TUTORIAL 2

CRYPTANALYSIS

SUBMITTED BY-
AMAN BHARDWAJ
2019SIY7580

Q1 Playfair Cipher - Steps

Soln. Given :- EG → TH PH → HE GQ → IN DP → ER

BM → AN

- Also Their reverse will be reverse of Plain text eg EG → TH → GE → HT
- Replace Them in cipher Text.
- Sentence is most likely to start with The when first two letters are TH ∴ EG HX → THE_ ⇒ HX → E_ & XH → _E
- [PH → HE and in Trigrams EPH occurs 3 times ⇒ _E PH should also be _THE] ✗ not working ignore this assumption
- J is missing from Key.
- HE → PH ∴ EHP__ or key has

E				
H				
P				
_				
_				

— (I)

Also TH → EG key has ⇒ TE HG or

T	E			
G	H			

— (II)

This cannot be Possible From (I)

This is correct ✓

Combine (I) & (II) we get Part of Key

T	E			
G	H			
	P			

— (III)

- Consider IN → GQ ⇒ Part of Key Should be I G or Q N from (III) this is wrong

G	I			
N	Q			

Combine with (III) Put Q next to P

T	E			
G	H	I		
N	P	Q		

— (IV)

- Consider ER → DP ⇒ From (IV) E D ∴ Put R to Right of Q. as Per P R Sequence

T	E		D	
G	H	I		
N	P	Q	R	

— (VI)

- ~~XYZ should be last~~
- Complete the Plain text from These Known key. with Pencil

- Consider AN → BM and combine with (IV), Also Put XYZ in last 3 chars.

A	B			
	T	E	C	D
O	G	H	I	
M	N	P	Q	R
	X	Y	Z	

Observations -
- O Must be the part of "Key Phrase".
- Either one of K/L must be part of Key Phrase
- □ must be C as A B E are already there and D is after E
- ○ must be F. as per Sequence

The matrix becomes

A	B	_	O	_
_	T	E	C	D
F	G	H	I	_
M	N	P	Q	R
_	_	X	Y	Z

→ (VI)

Now complete Plain Text as much as possible with these known key square elements.

- Now we can see is AI = _F = OF Put in Key. (VI) with circle
- Letters remaining K, L, S, U V W } → (VII)
- Key = A B _ O _ _ T E

From above K V W doesn't make sense also clearly words is ABSOLUTE → KEY

- Square =

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

Now decrypt the cipher Text

Q1 PLAY FAIR CIPHER (Broken in Pairs for Play Pair)

EG	HX	BY	DP	AI	IK	EH	XC	BX	BO	IC	PB	KC	DP
TH	EP	OW	ER	OF	HI	SE	YE	SW	AS	CO	NS	ID	ER

BS	OZ	TP	FS	QT	CU	OW	EG	CH	MQ	LO	GC	QC	PQ
AB	LY	EN	HA	NC	ED	BY	TH	EI	RP	OS	IT	IO	NP

AB	DC	UL	BE	PH	ZX	DP	TS	CE	XT	TP	EG	HX	OF
LA	CE	DA	ST	HE	YW	ER	EB	ET	WE	EN	TH	EP	AI

WG	CU	IA	PD	PH	LU	BM	UE	PH	UL	ZR	XG	HO	HD
NT	ED	FO	RE	HE	AD	AN	DT	HE	DA	RK	WH	IS	KE

PL	XG	QI	PE	DN	US	PU	EZ	CL	BW	IK	OE	PH	DH
RS	WH	IC	HS	TR	EA	ME	DX	DO	WN	HI	SC	HE	EK

EH	XU	MB	FS	AK	YG	EB	CX	HE	YB	DA	EL	MS	ZR
SE	VE	NA	HA	LF	WI	TS	EY	ES	WO	UL	DS	PA	RK

SD	GQ	AE	EI	BO	CE	CG	WN	CB	DQ	BY	WG	PH	UH
LE	IN	SU	CH	AS	ET	TI	NG	TO	CK	OW	NT	HE	EF

HU	DE	PH	YB	TM	UL	OB	HV	KM	BQ	IC	AL	DM	CU
FE	CT	HE	WO	UN	DA	SA	FX	FR	ON	CO	LO	UR	ED

ET	NL	BM	LM	AC	RT	IK	EP	US	UE	IK	OE	LA	XA
TU	RB	AN	AR	OU	ND	HI	SH	EA	DT	HI	SC	OL	VS

CP	LE	IU	PT	PU	XD	PM	UK	OC	UX	HS	QS	DX	TP
EQ	SD	FC	NE	ME	ZE	NR	DF	YO	EV	EX	PO	EZ	EN

DB	UD	NO	UE	CU	ES	IF	QB	OS	TH	EL	MU	SE	WD
TL	DC	OB	DT	ED	SX	HK	NO	SB	EG	DS	FA	XS	ZT

NO	UE	CU	EC	IL	OQ	AO	LZ	KS	FO	KB	OU	BD	RE
OB	DT	ED	TE	KO	YI	LS	ZR	HL	JA	GL	AC	LT	PD

S
X

Bigram (CText)

