Mono alphabetic substitution cipher

Consider we have the plain text “cryptography”. By using the substitution table shown below, we can encrypt our plain text as follows

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

one permutation of the possible 26!

plain text : c r y p t o g r a p h y

cipher text : B S E Z W U C S J Z N E

Hence we obtain the cipher text as “BSEZWUCSJZNE”

Mono alphabetic substitution cipher- cryptanalysis

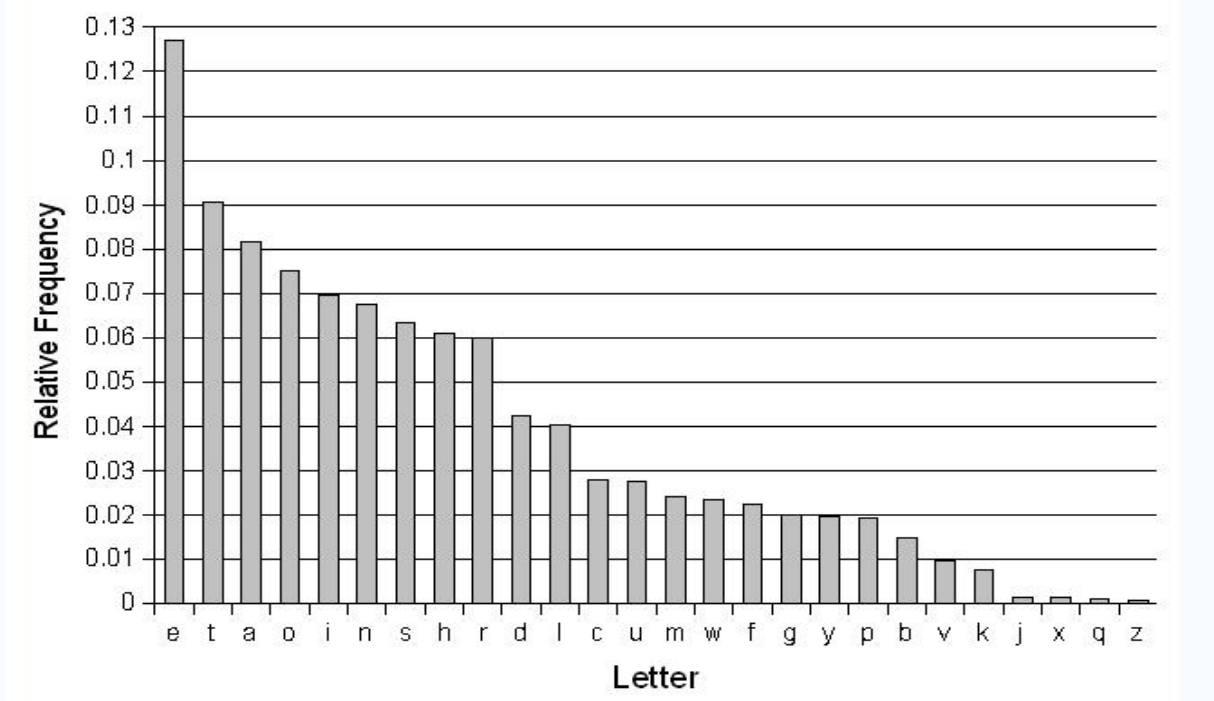
Consider we have the following cipher text

“LMCOTKOMSFKSWIMCQTGAUECTGKTGWFEZEWISKKTWG
VGWLLSDDOMCOTMCQSTOTGNSOWNCVSNRGCNSICN
WFKGWNCGDTQSKWEMCKSQSEDTQSYLMWMCKUEWFA
MOOMSKCNSCNWFGOWIKOFYRCGYWIGCOFECDOCDSGO
OWOMSYSOSJOTWGWIJETNSLMTJMTMCQSYWGSCGYLM
COTKOMSESKFDOOMSESTKGWJETNSOWYSOSJO”

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
2	0	20	7	11	8	17	0	6	5	14	6	17	10	24	0	6	2	28	18	2	2	20	0	7	1

