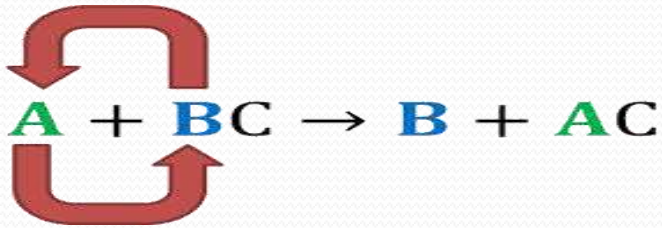
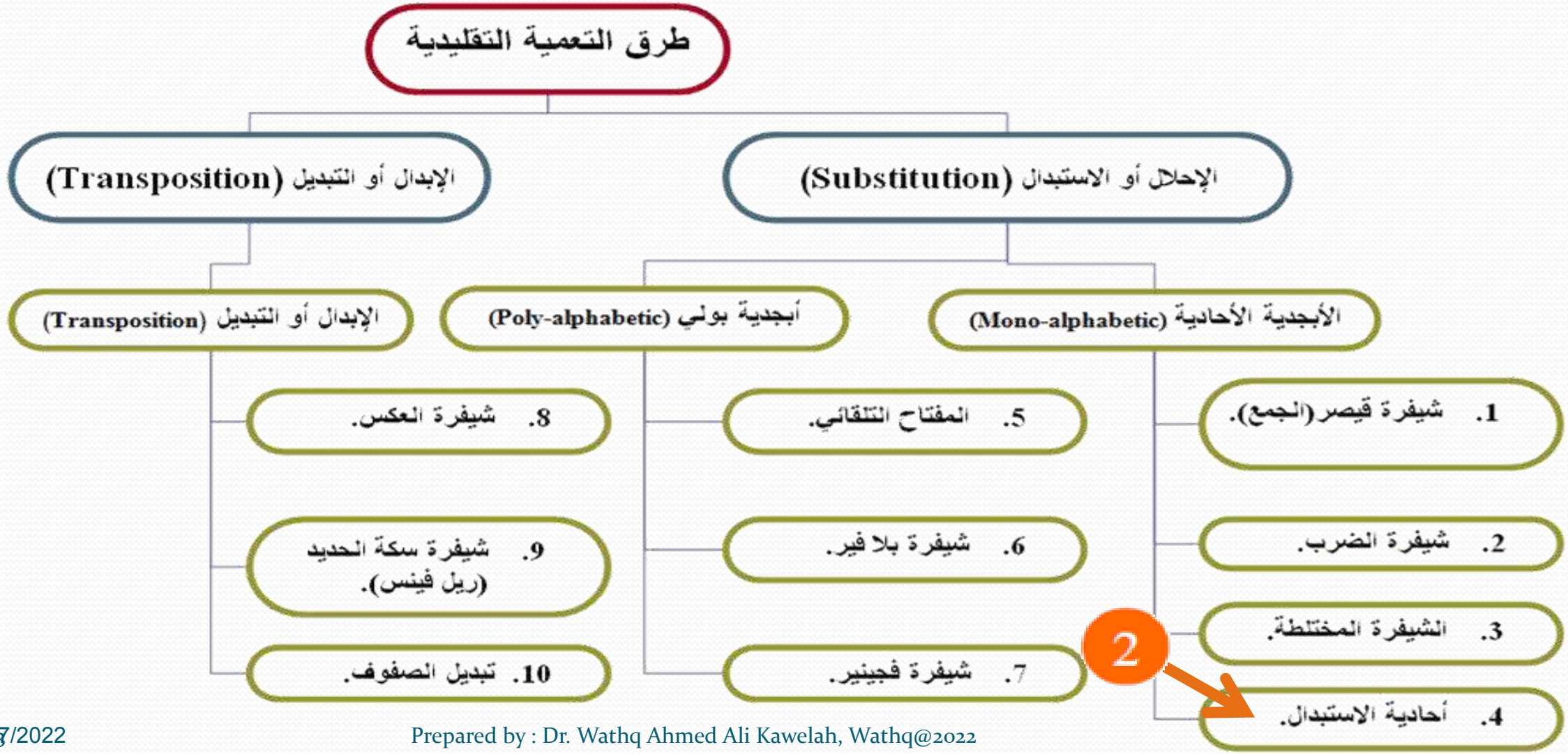
Main Points



- **Traditional Ciphers (Substitution):**
- **Single Replacement Cipher.**
- **Attacking the Single Replacement Cipher.**

Traditional Ciphers (Substitution)



Single Replacement

- **Single Replacement** :

- Uses only one letter.
- It is a type of substitution cipher in which each letter of special table in the plaintext is replaced by a anther letter.

- **Single Replacement Problems:**

- Special Table is too short.
- No Symbol.

Single Replacement

- **Single Replacement Encryption :**

1. Create a special table for all letters .
2. Replace each letter of the original text with its corresponding letters in the special table.

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	Plain
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	Cipher

- **Single Replacement Decryption :**

1. Show special table for all letters.
2. Replace each letter from the cipher text with its corresponding letters in the special table.

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	Plain
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	Cipher

Cryptosystem (Single Replacement)

- Fivefold (**E**, **D**, **M**, **K**, **C**)
  - **M** set of plaintexts (letters , words).
  - **K** set of **K**eys (**Special Table** of letters (English)).
  - **C** set of **C**iphertexts (letters , words).
  - **E** set of **E**ncryption functions:

  First$^{\text{letter}}$ in First$^{\text{Special Table}}$ & Second$^{\text{letter}}$ in Second$^{\text{Special Table}}$... etc → C.
  - **D** set of **D**ecryption functions:

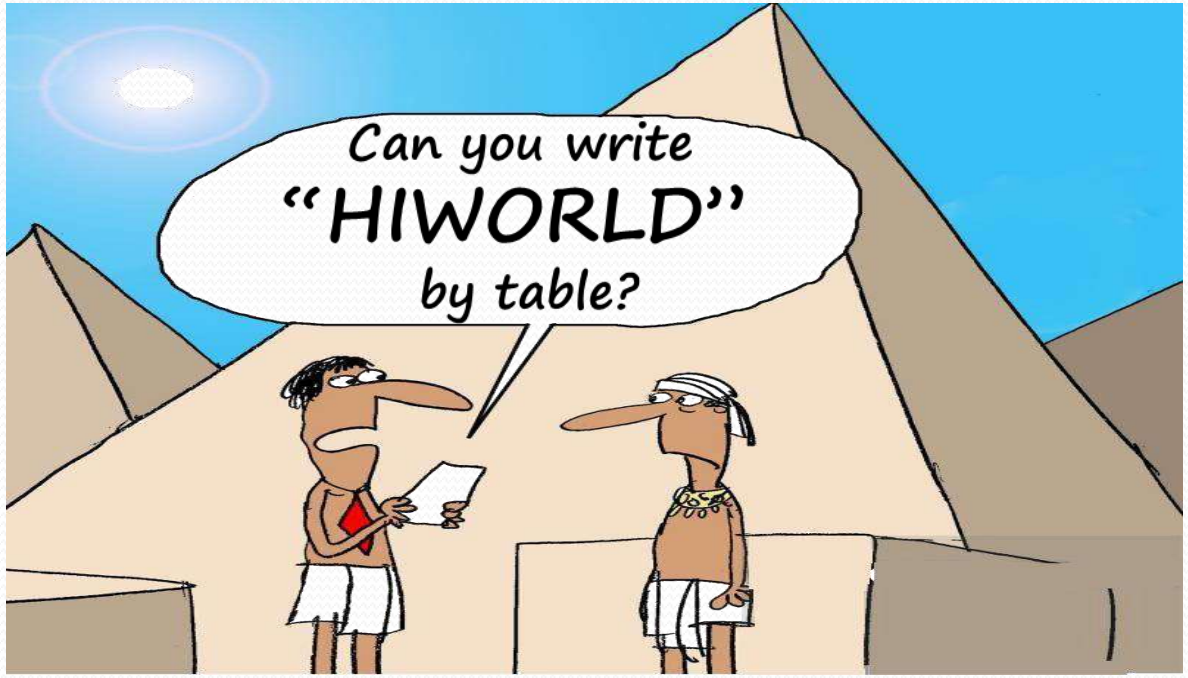
  First$^{\text{letter}}$ in First$^{\text{Special Table}}$ & Second$^{\text{letter}}$ in an Second$^{\text{Special Table}}$... etc → M.

Example "1"

Original Text :

HIWORLD

Cipher Text = ????

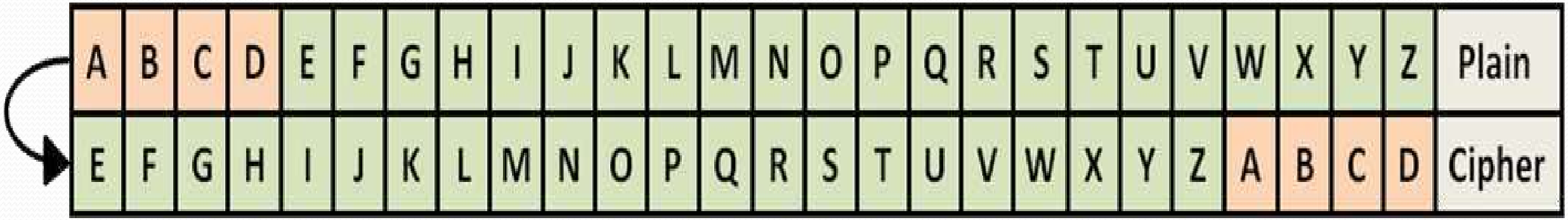


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Plain
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	Cipher

Solution "1"

Original Text	H	I	W	O	R	L	D
Replacement	L	M	A	S	V	P	H
Cipher Text	L	M	A	S	V	P	H

LMASVPH



Cipher Text	L	M	A	S	V	P	H
Replacement	H	I	W	O	R	L	D
Original Text	H	I	W	O	R	L	D

HIWORLD

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	Plain
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	Cipher

Example "2"

Original Text :

LABSEVEN

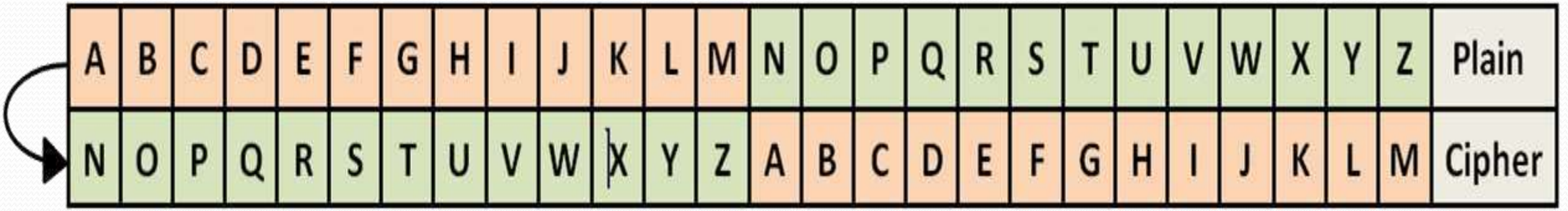
Cipher Text = ????

