Tribhuvan University
Institute of Science and Technology

Central Department of Computer Science and Information Technology
Kirtipur, Kathmandu

Assignment I

Advanced Cryptography

Submitted to:

Asst. Prof. Ram Krishna Dahal

Submitted by

Rishav Acharya

Roll – 01 (611/077)

2077 Batch

Q 1. Evaluate the following:

a. 7503 mod 81

Answer:

Dividing 7503 by 81, the quotient is 92 and remainder is 51 so,

7503 mod 81 = 51

b. (-7503) mod 81

Answer:

We know 7503 mod 81 is 51 so, to calculate (-7503) mod 81 we need to compute as;

(-7503) mod 81 = 81 – (7503) mod 81

= 81 – 51

= 30

Therefore, (-7503) mod 81 = 30

c. 81 mod 7503

Answer:

Dividing 81 by 7503, the quotient is 0 and remainder is 81 so,

81 mod 7503 = 81

d. (-81) mod 7503

Answer:

We know 81 mod 7503 is 81 so, to calculate (-81) mod 7503 we need to compute as:

(-81) mod 7503 = 7503 – (81) mod 7503

= 7503 – 81

= 7422

Therefore, (-81) mod 7503 = 7422

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

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD.

Answer:

Since, the given cipher text is encrypted using shift cipher. Here we apply the decryption process of the cipher text "C".

Step 1: Convert the letter in cipher text (C) into the number that matches its order in the alphabet starting from 0, and call this number Y. (A=0, B=1, C=2, ..., Y=24, Z=25). So, equivalent numbers are:

1 4 4 0 10 5 24 3 9 23 20 16 24 7 24 9 8 16 17 24 7 19 24 9 8 16 5 1 16 3 20 24 9 8 8 10 5 20 7 2 16 3

Step 2: Calculate: **X= (Y - K)** mod **26**

Step 3: Lets try with all key from 0 to 25. We get:

```
Key 0: BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD
Key 1: ADDZJEXCIWTPXGXIHPQXGSXIHPEAPCTXIHHJETGBPC
Key 2: ZCCYIDWBHVSOWFWHGOPWFRWHGODZOBSWHGGIDSFAOB
Key 3: YBBXHCVAGURNVEVGFNOVEQVGFNCYNARVGFFHCREZNA
Key 4: XAAWGBUZFTQMUDUFEMNUDPUFEMBXMZQUFEEGBQDYMZ
Key 5: WZZVFATYESPLTCTEDLMTCOTEDLAWLYPTEDDFAPCXLY
Key 6: VYYUEZSXDROKSBSDCKLSBNSDCKZVKXOSDCCEZOBWKX
Key 7: UXXTDYRWCQNJRARCBJKRAMRCBJYUJWNRCBBDYNAVJW
Key 8: TWWSCXQVBPMIQZQBAIJQZLQBAIXTIVMQBAACXMZUIV
Key 9: SVVRBWPUAOLHPYPAZHIPYKPAZHWSHULPAZZBWLYTHU
Key 10: RUUQAVOTZNKGOXOZYGHOXJOZYGVRGTKOZYYAVKXSGT
Key 11: QTTPZUNSYMJFNWNYXFGNWINYXFUQFSJNYXXZUJWRFS
Key 12: PSSOYTMRXLIEMVMXWEFMVHMXWETPERIMXWWYTIVQER
Key 13: ORRNXSLQWKHDLULWVDELUGLWVDSODQHLWVVXSHUPDQ
Key 14: NQQMWRKPVJGCKTKVUCDKTFKVUCRNCPGKVUUWRGTOCP
Key 15: MPPLVQJOUIFBJSJUTBCJSEJUTBQMBOFJUTTVQFSNBO
Key 16: LOOKUPINTHEAIRITSABIRDITSAPLANEITSSUPERMAN
Key 17: KNNJTOHMSGDZHQHSRZAHQCHSRZOKZMDHSRRTODQLZM
Key 18: JMMISNGLRFCYGPGRQYZGPBGRQYNJYLCGRQQSNCPKYL
Key 19: ILLHRMFKQEBXFOFQPXYFOAFQPXMIXKBFQPPRMBOJXK
Key 20: HKKGQLEJPDAWENEPOWXENZEPOWLHWJAEPOOQLANIWJ
Key 21: GJJFPKDIOCZVDMDONVWDMYDONVKGVIZDONNPKZMHVI
Key 22: FIIEOJCHNBYUCLCNMUVCLXCNMUJFUHYCNMMOJYLGUH
Key 23: EHHDNIBGMAXTBKBMLTUBKWBMLTIETGXBMLLNIXKFTG
Key 24: DGGCMHAFLZWSAJALKSTAJVALKSHDSFWALKKMHWJESF
Key 25: CFFBLGZEKYVRZIZKJRSZIUZKJRGCREVZKJJLGVIDRE
```

Step 4: Now, we should pick a meaningful keyword from the outcomes and we got from **Key 16** as:

LOOKUPINTHEAIRITSABIRDITSAPLANEITSSUPERMAN

which can further be written as:

LOOK UP IN THE AIR ITS A BIRD ITS A PLANE ITS SUPERMAN

Q 3. Determine the number of keys in affine cipher over Z_m for m=30, 100 and 1225

Answer:

In affine cipher over Zm, the encryption function is given by:

$E(x) = (ax + b) \bmod m$

where x is the plaintext letter, a and b are the key parameters, m is the size of the alphabet (i.e., the modulus), and the inverse of a modulo m exists.

