CRYPTOGRAPHY & NETWORK SECURITY

ASSIGNMENT - 1

Anish Sachdeva
DTU/2K16/MC/13

30th August '2020

Scanned with CamScanner

Topic: ..... Date: ..... Page No: .....

29th August '2020

Cryptography & Network Security.
MC - 407
Assignment - 1

DTU/2K16/MC/13 - Anish Sachdeva

Q1) Describe different types of attacks threatening the confidentiality of information.

Ans 1)

Attacks Threatening Confidentiality

In general 2 types of attacks threaten the confidentiality of information: Snooping and traffic analysis.

Snooping

Snooping refers to unauthorized access to or interception of data. For example, a file transferred through the internet may contain confidential information.

An unauthorized entity may intercept the transmission and use the contents for her own benefit.

To prevent snooping, the data can be made non-intelligible to the interpreter by using encipherment techniques discussed in this book.

GOOD WRITE
A Mark of Quality

Teacher Sign. .....

Scanned with CamScanner

Traffic Analysis

Although encipherment of data may make it unintelligible for the interpreter, she can obtain some other type of information by monitoring online traffic.

For example, she can find the address (such as e-mail) address of the sender to the reciever. She can collect hours of requests and responses to help her guess the nature of the transaction.

Traffic analysis can also be performed by just visually seeing the direction of the dish antena that the country has pointed to. Just by observing the direction of a satellite dish and adversary such as Eve can figure out which country is the government in communication with. This is the reason why the satellite dishes and communication towers are covered.

Scanned with CamScanner

Topic: ..... Date: ..... Page No: .....

DTU/2K16/MC/13 - Anish Sachdeva

Q2) Describe security services defined by the ITU-T(X.800) related to the security goals and attacks.

Ans2) The International Telecommunication Union- Telecommunication Standardization Sector (ITU-T) provides some security services and some mechanisms to implement those services.

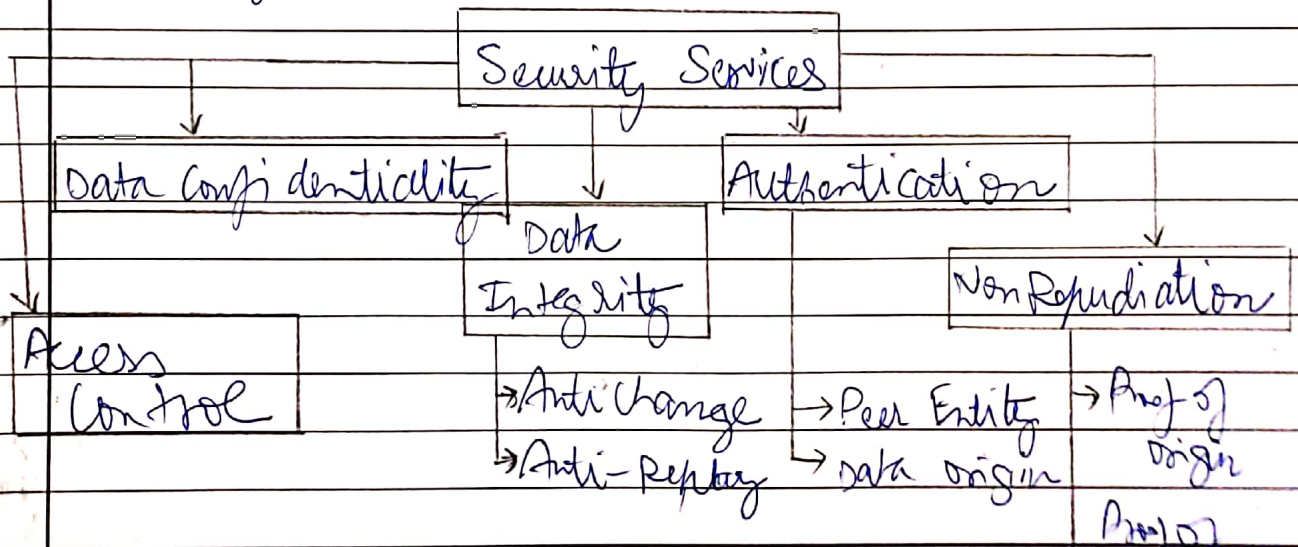
Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service.