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	Plain
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	Cipher

Solution "2"

Original Text	L	A	B	S	E	V	E	N
Replacement	Y	N	O	F	R	I	R	A
Cipher Text	Y	N	O	F	R	I	R	A

YNOFRIRA



Cipher Text	Y	N	O	F	R	I	R	A
Replacement	L	A	B	S	E	V	E	N
Original Text	L	A	B	S	E	V	E	N

LABSEVEN

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	Plain
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	Cipher

Attacking the Single Replacement Cipher

1. Exhaustive Search:

- Try all possible special table ! (**25**).

2. Statistical Analysis:

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

Example "1"

Cipher Text :

YNOFRIRA

E,A,O,I & U

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

Solution “1”

YNOFRIRA

1. **Y**:1, **N**:1, **O**:1, **F**:1, **R**:2, **I**:1, **A**:1.
2. **R**:2
3. **R=E**

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	Plain
																	E									Cipher

Solution "1"

4

R=E

YNOFRIRA

↓

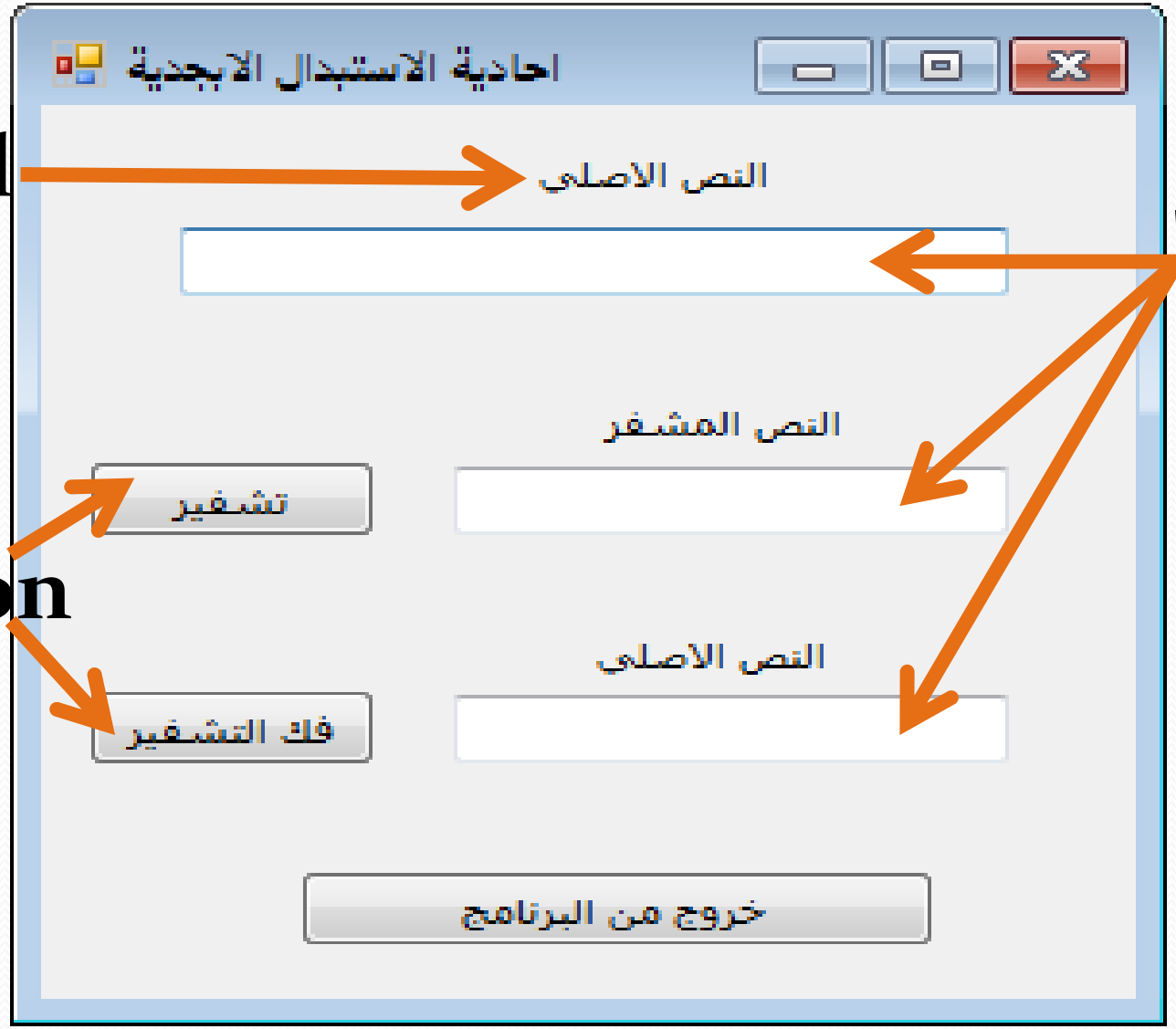
LABSEVEN

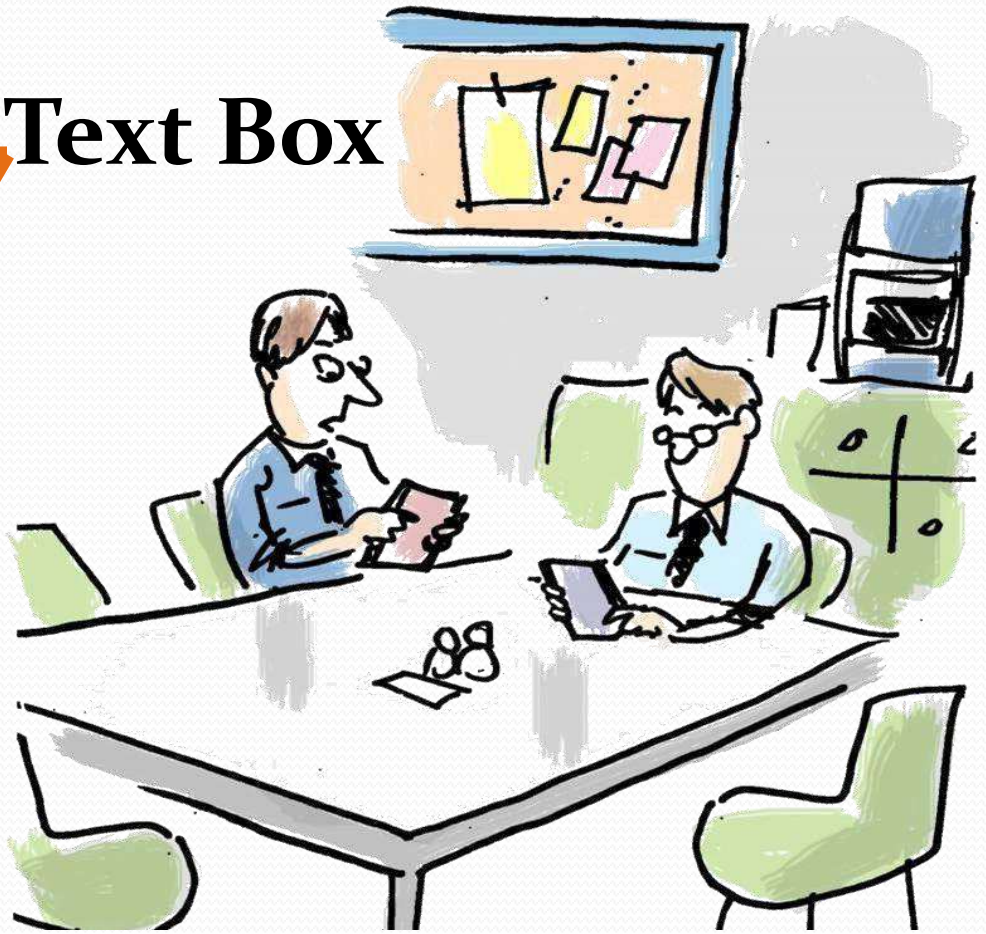
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Plain
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	Cipher

Label

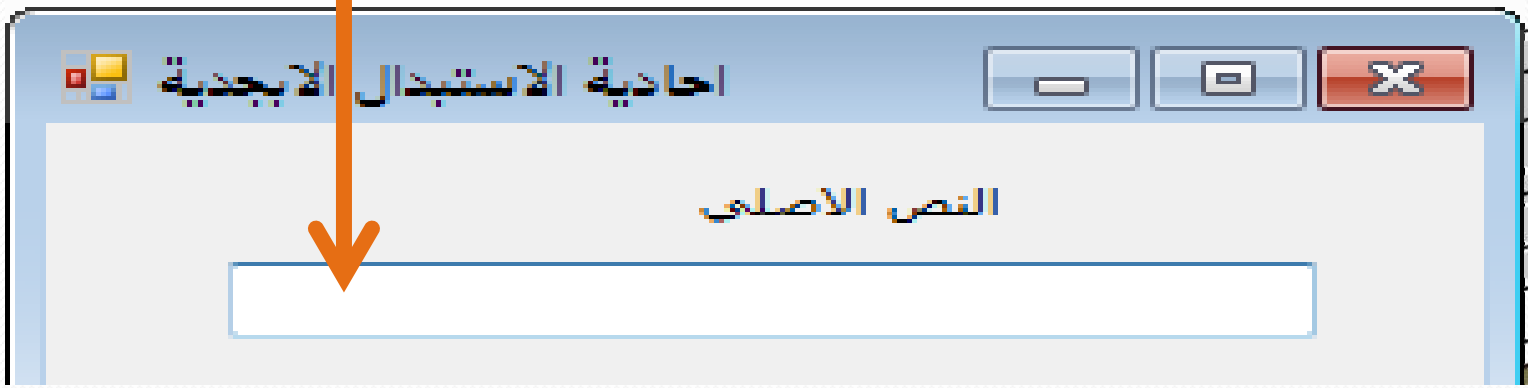
Text Box

Button

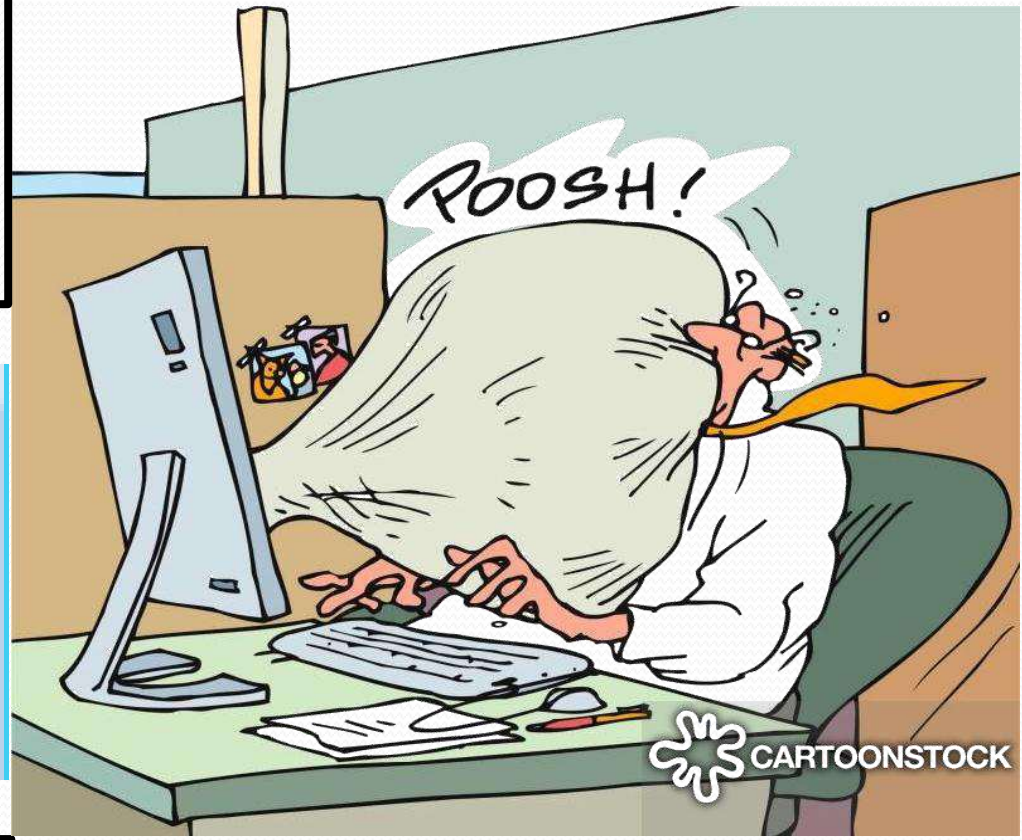




```
private void textBox1_TextChanged(object sender, EventArgs e)
{
textBox1.CharacterCasing = CharacterCasing.Upper;
}
```



```
private void button1_Click(object sender, EventArgs e)
{
textBox2.Text = en(textBox1.Text);
}
```




```
private void textBox2_TextChanged(object sender, EventArgs e)
                                  {    }
```

