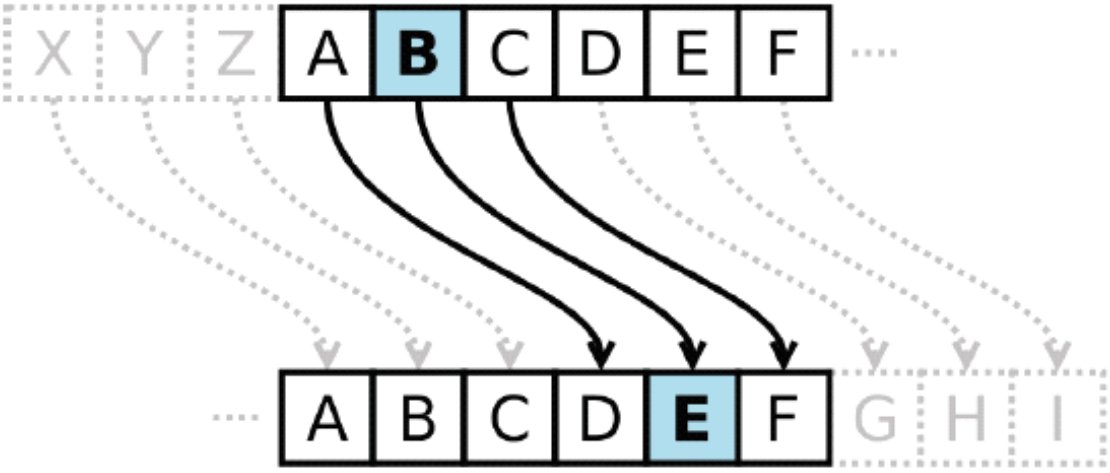
1. Caesar 凯撒密码

1.1 密码分析

凯撒密码是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。



由于已知凯撒密码采用偏移进行加密，总可能性为26种，因此采用了暴力破解的方法。

1.2 破解操作

1.2.1 解密算法

密文： AWPLDPPYNCJAEJZFCYLXPHTESESPDLXPVPJLYODPYOEZESPEL

将每一个字符都进行位移，共移动26次，使每一个字母都有相对应的字母。

```
int i,j;
    for (i = 0; i < 26; i++) {      //move 26 times with different displacement;
        cout << i << "\t";
        for (j = 0; j < str_len; j++)       //decode;
        {
            cout << (char)((ch[j] - 'A' + i) % 26 + 'A');
        }
        cout << endl;       //output the plaintext;
    }
```

1.2.2 加密算法

根据结果得到位移15位为该凯撒密码加密方式，根据明文再对名字进行加密。

```
for (j = 0; j < str_len2; j++)
    {
        cout << (char((ch2[j] - 'A' + 15) % 26 + 'A'));     //encode according the subs
titution table ;
    }
    cout << endl;
```

1.2.3 程序代码

```cpp
#include <iostream>
#include <fstream>
#include <string>
#include <cstring>

using namespace std;

int main()
{
    string str;     //input the ciphertext
    cin >> str;

    char ch[100];
    strcpy_s(ch, str.c_str());

    int str_len;
    str_len = str.length();


    //decode the ciphertext;
    int i,j;
    for (i = 0; i < 26; i++) {      //move 26 times with different displacement;
        cout << i << "\t";
        for (j = 0; j < str_len; j++)       //decode;
        {
            cout << (char)((ch[j] - 'A' + i) % 26 + 'A');
        }
        cout << endl;       //output the plaintext;
    }


    //encode my name according the plaintext;
    string str2;            //input my name;
    cin >> str2;

    int str_len2;
    str_len2 = str2.length();

    char ch2[100];
    strcpy_s(ch2, str2.c_str());

    for (j = 0; j < str_len2; j++)
    {
        cout << (char((ch2[j] - 'A' + 15) % 26 + 'A'));     //encode according the subs
titution table ;
    }
    cout << endl;       //output the ciphertext of my name;

    system("pause");
}
```