Also a mechanism can be used in one or more services. We discuss them now:-

Security Services

ITU-T(X.800) has defined 5 services related to the security goals and attacks. The taxonomy of the services is given below.

Security Services



GOOD WRITE A Mark of Quality

Teacher Sign. .....

Scanned with CamScanner

It is easy to route one or more of these services to one or more of the security goals. It is also easy to see that these services have been designed to prevent the security attacks mentioned.

Data Confidentiality

Data confidentiality is defined to defend Disclosure attack. The service as defined by X.800 is very broad and encompasses confidentiality of the whole message or part of a message and also protection against traffic analysis attack.

- Data Integrity

Data Integrity is designed to protect data from modification, insertion, deletion, and replaying by an adversary. It may protect the whole message or a part of it.

- Authentication

This service provides the authentication of a party at the other end of the line. In connection-oriented communication, it provides authentication of the sender or reciever during the connection establishment (peer entity authentication). In connectionless communication it authenticates the source of the data (data origin authentication).

Scanned with CamScanner

Topic: ..... Date: ..... Page No: .....

- **Non Repudiation**

Non Repudiation service protects against repudiation by either the sender or the reciever of the data. In non-repudiation with proof of the origin, the reciever of the data can later prove the identity of the sender if denied.

In non-repudiation with proof of delivery the sender of data can later prove the data were delivered to the intended recipient.

- **Access control**

Access control provides protection against unauthorized access to data. The term access in this definition is very broad and can involve reading, writing, modifying, executing programs and so on.

Q3) DTU/2K16/MC/13

* **Security Mechanisms**

ITU-T (x.800) also recommends some security mechanisms to provide the security services defined above. Following is the taxonomy of these services.

→ Encipherment
→ Data Integrity
→ Digital Signature
→ Authentication Exchange
→ Traffic Padding
→ Routing Control
→ Notarization
→ Access Control

GOOD WRITE
A Mark of Quality

Teacher Sign. .....

Scanned with CamScanner

- **Encipherment**

Encipherment, hiding or covering data, can provide confidentiality. It can also be used to complement other mechanisms to provide other services. Today - 2 techniques Cryptography and Steganography - are used for enciphering.

- **Data Integrity**

The data integrity mech mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself. The reciever receives the data and the checkvalue. He creates a new checkvalue from the data and compares the newly created checkvalue with the one he has received. If the 2 checkvalues are the same, the integrity of the data has been preserved.

- **Digital Signature**

A digital signature is a means by which sender can electronically sign the data and the reciever can electronically verify the signature. The sender uses a process that involves proving that she owns a private key related to the public key and she has announced publically. The reciever uses the sender's public key to prove that the message is in deed signed by the sender who claims to have sent the message.

Scanned with CamScanner

Topic: ..... Date: ..... Page No: .....

- **Authentication Exchange**
  In authentication exchange two entities exchange some messages to prove their identities to each other. For example one entity can prove that she knows something that only she is supposed to know.

- **Traffic Padding**
  Traffic Padding means inserting some bogus data into the data traffic to thwart the adversary's attempts to use traffic analysis.

- **Routing Control**
  Routing control means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

- **Notarization**
  Notarization means selecting a third party (trusted) to control the communication between 2 entities. This can be done for example to prevent repudiation. The reciever can involve a trusted party to store the sender request in order to prevent the sender from later denying that she had made such a request.

- **Access Control**
  Access control uses methods to prove that a user has access rights to the data or resources owned by a system. Examples of proofs are passwords or PIN's.

GOOD WRITE
A Mark of Quality

Teacher Sign. .....

