أمنية الحاسبات والبيانات
COMPUTER & DATA SECURITY

وزارة التعليم العالي والبحث العلمي
جامعة الفرات الاوسط
المعهد التقني /السماوة
قسم تكنولوجيا المعلومات والاتصالات
مدرس المادة :م.م بيداء هادي محمد

- **المحاضرة السابعة**

الهدف من المحاضرة

سيتعرف الطالب في هذه المحاضرة على ما يلي:

- التعرف على خوارزمية تشفير(شفرة قيصر)
- طريقة التشفير وفك التشفير

السؤال القبلي

س١ :ماذا نقصد بالتشفير

أ-هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الاطلاع عليها.

ب-هي عملية تحويل النص أو البيانات إلى شكل غير مفهوم بغرض إخفاء هذه البيانات

ج- هو خدمة تستخدم لاثبات هوية التعامل مع البيانات

س٢ :ماهي عناصر التشفير؟

أ-الخوارزمية -مفتاح التشفير-النص الأصلي - نص المشفر

ب- الخوارزمية -مفتاح التشفير-النص الأصلي

ج-نص مشفر-مفتاح التشفير-النص الأصلي

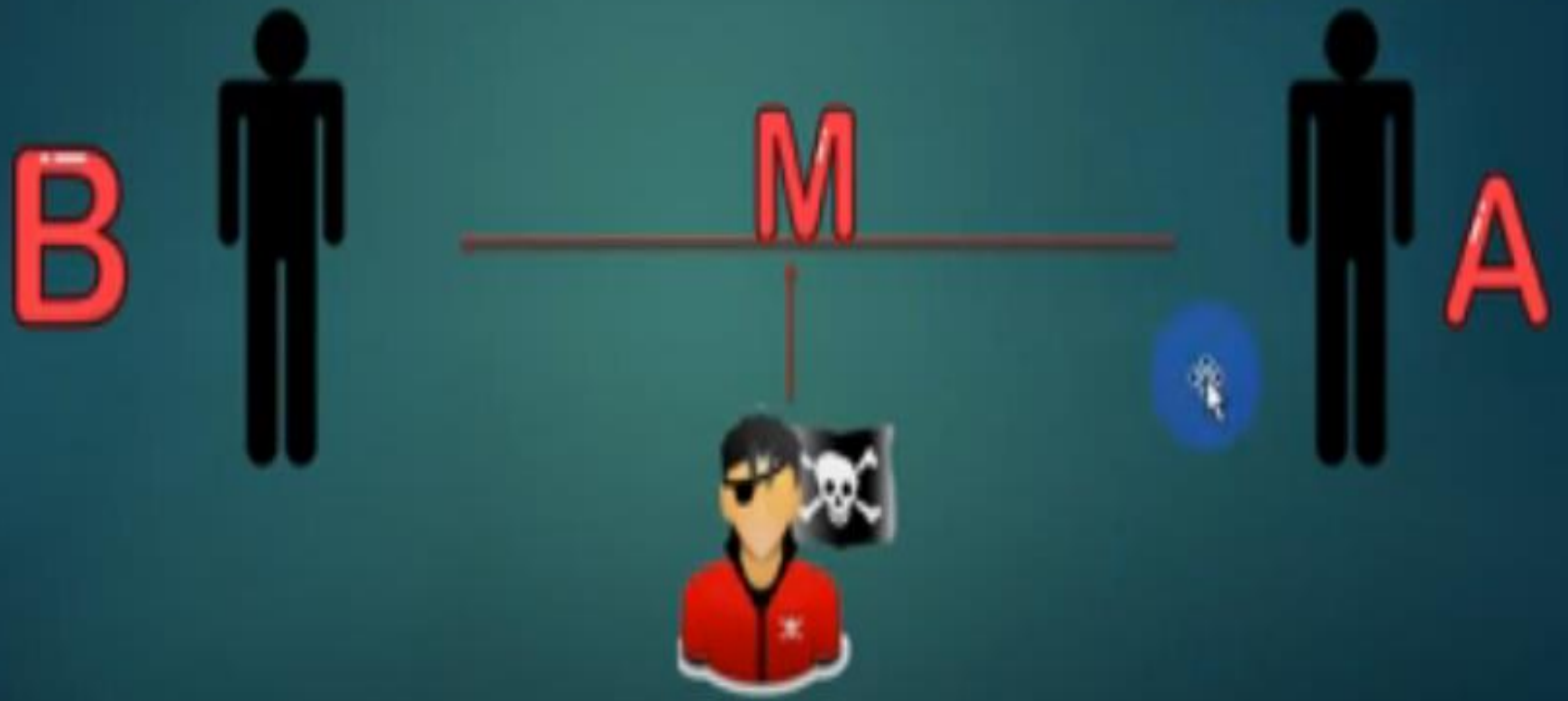
س٣:يمكن تصنيف التشفير بناءً على المفاتيح المستخدمة في التشفير وفك التشفير؟

