Systems and Networks Security

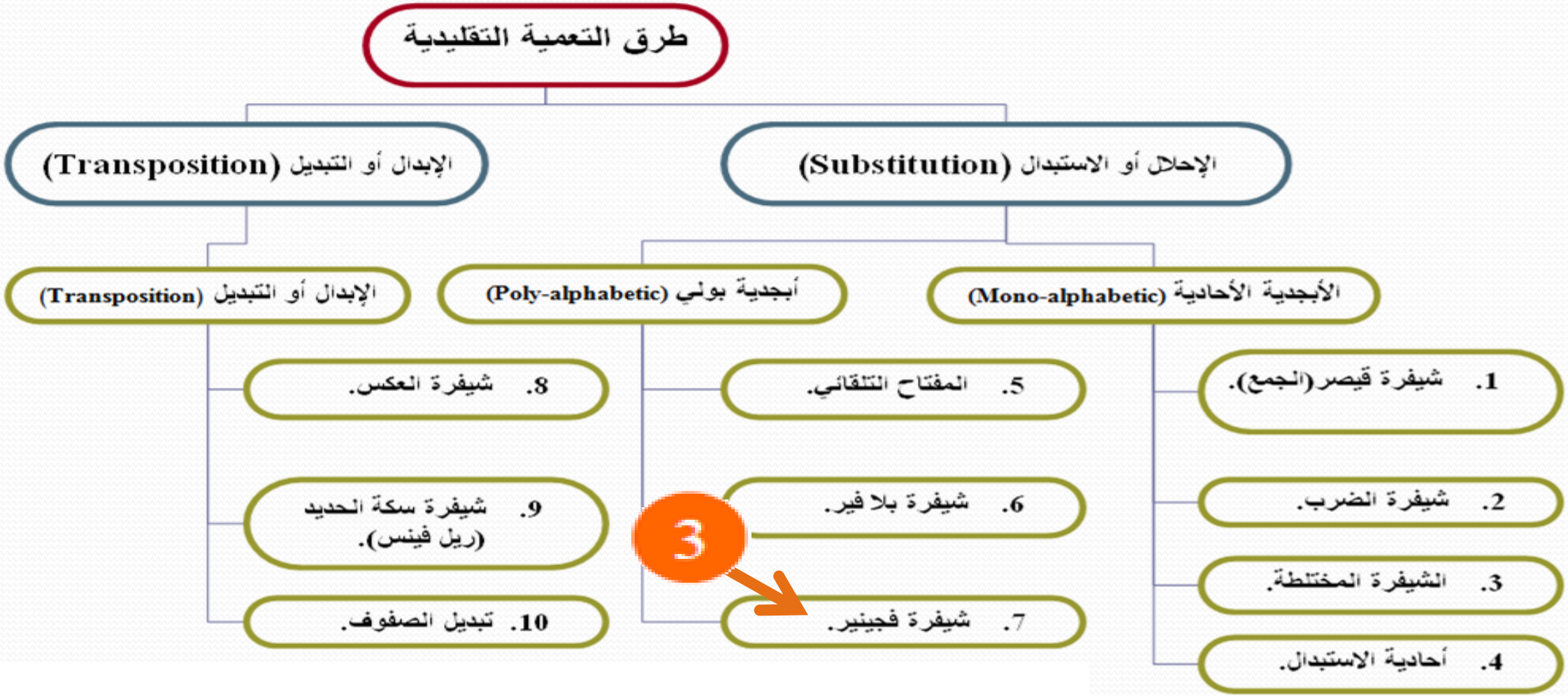
Lecture 3

Main Points

- **Traditional Ciphers (Substitution):**
- **Simple Shift (Vigenere Cipher).**
- **Attacking the Simple Shift (Vigenere Cipher).**

Traditional Ciphers (Substitution)

(Mono-alphabetic Ciphers) & (Poly-alphabetic Ciphers).