1.3 破解结果

1.3.1 暴力破解结果

```
AWPLDPPYNCJAEJZFCYLXPHTESESPDLXPVPJLYODPYOEZESPEL
0       AWPLDPPYNCJAEJZFCYLXPHTESESPDLXPVPJLYODPYOEZESPEL
1       BXQMEQQZODKBFKAGDZMYQIUFTFTQEMYQWQKMZPEQZPFAFTQFM
2       CYRNFRRAPELCGLBHEANZRJVGUGURFNZRXRLNAQFRAQGBGURGN
3       DZSOGSSBQFMDHMCIFBOASKWHVHVSGOASYSMOBRGSBRHCHVSHO
4       EATPHTTCRGNEINDJGCPBTLXIWIWTHPBTZTNPCSHTCSIDIWTIP
5       FBUQIUUDSHOFJOEKHDQCUMYJXJXUIQCUAUOQDTIUDTJEJXUJQ
6       GCVRJVVETIPGKPFLIERDVNZKYKYVJRDVBVPREUJVEUKFKYVKR
7       HDWSKWWFUJQHLQGMJFSEWOALZLZWKSEWCWQSFVKWFVLGLZWLS
8       IEXTLXXGVKRIMRHNKGTFXPBMAMAXLTFXDXRTGWLXGWMHMAXMT
9       JFYUMYYHWLSJNSIOLHUGYQCNBNBYMUGYEYSUHXMYHXNINBYNU
10      KGZVNZZIXMTKOTJPMIVHZRDOCOCZNVHZFZTVIYNZIYOJOCZOV
11      LHAWOAAJYNULPUKQNJWIASEPDPDAOWIAGAUWJZOAJZPKPDAPW
12      MIBXPBBKZOVMQVLROKXJBTFQEQEBPXJBHBVXKAPBKAQLQEBQX
13      NJCYQCCLAPWNRWMSPLYKCUGRFRFCQYKCICWYLBQCLBRMRFCRY
14      OKDZRDDMBQXOSXNTQMZLDVHSGSGDRZLDJDXZMCRDMCSNSGDSZ
15      PLEASEENCRYPTYOURNAMEWITHTHESAMEKEYANDSENDTOTHETA
16      QMFBTFFODSZQUZPVSOBNFXJUIUIFTBNFLFZBOETFOEUPUIFUB
17      RNGCUGGPETARVAQWTPCOGYKVJVJGUCOGMGACPFUGPFVQVJGVC
18      SOHDVHHQFUBSWBRXUQDPHZLWKWKHVDPHNHBDQGVHQGWRWKHWD
19      TPIEWIIRGVCTXCSYVREQIAMXLXLIWEQIOICERHWIRHXSXLIXE
20      UQJFXJJSHWDUYDTZWSFRJBNYMYMJXFRJPJDFSIXJSIYTYMJYF
21      VRKGYKKTIXEVZEUAXTGSKCOZNZNKYGSKQKEGTJYKTJZUZNKZG
22      WSLHZLLUJYFWAFVBYUHTLDPAOAOLZHTLRLFHUKZLUKAVAOLAH
23      XTMIAMMVKZGXBGWCZVIUMEQBPBPMAIUMSMGIVLAMVLBWBPMBI
24      YUNJBNNWLAHYCHXDAWJVNFRCQCQNBJVNTNHJWMBNWMCXCQNCJ
25      ZVOKCOOXMBIZDIYEBXKWOGSDRDROCKWOUOIKXNCOXNDYDRODK
```

观察上图暴力破解结果，可发现位移15位后出现有意义的英文句子，从而得到该凯撒密码的明文:"Please encrypt your name with the same key and send to the TA"。

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
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

1.3.2 加密

由解密结果可知，在完成密码破解后需要对自己的名字进行加密，因此采用与破解相反的算法来完成操作。(名字：来舒悦 LAISHUYUE -> APXHWJNJT)

```
LAISHUYUE
APXHWJNJT
```

2. Vignere

2.1 密码分析

密文： ktbueluegvitnthuexmonveggmrcgxptlyhhjaogchoemqchpdnetxupbqntietiabpsmao
ncnwvoutiugtagmmqsxtvxaoniiogtagmbpsmtuvvihpstpdvcrxhokvhxotawswquune
wcgxptlcrxtevtubvewcnwwsxfsnptswtagakvoyyak

2.1.1 卡西斯基试验

2.1.1.1 原理

> 如果密钥相同的话，结果可能便为（使用密钥ABCD）：
>
> 密钥：ABCDAB CD ABCDA BCD ABCDABCDABCD
> 明文：CRYPTO IS SHORT FOR CRYPTOGRAPHY
> 密文：CSASTP KV SIQUT GQU CSASTPIUAQJB
>
> 此时卡西斯基试验就能产生效果。对于更长的段落此方法更为有效，因为通常>密文中重复的片段会更多。如通过下面的密文就能破译出密钥的长度：
>
> 密文：DYDUXRMHTVDVNQDQNWDYDUXRMHARTJGWNQD
>
> 其中，两个DYDUXRMH的出现相隔了18个字母。因此，可以假定密钥的长度是18的约数，即长度为18、9、6、3或2。而两个NQD则相距20个字母，意味着密钥长度应为20、10、5、4或2。取两者的交集，则可以基本确定密钥长度为2。
> 来源：维基百科/维吉尼亚密码