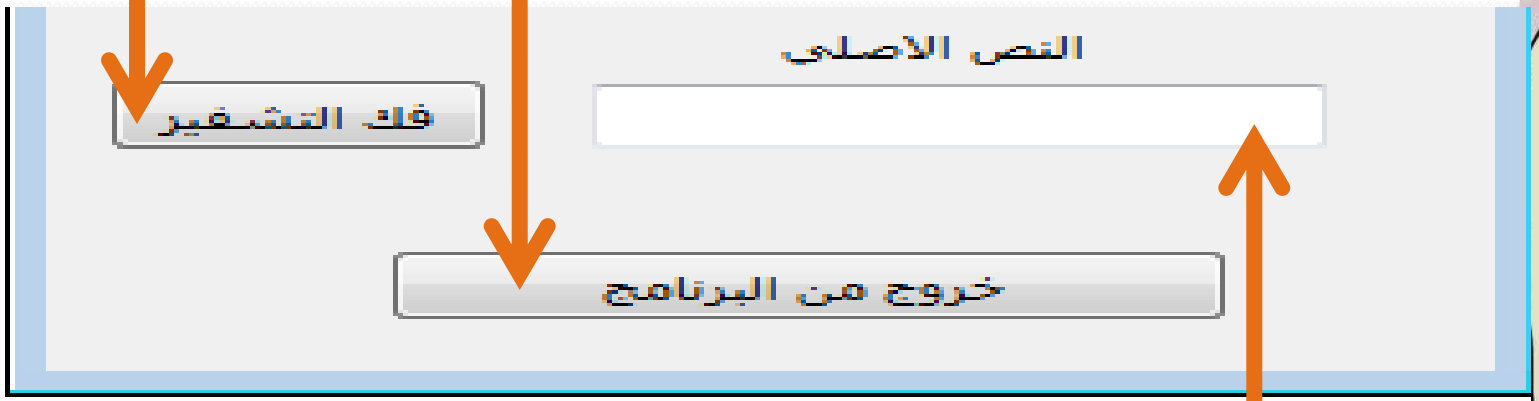
1

```
string en(string a)
{
StringBuilder  entext = new StringBuilder();
foreach (char ac in a)
{
entext.Append((char)(((int)ac - 65 + 4) % 26 + 65));
}
return (entext.ToString());
}
```

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	Plain
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	Cipher

```
private void button2_Click(object sender, EventArgs e)
{
textBox3.Text = de(textBox2.Text);
}
```

```
private void button3_Click(object sender, EventArgs e)
        {   Application.Exit();    }
```



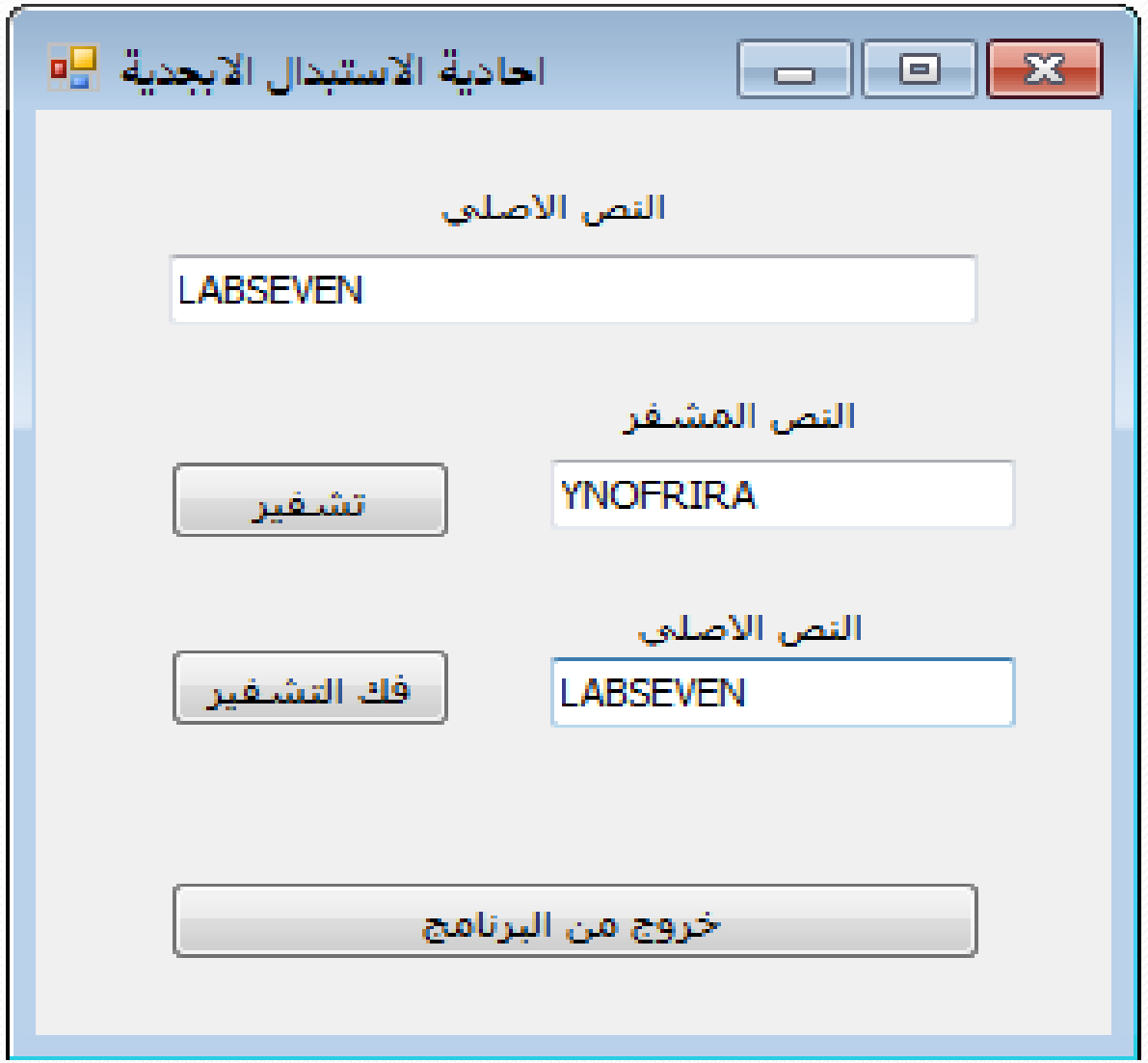

```
private void textBox3_TextChanged(object sender, EventArgs e)
        {        }
```

2

```
string de(string a)
{
StringBuilder  detext = new StringBuilder();
foreach (char ac in a)
{
detext.Append((char)(((int)ac - 65 - (4 - 26)) % 26 + 65));
}
return (detext.ToString());
}
```

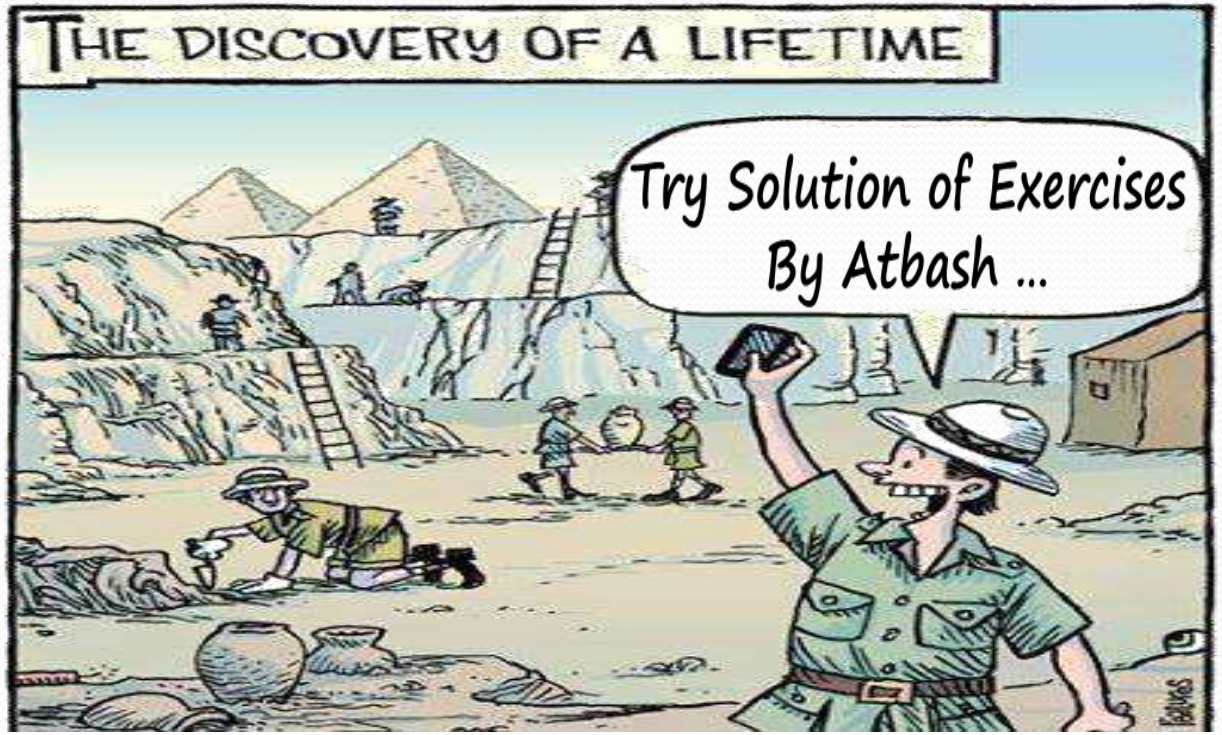
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Plain
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	Cipher


احادية الاستبدال الابجدية
النص الاصلي
HIWORLD
النص المشفر
تشفير
LMASVPH
النص الاصلي
فك التشفير
HIWORLD
خروج من البرنامج


احادية الاستبدال الابجدية
النص الاصلي
LABSEVEN
النص المشفر
تشفير
YNOFRIRA
النص الاصلي
فك التشفير
LABSEVEN
خروج من البرنامج

- اكتب برنامج يقوم بتشفير النصوص وفق الخوارزمية التالية :
- الخوارزمية تقوم بجعل الحرف الأول من النص الأصلي هو الحرف الأخير في النص المشفر، والحرف الثاني هو قبل الأخير ، وهكذا ...