أ-تشفير متماثل وتشفير غير متماثل

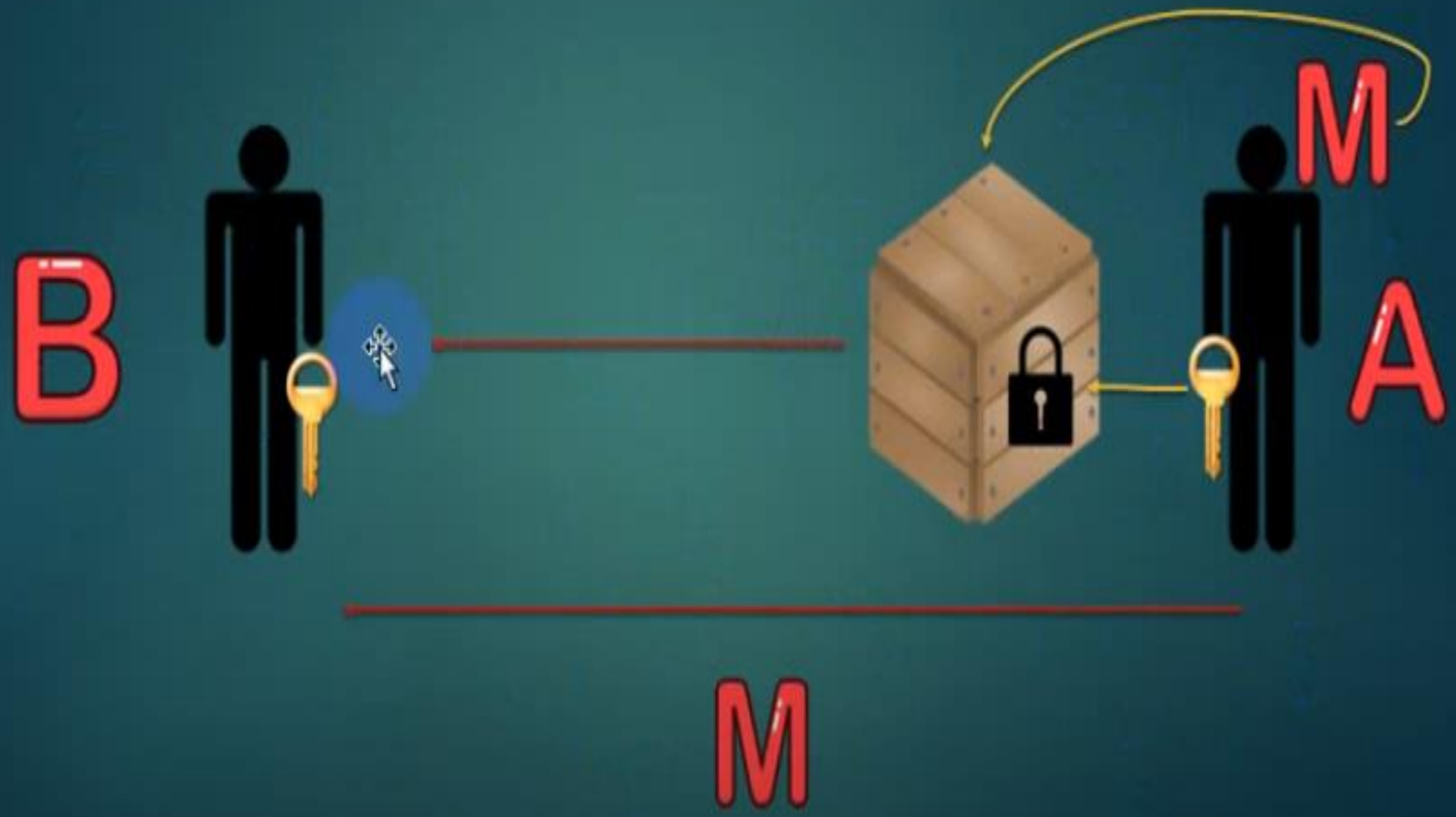
ب-تشفير متماثل والتشفير العام

ج- التشفير باتجاهين والتشفير باتجاه واحد

الحاجة للتشفير



التشفير المتناظر

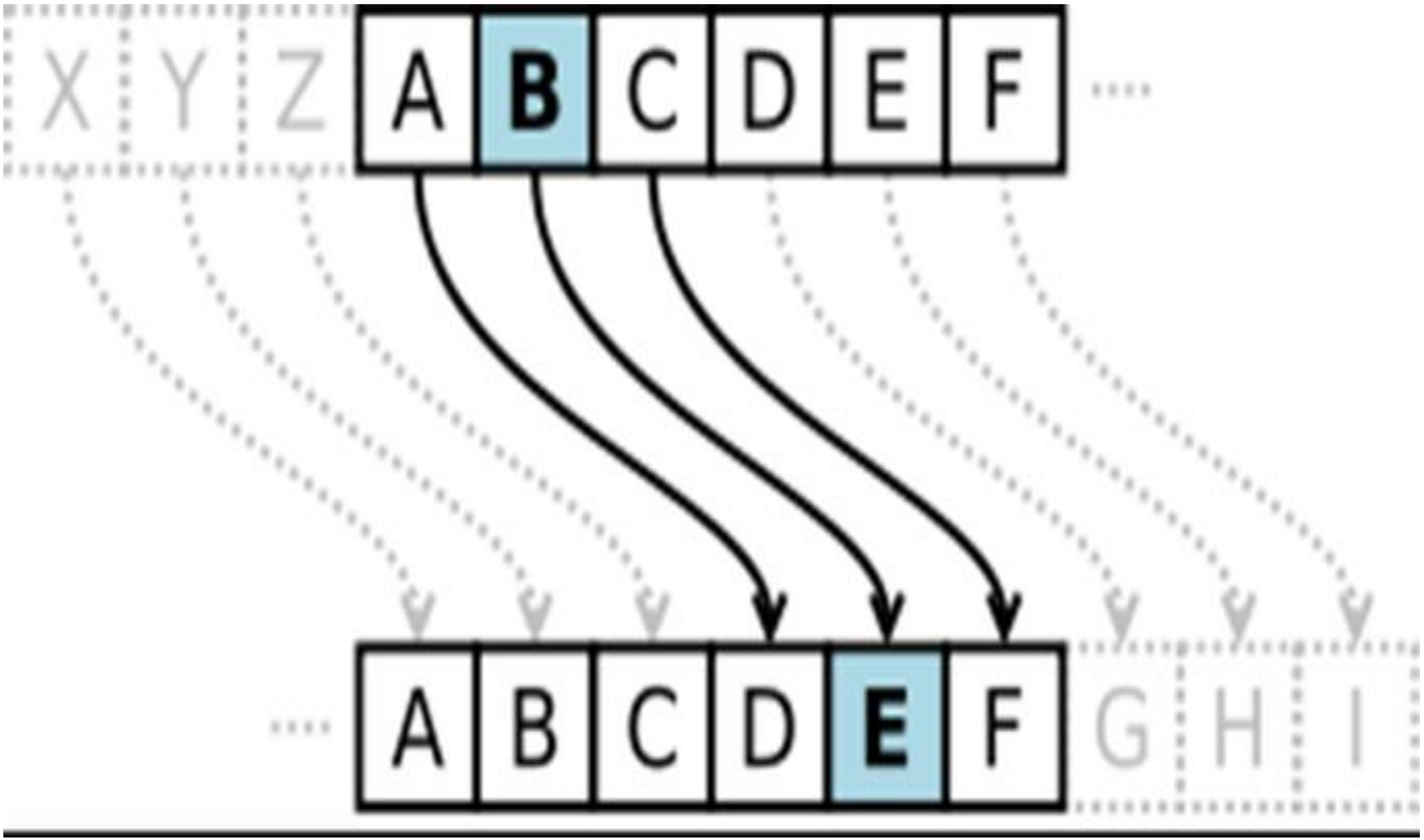


Caesar Cipher

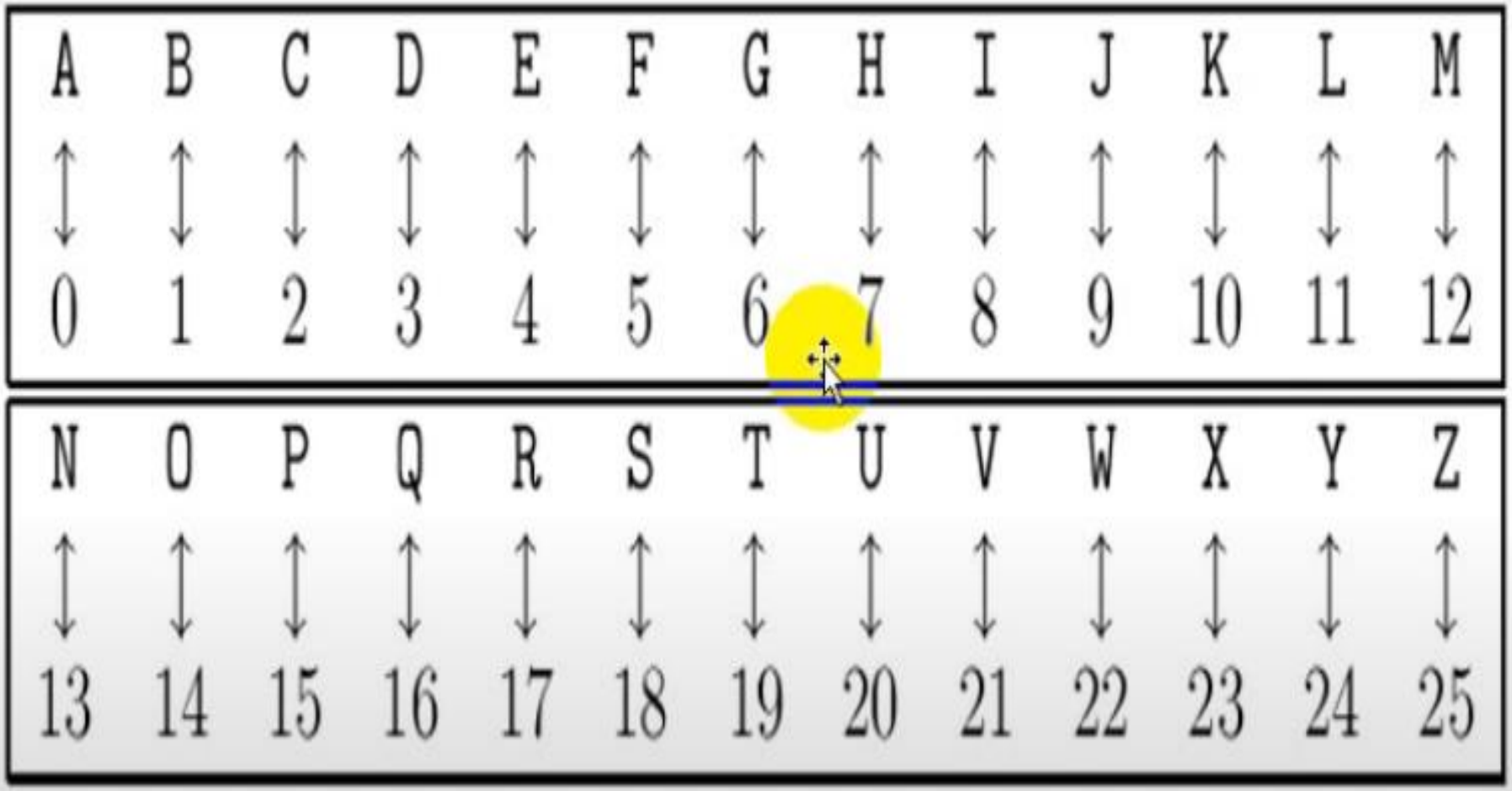
طريقة التشفير بشفرة قيصر

- شيفرة قيصر هي من أقدم أنواع التشفير باستخدام تقنيات تبديل الحروف وأبسطها.