Simple Shift (Vigenere Cipher)

- **Simple Shift (**Vigenere Cipher) :
- Method of encrypting alphabetic text by using a series of interwoven Caesar ciphers.
- Using two of more letters of a keyword.

- **Simple Shift (Vigenere Cipher) Problems:**
- Key is keyword.
- No Symbol.

Simple Shift (Vigenere Cipher)

- **Vigenere Encryption :**

Ciphertext = (Plaintext$^{\text{Char First}}$ + key$^{\text{First}}$) mod 26$^{\text{Letters}}$.

- **Vigenere Decryption :**

Plaintext = (Ciphertext$^{\text{Char First}}$ – key$^{\text{First}}$) mod 26$^{\text{Letters}}$.

Plaintext →	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
	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cryptosystem (Vigenere Cipher)

- Fivefold (**E**, **D**, **M**, **K**, **C**)
  - **M** set of plaintexts (letters , words).
  - **K** set of **K**eys (**i** = two or more of letters (English) $\mathbf{0 \leq i \leq 25}$).
  - **C** set of **C**iphertexts (letters , words).
  - **E** set of **E**ncryption functions: $(\mathbf{M}^{\mathbf{Char\ First}} + \mathbf{K}^{\mathbf{First}}) \bmod 26 \rightarrow \mathbf{C}$.
  - **D** set of **D**ecryption functions: $(\mathbf{C}^{\mathbf{Char\ First}} - \mathbf{K}^{\mathbf{First}}) \bmod 26 \rightarrow \mathbf{M}$.

Plaintext →	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
	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example “1”

Original Text (Key = ONE) :

MYNAME

Cipher Text = ????

Solution "1"

Original Text	M	Y	N	A	M	E
Original Text Value	12	24	13	0	12	4
Key	O	N	E	O	N	E
Key Value	14	13	4	14	13	4
Original Text Value + Key Value	26	37	17	14	25	8
Cipher Text	A	L	R	O	Z	I

Key = ONE

ALROZI

Plaintext →	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
	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cipher Text	A	L	R	O	Z	I
Cipher Text Value	0	11	17	14	25	8
Key	O	N	E	O	N	E
Key Value	14	13	4	14	13	4
Cipher Text Value - Key Value	-14	-2	13	0	12	4
Original Text	M	Y	N	A	M	E