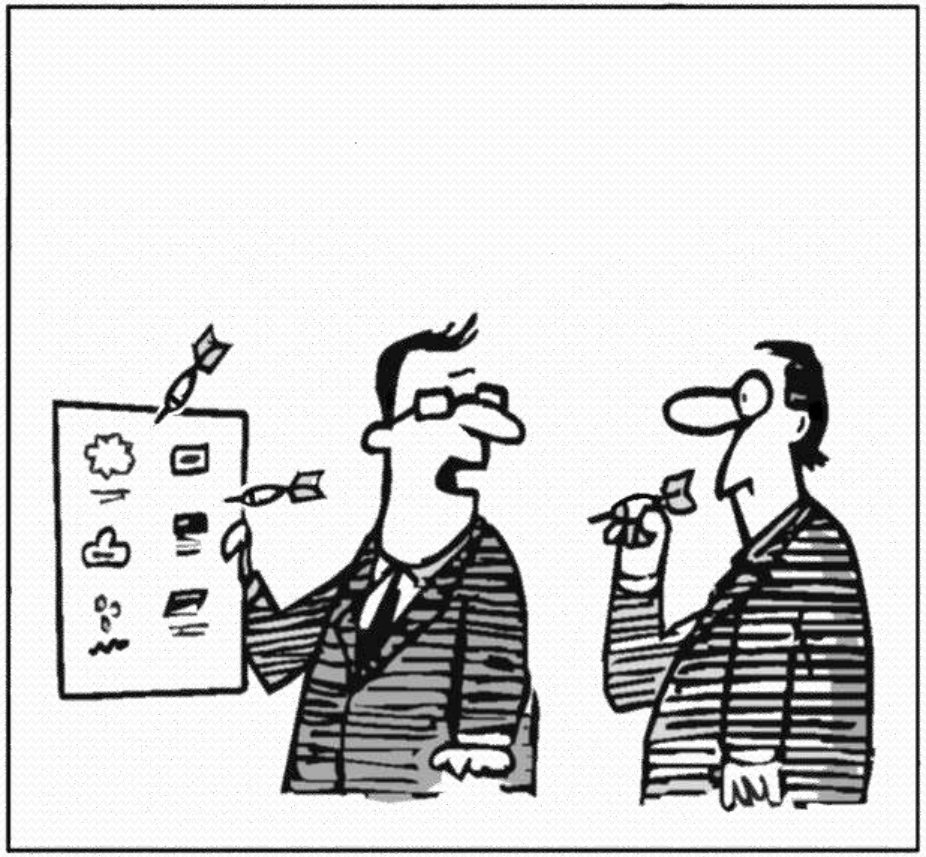
فمثلاً : لتشفير كلمة MONEY يصبح لدينا YENOM .



Thank you for Listening!

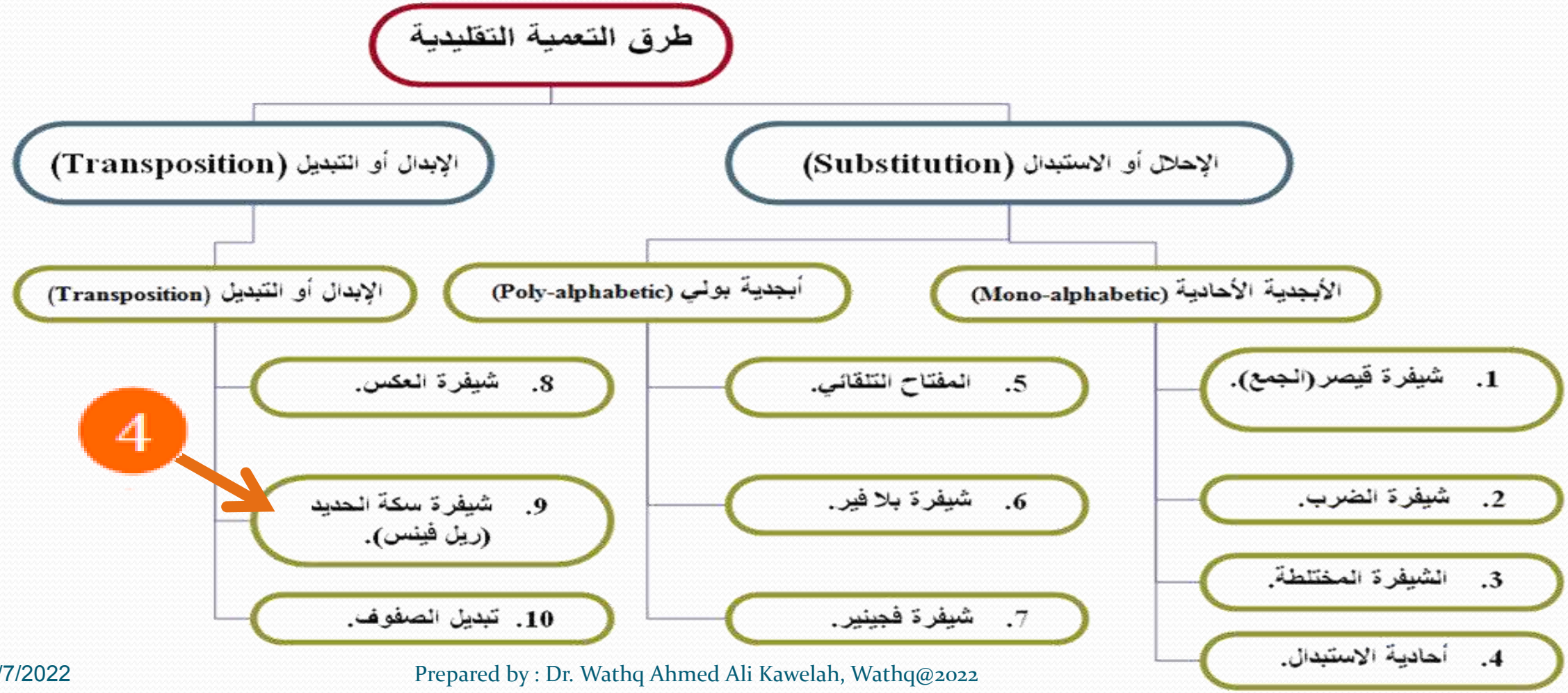
Main Points

- **Traditional Ciphers (Transposition):**
- **Rail-Fence Cipher.**
- **Attacking the (Rail-Fence Cipher).**



Traditional Ciphers (Transposition)

(Transposition)



Rail-Fence Cipher

- **Rail-Fence Cipher :**
  - The ciphertext is created reading the pattern row by row.
  - Using key value (2 or more level).
  - Cipher Name from the way in which it is encoded.

- **Rail-Fence Cipher Problems:**
  - Key is small (Using key value) level.
  - No Symbol.

Rail-Fence Cipher

- **Rail-Fence Encryption :**

1. Divides the Plaintext into levels (key value).
2. The Plaintext divides:

(First**letter** in First**level** & Second**letter** in Second**level**… etc.).

3. Elements of each level come together.

- **Rail-Fence Decryption :**

1. Divides the Ciphertext into levels(key value).
2. The Ciphertext divides :

(First**letter** in First**level** & Second**letter** in an opposite**level**… etc.).

3. Items fall for each level.

Cryptosystem (Rail-Fence)

- Fivefold (**E**, **D**, **M**, **K**, **C**)
  - **M** set of plaintexts (letters , words).
  - **K** set of **K**eys (**i** = two or more of level).
  - **C** set of **C**iphertexts (letters , words).
  - **E** set of **E**ncryption functions:

First^{letter} in First^{level} & Second^{letter} in Second^{level}… etc → C.

  - **D** set of **D**ecryption functions:

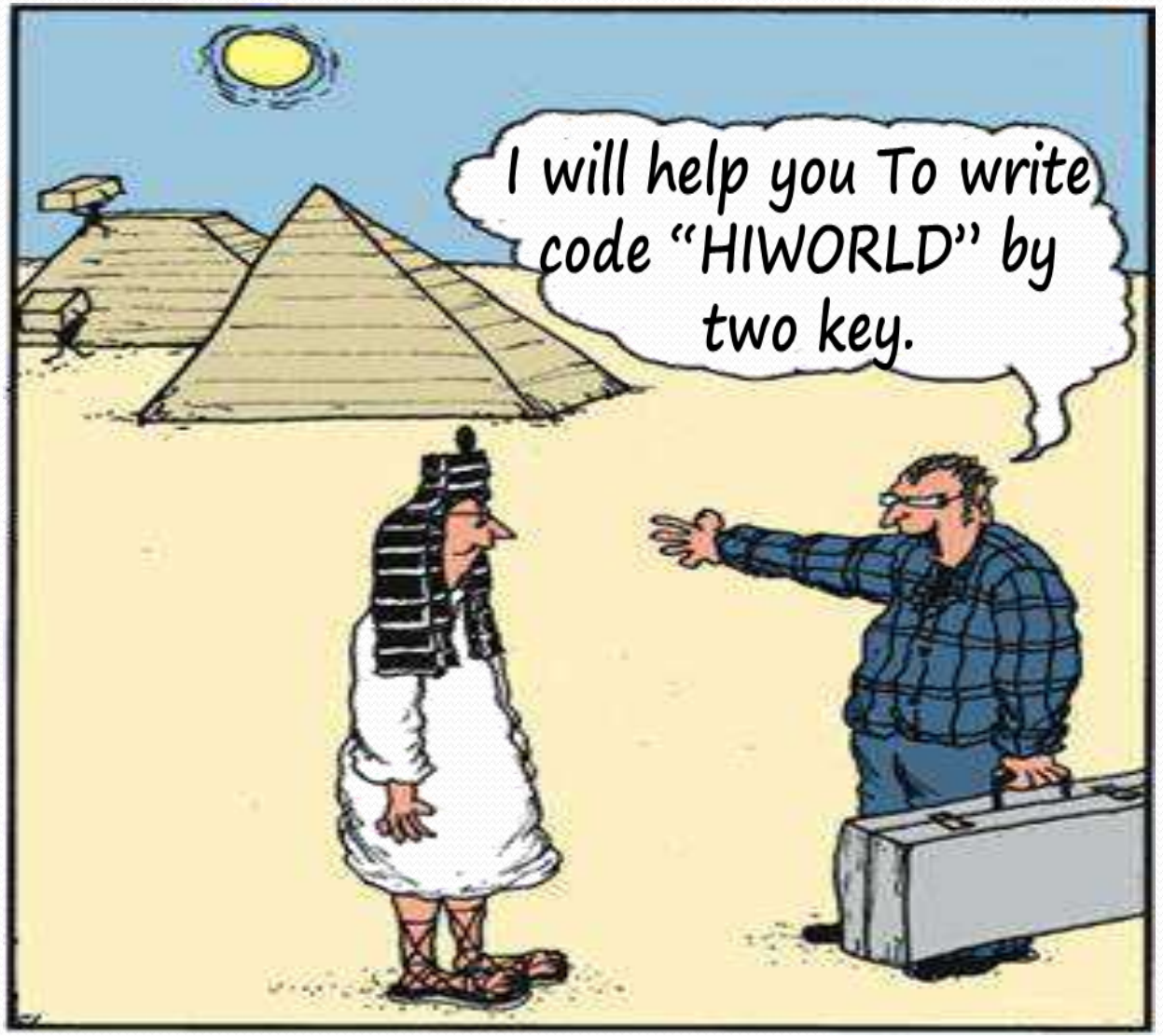
First^{letter} in First^{level} & Second^{letter} in an opposite^{level}… etc → M.

