Name: Brihat Ratna Bajracharya

Roll No.: 19/075

Assignment #1 (Advanced Cryptography)

1. Evaluate the following:

a) 7503 mod 81

b) -7503 mod 81

c) 81 mod 7503

d) -81 mod 7503

Answer

a. 7503 = *(92 × 81 + 51)*

So, 7503 mod 81 = **51**

b. -7503 = *(-93 × 81 + 30)*

So, -7503 mod 81 = **30**

c. 81 = *(0 × 7503 + 81)*

So, 81 mod 7503 = **81**

d. -81 = *(-1 × 7503 + 7422)*

So, -81 mod 7503 = **7422**

2. Use exhaustive key search to decrypt the following cipher text, which was encrypted using shift cipher:

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD

Answer

```
For Key:  1 Decrypted text: addzjexciwtpxgxihpqxgsxihpeapctxihhjetgbpc
For Key:  2 Decrypted text: zccyidwbhvsowfwhgopwfrwhgodzobswhggidsfaob
For Key:  3 Decrypted text: ybbxhcvagurnvevgfnoveqvgfncynarvgffhcrezna
For Key:  4 Decrypted text: xaawgbuzftqmudufemnudpufembxmzqufeegbqdymz
For Key:  5 Decrypted text: wzzvfatyespltctedlmtcotedlawlypteddfapcxly
For Key:  6 Decrypted text: vyyuezsxdroksbsdcklsbnsdckzvkxosdccezobwkx
For Key:  7 Decrypted text: uxxtdyrwcqnjrarcbjkramrcbjyujwnrcbbdynavjw
For Key:  8 Decrypted text: twwscxqvbpmiqzqbaijqzlqbaixtivmqbaacxmzuiv
For Key:  9 Decrypted text: svvrbwpuaolhpypazhipykpazhwshulpazzbwlythu
For Key: 10 Decrypted text: ruuqavotznkgoxozyghoxjozygvrgtkozyyavkxsgt
For Key: 11 Decrypted text: qttpzunsymjfnwnyxfgnwinyxfuqfsjnyxxzujwrfs
For Key: 12 Decrypted text: pssoytmrxliemvmxwefmvhmxwetperimxwwytivqer
For Key: 13 Decrypted text: orrnxslqwkhdlulwvdeluglwvdsodqhlwvvxshupdq
For Key: 14 Decrypted text: nqqmwrkpvjgcktkvucdktfkvucrncpgkvuuwrgtocp
For Key: 15 Decrypted text: mpplvqjouifbjsjutbcjsejutbqmbofjuttvqfsnbo
For Key: 16 Decrypted text: lookupintheairitsabirditsaplaneitssuperman
For Key: 17 Decrypted text: knnjtohmsgdzhqhsrzahqchsrzokzmdhsrrtodqlzm
For Key: 18 Decrypted text: jmmisnglrfcygpgrqyzgpbgrqynjylcgrqqsncpkyl
For Key: 19 Decrypted text: illhrmfkqebxfofqpxyfoafqpxmixkbfqpprmbojxk
For Key: 20 Decrypted text: hkkgqlejpdawenepowxenzepowlhwjaepooqlaniwj
For Key: 21 Decrypted text: gjjfpkdioczvdmdonvwdmydonvkgvizdonnpkzmhvi
For Key: 22 Decrypted text: fiieojchnbyuclcnmuvclxcnmujfuhycnmmojylguh
For Key: 23 Decrypted text: ehhdnibgmaxtbkbmltubkwbmltietgxbmllnixkftg
For Key: 24 Decrypted text: dggcmhaflzwsajalkstajvalkshdsfwalkkmhwjesf
For Key: 25 Decrypted text: cffblgzekyvrzizkjrsziuzkjrgcrevzkjjlgvidre
```

So decrypted text is

lookupintheairitsabirditsaplaneitssuperman

for key 16 i.e.