~~PH~~ – 6	TP-3
CU – 5	UL-3
IK – 4	HX-2
UE – 4	BY-2
~~EG~~-3	EH-2
~~DP~~-3	BO-2

1-Gram (CText)

E-30	D-19
U-26	O-18
B-23	L-16
P-23	S-15
C-23	X-14
H-20	I-13

3-Gram (CText)

EPH-3
CUE-3
~~EGTH-1~~
ELM-2
OUE-2

4 Gram (CText)

~~EGTHX~~-2
IKOE-2
NOUE-2
UECU-2

Cross which have been Used

Question 2: Simple Cipher

Nbzmnzi rh z xlfmgib rm Zhrz. Nzmb Ilsrmtbz Nfhornh orev gsviv. Gsvri orevh ziv evib

is a in Asia Many muslims there Their are
Myanmar Country Rohingya live lives very

wruurxfog. Gsvb nfhg nrtizgv z olg. Rm 2017, gsviv rh hgilmt nrorgzib zxgrlm ztzrmhg Ilsrmtbz

difficult They must a Lot In There is military against
migrate Strong action Rohingya

Nfhornh. Gsviv rh z olg lu erlovmxv. Nzmb kvlkov wrv. Z olg lu kvlkov ifm zdzb gl zmlgsvi

Muslims There is a lot of violence Many people die A lot of people run away to the another

xlfmgib. Hlnv kvlkov yvorvev gszg gsviv rh tvmlxrwv lu gsv Ilsrmtbzh. Gsv Nbzmnzi tlevimnvmg

Country people that there is of the The government
Some believe genocide Rohingya Myanmar

zhph z xlnnrggvv gl urmw lfg dszg szkkvmh. Gsv xlnnrggvv hzbh gszg gsviv rh ml tvmlxrwv.

a to out The says that there is no
asks committee Find what committee genocide
happened

Sldvevi, gsviv rh hvirlfh xirnv. Z olg lu kvlkov wl mlg yvorvev gsrh. Gsvb hzb gszg gsv

However there is A lot of people do this They say that the
serious crime not believe

tlevimnvmg dzmgh gl srwv gsv gifgs.

government to the truth
hide
want

□ means Final

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

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

Q2. Simple Cipher.

Steps Followed :-

- GSV is the most frequent trigram so it must be english word THE as per freq. Analysis
  ∴ G → T S → H V → E
- Replace GSV with THE in the text and try to figure out words containing GSV.
  GSVIV → THERE This should be THERE
  ∴ I → R
- Z occurs as single word ∴ It should be either I or A but It can not be I as per placement ∴ A makes sense
  Z → A Replace Z with A
- Now look at multiple words with rh having known text in surrounding
  GSVIV rh Z and rh Z ⇒ H → S
  THERE IS a I _ a
- GL → .T_ as TO occurs in english ⇒ GL = TO L → O
- GSZG → TH_T clearly "THAT" ⇒ Z → A
- Consider Phrase
  GSVV rh Z olg lu
  There is a _ot o_ (lot of) fits here
  ⇒ O → L, u → F

  Replace olg → lot lu → of and complete the words with known letters so far
- Consider [HLNV → SO_E DSAG → _S_T] Multiple combinations Possible ∴ Ignore for now
  GIFGS → TR_TH clearly truth ⇒ F = U
- consider gl srwv gsv gifgs
  to hi_e the truth ∴ (srwv → hide) ⇒ W → D
- Complete the words with known plain text letters so far

- Consider Phrase
  Z olg lu KVlKOV wl mlg ⇒ K=P
  A lot of people do not M→N
  p p n
- Complete things with known letters so far.
- NZMB people die ∴ clearly MANY ⇒ N→M, B→Y
  _ A N _
- After completing Consider following string.
  Z olg lu KVlKOV wl mlg YVORVEV gsrh
- A lot of People do not BELIEVE this ⇒ Y→B, E→V
  B E V
- Complete the words.
- W R U U R X F O G
  D I F F I _ U L T ⇒ X→C
  C
- g s v i v r h h g i l m t
  this is strong ⇒ t→g
  g
- Z d z b → a _ a y ⇒ D→W
- Complete the Text now.