- تعتمد عملية التبديل على المفتاح المستخدم في التشفير اذا كان المفتاح =٣ يتم وفق هذه الطريقة تبديل حرف من حروف الابجدية بالحرف الذي يقع في المرتبة الثالثة بعده، أي :
الحرف المشفر


X Y Z A B C D E F ....
.... A B C D E F G H I

المبدأ الاساسي



- مثال :
- النص الصريح
- MR CARTER IS A COOL TEACHER :

الحل:

النص المشفر:

PU FDUWHU LV D FRRO WHDFKH

النص الصريح:

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

النص المشفر:

DEFGHIJKLMNOPQRSTUVWXYZABC

تشفير النص

C يمثل النص المشفر
M يمثل النص الاصلي
key يمثل المفتاح
N يمثل عدد الحروف

$$C = (M + KEY) \ modulo \ N$$

- س/حول النص الصريح الى نص مشفر اذا علمت ان المفتاح=٥

- COMPUTER DATA SECURITY

- المفتاح= ٥

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

C=(m+k)mod 26

C=(2+5)mod 26=7=H

=(14+5)mod 26=19=T

=12+5 mod 26=17=R

Cipher text:HTRUZYJWIFYFXJHZWNYD

Cيمثل النص المشفر
Mيمثل النص الاصلي
keyيمثل المفتاح
Nيمثل عدد الحروف

حول النص المشفر الى نص صريح اذا علمت ان المفتاح=٥

Cipher text:HTRUZYJWIFYFXJHZWNYD

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

M=(c-k)mod 26

في حالة ان ناتج عملية الطرح يكون عددا سالبا سوف تتم معالجة المعادلة بالشكل التالي:

