Principles of Cryptography

Lecture 2

Main Points

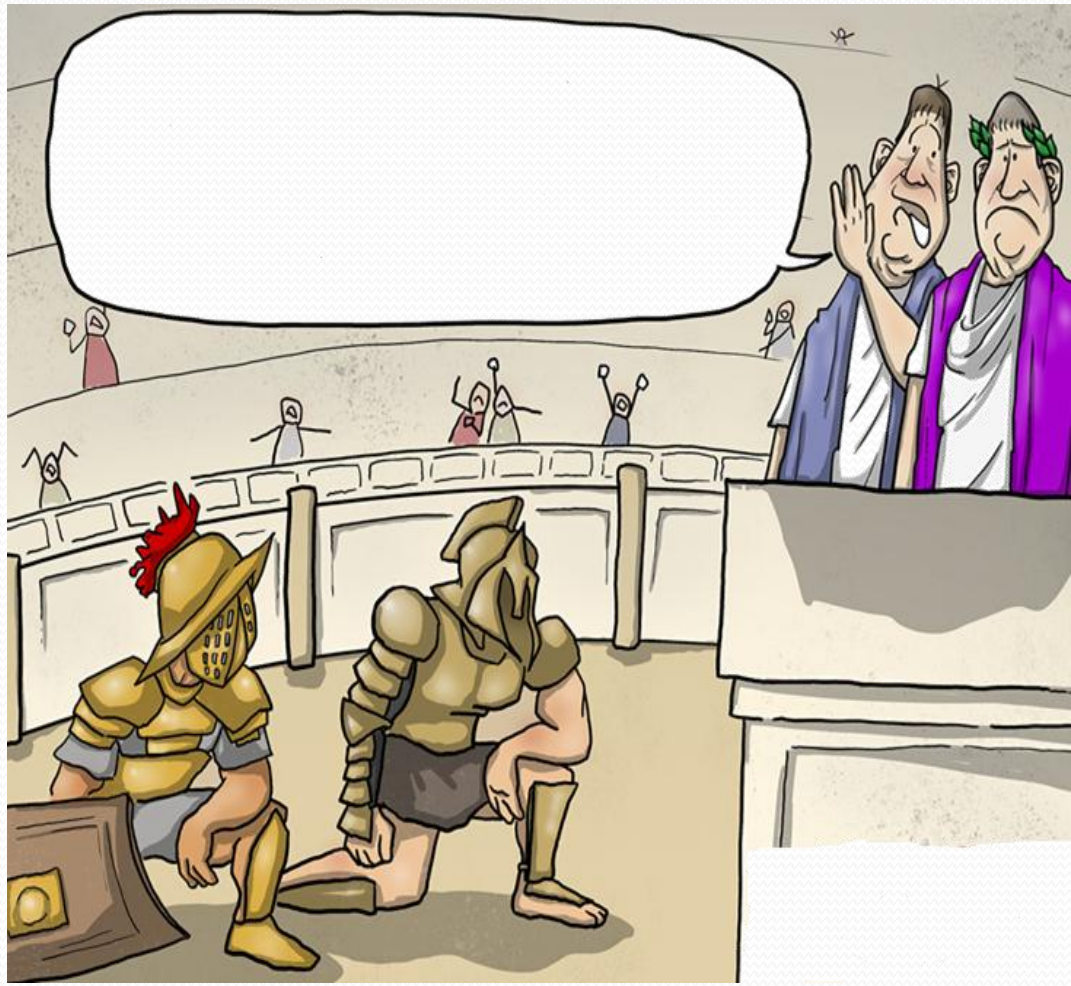
- **General Concepts.**
- **Cryptosystem.**
- **Traditional Ciphers (Substitution):**
  - **Caesar Cipher.**
  - **Attacking the Caesar Cipher.**

General Concepts

- **Cryptography** : “hidden, secret” and “writing”.
- As **Cryptography** is the science and art of creating secret codes.(Invents encryption algorithms)
- **Cryptanalysis** is the science and art of breaking those codes.