Example "1"

Original Text (Key = 2) :

HIWORLD

Cipher Text = ????



Solution “1”

Original Text	H	I	W	O	R	L	D	L.Key = 7
Rail-Fence	H		W		R		D	Key=1
Key=2		I		O		L		Key=2
Cipher Text	H	W	R	D	I	O	L	

HWRDIOL

Cipher Text	H	W	R	D	I	O	L	L.Key = 7
Rail-Fence	H		W		R		D	Key=1
Key=2		I		O		L		Key=2
Original Text	H	I	W	O	R	L	D	

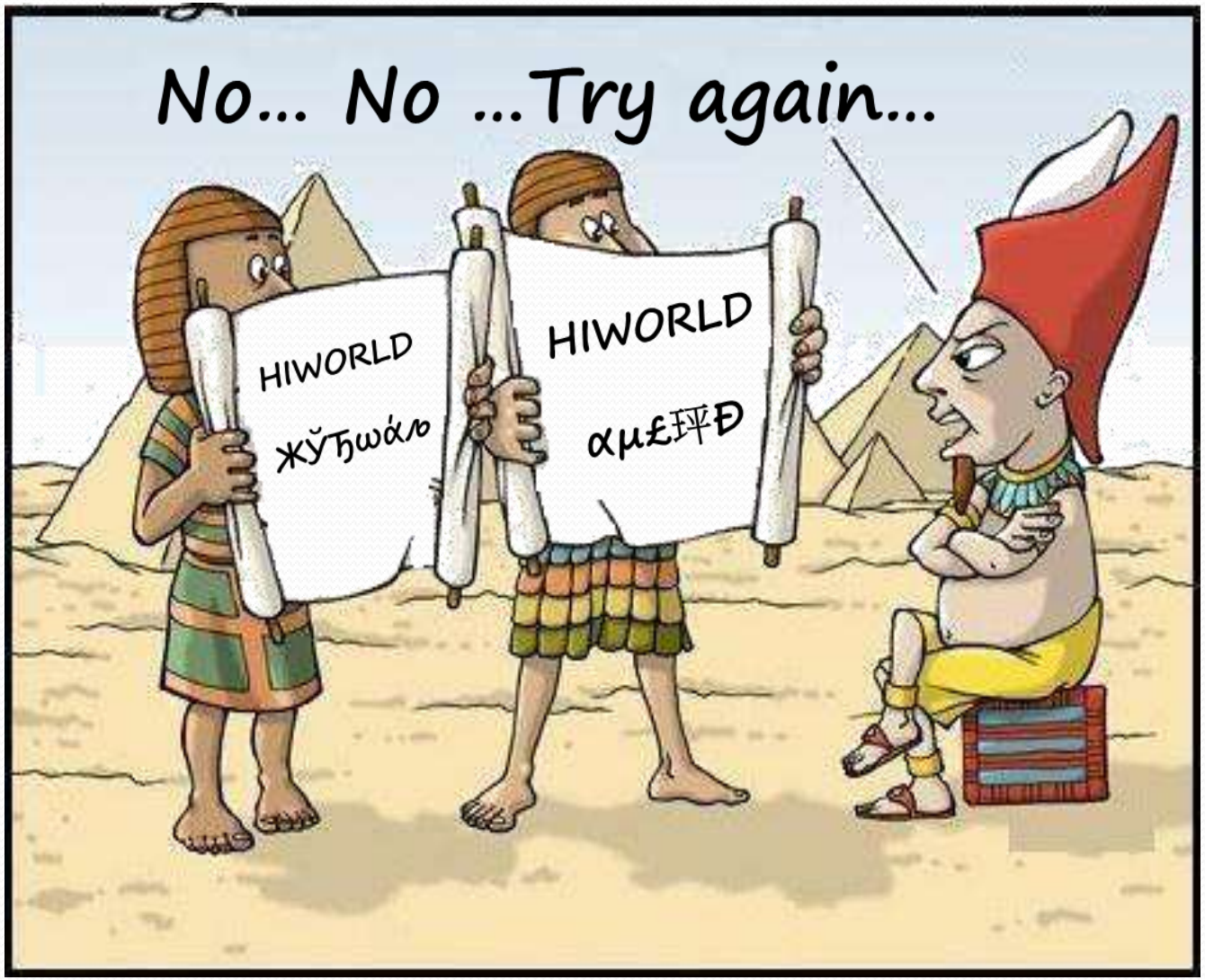
HIWORLD

Example "2"

Original Text (Key = 3) :

HIWORLD

Cipher Text = ????



Solution "2"

Original Text	H	I	W	O	R	L	D	L.Key = 7
Rail-Fence Key=3	H			O			D	Key=1
		I			R			Key=2
			W			L		Key=3
Cipher Text	H	O	D	I	R	W	L	

HODIRWL

Cipher Text	H	O	D	I	R	W	L	L.Key = 7
Rail-Fence Key=3	H			O			D	Key=1
		I			R			Key=2
			W			L		Key=3
Original Text	H	I	W	O	R	L	D	

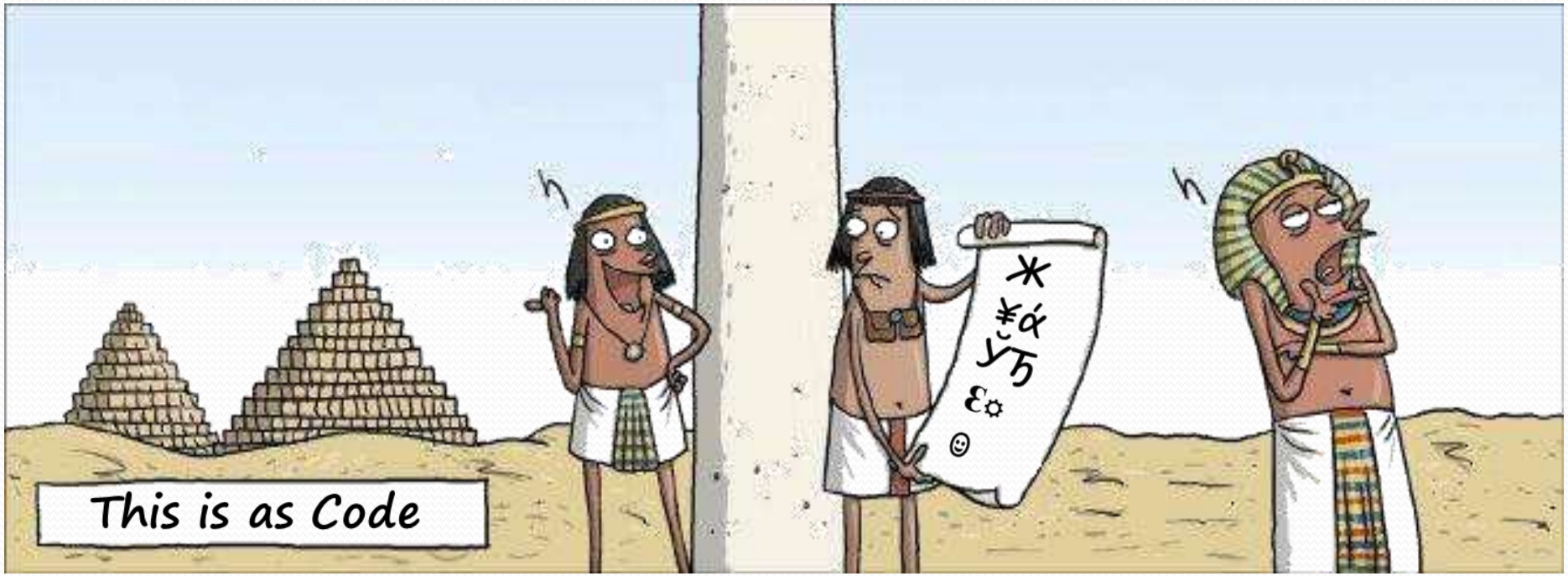
HIWORLD

Example "3"

Original Text (Key = 2) :

THISISASCODE

Cipher Text = ????



Solution “3”

Original Text	T	H	I	S	I	S	A	S	C	O	D	E	L.Key = 12
Rail-Fence	T		I		I		A		C		D		Key=1
Key=2		H		S		S		S		O		E	Key=2
Cipher Text	T	I	I	A	C	D	H	S	S	S	O	E	

TIIACDHSSSOE

Cipher Text	T	I	I	A	C	D	H	S	S	S	O	E	L.Key = 12
Rail-Fence	T		I		I		A		C		D		Key=1
Key=2		H		S		S		S		O		E	Key=2
Original Text	T	H	I	S	I	S	A	S	C	O	D	E	

THISISASCODE

Attacking the (Rail-Fence)

1. Exhaustive Search:

- Try all possible keys!

2. Statistical Analysis:

- with key(**5 Steps**).
- without key.
  1. Letters (**3 Steps**).
  2. Select Letters Together (**3 Steps**).

Example "1"

Cipher Text (Key =2) :

HWRDIOL

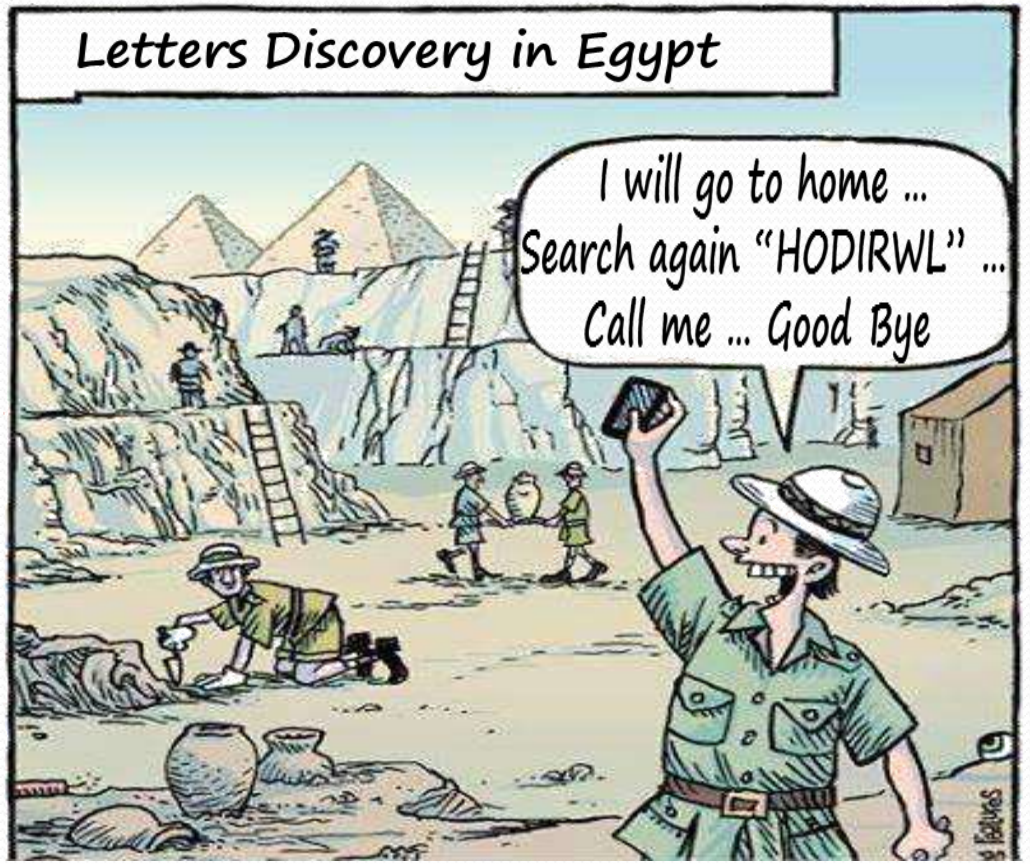
Solution “1”