Scanned with CamScanner

· Relation Between Services & Mechanisms

The above table shows the relation between security services and mechanisms. The table shows that 3 mechanisms, Encipherment, digital signatures and authentication exchange can be used to provide authentication. The table also shows encipherment mechanism may be involved in three services (Data Confidentiality, Data Integrity, and Authentication)

Security Service	Security Mechanism
Data Confidentiality	Encipherment and Routing control
Data Integrity	Encipherment, Digital Signature, Authentication Exchanges
Authentication	Encipherment, Digital Signature, Authentication Exchange
Non-Repudiation	Digital Signature, Data Integrity and Notarization
Access Control	Access Control Mechanism

Scanned with CamScanner

Topic: ..... Date: ..... Page No: .....

DTU/2K16/MC/13

Q4) A generalization of the Caesar cipher, known as the Affine Cipher generates the ciphertext letter C for any plaintext P using the formula $C = E([a,b], p) = (ap+b) \bmod 26$. A basic requirement of any encryption is that it be one-to-one. That is if $p \neq q$, then $E(K,p) \neq E(K,q)$. Otherwise decryption is impossible, because more than one plaintext character maps to the same ciphertext.

The affine Caesar cipher is not one-to-one for all values of a. For example, for $a=2$ and $b=3$, then $E([2,3], 0) = E([2,3], 13) = 3$. In such a case determine which values of a are not allowed so that the given cipher is one-to-one.

Ans 4) We define the Affine cipher which encrypts/produces the ciphertext character C for plaintext character P as.

$$C = E([a,b], P) = (aP + b) \bmod 26$$

and the decryption algorithm as

$$P = D([a,b], C) = (C-b)\,a^{-1} \bmod 26$$

Now, both operation, substraction by 'b' and 'a^{-1}' congruent to $\equiv \bmod 26$ need to be invisible operations.

GOOD WRITE A Mark of Quality

Teacher Sign. .....

Scanned with CamScanner

The shift operation is congruent for all elements in the set $\mathbb{Z}_{26}$.

So, $b \in \{0, 1, 2, 3, 4, 5, 6, \ldots 21, 22, 23, 24, 25\}$

Now, we the (a') inverse operation under $\mathbb{Z}_{26}$ which isn't defined for for every element in $\mathbb{Z}_{26}$. We will use the multiplicative set $\mathbb{Z}_{26}^*$ for that.

$a \in \mathbb{Z}_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

Every element in this set has an inverse also present in $\mathbb{Z}_{26}^*$ such that $(a * a^{-1}) \bmod 26 = 1$ where a^{-1} is called the multiplicative inverse.

A few examples are

$(1 * 1) \bmod 26 = 1$
$(3 * 9) \bmod 26 = 1$
$(5 * 21) \bmod 26 = 1$
$(7 * 15) \bmod 26 = 1$ etc.

$(9 * 3) \bmod 26 = 1$
$(11 * 19) \bmod 26 = 1$
$(17 * 23) \bmod 26 = 1$
$(25 * 25) \bmod 26 = 1$

So, $\boxed{\text{DE} = a \in \mathbb{Z}_{26}^*}$

Q5) DTU/2k16/MC/13

Using the playfair matrix: Encrypt the message "Must See You over Cadogan West coming at Once"

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

Scanned with CamScanner

Topic: ..... Date: ..... Page No: .....

Ans 5) The plaintext message.

MUST SEE YOU OVER CADOGAN WEST COMING AT ONCE

i) Converting to lowercase and removing spaces

mustseeyouovercadoganwestcomingatonce

ii) Inserting character 'x' between all repeating characters

mustsexeyouovercadoganwestcomingatonce

iii) Inserting extra padding characters if the length is odd.

→ This is an even length string, and hence no character is inserted.

iv) Dividing the string into blocks of 2.

mu st se xe yo uo ve re ad og an we st co mi ng at on ce

v) Encrypting each block using the playfair cipher.