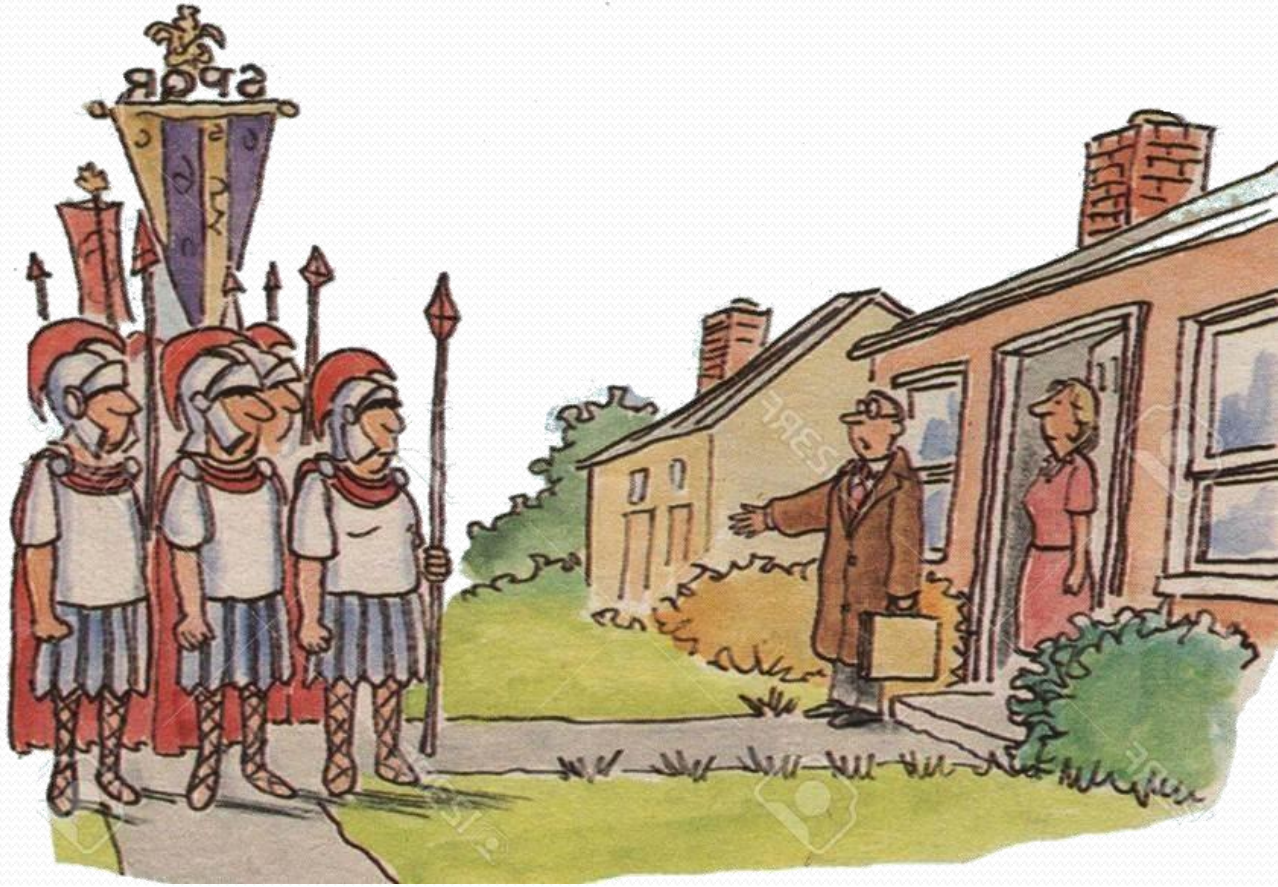
General Concepts

- **Encryption** : Process of transforming a message such that its meaning is concealed.
- **Decryption** : Process of transforming an encrypted message back into original form.
- **Cryptosystem** : A system that describes how to encrypt or decrypt messages.
- **Plaintext** : Message in its original form.
- **Ciphertext** : Message in its encrypted form.