Key = ONE

MYNAME

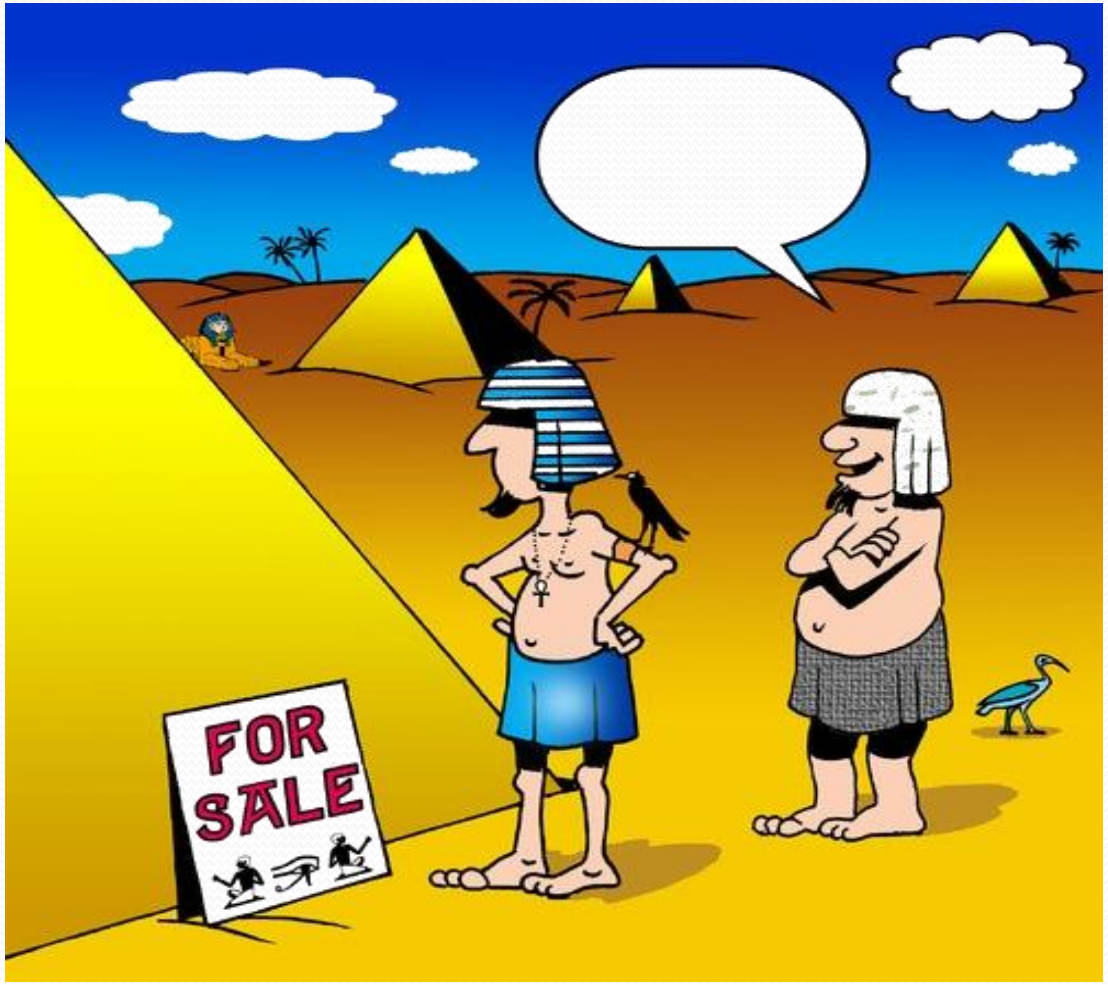
Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example “2”

Original Text (Key = LAB) :

COMPUTER

Cipher Text = ????



Solution "2"

Original Text	C	O	M	P	U	T	E	R
Original Text Value	2	14	12	15	20	19	4	17
Key	L	A	B	L	A	B	L	A
Key Value	11	0	1	11	0	1	11	0
Original Text Value + Key Value	13	14	13	26	20	20	15	17
Cipher Text	N	O	N	A	U	U	P	R

Key = LAB

NONAUUPR

Plaintext →	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
	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cipher Text	N	O	N	A	U	U	P	R
Cipher Text Value	13	14	13	0	20	20	15	17
Key	L	A	B	L	A	B	L	A
Key Value	11	0	1	11	0	1	11	0
Cipher Text Value - Key Value	2	14	12	-11	20	19	4	17
Original Text	C	O	M	P	U	T	E	R

Key = LAB

COMPUTER

Plaintext →	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
	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Attacking the Simple Shift (Vigenere Cipher)

1. Exhaustive Search:

- Try all possible keys!

2. Statistical Analysis:

- KAISISKI (know key):

1. Key Length(**3 Steps**).
2. Most Common Letters(**3 Steps**).
3. Select a Word(**3 Steps**).

Example "1"

Cipher Text :

OPKWWECIYOPKWIRG

Example "1"

Cipher Text : OPKWWECIYOPKWIRG

Key Length = ? Most Common Letters = ? Select a Word = ?

1 → OPKWWECIYOPKWIRG

2 → OPKWWECIY = 9 OPKWIRG

Category	No. Char	
1	9	
OP'1'	3+3+3=9	3

Key Length = 3

Key Length

3

Solution "1"

Key Length = 3

Most Common Letters = ?