look up in the air its a bird its a plane its superman

Python Code GitHub Link:

https://raw.githubusercontent.com/Brihat9/AdvancedCryptography/master/ac_shift_cipher.py

3. Determine the number of key in affine cipher over Z_m for m=30, and 1225.

Answer

We know,

Number of keys in affine cipher is **m × ϕ(m),**

where **ϕ(m)** is euler phi function

$$m=\prod_{i=1}^{n} p_i^{e_i}$$

where $\mathbf{p_i}$ are distinct primes and $\mathbf{e_i > 0, 1 \le i \le n}$ and

$$\phi(m)=\prod_{i=1}^{n}\left(p_i^{e_i}-p_i^{e_i-1}\right)$$

Solution

So, for m = 30,

$$30 = 2^1 \times 3^1 \times 5^1$$

$$\phi(30) = (2 - 1) \times (3 - 1) \times (5 - 1) = 8$$

So, number of keys for **m = 30** is *30* × *8* = **240**

Similarly, for m = 1225,

$$1225 = 5^2 \times 7^2$$

$$\phi(1225) = (25 - 5) \times (49 - 7) = 840$$

So, number of keys for **m = 1225** is *1225* × *840* = **1029000**

4. Suppose that π is the following permutation of (1,…,8}

x	1	2	3	4	5	6	7	8
π(x)	4	1	6	2	7	3	8	5

4.1. Compute the permutation π^{-1}

Answer

x	1	2	3	4	5	6	7	8
π^{-1}(x)	2	4	6	1	8	3	5	7

4.2. Decrypt the following ciphertext, for a Permutation Cipher with m = 8, which was encrypted using the key π

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM

Answer

First splitting above cipher text into group of eight character (m = 8) and then rearranging the characters using Permutation π, we get

TGEEMNEL	**NNTDROEO**	**AAHDOETC**	**SHAEIRLM**
=	**=**	**=**	**=**
GENTLEME	**NDONOTRE**	**ADEACHOT**	**HERSMAIL**

Now combining all decrypted characters, we get

gentlemendonotreadeachothersmail

which decrypts to following text:

gentlemen do not read each others mail

5. Here is how we might crypt-analyze the Hill Cipher using a cipher text only attack. Suppose that we know that m=2. Break the cipher text into blocks of length two letters (digrams). Each such digrams are the encryption of a plain text digrams and assume it in the encryption of a common digrams for example, TH or ST. Each such guess, proceed as in the known plain-text attack, until the correct encryption matrix is found.

Here is a sample of cipher text to decrypt using this method:

LMQETXYEAGTXCTUIEWNCTXLZEWUAISPZYVAPEWLMGQWYA
XFTCJMSQCADAGTXLMDXNXSNPJQSYVAPRIQSMHNOCVAXFV

<u>Solution</u>

Breaking the cipher text into groups of two letters:

LM QE TX YE AG TX CT UI EW NC TX LZ EW UA IS PZ YV AP EW LM GQ WY AX
FT CJ MS QC AD AG TX LM DX NX SN PJ QS YV AP RI QS MH NO CV AX FV

Here, we can see that most frequent digrams are **LM** (3 times) and **TX** (4 times). Also from book, we know 30 most common digrams of English Language:

TH, HE, IN, ER, AN, RE, ED, ON, ES, ST,
EN, AT, TO, NT, HA, ND, OU, EA, NG, AS,
OR, TI, IS, ET, IT, AR, TE, SE, HI, OF.