UZ TB DL ZR WQ NP ZL GB ET QA LO ZA TB TQ FK QL TH PO DG

So, the resulting ciphertext is :-

UZTBDLZRWQNPZLGBETQALOZATBTQFKQLTHPODG

GOOD WRITE A Mark of Quality

Teacher Sign. .....

Scanned with CamScanner

Q.6) DTU/2K16/MC/013

How many possible keys does the Playfair cipher have? Ignore the fact that some keys might produce identical encryption results. Now take into account the fact that some playfair keys produce the same encryption results. How many effectively unique keys does the playfair cycle have?

Ans 6) When we consider the playfair key consists of the alphabet (reduced to 25 letters) spread on a 5×5 square, that's

25! keys.

The rule of playfair are such that any rotation of the lines in the square, and any rotation of it's columns, lead to an equivalent key, in other words, the square reduces to a torus.

So, the distinct key classes considering those keys which lead to similar encipherment are $25!/5^2$ ciphers

Scanned with CamScanner

Topic: ..... Date: ..... Page No: .....

DTU/2K16/MC/13

Q7) Use the vigenere cipher with the word 'key' 'LEG' to encipher the message 'EXPLANATION'.

Ans 7)

Plaintext	E	X	P	L	A	N	A	T	I	O	N	
value	4	23	15	11	0	13	0	19	8	14	13	
Key	L	E	G	L	E	G	L	E	G	L	E	
k_i	11	4	6	11	4	6	11	4	6	11	4	
$C_i=(P_i+k_i)\%26$	15	1	21	22	4	19	11	23	14	25	17	
C	P	B	V	W	E	T	L	X	O	Z	R	

This is the encrypted message:

PBVWETLXOZR

DTU/2K16/MC/13

Q8) Use the playfair cipher to encipher the message "The key is hidden under the door pad". The secret key can be made using the word "GUIDANCE".

k_{key} =

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

GOOD WRITE A Mark of Quality

Teacher Sign. .....

Scanned with CamScanner

P = THE KEY IS HIDDEN UNDER THE DOOR PAD

i) Adding 'x' between similar characters

THE KEYIS HIDXDEN UNDER THE DOXOR PAD

ii) Padding extra 'x' to make it even length and splitting in 2

TH EK EY IS HI DX DE NU ND ER TH ED OX OR PA DX

iii) Now, applying Playfair cipher.

PO CL BX DR LG IY IB CG BG LX PO BI LZ LT TG IY

This is the encrypted message.

Scanned with CamScanner

Topic: ..... Date: ..... Page No: .....

DTU/2K16/MC/13 - Anish Sachdeva

Q 9) Eve secretly gets access to Alice's computer and using her cipher she types "abcdefghij". The screen shows "CABDEHFGIJ".

If Eve knows that Alice is using a keyed transposition cipher, answer the following questions:

a) What type of attack is eve launching?

Ans 9)a) Eve has launched a chosen plaintext attack. Eve has access to Alice's computer and also her algorithm that she is using for encryption.

With her chosen plaintext attack she can try to break the algorithm and understand how the encryption is taking place.

b) What is the size of the permutation key?

The size of the permutation key is 5 and we divide our initial message into blocks of 5 and permutate it as :-

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$ so,

P = abcde fghij
C = cabde hfgij
C = CABDEHFGIJ

GOOD WRITE A Mark of Quality

Teacher Sign. .....

Scanned with CamScanner

Q10) The following ciphertext is obtained using a substitution cipher. Give a clearly written description of steps you followed to decrypt the ciphertext. F → W

The first thing that I noticed from the ciphertext description is that this is a substitution cipher and as F → W, then it is a monoalphabetic substitution cipher.

i) The first thing I did was perform a frequency analysis on the ciphertext to identify frequency of N-grams. 1-gram is the single letter occurrences, so 26 monograms in the english alphabet. I also find a frequency of diagrams and triagrams and 4-grams. Frequency has been computed using a small script written on Python.