1 → OPK WWE CIY OPK WIR G

2 → OPK WWE CIY OPK WIR G

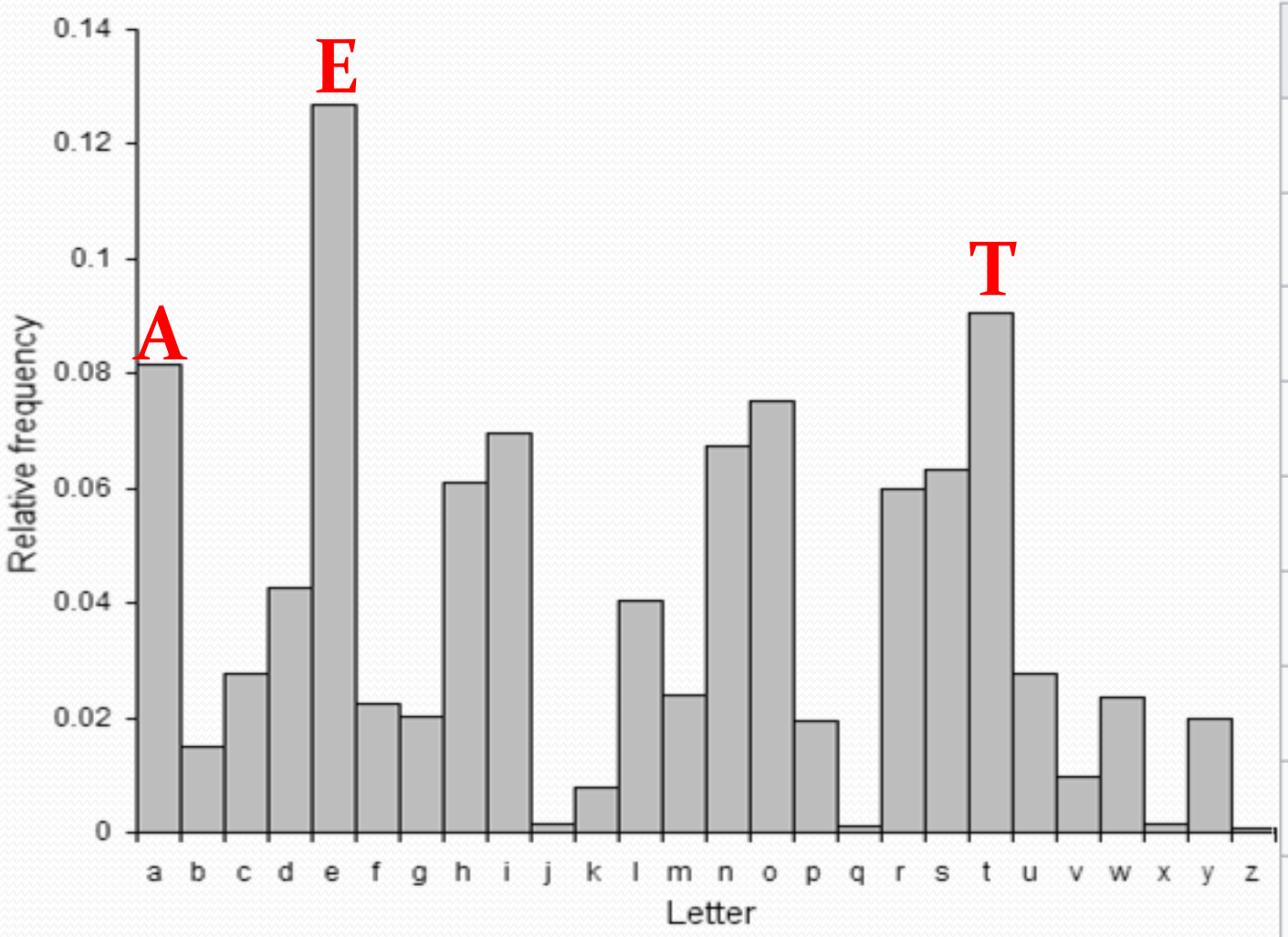
Most Common Letters = OPK/WPK

3

Category	Letters	Most Common Letters
1	OWC OWG	O,W
2	PWI PI	P
3	KEY KR	K

1. the	21. at	41. there	61. some	81. my	11. he	31. but	51. will	71. two	91. find
2. of	22. be	42. use	62. her	82. than	12. was	32. not	52. up	72. more	92. long
3. and	23. this	43. an	63. would	83. first	13. for	33. what	53. other	73. write	93. down
4. a	24. have	44. each	64. make	84. water	14. on	34. all	54. about	74. go	94. day
5. to	25. from	45. which	65. like	85. been	15. are	35. were	55. out	75. see	95. did
6. in	26. or	46. she	66. him	86. call	16. as	36. we	56. many	76. number	96. get
7. is	27. one	47. do	67. into	87. who	17. with	37. when	57. then	77. no	97. come
8. you	28. had	48. how	68. time	88. oil	18. his	38. your	58. them	78. way	98. made
9. that	29. by	49. their	69. has	89. its	19. they	39. can	59. these	79. could	99. may
10. it	30. word	50. if	70. look	90. now	20. I	40. said	60. so	80. people	100. part

English Word Frequencies



Type	Occurrences	Rank