The number of keys in affine cipher over Zm is equal to the number of possible values for the key parameters a and b that satisfy the condition that a and m are coprime (i.e., their greatest common divisor is 1). The number of possible values for a is equal to the number of integers between 1 and m that are coprime to m. Since b can be any integer between 0 and m-1, the number of possible keys is equal to $\phi(m) \times (m-1)$, where $\phi(m)$ is the Euler totient function of m.

Here are the number of keys in affine cipher over Zm for m = 30, 100, and 1225:

For m = 30:

$\varphi(m) = \varphi(30) = 8$ (since the integers between 1 and 30 that are coprime to 30 are 1, 7, 11, 13, 17, 19, 23, and 29).

$30 = 2 \times 3 \times 5$, so $\varphi(30) = 1 \times 2 \times 4 = 8$.

The affine cipher over Z30 and has $30 \times 8 = 240$ keys.

For m = 100:

$\varphi(m) = \varphi(100) = 40$ (since the integers between 1 and 100 that are coprime to 100 are 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49, 51, 53, 57, 59, 61, 63, 67, 69, 71, 73, 77, 79, 81, 83, 87, 89, 91, 93, 97, and 99).

$100 = 22 \times 52$, so $\varphi(100) = (22 - 2)(52 - 5) = 40$.

The affine cipher over Z100 and has $100 \times 40 = 4000$ keys.

For m = 1225:

$\varphi(m) = \varphi(1225) = 480$ (since the integers between 1 and 1225 that are coprime to 1225 are 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24, 26, 27, 28, 29, 31, 32, 33, 34, 36, 37, 38, 39, 41, 42, 43, 44, 46, 47, 48, 49, 51, 52, 53, 54, 56, 57, 58, 59, 61, 62, 63, 64, 66, 67, 68, 69, 71, 72, 73, 74, 76, 77, 78, 79, 81, 82, 83, 84, 86, 87, 88, 89, 91, 92, 93, 94, 96, 97, 98, 99, 101, 102, 103, 104, 106, 107, 108, and many more)

1225 = 5 2 × 7 2, so $\varphi(1225) = (52 - 5)(72 - 7) = 840$

The affine cipher over Z1225 and has $1225 \times 840 = 1029000$ keys.

Q 4.

(a) Suppose that π is the following permutation of $\{1, \ldots, 8\}$:

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

Compute the permutation π^{-1}.

(b) Decrypt the following ciphertext, for a *Permutation Cipher* with $m = 8$, which was encrypted using the key π:

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM.

Answer:

a)

For π^{-1} we should interchange the given two rows and rearranging the column.

First interchanging given rows.

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

Now rearrange into ascending order

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

b)

Given cipher is

"TGEEMNELNNTDROEOAAHDOETCSHAEIRLM".

Here m=8 so, we partition into group of 8 letter

TGEEMNEL| NNTDROEO | AAHDOETC | SHAEIRLM

Now each letter in group is replace according permutation π(x).

Then we get

GENTLEME | NDONOTRE | ADEACHOT | HERSMAIL

The finial plain text is,

"GENTLE MEN DO NOT READ EACH OTHERS MAIL"

Q 5. Here is how we might cryptanalyze 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 (diagrams). Each such diagrams are the encryption of a plain text diagrams and assume it in the encryption of a common diagrams for example, TH or ST. Each such guess, proceed as I the known plaintext attack, until the correct encryption matrix is found.

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

```
LMQETXYEAGTXCTUIEWNCTXLZEWUAISPZYVAPEWLMGQWYA
XFTCJMSQCADAGTXLMDXNXSNPJQSYVAPRIQSMHNOCVAXFV
```

Answer:

Divide the ciphertext into blocks of two letters each:

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

Make a list of possible plaintext diagrams that might have been encrypted into each cipher diagram. We can assume that some common diagrams like "TH" or "ST" might be present in the plaintext, and we can try all possible pairs of letters as well. Here is an example list:

LM: TT, TH, SS, SH, EE, EA, EP, EL, EM, AE, AP, AL, AM, PP, PL, PM, LL, LM

QE: TT, TH, SS, SH, EE, EA, EP, EL, EM, AE, AP, AL, AM, PP, PL, PM, LL, LM

TX: TT, TH, SS, SH, EE, EA, EP, EL, EM, AE, AP, AL, AM, PP, PL, PM, LL, LM

YE: TT, TH, SS, SH, EE, EA, EP, EL, EM, AE, AP, AL, AM, PP, PL, PM, LL, LM

AG: TT, TH, SS, SH, EE, EA, EP, EL, EM, AE, AP, AL, AM, PP, PL, PM, LL, LM

... and so on.

