a given S-box?
11. DES: How round keys are generated? What is the aim of Permuted choice 1?
12. *Invert permutation:*

P=(159742638)

=(168527493)

P(578632149)=(539167284)

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

1. *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. *Viginere cipher*

We can code each letter by respective number:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** |

Then instead of letters we can use respective numbers. For example, we have 5 letters numbered from 0 to 4. Then, Viginere tableau will be as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **0** | **1** | **2** | **3** | **4** |
| **0** | **0** | **1** | **2** | **3** | **4** |
| **1** | **1** | **2** | **3** | **4** | **0** |
| **2** | **2** | **3** | **4** | **0** | **1** |
| **3** | **3** | **4** | **0** | **1** | **2** |
| **4** | **4** | **0** | **1** | **2** | **3** |

Top row has letters of the plaintext, leftmost column defines letters from the keyword. Ciphertext letter is taken from the cross of plaintext letter’s column and keyword letter’s row, for example, plaintext value 2, if respective keyword letter is 3, will be substituted by letter 0, taken from intersection of column 2 and row 3. This table may be viewed as a function VT(p,k) of 2 arguments: plaintext letter p and keyword letter k, value of which is entry of this table on the cross of column p and row k. We may write out:

VT(p,k)=(p+k)modn

Where n is a number of different letters (in our example, n=5). When English language is used, n=26. Let’s consider example from lecture (Lecture Notes, Slide 5; Textbook, p.44):

Ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

Key: mf u g p mi yd g axg ou f hkl l l mhs qd qo g t e wbqf q yov u h wt

Plaintext: mi s s s c ar l e t wi t h t he kn if e i n t he l ib r a r y

In this example, n=27 (with additional blank symbol) and 1st ciphertext symbol:

C1=A=0 =VT(m,m)=VT(12,12)=(12+12)mod 27=24=Y, so 1st letter is not valid, but

C1=A=0= VT(m,p)=VT(12,15)=(12+15)mod 27=0=A

Let’s consider 2nd symbol:

C2=N=13= VT(i,f)=VT(8,5)=(8+5)mod27=13=N

Similar, 3rd symbol:

C3=K=10=VT(s,u)=(20+18)mod27=38mod27=11=L, so 3rd letter is not valid, but

C3=K=10=VT(s,t)=(18+19)mod27=37mod27=10=K

Similar, 4th symbol

C4=Y=24=VT(s,g)=(18+6)mod27=24=Y.

So, first 4 letters of the key should be pftg instead of mfug.

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.

Decipher this message

basalisk to leviathan blake is contact

1. When the PT-109 American patrol boat, under the command of Lieutenant John F. Kennedy, was sunk by a Japanese destroyer, a message was received in an Australian wireless station in Playfair code:

KXJEY UREBE ZWEHE WRYTU HEYFS

KREHE GOYFI WTTTU OLKSY CAJPO

BOTEI ZONTX BYBWT GONEY CUZWR

GDSON SXBOU YWRHE BAAHY USEDQ

The key used was:

Royal new Zealand navy.

Decrypt the message.

PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO

MILES SW MERESU COVE X CREW OF TWELVE X REQUEST ANY

INFORMATION

1. Use multiplication mod 26 to encrypt and decrypt back “Plain”
2. One-time pad
3. Transposition technique
4. Rotor machine