Steps	Cipher Text	HWRDIOL						
1	L.Key	7						
3	S=(L.Key/key)	(7/2)=(4+3)/2						
4	Split Word	H	W	R	D	I	O	L
	Key=1	H		W		R		D
	Key=2		I		O		L	
5	Original Text	H	I	W	O	R	L	D

Example "2"

Cipher Text (Key =3) :

HODIRWL



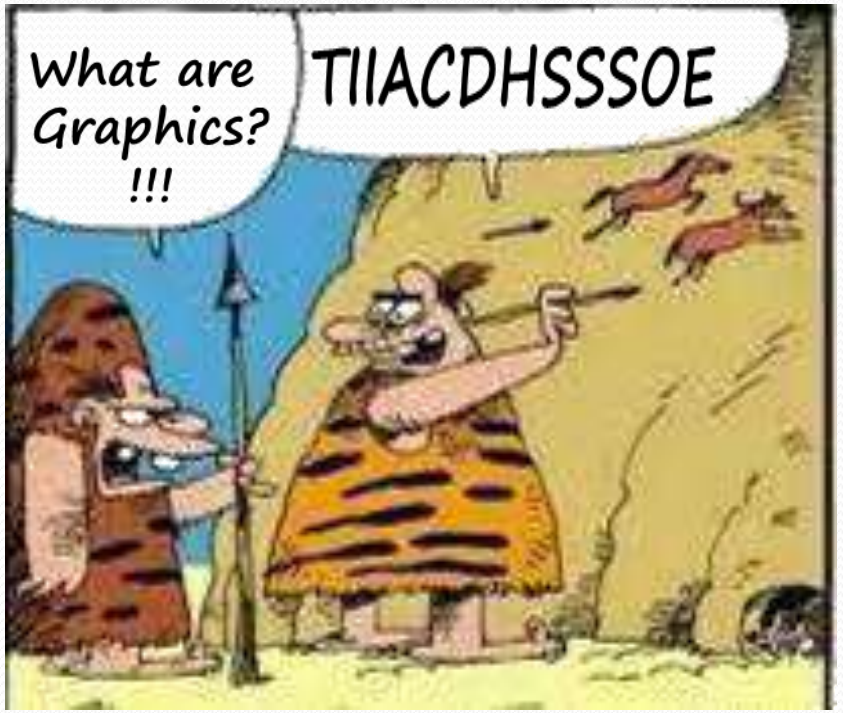
Solution "2"

Steps	Cipher Text	HODIRWL						
1	L.Key	7						
3	S=(L.Key/key)	(7/3)=(3+2+2)/3						
4	Split Word	H	O	D	I	R	W	L
	Key=1	H			O			D
	Key=2		I			R		
	Key=3			W			L	
5	Original Text	H	I	W	O	R	L	D

Example “3”

Cipher Text (Key =2) :

TIIACDHSSSOE

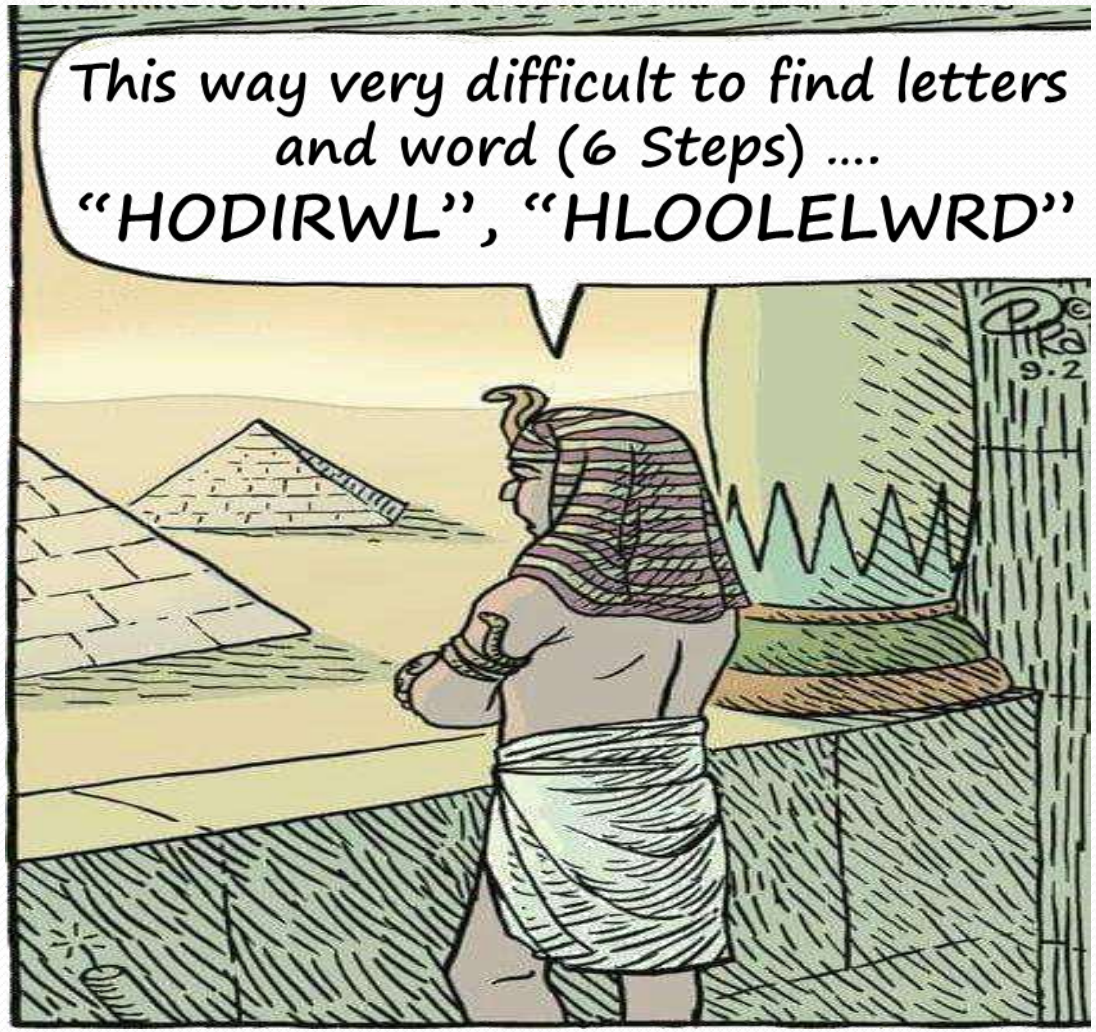


Solution “3”

Steps	Cipher Text	TIIACDHSSSOE											
1	L.Key	12											
3	S=(L.Key/key)	(12/2)=(6+6)/2											
4	Split Word	T	I	I	A	C	D	H	S	S	S	O	E
	Key=1	T		I		I		A		C		D	
	Key=2		H		S		S		S		O		E
5	Original Text	T	H	I	S	I	S	A	S	C	O	D	E

Statistical Analysis (without key)

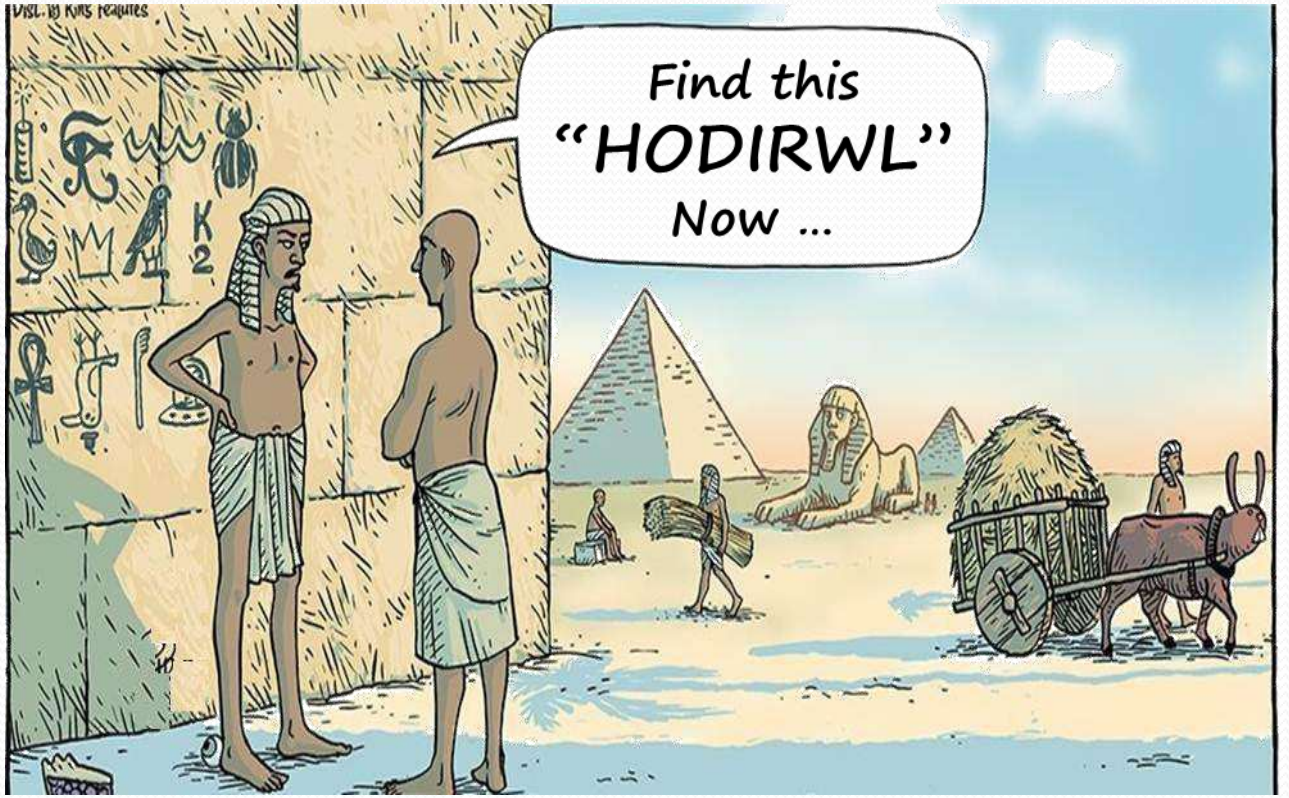
1. Letters (3 Steps).
2. Select Letters Together (3 Steps).