Plain Text –

Myanmar is a country in Asia. Many Rohingya muslims live there. Their lives are very difficult. They must migrate a lot. In 2017, there is strong military action against Rohingya muslims. There is a lot of violence. Many people die. A lot of people run away to another country. Some people believe that there is genocide of the Rohingya. The myanmar government asks a committee to find out what happened. The committee says there is no genocide. However, there is serious crime. A lot of people do not believe this. They say that the government wants to hide the truth

Question 3 Simple Cipher

Htghst xlt lxflekttfl zg hkgztez zitok laof ykgd zit lxf. Zitkt ol q ftv lzxrn. Oz lqnl ziqz lgdt

People ↓ use ↓ sunscreen to ↓ protect their ↓ skin from the ↓ sun. There is a ↓ new ↓ study. It says that some

eitdoeqsl of lxflekttfl utz ofzg htghst'l wsggr Leotfzolzl ztlz ygxk royytktfz lxflekttfl qfr lob

chemicals in ↓ sunscreen get into ↓ people's blood ↓ scientists test ↓ four different ↓ sunscreen and six

eitdoeqsl. Zitn yofr ziqz qss lob eitdoeqsl utz ofzg zit wgrn. Zitn rg fgz afgv viqz zitlt eitdoeqsl

chemicals ↓ They ↓ find that six ↓ chemicals all ↓ get into the ↓ body. They ↓ do not ↓ know ↓ what these ↓ chemicals

rg zg htghst. Oz ol vgkknofu. Leotfzolzl dxlz rg dgkt ktltqkei zg xfrtklzqfr igv eitdoeqsl utz ofzg

to ↓ people. It is ↓ worrying. Scientists ↓ must do more ↓ research to understand. How ↓ chemicals get into

zit wgrn.

the body

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
K	X		M	C	N	O	P	H		R	S		Y	I

P	Q	R	S	T	U	V	W	X	Y	Z
	A	D	L	E	G	W	B	V	F	T

Digraphs	Tri	Quad
zg - 3	xlt	
ol - 2	zit + 1+1+1 zitn	
oz - 2	Lxf	
of - 1	ftv	
rg - 3	utz + 1 + 1	
	qfr	
	lob + 1	
	qss	
	fgz	
	igv	

Q3. Simple Substitution cipher

Steps followed -

- Write Bigrams & Trigrams from text.

Bi→ Zg-3 ol-2 oz-2 of-1 rg-3

Tri→ xlt-1 zit-4 Lxf-1 FTV-1 UTZ-3 QFR-1 LOB-2

Quad→ zitn

zitkt

It seems clear that ZIT → THE ⇒ Z→T | I→H | T→E

~~Now fill the blanks with~~

- Single letter q. Consider as A ⇒ Q→A ⇒ ziqz → THAT
- Replace with these characters
- A lot of words start with Zit ie The

ZITOK ZITKT ZITN ZITLT

THEIR THERE THEY THE_E

K→R, O→I | K→R | not sure for this. So for now consider N=Y as THEY is frequent letter.

- Zg comes 3 times TO ∴ it should be TO as per freq analysis.

⇒ G→O

Complete words with these known letters.

- RG ZG Consider these too Consecutive words.

GO TO ∴ DO GO TO makes sense

⇒ R→G or R→D But DO makes more sense when we look at positions of R ⇒ R=D

- Consider ZITKT OL Q

THERE IS A ⇒ There is a ⇒ L→S

⇒ THE_E → THESE

- QFZG → I_TO ∴ "Into" ⇒ F=N

Complete with these two ~~two~~ letters

- Consider Phrase zitn rg fgz afgv

They do not know ⇒ A→K, V→W

- Consider W GRN
  into the B O D Y makes Sense → ⇒ B W → B
- UTZ ofzg zit Wgrn
  GET into the Body ⇒ U → G
- Consider words W S G G R → B _ O O D } Both have same letter
  A S S A _ _ } missing ∴ Blood & all
  makes sense
  ⇒ S → L
- Consider word H T G H S T
  P E O P L E → H → P
- Consider Zitkt ol q ftv L Z X R N
  There is a new S T U D Y. ⇒ X → U

Now complete words with these known letters.

- Consider word L X F L E K T T L
  S U N S C R E E N ⇒ E → C
- Consider zitok laot ykgd zit LxF
  their skin E ROM The Sun ⇒ Y → F

Complete the words

- Consider qfor lob eitdo eqsl
  and si X cheMicals → D → M

as Four is used in this line ∴ Let ~~xxx~~ consider Four _ and Six _
for now consider B → X

- Consider K t l t q kei → R e s e a r c h

Plain Text →

People use Sunscreen to protect their skin from the Sun. There is a new study. It says that some chemicals in Sunscreen get into people's blood. Scientists test four different Sunscreens and six chemicals. They find that all six chemicals get into body. They do not know what these chemicals do to people. It is worrying. Scientists must do more research to understand how chemicals get into the body.