M=(c-k+26)mod 26

لنفرض الحرف D

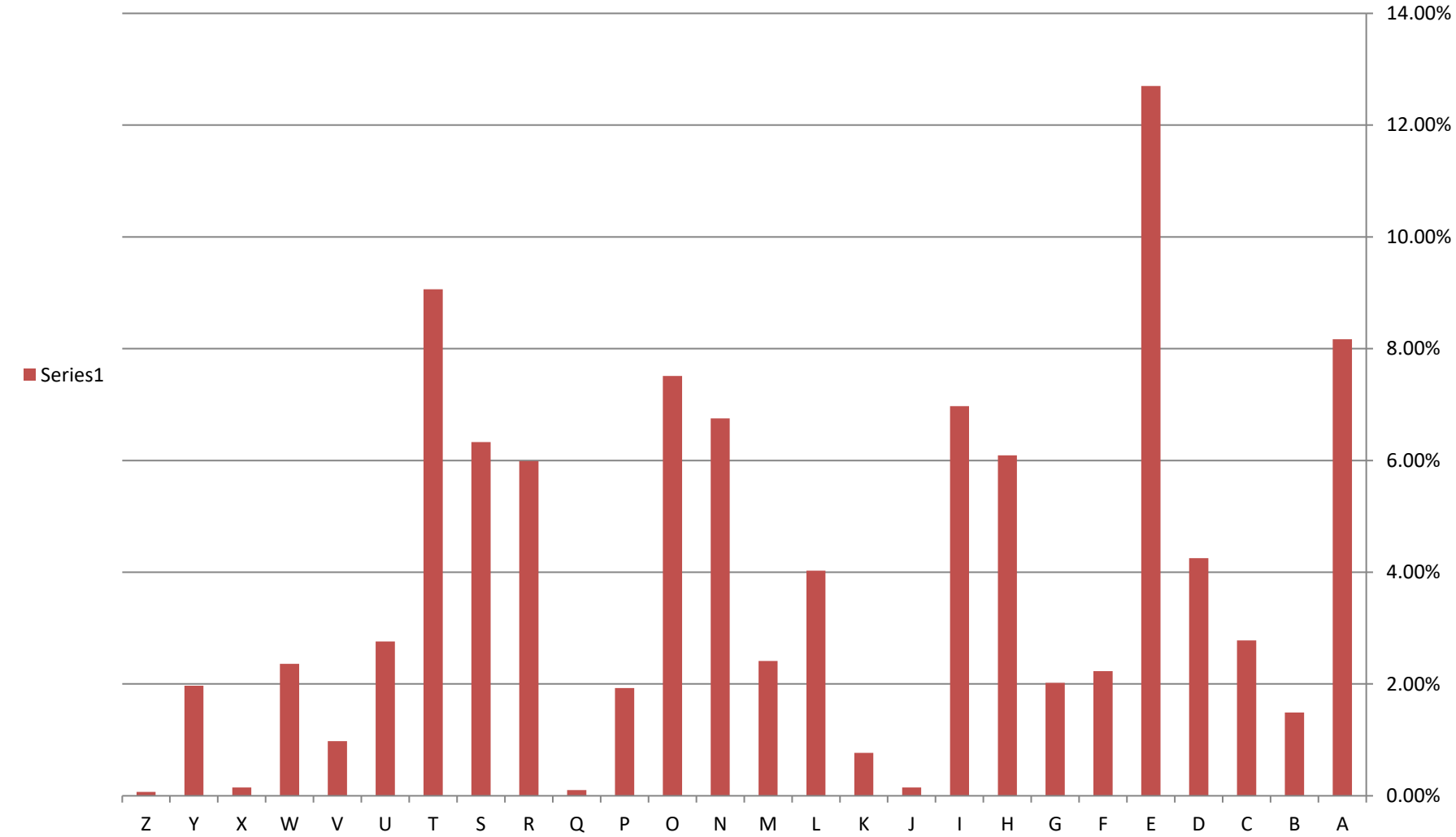
M=(3-5+26)mod26=(-2+26)mod26=24=Y

هناك ثلاث مميزات للطريقة السابقة في التشفير، وهي:

١. خوارزمية التشفير وفك التشفير معروفتان.
٢. هناك ٢٥ مفتاحاً محتمل فقط.
٣. اللغة التي كتب فيها النص معروفة ويمكن تمييزها بسهولة.