1-Gram frequencies =

{ C:37, G:24, S:20, K:18, Y:15, I:15, V:14, N:13, Z:13, E:12
O:10, F:9, D:8, L:7, X:7, J:7, P:6, M:5, W:5, H:5, A:5, Q:4}

From the 1-gram frequencies we can see that only 22 characters appear in the ciphertext and these are 4 characters which were never encrypted. The 4 characters to not occur in ciphertext are 'B', 'R', 'T', 'V'. These ciphertexts most probably represent very infrequently occurring letters in the english alphabet such as X, Q, J and Z.

Scanned with CamScanner

ii) Similarly I perform bigram, trigram and quadgram and pentagram frequency analysis of the ciphertext which leads to the following result :—

- Bigram Frequencies

CG : 7
ZC : 7
NC : 5
YS : 5
GO : 5
CK : 5
AC : 5
CN : 5
SF : 4
GY : 4
YK 4
FZ : 4
MG : 3
GL : 3
US : 3
IC : 3
SI : 3
KU : 3
KS : 3
XE : 3
CJ : 3
SH : 3
XC : 3

OI : 3
KG : 3
CC : 3
CI : 3
ZE : 3
WY : 2
NS : 2
YK : 2
DP : 2
VM : 2
JC : 2
PK : 2
UG : 2
OL : 2
GI : 2
GA : 2
SA : 2
KZ : 2
KX : 2
DS : 2
LK : 2
IU : 2
IG : 2
ND : 2

DG : 2
YY : 2
EO : 2
JN : 2
EU : 2
JU : 2
UC : 2
UZ : 2
CF : 2
CS : 2
EJ : 2
EM : 1
LO : 1
OJ : 1
SU : 1
UP : 1
DC : 1
GD : 1
DN : 1
CU : 1
⋮

Scanned with CamScanner

From the bigram frequencies we observe that {CG and ZC} occur many times. The most common bigrams in English are :-

th, he, in, en, nt, re, er, an, ti .....

but we have already assumed that C → e so G could be either {n, t, a} or some other consonant. We also see FZ occurring 4 times. We know F → W so, Z could be {i, h, o} but we also know that ZC occurs very often and C → e so Z can't be 'o' and could be 'i' or 'h'.

iii) Now, we compute 3-gram (Trigram Frequencies)

YSF : 3
GOI : 3
FZC : 3
ZCC : 3
CCN : 3
CYK : 2
JCK : 2
GOL : 2
ICG : 2
[illegible]
CGI : 2
NCG : 2

GAC : 2
CKS : 2
SAC : 2
CKX : 2
KSH : 2
ZCN : 2
KGO : 2
CDN : 2
NDG : 2
DGY : 2
GYY : 2
YYS : 2
JNC : 2

CJU : 2
UZC : 2
CFZ : 2
ZEJ : 2
EMG : 1
MGL : 1
GLO : 1
⋮

Scanned with CamScanner

We observe from the bigram frequencies that we get {YSF, QOI, FZC} 3 times

FZC → wZe so Z should most likely be h

Hence Z → h

We also see that {QYY, YYS} occur 2 times and {YY} occurs 2 times in the bigram frequencies. The most common same letter bigrams in the English language are {'ee', 'll', 'nn', 'mm', 'rr'} so Y probably belongs to one of them.

(iv) Performing quadgram (4-grams) frequency analysis

FZCC : 3	EMQL : 1
ZCCN : 3	MQLO : 1
ICQE : 2	QLOS : 1
CCND : 2	⋮
CNDQ : 2	
NDQY : 2	
DQYY : 2	
QYYS : 2	
CFZC : 2	

We see, we have ZCCN occurring 3 times. We also know ZCCN → heeN so N could be {'l', 'r'} etc.