Cryptosystem

- Fivefold (**E**, **D**, **M**, **K**, **C**)
  - **M** set of plaintexts.
  - **K** set of **K**eys.
  - **C** set of **C**iphertexts.
  - **E** set of **E**ncryption functions.
  - **D** set of **D**ecryption functions.



Traditional Ciphers (Substitution)

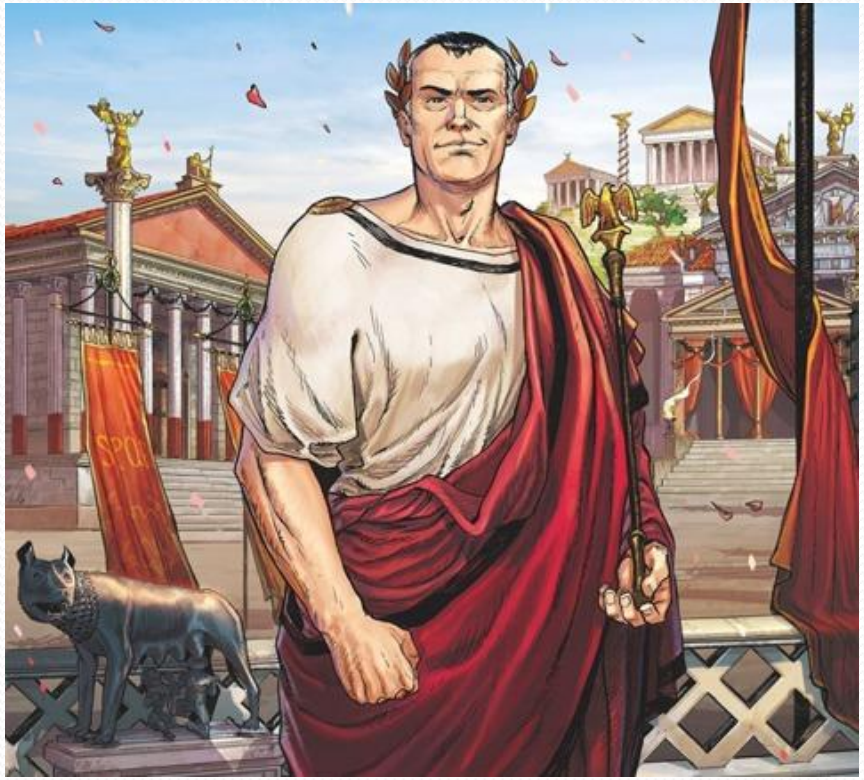
A **substitution** cipher replaces one symbol with another.

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

Caesar Cipher

- **Caesar Cipher (**Julius Caesar) :

- To protect military messages.
- It is a type of substitution cipher in which each letter in the plaintext is replaced by a anther letter.



- **Caesar Cipher Problems:**

- Key is too short.
- No Symbol.

Caesar Cipher

- **Caesar Encryption :**

Ciphertext = (Plaintext + key) mod 26^{Letters} .

- **Caesar Decryption :**

Plaintext = (Ciphertext – key) mod 26^{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 (Caesar Cipher)

- Fivefold (**E**, **D**, **M**, **K**, **C**)
  - **M** set of plaintexts (letters , words).
  - **K** set of **K**eys (**i** = one of letters (English) **1≤ i ≤ 25**).
  - **C** set of **C**iphertexts (letters , words).
  - **E** set of **E**ncryption functions: **(M + K)** mod 26 **→ C**.
  - **D** set of **D**ecryption functions: **(C – K)** mod 26 **→ 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 = D) :

BOOK

Cipher Text = ????