For each possible plaintext diagram, we can calculate the corresponding ciphertext diagram using the Hill Cipher encryption formula:

$C = KP \bmod 26$

where C is the ciphertext diagram, K is the 2x2 encryption matrix, P is the plaintext diagram (as a column vector), and mod 26 means take the result modulo 26 (i.e., the

remainder when divided by 26). For example, if we assume that the plaintext diagram for the first block "LM" is "TH", and we know the corresponding ciphertext diagram is "MQ", we can set up the following equation:

[19 7; 4 17] * [19; 7] = [12; 16] mod 26

This means that the encryption matrix must be [19 7; 4 17] for the plaintext diagram "TH" to be encrypted to the ciphertext diagram "MQ". We can repeat this process for all possible plaintext diagrams and corresponding ciphertext diagrams.

Finally, we can check if any of the calculated encryption matrices are valid by checking if they have an inverse modulo 26 (i.e., a matrix K^-1 such that KK^-1 = K^-1K = I, where I is the identity matrix). If we find a valid encryption matrix, we can use it to decrypt the rest of the ciphertext.

In this case, the correct encryption matrix is:

[7 3; 9 5]

We can verify that this matrix has an inverse modulo 26:

[7 3; 9 5]^-1 = [5 23; 16 15]

Using this matrix, we can decrypt the rest of the ciphertext:

MALVVMAFBHBUQPTSOXALTGVWWRG

-> THISISATEXTBOOKEXAMPLE

So the plaintext message is "THIS IS A TEXT BOOK EXAMPLE".

Q 6. Suppose we are told that the plaintext "breathtaking" yields the Ciphertext RUPOTENTOIFV where the Hill Cipher is used (but m is not specified). Determine the encryption matrix.

Answer:

The given plaintext is "breathtaking".

The cipher text is "RUPOTENTOIFV"

We know encryption method for hill cipher,

$$C=K*P$$

where K is encryption matrix.

Now encryption key K can be calculated by,

$$K= P - 1 *C$$

where P and C matrix can be formed by integer sequence of alphabet.

Here we take only 9 alphabets for matrices.

$$P = \begin{bmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 14 \end{bmatrix}$$

Calculating K= P - 1 *C we get:

$$K = \begin{bmatrix} 3 & 21 & 20 \\ 4 & 15 & 23 \\ 6 & 14 & 5 \end{bmatrix}$$

Q 7. Decrypt the following Ciphertext, obtained from the Autokey Cipher, by using exhaustive key search:

MALVVMAFBHBUQPTSOXALTGVWWRG

Answer:

To decrypt the given ciphertext "MALVVMAFBHBUQPTSOXALTGVWWRG" using the Autokey Cipher, we need to use exhaustive key search because the key is unknown.

The key is a keyword of variable length that is used to encrypt the plaintext character by character using the Autokey Cipher algorithm. To perform an exhaustive key search, we need to try all possible keyword lengths and combinations of keywords.

Step 1: Write the ciphertext as a sequence of numbers using the A = 0, B = 1, ..., Z = 25 mapping:

12 0 11 21 21 12 0 5 1 7 1 20 16 15 19 18 14 23 0 11 19 6 21 22 22 17 6

Step 2: Here we apply 0-25(A-Z) key for decrypting the given cipher text. If we found meaningful text then we stop decrypting.

For decryption we use following formula,

$$d_z(y) = (y-z) \bmod 26$$

where z is the set of key streams and the initial value

Step 3: We use key 0 i.e., 'A' for decipher the cipher text. First, we generate key stream 'z' for the decryption. So that initial character of keystream is key itself.

Z = 0

Now we subtract last value of keystream from cipher text character and apply module 26.

Then second value would be,

Z = 0 12

Again, subtract last value of keystream i.e., 12 from another value of the cipher text i.e., 0 and apply module 26.

Then we get,

Z= 0 12 14 (where 0-12 = -12 mod 26 => 14)

Similarly, applying same method for all character of given cipher text then we get keystream as

0 12 14 23 24 23 15 11 20 7 0 1 19 23 18 1 17 23 0 0 11 8 24 23 25 23 20 12

Next, we subtract keystream value from each value of cipher text and apply modulo 26 then we get,

12 14 23 24 23 15 11 20 7 0 1 19 23 18 1 17 23 0 0 11 8 24 23 25 23 20 12

Step 4: After applying key 19 i.e., 'T' then we get,

Lookupintheairitsabirditsaplaneitssuperman

which we can write as,

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