Now, let us perform the quadgram (5-grams) frequency analysis

Scanned with CamScanner

v) 5-Gram (Pentagram Frequency Analysis)

FZCCN : 3	DGYYS : 2
ZCCND : 2	GYYSF : 2
CCNDG : 2	CFZCC : 2
CNDGY : 2	EMGLO : 1
NDGYY : 2	MGLOS : 1
	⋮

We have FZCCN occurring 3 times, so this could most probably be :-

FZCCN → WZeeN → WheeN so, N is most probably 'h' and we have FZCCN → wheel

Now, from monogram frequencies we can see

C : 37	K : 18	N : 13	H : 5
G : 24	Y : 15	Z : 13	A : 5
S : 20	V : 14	E : 12	Q : 1

So, we can see from lower frequencies that most probably

{Q, B, R, T, V} → {K, X, Q, J, Z} and

{G, S, K, Y, V} → {E, T, A, O, I, N}

We know C → e so {G, S, K, Y, V} → {T, A, O, I, N}

also

{N, Z, E, O, F, D, L} → {S, R, H, D, L, U, C}

We know Z → h and N → l so,

{E, O, F, D, L} → {S, r, d, u, c}

Scanned with CamScanner

vii) Now, we see occurrences of F with other ciphertext characters.

FZE in trigram frequency

FZE → WhE , so E may be 'i'

The most frequent bigraph in ciphertext is 'CG'.

CG → eG so G may be 'a', 'l', 'n', h' etc.

So, as has frequency of 4, or G → a.

We have test out this mapping on a few examples.

CNDGY → elDaY

If we take C → a, we can apply it to solve GYY and GYS

YY → {'ll', 'ee', 'hh', 'mm'....}

GYY → aYY This implies Y → r

CNDGY → elDar so D → {'C', 'B', 'M', 'N'} etc.

Observing quadgram and pentagram frequencies for D, we see DGYY:2, DGYYS:2, DGYYSF:2

Darr DarrS DarrSw

arrSw → arrow would be a plausibility

so, we see that {S → o} and that leaves only one possibility {D → b}, hence

DGYYSF → barrow

Scanned with CamScanner

vii) Going back to monogram frequencies, we had seen {G, S, K, Y, U} → {t, a, e, i, n} but now we know G → a and Y → 'r' so

{S, K, U} → {t, o, i, n}

The total encryptions we have deciphered are:—

W → F
h → Z
e → C
l → N
b → D
a → G
r → Y
o → S

Now, let us decipher the ciphertext using what we know

~~EMaLl~~

EMGLOSU D C GDN CU SWY S FHNSFCY KD PUMLWGYI.

EMaLOoU beable Uo WroW Hlower Kb PUMLWarI ....

Using this section of the deciphered plaintext, we can make out Hlower → is most probably flower and Uo is most probably to. So, we get f → H and t → U in encryption.

Scanned with CamScanner

viii) Now, the decryption we know are

f → H
l → N
o → S
w → F
e → C
r → Y
h → Z
b → D
a → G
t → V

EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMCWGYICOXY ICOX
YSIPTCKQPKUGKMGOLICGINCGACKSNISACYKZSCKX.

EMaLOotbe able to Wrow flowerK bPt MG WarIeS
XroIPJeK QPKtakMPJh deaI leaAek. ...

from this decrypted message we can further identify :-
{S → K, g → W, μ → P, d → I, v → A} in the encryption table

ix) We again decipher the encrypted message :-
EMaLOot be able to grow flowers but MG gardeS
XrodwJes rust as MaOL dead leaves old over
shoe sXEJes of roXe and bushells of dead
grass as anLbodLs and todaL E bought
a wheel barrow to helX in EnJlearEng Et it....

Using the above text we identify words and once again identify the substitutions: {m → M, y → L, P → X, c → J, j → Q

Scanned with CamScanner

n → O, y → L, i → E, c → J

x) We again decipher the ~~plaintext~~ ciphertext

I i may not be able to grow flowers but my garden produces just as many dead leaves old over shoe species of rope and bushells of dead grass as anybodys and today i bought a wheel barrow to help in clearing it up i have always loved and respected the wheel barrow it is the one wheeled vehicle of which i am perfect master.

