برمجة الخوارزمية التشفير

المحاضرة العملي

المصطلحات الأساسية :

plaintext :الرسالة الأصلية / المرسلة.

ciphertext: الرسالة المشفرة .

cipher: الخوارزمية المستخدمة لتحويل الرسالة الاصلية إلى رسالة مشفرة.

key :معلومات مستخدمة للتشفير معروفة فقط للمرسل والمستقبل.

encrypt (encipher:) عملية تحويل الرسالة الاصلية إلى الرسالة المشفرة (التشفير).

decrypt (decipher):عملية إستخراج والحصول على الرسالة الاصلية من المشفرة.

خوارزمية التشفير :طريقة التشفير بشفرة قيصر

شُفرة قٌيصرمن أقدم أنواع التشفٌير باستخدام تقنٌيات تبدٌيل الحروف وأبسطها.

ٌ تم وفق هذه الطرٌيقة تبدٌيل حرف من حروف الابجدية

بالحرف الذيٌ يقع فَي المرتبة الثالثة بعده، أي : الحرف المشفر.

مثال: فك النص المشفر بطريقة شفرة قيصر

9	8	7	6	5	4	3	2	1	0	19	18	17	16	15	14	13	12	11	10	25	24	23	22	21	20
j	i	h	g	f	e	d	c	b	a	t	s	r	q	p	o	n	m	l	k	Z	y	x	w	v	u

Key is:3

PHHW PH DIWHU WKH WRJD SDUWB:النص المشفر

meet me after the toga party:النص الأصلي

برمجة النص المشفر بطريقة شفرة قيصر:

As: الاسكي كود للاحرف
s: النص المشفر
C: النص الاصلي

```
 #include<iostream>
 #include<conio.h>
#include<string>
using namespace std;
void main(){
    int as;
string s;
char c;
```

برمجة النص المشفر بطريقة شفرة قيصر:

```
cout<<"Enter the ciphertext:";//ادخال النص المشفر
     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();
}
```

دالة :length()حساب طول النص

S[i]: مصفوفة أحادية تشمل طول النص

جدول الاسكي كود

Ascii	Char	Ascii	Char	Ascii	Char	Ascii	Char
0	Null	32	Space	64	@	96	`
1	Start of heading	33	!	65	A	97	a
2	Start of text	34	"	66	B	98	b
3	End of text	35	#	67	C	99	c
4	End of transmit	36	$	68	D	100	d
5	Enquiry	37	%	69	E	101	e
6	Acknowledge	38	&	70	F	102	f
7	Audible bell	39	'	71	G	103	g
8	Backspace	40	(	72	H	104	h
9	Horizontal tab	41	)	73	I	105	i
10	Line feed	42	*	74	J	106	j
11	Vertical tab	43	+	75	K	107	k
12	Form feed	44	,	76	L	108	l
13	Carriage return	45	-	77	M	109	m
14	Shift in	46	.	78	N	110	n
15	Shift out	47	/	79	O	111	o
16	Data link escape	48	0	80	P	112	p
17	Device control 1	49	1	81	Q	113	q
18	Device control 2	50	2	82	R	114	r
19	Device control 3	51	3	83	S	115	s
20	Device control 4	52	4	84	T	116	t
21	Neg. acknowledge	53	5	85	U	117	u
22	Synchronous idle	54	6	86	V	118	v
23	End trans. block	55	7	87	W	119	w
24	Cancel	56	8	88	X	120	x
25	End of medium	57	9	89	Y	121	y
26	Substitution	58	:	90	Z	122	z
27	Escape	59	;	91	[	123	{
28	File separator	60	<	92	\	124	|
29	Group separator	61	=	93	]	125	}
30	Record separator	62	>	94	^	126	~
31	Unit separator	63	?	95	_	127	Forward del.

مثال:فك النص المشفر :khoor

- as=s[i]
- معناه ان as=k أي مايقابل رقم الاسكي كود

as=as-97-3+26

- رقم الاسكي كود للحرف k)) هو(107) وبالتالي تكون المعالجة as=107-97-3+26
- اذا as=33
- as=as%26 أي 33%26
- as=7
- as=as+97 أي as=7+97
- as=104 أي حرف (h) و هكذا برمجة باقي الاحرف

سؤال: شفر النص الأصلي الى نص مشفر بطريقة قيصر

- النص الأصلي :
- Good morning
- النص المشفر:
- jrrgpruqlqj