Encryption

Original Text	B	O	O	K
Original Text Value	1	14	14	10
Key Value	3	3	3	3
Original Text Value + Key Value	4	17	17	13
Cipher Text	E	R	R	N

Key = D = 3

ERRN

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

Decryption

Cipher Text	E	R	R	N
Cipher Text Value	4	17	17	13
Key Value	3	3	3	3
Cipher Text Value - Key Value	1	14	14	10
Original Text	B	O	O	K

Key = D = 3

BOOK

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 = U) :

LABONE

Cipher Text = ????

Solution "2"

Original Text	L	A	B	O	N	E
Original Text Value	11	0	1	14	13	4
Key Value	20	20	20	20	20	20
Original Text Value + Key Value	31	20	21	34	33	24
Cipher Text	F	U	V	I	H	Y

Key = U = 20

FUVIHY

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
Ciphertext →	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

Lecture 2

Cipher Text	F	U	V	I	H	Y
Cipher Text Value	5	20	21	8	7	24
Key Value	20	20	20	20	20	20
Cipher Text Value - Key Value	-15	0	1	-12	-13	4
Original Text	L	A	B	O	N	E

Key = U = 20

LABONE

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
Ciphertext →	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 Caesar Cipher

1. Exhaustive Search:

- Try all possible keys! **(1 ⟶ 25).**

2. Statistical Analysis:

- Compare to model of English(**4 Steps**).

Example "1"

Cipher Text :