2.1.1.2 代码实现

```
//Kasiski examination;
    int i, j;
    char ch2[200];          //store the char[] after moving;
    int count[26];          //store the number of the same alphabets of the original ch
ar[] after moving;
    for (j = 0; j < 26; j++)
    {
        count[j] = 0;
        for (i = 0; i < strlen; i++)
        {
            ch2[i] = ch1[(i + j) % strlen];
            if (ch1[i] == ch2[i])
            {
                count[j]++;
            }
        }
        cout << j << "\t" << count[j] << endl;
    }
```

2.1.1.3 结果分析

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
183	9	4	13	9	4	12	8	11	7	7	2	12	4	3	12	9	5	20	9	6	13	9	5	10	3

由上图的卡西斯基试验结果可以得到，位移3，6，12，15，18，21，24时重复字母较多，位移公因子为3，因此猜测key的长度为3。

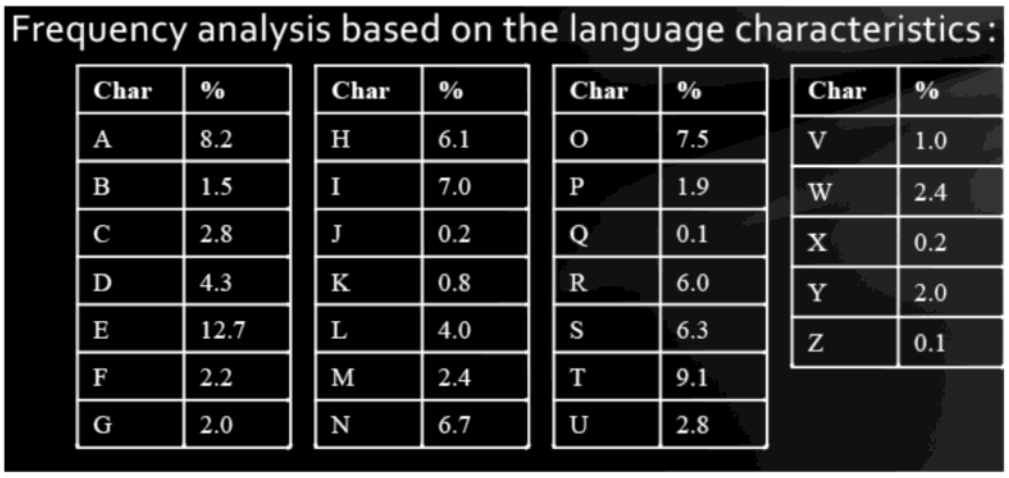
2.1.2 频率分析

2.1.2.1 原理
得到key长度为3之后，将文本分为key长度份。

第一份	第二份	第三份

ch[0],ch[3],ch[6]…	ch[1],ch[4],ch[7]…	ch[2],ch[5],ch[8]…

然后对每一分字符组合中出现的字符进行频率分析，将之与英文明文字母的频率进行分析，得到对应关系，且可知：普通英语文本中 e, t, a, i, n, o频率也较高。



2.1.2.2 代码实现

```
//Frequency Analysis;
    int count2[3][26];
    int temp;
    for (i = 0; i < 3; i++)          //Initialize;
    {
        for (j = 0; j < 26; j++)
        {
            count2[i][j] = 0;
        }
    }
    for (i = 0; i < strlen; i++)     //frequency sum;
    {
        count2[i%3][ch1[i]- 'a']++;
    }
    for (i = 0; i < 3; i++)
    {
        for (j = 0; j < 26; j++)
        {
            cout << char('a'+j) << "\t" << count2[i][j] << "\t";
        }
        cout << endl;
    }
```

2.1.2.3 结果分析

```
a       2       b       0       c       6       d       0       e       1       f       1       g       7       h
l       i       3       j       1       k       1       1       0       m       1       n       2       o       2
p       8       q       4       r       0       s       0       t       5       u       4       v       7       w
3       x       0       y       2       z       0
```

第一份字符完成频率分析后可以看出 ：

p	g	v	c
8	7	7	6

上述四个字符在语句中出现的频率较高，而而一份维吉尼亚密码相当于一个凯撒密码，即位移相同字符数，因此推断：

p	g	v	c
g	v	c	p

同理对第二份、第三份字符进行频率分析：

```
a       4       b       0       c       2       d       2       e       9       f       0       g       2       h
2       i       4       j       0       k       0       l       0       m       3       n       3       o       6
p       l       q       0       r       2       s       7       t       10      u       3       v       l       w
0       x       0       y       0       z       0
a       4       b       5       c       0       d       0       e       0       f       0       g       2       h
5       i       0       j       0       k       3       l       3       m       4       n       5       o       2
p       0       q       0       r       l       s       l       t       4       u       3       v       3       w
5       x       10      y       l       z       0
```