To find the key, lets map the most frequent digrams from cipher text with most common digrams. The most common digrams will be the plain text for our analysis

Also, encoding the characters into numbers starting from **`A = 0 to Z = 25`**, we get for cipher text,

`L = 11, M = 12, T = 19, X = 23` and so on

and, for most common digrams,

`T = 19, H = 7, E = 4, I = 8, N = 13` and so on

Representing in Matrix form for **`LM`** and **`TX`** of cipher text and **`TH`** and **`HE`** for plain text, we get,

Plain Text Matrix = $\begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix}$ and Cipher Text Matrix = $\begin{pmatrix} 11 & 12 \\ 19 & 23 \end{pmatrix}$

As we know,

```
cipher_text_matrix = plain_text_matrix * KEY_matrix
```

So,

```
KEY_matrix = inverse(plain_text_matrix) * cipher_text_matrix
```

Now,

To calculate the inverse of $\begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix}$

$$determinant = 19 \times 4 - 7 \times 7 = 27 \, mod \, 26 = 1$$

$$inverse \, determinant = 1^{-1} \, mod \, 26 = 1$$

$$adjoint = \begin{pmatrix} 4 & -7 \\ -7 & 19 \end{pmatrix}$$

$$Inverse = \begin{pmatrix} 4 & -7 \\ -7 & 19 \end{pmatrix}$$

Now, calculating key matrix as,

$$KEY = \begin{pmatrix} 4 & -7 \\ -7 & 19 \end{pmatrix} \times \begin{pmatrix} 11 & 12 \\ 19 & 23 \end{pmatrix} = \begin{pmatrix} -89 & -113 \\ 284 & 353 \end{pmatrix} mod \, 26 = \begin{pmatrix} 15 & 17 \\ 24 & 15 \end{pmatrix}$$

This key is used to encrypt the plain text to cipher text.

Now using the inverse matrix procedure we can calculate decryption key as

$$INVKEY = \begin{pmatrix} 11 & 24 \\ 17 & 11 \end{pmatrix}$$

Using this **`INVKEY`** on all groups of cipher text blocks we obtain following plain text:

`thmehewkoohekjwmayjjhetuaymcawlkopwjaythismog`

`triedsmqiuhoohethnstgqhrqkcopwjpnkcovllgfgtne`

This <u>does not</u> seems to be original plain text.

So, choosing another group of common digram as plain text.

Choosing **`TH`** and **`IN`**

Plain Text Matrix will be $\begin{pmatrix} 19 & 7 \\ 8 & 13 \end{pmatrix}$ and Cipher Text Matrix is same as $\begin{pmatrix} 11 & 12 \\ 19 & 23 \end{pmatrix}$

Proceeding as previous, we get,

To calculate the inverse of $\begin{pmatrix} 19 & 7 \\ 8 & 13 \end{pmatrix}$

$$determinant = 19 \times 13 - 8 \times 7 = 191 \, mod \, 26 = 9$$

$$inverse \, determinant = 9^{-1} \, mod \, 26 = 3$$

$$adjoint = \begin{pmatrix} 13 & -7 \\ -8 & 19 \end{pmatrix}$$

$$Inverse = 3 \times \begin{pmatrix} 13 & -7 \\ -8 & 19 \end{pmatrix} = \begin{pmatrix} 39 & -21 \\ -24 & 57 \end{pmatrix}$$

Now calculating key matrix

$$KEY = \begin{pmatrix} 39 & -21 \\ -24 & 57 \end{pmatrix} \times \begin{pmatrix} 11 & 12 \\ 19 & 23 \end{pmatrix} = \begin{pmatrix} 30 & -15 \\ 819 & 1023 \end{pmatrix} mod \, 26 = \begin{pmatrix} 4 & 11 \\ 13 & 9 \end{pmatrix}$$

This key is used to encrypt the plain text to cipher text

Now using the inverse matrix procedure we can calculate decryption key as

$$INVKEY = \begin{pmatrix} 23 & 13 \\ 21 & 16 \end{pmatrix}$$

Using this **INVKEY** on all groups of cipher text blocks we obtain following plain text:

```
thekingwasinhiscountinghousecountingouthismon
eythequeenwasintheparloureatingbreadandhoneyz
```

This seems to be the valid plain text. We can decrypt above text as follows

```
the king was in his counting house counting out his money
the queen was in the parlour eating bread and honey z
```

Python Code GitHub Link:

https://raw.githubusercontent.com/Brihat9/AdvancedCryptography/master/ac_hill_cipher_digram.py