Number of occurrences of each alphabet in the given cipher text

Mono alphabetic substitution cipher- cryptanalysis



Frequencies of occurrence of each alphabet in an eglish text

th	he	an	re	er	in	on	at	nd	st	es	en	of	te	ed
168	132	92	91	88	86	71	68	61	53	52	51	49	46	46

Most common English bigrams (frequency per 1000 words)

Mono alphabetic substitution cipher- cryptanalysis

In the given cipher, we observe that ‘S’ has the highest count followed by ‘O’ Hence we make the substitutions S=e and O=t. Similarly we have C=a, W=o and T=I

“LMatiKtMeFKeoIMaQiGAUEaiGKiGoFEZEoIeKKioG
iVGoLLeDDtMatiMaQeitiGNetoNaVeNRGaNeIaN
oFKGoNaGDiQeKoEMaKeQeEDiQeYLMoMaKUEoFA
MttMeKaNeaNoFGtoIKtFYRaGYoIGatFEaDtaDeGt
totMeYeteJtioGoIJEiNeLMiJMiMaQeYoGeaGYLM
atiKtMeEeKFDttMeEeiKGoJEiNetoYeteJt”

In the above text we observe many trigrams ‘tMe’ which would be ‘the’ and so we can use M=h and obtain the new text as follows

Mono alphabetic substitution cipher- cryptanalysis

"LhatiKtheFKeoIhaQiGAUEaiGKiGoFEZEoIeKKioG
iVGoLLeDDthatihaQeitiGNetoNaVeNRGaNeIaN
oFKGoNaGDiQeKoEhaKeQeEDiQeYLhohaKUEoFA
httheKaNeaNoFGtoIKtFYRaGYoIGatFEaDtaDeGt
to the YeteJtioGoIJEiNeLhiJhihaQeYoGeaGYLh
atiKtheEeKFDttheEeiKGoJEiNetoYeteJt"

We find 'Lhat' at 2 places which can be guessed to be 'what' and so we know that L=w. We make these substitutions in our text

Mono alphabetic substitution cipher- cryptanalysis

" what iK the FKeoIhaQiGAUEaiGKiGoFEZEoIeKKioG
iVGowweDDthatihaQeitiGNetoNaVeNRGaNeIaN
oFKGoNaGDiQeKoEhaKeQeEDiQeYwhohaKUEoFA
httheKaNeaNoFGtoIKtFYRaGYoIGatFEaDtaDeGt
to the YeteJtioGoIJEiNewhiJhihaQeYoGeaGYwh
atiKtheEeKFDttheEeiKGoJEiNetoYeteJt"

Now clearly K=s. Also 'YeteJt' would be 'detect' and 'YeteJtioG' would be 'detection' So Y=d and J=c and G=n

Mono alphabetic substitution cipher- cryptanalysis

" what is the FseoIhaQinAUEainsinoFEZEoIession
iVnowweDD that I haQe it in Ne to NaVeNRnaNeIaN
oFsnoNanDiQesoE has eQeEDiQed who has UEoFA
ht the saNeaNoFntoIstFdR and oInatFEaDtaDent
to the detectionoIcEiNe which i haQe done and what
is the EesFDttheEe is no cEiNe to detect"

A little inspection of the above text would suggest that : F=u, Q=v , A=g and E=r. Also we find many digrams 'oI' which we can safely deduce to be 'of' and so I=f.

Mono alphabetic substitution cipher- cryptanalysis

" what is the use of having Urains in our Zr of ession
i VnowweDD that i have it in Ne to NaVeNRnaNefaN
ous no NanDives or has ever Dived who has Uroug
ht the saNeaNount of studR and of naturaDtaDent
to the detection of criNe which i have done and what
is the resuDtthere is no criNe to detect"

Now it is easy to make the remaining substitutions by just observing the text and we finally get our plain text as follows

Mono alphabetic substitution cipher- cryptanalysis

" what is the use of having brains in our profession. I know well that I have it in me to make my name famous. No man lives, or has ever lived, who has brought the same amount of study and of natural talent to the detection of crime, which i have done And what is the result There is no crime to detect"