the	3789654	1st
he	2098762	2nd
[...]		
king	57897	1,356th
boy	56975	1,357th
[...]		
stringyfy	5	34,589th
[...]		
transducionalify	1	123,567th

Solution "1"

Key Length = 3

Most Common Letters = OPK

Select a Word = ?

HE
THE
FOR
GOOD

1

OPK = THE

2

O-T = 14-19 = -5 = 21= V

P-H = 15-7 = 8 = I

K-E = 10-4 = 6 = G

OPK-THE =VIG

Plaintext →	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
	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Solution "1"

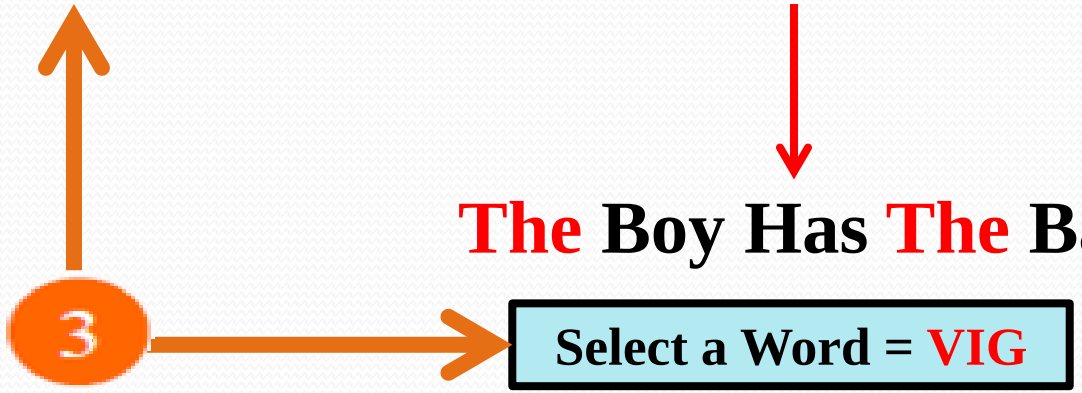
Key Length = 3

Most Common Letters = OPK

Select a Word = VIG

Original Text : OPKWWECIYOPKWIRG

Key (VIG): THEBOYHASTHEBALL



The Boy Has The Ball

Example “2”

Cipher Text (Key Length = 4):

UMYEFTKORKCXUMYEABFST

Example "2"

Cipher Text : UMYEFTKORKCXUMYEABFST

Key Length = 4 Most Common Letters = ? Select a Word = ?

1 → UMYEFTKORKCXUMYEABFST

2 → UMYEFTKORKCX = 12 UMYEABFST

Category	No. Char	
1	12	
OP'1'	3+3+3+3=12	3
OP'2'	4+4+4=12	4
OP'3'	6+6=12	6

Key Length = 3,4,6

3 → **Key Length**

Solution "2"

Key Length = 4

Most Common Letters = ?