المأخذ على خوارزمية قيصر للتشفير انها سهلة الكسر .

مخطط يوضح الحروف الأكثر استخداما في اللغة الإنجليزية



شفر النص التالي الذا علمت ان المفتاح=٢ فيصبح لديك نص مشفر اكشف المفتاح من خلال حساب تكرار الحروف ومعرفة اي الحروف اكثر تكراروايتم توضيح ذلك في تقريريرفع بالكلاس

Computer Security :- is the protection of computing systems and the data

that they store or access. It refers to the technological safeguards and

managerial procedures that can be applied to computer hardware, programs,and data

1	Start of heading	32	Space	64	@	96	`
2	Start of text	33	!	65	A	97	a
3	End of text	34	"	66	B	98	b
4	End of transmit	35	#	67	C	99	c
5	Enquiry	36	$	68	D	100	d
6	Acknowledge	37	%	69	E	101	e
7	Audible bell	38	&	70	F	102	f
8	Backspace	39	'	71	G	103	g
9	Horizontal tab	40	(	72	H	104	h
10	Line feed	41	)	73	I	105	i
11	Vertical tab	42	*	74	J	106	j
12	Form feed	43	+	75	K	107	k
13	Carriage return	44	,	76	L	108	l
14	Shift in	45	-	77	M	109	m
15	Shift out	46	.	78	N	110	n
16	Data link escape	47	/	79	O	111	o
17	Device control 1	48	0	80	P	112	p
18	Device control 2	49	1	81	Q	113	q
19	Device control 3	50	2	82	R	114	r
20	Device control 4	51	3	83	S	115	s
21	Neg. acknowledge	52	4	84	T	116	t
22	Synchronous idle	53	5	85	U	117	u
23	End trans. block	54	6	86	V	118	v
24	Cancel	55	7	87	W	119	w
25	End of medium	56	8	88	X	120	x
26	Substitution	57	9	89	Y	121	y
27	Escape	58	:	90	Z	122	z
28	File separator	59	;	91	[	123	{
29	Group separator	60	<	92	\	124	|
30	Record separator	61	=	93	]	125	}
31	Unit separator	62	>	94			

برمجة خوارزمية قيصر :-

١-برمجة التشفير :
٢-as: رقم الاسكي كود للأحرف
٣-s: النص الأصلي
٤- c: الحرف المشفر

```
  #include<iostream>
 #include<conio.h>
#include<string>
using namespace std;
void main(){
   int as;
string s;
char c;
   cout<<"Enter the plantext:";//ادخال النص الاصلي
   cin>>s;

   for(int i=0;i<s.length();i++)
   {  if(s[i]>='a'&& s[i]<='z')//شرط للاحرف الصغيرة
     {
           as=s[i];
           as=as-97+3+26;
           as=as%26;
           as=as+97;
           c=as;
          cout<<c;
      }
   }
   _getch();
}
```

نفرض انه ادخلنا النص التالي hello
يتم وضعه في المصفوفة s[i]وتكون بهذا الشكل

٠	١	٢	٣	٤	٥
h	e	l	l	o	

٦ as=s[i];

- as=as-97-3+26;
- بمعنى as=hوبالتالي ما يقابل بالاسكي كود =
- As= 104 -97-3+26
- As=36
- As=36 mod 26
- 107=97+10
- يقابل k
- khoor

١. c: الحرف المشفر

```
#include<iostream>
#include<conio.h>
#include<string>
using namespace std;
void main(){
int as,k;string s;char c;
ادخال النص المشفرcout<<"Enter the Dplantext:";//
cin>>s;
for(int i=0;i<s.length();i++)
شرط للاحرف الصغيرة{  if(s[i]>='a'&& s[i]<='z')//
}
as=s[i];
  as=as-97-3+26;
  as=as%26;
  as=as+97;
  c=as;
 cout<<c;
   }
}
_getch();
}
```


شكراً لحسن استماعكم