So, we end up with the following encipherment table:-

P:	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
C:	G	D	J	I	C	H	W	Z	E	Q	-	N	M	O	S	X	_	Y	K	U	P	A	F	_	L	-

Here we never see the letters k, q, r and z and hence they can represent any of the following: Q, B, R, T, V

Scanned with CamScanner

Q13) The plaintext "letusmeetnow" and the corresponding ciphertext "HBCDFFNOPIKLB" are given. You know that the algorithm is a hill cipher, but you don't know the size of the encryption matrix. Find the key matrix.

(Ans 11) The length of the ciphertext and plaintext is 12.

So, the different key lengths that are possible are 1, 2, 3, 4, 6, 12. The amount of plaintext/ciphertext pairs that we need to cipher key size m is m^2. So, for:-

1 : 1
2 : 4
3 : 9
4 : 16
5
6 : 36

pairs of ciphertext/plaintext are required.

We have only 12 pairs of plaintext/ciphertext, so we can only check for key size $m=1, 2, 3$.

- $m=1$

We know that $C = P \cdot K$ in hill cipher where C is the resulting ciphertext matrix and P is the original plaintext matrix. We also know K is the hill cipher encryption key where K is invertible and the operation $P = K \cdot k$ is in $\mathbb{Z}_{26}$ and congruent to mod(-) 26.

$C = P \cdot K$
$K = P^{-1} \cdot C$, here P^{-1} is the modular inverse of P congruent to 26. (mod)

Scanned with CamScanner

This is not the correct encryption, hence the key we have selected [3] is incorrect and we will now search for a 2×2 key for Hill Cipher.

• 2×2

Let us consider Plaintext/Ciphertext pair LEUT/HBDI

We have

$$P = \begin{bmatrix} 11 & 4 \\ 20 & 19 \end{bmatrix} \quad C = \begin{bmatrix} 7 & 1 \\ 3 & 8 \end{bmatrix} \quad P^{-1} = \begin{bmatrix} 7 & 4 \\ 20 & 15 \end{bmatrix} \bmod 26$$

We get $K = P^{-1} \cdot C$

$$= \begin{bmatrix} 7 & 4 \\ 20 & 15 \end{bmatrix} \begin{bmatrix} 7 & 1 \\ 3 & 8 \end{bmatrix} \% 26$$

$$= \begin{bmatrix} 61 & 39 \\ 285 & 140 \end{bmatrix} \% 26$$

$$= \begin{bmatrix} 9 & 13 \\ 3 & 10 \end{bmatrix}$$

We also have $K^{-1} \bmod 26 = \begin{bmatrix} 16 & 13 \\ 3 & 17 \end{bmatrix} \bmod 26$

So, this can definately be a key. We now encrypt our plaintext using this key and compare results with the given ciphertext

$$C = \begin{bmatrix} 11 & 4 \\ 19 & 20 \\ 18 & 12 \\ 4 & 4 \\ 19 & 13 \\ 14 & 22 \end{bmatrix} \begin{bmatrix} 9 & 13 \\ 3 & 10 \end{bmatrix} = \begin{bmatrix} 7 & 1 \\ 23 & 5 \\ 16 & 16 \\ 22 & 14 \\ 2 & 13 \\ 10 & 12 \end{bmatrix} = \text{HBXFQQWOCNKM}$$

Scanned with CamScanner

Not every plaintext matrix is invertible, but for an invertible pair the $K = P^{-1} \cdot C$ is solvable and the resulting matrix for K should also be modular matrix invertible.

If the resulting key matrix is not invertible, then no solution exists for that particular key size.

We can prove this by proof of contradiction. Let us assume that a key exists for Hill cipher of size m that converts plaintext P to ciphertext C, hence

$$C = P \cdot K$$

$K = P^{-1} \cdot C$ and if we take $P^{-1} \cdot C$, the result we get must be that key and if the result isn't invertible, then the key we have obtained was never a key to begin with.