1 → UMYE FTKO RKCX UMYE ABFS T

2 → UMYE FTKO RKCX UMYE ABFS T

Most Common Letters = UMYE

3

Category	Letters	Most Common Letters
1	UFRU AT	U
2	MTKM B	M
3	YKCY F	Y
4	EOXE S	E

Solution "2"

Key Length = 4

Most Common Letters = UMYE

Select a Word = ?

NEWS
NEW
HEWA
GOOD

2

1

UMYE = HEWA

U-H = 20-7 = 13 = N
M-E = 12-4 = 8 = I
Y-W = 24-22= 2 = C
E-A = 4-0 = 4 = E

UMYE - HEWA = NICE

Plaintext →	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
	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Solution "2"

Key Length = 4

Most Common Letters = UMYE

Select a Word = NICE

NICE [HEWASLIKECATHEWANTDOG]

He Was Like Cat He Want Do

3

Select a Word = NICE

Example “3”

Cipher Text :

LJVBQSTNEZLQMEDLJVMAMPKA
UFAVATLJVDAYYVNFJQLNP
LJVHKVTRNFLJVCMLKETALJVH
UYJVSFKRFTTWEFUXVHZNP

Example "3"

Cipher Text : LJVBQSTNEZLQMEDLJVMAMPKAUFAVATLJVDAYYVNFJQLNP
LJVHKVTRNFLJVCMLKETALJVHUYJVSFKRFTTWEFUXVHZNP

Key Length = ? Most Common Letters = ? Select a Word = ?

1 →

LJVBQSTNEZLQMEDLJVMAMPKAUFAVATLJVDAYYVNFJQLNP
LJVHKVTRNFLJVCMLKETALJVHUYJVSFKRFTTWEFUXVHZNP

2 →

LJVBQSTNEZLQMED = 15 LJVMAMPKAUFAVAT =15 LJVDAYYVNFJQLNP = 15
LJVHKVTRNF = 10 LJVCMLKETA =10 LJVHUYJVSFKRFTTWEFUXVHZNP

Category	No. Char	
1	15	
2	15	
3	15	5
4	10	5
5	10	

Key Length = 5

3 → **Key Length**

Solution "3"

Key Length = 5

Most Common Letters = ?

1

LJVBQ	STNEZ	LQMED	LJVMA	MPKAU	FAVAT	LJVDA	YYVNF	JQLNP
LJVHK	VTRNF	LJVCM	LKETA	LJVHU	YJVSF	KRFTT	WEFUX	VHZNP

2

LJVBQ	STNEZ	LQMED	LJVMA	MPKAU	FAVAT	LJVDA	YYVNF	JQLNP
LJVHK	VTRNF	LJVCM	LKETA	LJVHU	YJVSF	KRFTT	WEFUX	VHZNP

Category	Letters	Most Common Letters
1	LSLLM FLYJL VLLLY KWV	L
2	JTQJP AJYQJ TJKJJ REH	J
3	VNMVK VVVLV RVEVV FFZ	V
4	BEEMA ADNNH NCTHS TUN	N
5	QZDAU TAFPK FMAUF TXP	A

3

Most Common Letters = LJVNA

Solution "3"

Key Length = 5

Most Common Letters = LJVNA

Select a Word = ?

THERE
THENO
NEWA
GOOD

LJVNA = THENO ← 1

2

L-T = 11-19 = -8 = 18 = S
J-H = 9-7 = 2 = C
V-E = 21-4 = 17 = R
N-N=13-13=0=A
A-O=0-14=-14=M

LJVNA - THENO = SCRAM

Plaintext →	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
	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Solution "3"

Key Length = 5

Most Common Letters = LJVNA

Select a Word = SCRAM

SCRAM

[THEBEARWENTOVERTHEMOUNTAINYEAHTHEDOGWENTROUNDTHEHYDRANTTHECATINTOTHEHIGHESTSPOTHECOULDFIND]

The Bear Went Over The Mountain Yeah The Dog Went Round The Hydrant The Cat Into The Highest Spot He Could Find

Thank you