**Problem Session CMPE-553 “Cryptography and Network Security” 23.11.2020**

**Classical Ciphers, DES**

1. *DES structure*



1. *Initial permutation*

|  |
| --- |
| 1. IP
 |
| 58 50 42 34 26 18 10 260 52 44 36 28 20 12 462 54 46 38 30 22 14 664 56 48 40 32 24 16 857 49 41 33 25 17 9 159 51 43 35 27 19 11 361 53 45 37 29 21 13 563 55 47 39 31 23 15 7 |

|  |
| --- |
| IP-1 |
|  40 8 48 16 56 24 64 3239 7 47 15 55 23 63 3138 6 46 14 54 22 62 3037 5 45 13 53 21 61 2936 4 44 12 52 20 60 2835 3 43 11 51 19 59 27 34 2 42 10 50 18 58 261. 41 9 49 17 57 25
 |

1. *DES round*



1. *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** | **26** |
| **d** | **e** | **f** | **g** | **h** | **i** | **j** | **k** | **l** | **m** | **n** | **o** | **p** | **q** | **r** | **s** | **t** | **U** | **v** | **w** | **x** | **y** | **z** | **a** | **b** | **c** |  |

C=p+3 mod 26

A=>d (0=>3) 3 =c=(0= p)+3 mod 26

C=p+k mod 26

P=c-k mod 26

Viginere just the same but each next plaintext letter is encrypted using other substitution table, or, other key

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):

 px

 Mr mustard with the candlestick in the hall

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

C=p+k mod 27

K=c-p mod 27=13-17=-4 mod 27=23=x

C1=A=12+12=24=y<>A?

C1=A=12+15=27 mod 27=0=A?

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.

Key=”cryptography”

M I s s s c a r l e t w ith the knife i n t he l ib r a r y

C r y p t o g r a p h y c ryptography

If key size=plaintext size => one-time pad

1. *Consider the following message:*

SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA

basilisk

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| **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** |

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

basilisk 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”