Example “4”

Cipher Text :

HODIRWL



2-gram English Bigram Frequencies (676)

2-gram		
TH	THE	1
	THERE	2
	THEN	3
	...	...
	ANTHER	116997844

TH	116997844	ET	32872552	CE	19803619
HE	100689263	SE	31532272	HO	19729026
IN	87674002	OU	31112284	BE	19468489
ER	77134382	OF	30540904	TT	19367472
AN	69775179	LE	30383262	FO	18923772
RE	60923600	SA	30080131	TS	18922522
ES	57070453	VE	29320973	SS	18915696
ON	56915252	RO	29230770	NO	18894111
ST	54018399	RA	28645577	EE	18497942
NT	50701084	RI	27634643	EM	18145294
EN	48991276	HI	27495342	AC	17904683
AT	48274564	NE	27331675	IL	17877600
ED	46647960	ME	27237733	DA	17584055
ND	46194306	DE	27029835	NI	17452104
TO	46115188	CO	26737101	UR	17341717
OR	45725191	TA	26147593	WA	16838794
EA	43329810	EC	25775798	SH	16773127
TI	42888666	SI	25758841	EI	16026915

Solution "4"

Steps	Cipher Text	HODIRWL						
1	Letters	H=1	O=1	D=1	I=1	R=1	W=1	L=1
2	No. Letters	7						
3	B- Letter	(7-1)=6	(7-1)=6	(7-1)=6	(7-1)=6	(7-1)=6	(7-1)=6	(7-1)=6
	E- Letter	(7-1)=6	(7-1)=6	(7-1)=6	(7-1)=6	(7-1)=6	(7-1)=6	(7-1)=6
4	Total	12	12	12	12	12	12	12

Solution "4"

HODIRWL								
Step 4	Step 5							Step 6
H=(1,12)	B- Letter	HO=19729	HD=828	HI=27495	HR=3843	HW=1403	HL=1169	HI
	E- Letter	OH=3254	DH=4585	IH=610	RH=2968	WH=11852	LH=1274	
O=(1,12)	B- Letter		OD=7610	OI=5336	OR=45725	OW=14610	OL=13726	OR
	E- Letter		DO=13120	IO=21210	RO=29230	WO=9106	LO=15596	
D=(1,12)	B- Letter			DI=21673	DR=5701	DW=4906	DL=3050	LD
	E- Letter			ID=12896	RD=9025	WD=432	LD=10245	
I=(1,12)	B- Letter				IR=11681	IW=922	IL=17877	
	E- Letter				RI=27634	WI=15213	LI=23291	
R=(1,12)	B- Letter					RW=3348	RL=4803	
	E- Letter					WR=1226	LR=1505	
W=(1,12)	B- Letter						WL=657	W
	E- Letter						LW=1836	
L=(1,12)								

?HI?OR?LD? = HIWORLD = HI WORLD

Example “5”

Cipher Text :

HLOOLELWRD

Solution "5"

Steps	Cipher Text	HLOOLELWRD						
1	Letters	H=1	L=3	O=2	E=1	W=1	R=1	D=1
2	No. Letters	7						
3	B- Letter	(7-1)=6	7	7	(7-1)=6	(7-1)=6	(7-1)=6	(7-1)=6
	E- Letter	(7-1)=6	7	7	(7-1)=6	(7-1)=6	(7-1)=6	(7-1)=6
4	Total	12	14	14	12	12	12	12

Solution "5"

WATHQ For Programming

HLOOLELWRD								
Step 4	Step 5							Step 6
H=(1,12)	B- Letter	HL=1169	HO=19729	HW=1403	HE=100689	HR=3843	HD=828	HE
	E- Letter	LH=1274	OH=3254	WH=11852	EH=7559	RH=2968	DH=4585	
L=(3,14)	B- Letter	LL=24636	LO=15596	LD=10245	LE=30383	LW=1836	LR=1505	LL
	E- Letter	LL=24636	OL=13726	DL=3050	EL=23092	WL=657	RL=4803	
O=(2,14)	B- Letter		OD=7610	OO=10168	OE=2616	OW=14610	OR=45725	OW
	E- Letter		DO=13120	OO=10168	EO=13524	WO=9106	RO=29230	
E=(1,12)	B- Letter				EW=14776	ER=77134	ED=46647	OR
	E- Letter				WE=13185	RE=60923	DE=27029	
W=(1,12)	B- Letter					WR=1226	WD=432	LD
	E- Letter					RW=3348	DW=4906	
R=(1,12)	B- Letter						RD=9025	
	E- Letter						DR=5701	
D=(1,12)								

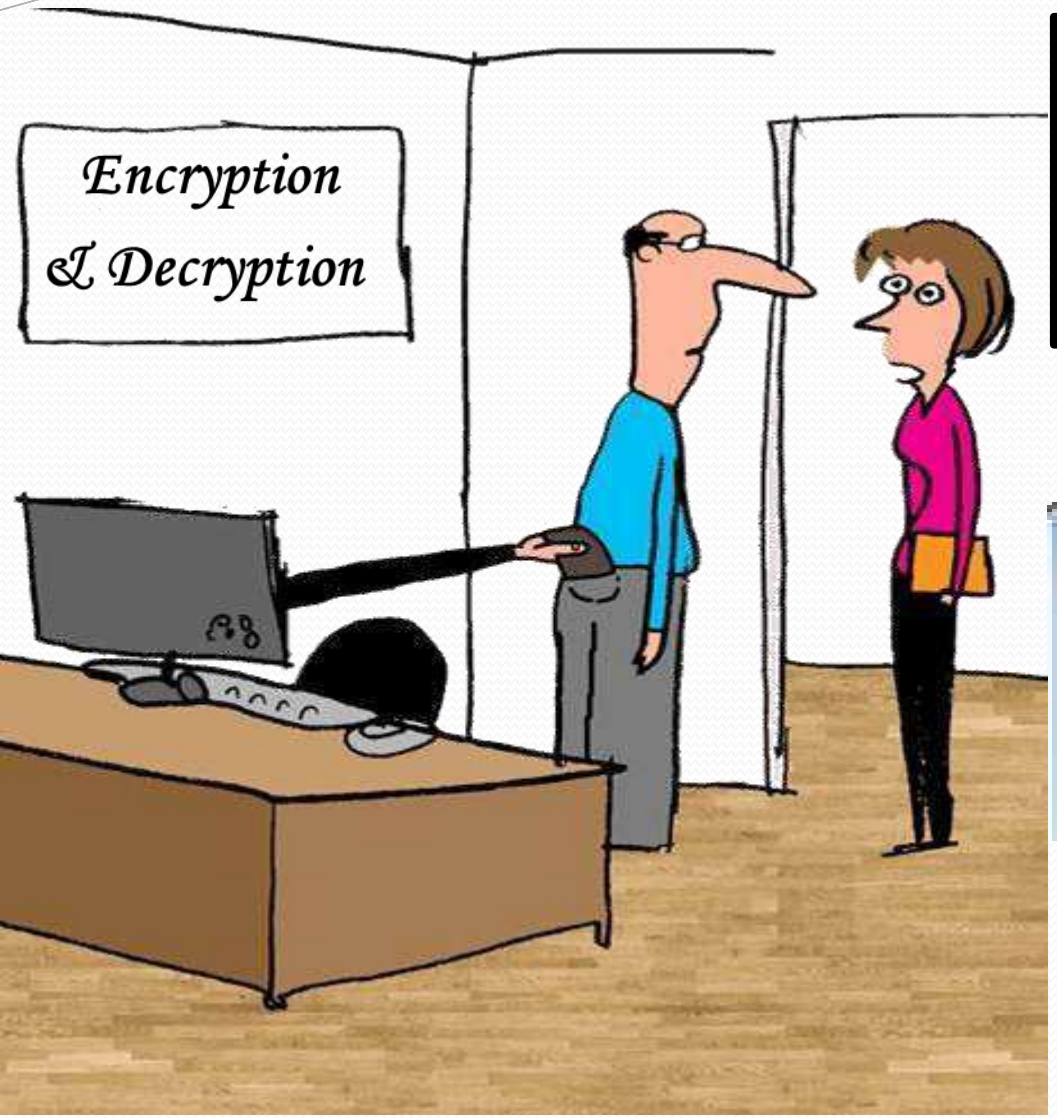
HELLOWORLD = HELLO WORLD

Thank you for Listening!

Label

Button

Text Box



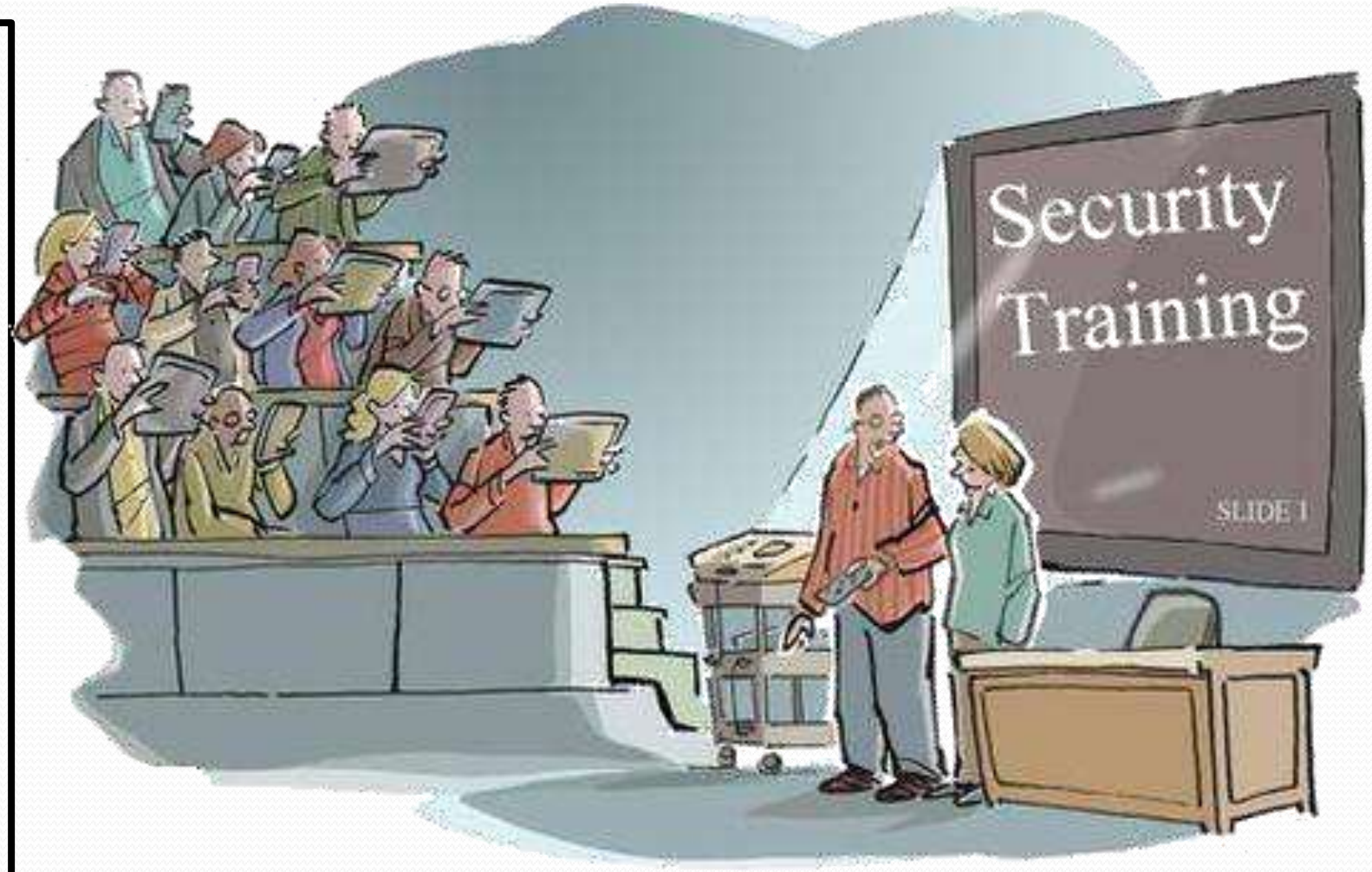

```
private void textBox1_TextChanged(object sender, EventArgs e)
{
textBox1.CharacterCasing = CharacterCasing.Upper;
}
```

```
private void button1_Click(object sender, EventArgs e)
{
textBox2.Text = en(textBox1.Text);
}
```