Now, for n=1, let us assume the plaintext / ciphertext pair as: L/H. We get

$$P = [11] \quad C = [7] \quad P^{-1} = [11]^{-1} = [19] \bmod 26$$

$$K = P^{-1} \cdot C$$
$$= [19][7]$$
$$= 3$$

Now, let us encrypt the plaintext message using this key and see encrypted message

$$C = [3][11\ 4\ 19\ 20\ 18\ 12\ 4\ 4\ 19\ 13\ 14\ 22]$$
$$C = [7\ 12\ 5\ 8\ 2\ 10\ 12\ 12\ 5\ 13\ 16\ 14]$$
$$= [H\ M\ F\ I\ C\ K\ M\ M\ F\ N\ Q\ O]$$

Scanned with CamScanner

As the ciphertext we are receiving is not the correct ciphertext, we conclude that a key size of 2 hasn't been used for encrypting the data.

• 3+3

We have plaintext and ciphertext as

$$P = [11\ 4\ 19\ 20\ 18\ 12\ 14\ 4\ 19\ 13\ 14\ 22]$$

It is arranged in blocks of 3 as follows:-

$$\begin{bmatrix} 11 & 4 & 19 \\ 20 & 18 & 12 \\ 4 & 4 & 19 \\ 13 & 14 & 22 \end{bmatrix} \cdot K = \begin{bmatrix} 7 & 1 & 2 \\ 3 & 5 & 13 \\ 14 & 15 & 8 \\ 10 & 11 & 1 \end{bmatrix}$$

ciphertext

We have to take 3 blocks of ciphertext/plaintext to find the key K such that P^{-1} exists and also K^{-1} exists, and resulting decryption/encryption is a match.

Let us take matrix block

$$P = \begin{bmatrix} 11 & 14 & 19 \\ 20 & 18 & 12 \\ 4 & 4 & 19 \end{bmatrix}$$

Here P^{-1} doesn't exist as $|P| = 2058$, which isn't coprime in 26 and hence a modular inverse doesn't exist.

Scanned with CamScanner

Now, we take

$$P = \begin{bmatrix} 11 & 14 & 19 \\ 20 & 18 & 12 \\ 13 & 14 & 22 \end{bmatrix}$$

$|P| = 2246$

2246 isn't coprime with 26. hence modular matrix inverse doesn't exist.

Let us now consider:-

$$P = \begin{bmatrix} 11 & 4 & 19 \\ 4 & 4 & 19 \\ 13 & 14 & 22 \end{bmatrix}$$

$|P| = -1246$

-1246 is not coprime with 26 and hence this matrix has no modular inverse and hence can't be used to find key. We now consider

$$P = \begin{bmatrix} 20 & 18 & 12 \\ 4 & 4 & 19 \\ 13 & 14 & 22 \end{bmatrix} \quad |P| = -650$$

-650 can't coprime with 26 and hence has no modular inverse. So, the key is definately not 3x3. We conclude either that the key size is higher 4x4, 6x6 or 12x12 or a key doesn't exist.

Scanned with CamScanner

Q.12) DTU/2K16/MC/13

Assume a one time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 to 26. For example, if the key is 3, 19, 5 then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on. Encrypt the plaintext "SENDMOREMONEY" with the key stream

9, 0, 1, 7, 23, 15, 21, 14, 11, 11, 2, 8, 9

P:	S	E	N	D	M	O	R	E	M	O	N	E	Y
P_i:	18	4	13	3	12	14	17	4	12	14	13	4	24
K_i:	9	0	1	7	23	15	21	14	11	11	2	8	9
$C_i = (P_i + K_i) \% 26$	1	4	14	10	9	3	12	18	23	25	15	12	7
C:	B	E	O	K	J	D	M	S	X	Z	P	M	H

Hence, the final ciphertext is:

BEOKJDMSXZPMH

Scanned with CamScanner