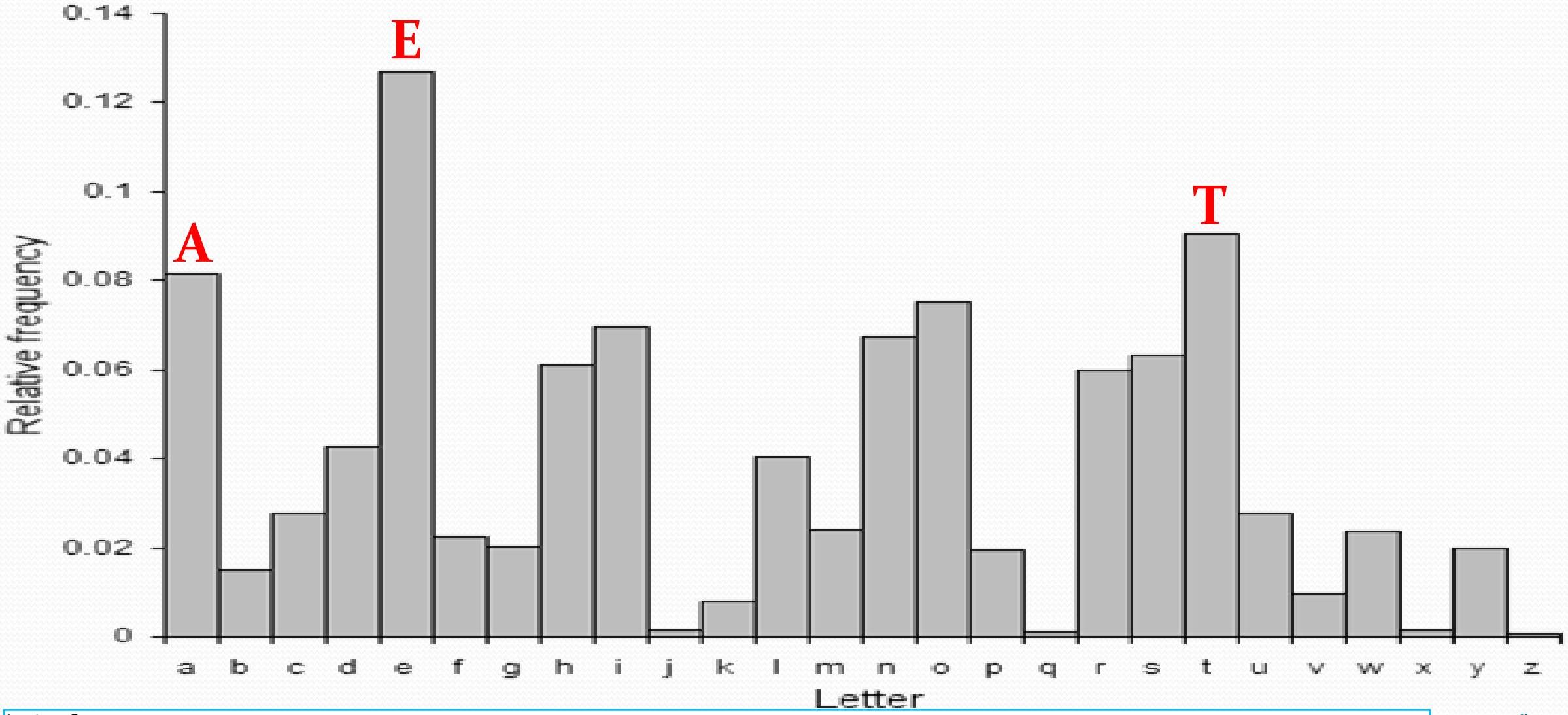
FQJCB RWJWJ VNJAX BNKHJ
WHXCQ NAWJV NFXDU MBVNU
UJBBF NNC

Lecture 2

A	B	C	D	E	F	G	H	I	J	K	L	M
8.2	1.5	2.8	4.3	12.7	2.2	2.0	6.1	7.0	0.2	0.8	4.0	2.4
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6.7	7.5	1.9	0.1	6.0	6.3	9.1	2.8	1.0	2.4	0.2	2.0	0.1

E	T	A	O	I	N	S	H	R	D	L	U	C
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8
M	W	F	Y	G	P	B	V	K	X	J	Q	Z
2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.2	0.2	0.1	0.1

English Character Frequencies



Solution "1"

FQJCB RWJWJ VNJAX BNKHJ WHXCQ NAWJV NFXDU MBVNU UJBBF NNC

1. **A**:2, **B**:5, **C**:3, **D**:1, **E**:0, **F**:3, **G**:0, **H**:2, **I**:0, **J**:7, **K**:1, **L**:0, **M**:1, **N** :7 **...etc.**

2. **J**:7 and **N** :7

3. **J-E = 9-4 = 5.** ⟶ **Key = 5.** **Key = 5 = F**

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"

4 **Key = 5 = F.** **(Char- key = F-5 = 5-5 = 0 =A) …etc.**

FQJCB RWJWJ VNJAX BNKHJ WHXCQ NAWJV NFXDU MBVNU UJBBFNNC

ALEXW MRERE QIEVS WIFCE RCSXL IVREQ IASYP HWQIP PEWWAIIX

!!

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

cont.... Solution "1"

FQJCB RWJWJ VNJAX BNKHJ WHXCQ NAWJV NFXDU MBVNU UJBBF NNC

1. **A**:2, **B**:5, **C**:3, **D**:1, **E**:0, **F**:3, **G**:0, **H**:2, **I**:0, **J**:7, **K**:1, **L**:0, **M**:1, **N** :7 **...etc.**
2. **J**:7 and **N** :7
3. **N-E = 13-4 = 9.** ⟶ **Key = 9.** **Key = 9 = J**

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"

4 **Key = 9 = J.** **(Char- key = F-9 = 5-9 = -4 = W) …etc.**

FQJCB RWJWJ VNJAX BNKHJ WHXCQ NAWJV NFXDU MBVNU UJBBFNNC

WHATS INANA MEARO SEBYA NYOTH ERNAM EWOUL DSMEL LASSWEET

What's in a name a rose by any other name would smell as sweet

Key = 9 = J

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

Thank you for Listening!