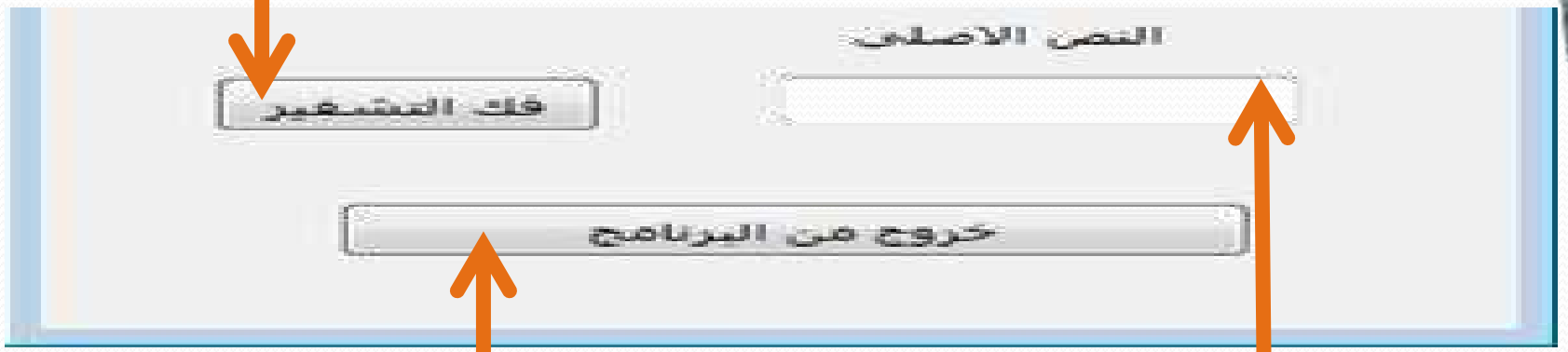

```
private void textBox2_TextChanged(object sender, EventArgs e)
                                    {    }
```

1

```
string en(string a)
{       string k1 = "";
        string k2 = "";
        for (int i = 0; i < a.Length; )
        {   k1 = k1 + a[i];
            i = i + 2;
         }
        for (int i = 1; i < a.Length; )
         {   k2 = k2 + a[i];
            i = i + 2;
         }
         return k1 + k2;
}
```



```
private void button2_Click(object sender, EventArgs e)
{
textBox3.Text = de(textBox2.Text);
}
```



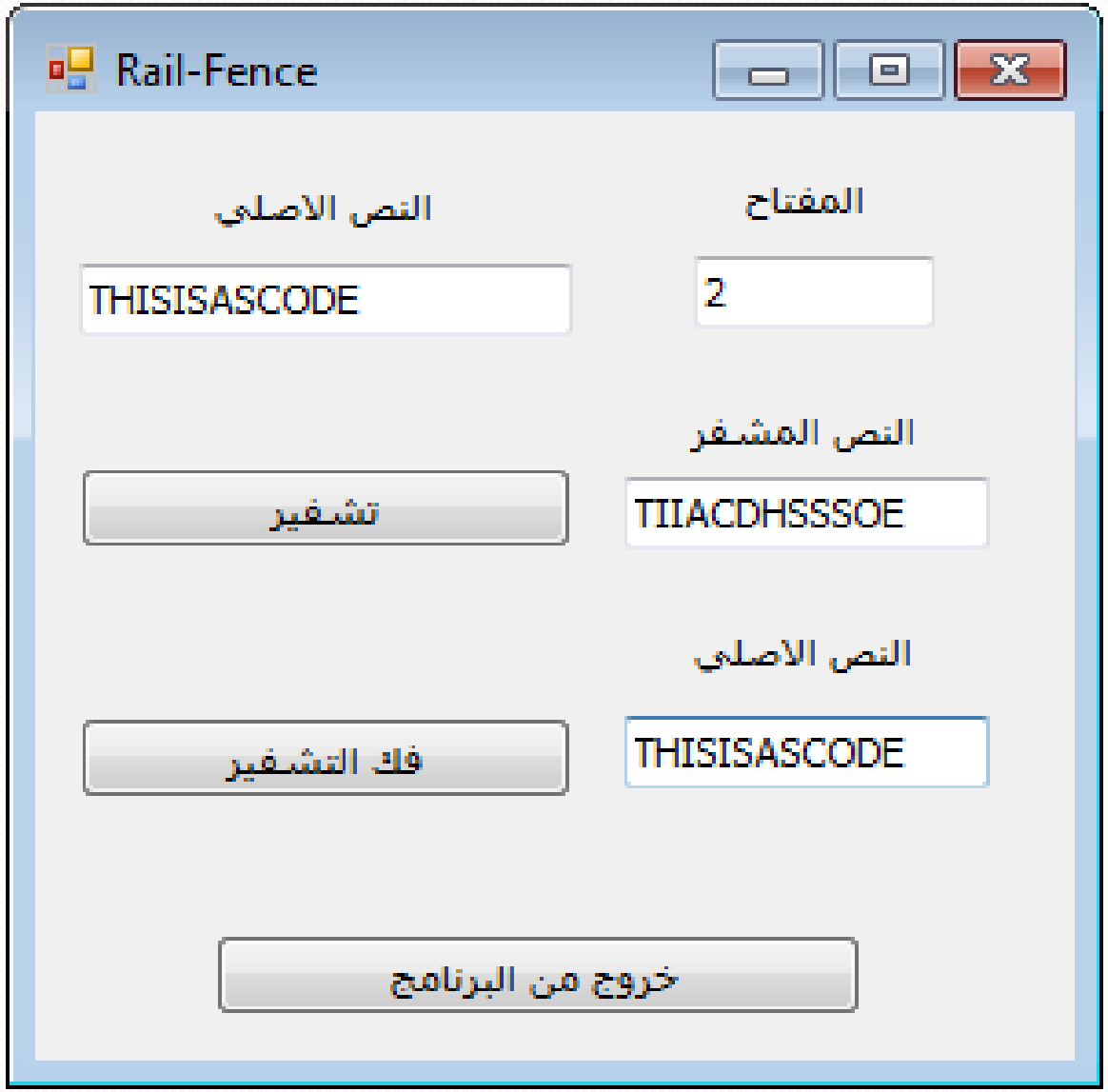
```
private void textBox3_TextChanged(object sender, EventArgs e)
                                    {        }
```

```
private void button3_Click(object sender, EventArgs e)
                    {   Application.Exit();    }
```

2

```
string de(string a)
{
string k1 = a.Remove((a.Length) / 2);
if ((a.Length) % 2 == 1)
k1 = k1 + a[(a.Length) / 2];
string k2 = a.Remove(0,(k1.Length) );
string k3 = "";
for (int i = 0; i < k2.Length; )
{
k3 = k3 + k1[i];
k3 = k3 + k2[i];
i = i + 1; }
if ((a.Length) % 2 == 1)
k3 = k3 + k1[(k1.Length)-1];
return (k3);
}
```


Rail-Fence Cipher
النص الاصلي
HIWORLD
النص المشفر
HWRDIOL
تشفير
النص الاصلي
HIWORLD
فك التشفير
خروج من البرنامج


Rail-Fence
المفتاح
2
النص الاصلي
THISISASCODE
تشفير
النص المشفر
TIIACDHSSSOE
فك التشفير
النص الاصلي
THISISASCODE
خروج من البرنامج


Rail-Fence
النص الاصلي
المفتاح
HIWORLD
3
النص المشفر
تشفير
HODIRWL
النص الاصلي
فك التشفير
HIWORLD
خروج من البرنامج


Exercises ???!
TABLETS

Thank you for Listening!

- **شيفرة قيصر : يوليوس قيصر(الجمع.) Caesar**

النص المشفر = النص الأصلي + مفتاح التشفير M + K % 26

النص الأصلي = c - K % 26

- **شيفرة فيجينير**

النص المشفر = $C_i=(A_i + K_i \bmod m) \% 26$

النص الأصلي = $A_i =(C_i - K_i \bmod m) \% 26$

- **شفرة احادية الاستبدال الابجدية. Single Replacement**

1. انشئ جدول متفق عمية لجميع الحروف.
2. استبدال كل حرف من النص الاصلي بما يقابله من الحروف في الجدول المتفق عميه.

- **شفرة ريل فينس. Rai lFence**

1. يقسم النص الاصمي الى مستويات(حسب قيمة المفتاح.)هنا مستويان
2. يقسم النص الاصمي(: الحرف الاولى في المستوى الاول والحرف الثاني في المستوى الثاني... الخ.)
3. تجمع عناصر كل مستوى مع بعض.

مثال

a= H I W O R L D

K1 = H W R D

K2 = I O L

K1+K2 = H W R D I O L

```
string en(string a)
{       string k1 = "";
        string k2 = "";
        for (int i = 0; i < a.Length; )
        {  k1 = k1 + a[i];
           i = i + 2;
        }
        for (int i = 1; i < a.Length; )
        {  k2 = k2 + a[i];
           i = i + 2;
        }
        return k1 + k2;
}
```

برنامج يشفر الحرف الأول في النص الأصلي بـ الحرف الأخير في النص المشفر

```
   string en(string a)
        {
            string k = "";
            for (int i = 1; i <= a.Length; i++)
            { k= k+a[a.Length - i];
            }

            return k;
        }
```

برنامج يشفر كل حرف بالذي بعده بخانتين

```
string en2(string a)
        {
            string k = ""; int d = 1;
            for (int i = 0; i < a.Length; i++)
            {
                d = i +2;
                if (d >= a.Length) d = d - a.Length;
                k = k + a[d];
            }

            return k;
        }
```

Active Attack Vs. Passive Attack

Active Attack:	Passive Attack
1. An attempt to alter system resources or affect their operation 2. Relatively hard to prevent, but easier to detect.	1. An attempt to learn or make use of information from the system that does not affect system resources. 2. Relatively hard to detect, but easier to prevent

Symmetric Encryption Vs. Asymmetric Encryption

Symmetric Encryption	Asymmetric Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key.	**Needed to Work:** 1. One algorithm is used for encryption and a related algorithm for decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one)