得出该密文的key为长度为3的"cat"。

2.1.3 解码

2.1.3.1 原理

最后根据已知key，对密文进行相对应的一一映射从而完成解码。

_	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
C	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
A	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
T	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

2.1.3.2 代码实现

```
for (i = 0; i < strlen; i+=3)       //decode;
{
    ch1[i] = char((ch1[i] + 26 - 'c') % 26 + 'a');
    ch1[i+2] = char((ch1[i+2] + 26 - 't') % 26 + 'a');
}
```

2.1.3.3 结果分析

```
Key: cat
itisessentialtoseekoutenemyagentswhohavecometoconductespionageagainstyouandtobribethemtoserv
eyougivetheminstructionsandcareforthemthusdoubledagentsarerecruitedandusedsuntzutheartofwar
```

明文：it is essential to seek out enemy agents who have come to conduct espionage against you and to bribe them to serve you give the minstructions and care for them thus doubled agents are recruited and used sun tzut heart of war

2.1.3.4 总代码

```cpp
#include <iostream>
#include <fstream>
#include <string>
#include <cstring>
#include <algorithm>

using namespace std;

int main()
{
    string str;
    cin >> str;

    int strlen;
    strlen = str.length();
    cout << strlen << endl;

    char ch1[200];          //string of the original ciphertext;
    strcpy_s(ch1, str.c_str());     //turn the string to char[];

    //Kasiski examination;
    int i, j;
    char ch2[200];          //store the char[] after moving;
    int count[26];          //store the number of the same alphabets of the original ch
ar[] after moving;
    for (j = 0; j < 26; j++)
    {
        count[j] = 0;
        for (i = 0; i < strlen; i++)
        {
            ch2[i] = ch1[(i + j) % strlen];
            if (ch1[i] == ch2[i])
            {
                count[j]++;
            }
        }
        cout << j << "\t" << count[j] << endl;
    }

    //Frequency Analysis;
    int count2[3][26];
    int temp;
    for (i = 0; i < 3; i++)         //Initialize;
    {
        for (j = 0; j < 26; j++)
        {
            count2[i][j] = 0;
        }
    }
    for (i = 0; i < strlen; i++)    //frequency sum;
    {
        count2[i%3][ch1[i]- 'a']++;
    }
    for (i = 0; i < 3; i++)
    {
        for (j = 0; j < 26; j++)
        {
            cout << char('a'+j) << "\t" << count2[i][j] << "\t";
        }
```

```
            cout << endl;
        }

        cout << "Key: cat" << endl;

        for (i = 0; i < strlen; i+=3)       //decode;
        {
            ch1[i] = char((ch1[i] + 26 - 'c') % 26 + 'a');
            ch1[i+2] = char((ch1[i+2] + 26 - 't') % 26 + 'a');
        }

        for (i = 0; i < strlen; i++)    //output the plaintext;
        {
            cout << ch1[i];
        }

        system("pause");
    }
```

3. 古典密码

3.1 密码分析

密文: MAL TIRRUEZF CR MAL RKZYIOL EX MAL OIY UAE RICF “MAL ACWALRM DYEUPLFWL CR ME DYEU MAIM UL IZL RKZZEKYFLF GH OHRMLZH”

1.密文中多次出现”MAL”三字符单词，推测英文行文规律应该为”the”; ‘M’->’t’, ‘A’->’h’, ‘L’->’e’ ;
2.密文中出现了”MAIM”由上已知为”th_t”，由于一般密码不会相同字符，因此推测’I’->’a’;
3.密文中出现”IZL”由上已知为”a_e”,推测为”are”,’Z’->’r’;
4.密文中出现”UL”由上已知为”_e”,且其后跟着“are”，推测为”we”, ‘U’->’w’;
5.密文中出现”ME”由上已知为”t _”二字符单词，推测为”to”, ‘E’->’o’;
6.密文中出现”EX”由上已知为”o_”二字符单词,推测为”of”, ‘X’->’f’;
7.密文中出现”CR”为二字符单词，推测为”is “, ‘C’->’i’, ‘R’->’s’;
8.密文中出现”RICF”由上已知为”sai_”,且其后跟着“，推测为”said”, ‘F’->’d’;
9.密文中出现”TIRRUEZF”由上已知为”_assword”,，推测为”password”, ‘T’->’p’;
10.密文中出现”OIY”为三字符单词，前连接“the”与“who”，为一人称，推测为”man”,’O’->’m’, ‘Y’->’n’;
11.密文中出现”ACWALRM”由上已知为”h i _h e s t”, 推测为”highest”, ‘W’->’g’;
12.密文中出现”DYEUPLFWLF”由上已知为”_ n o w _ e d g e”,，推测为”knowledge”, ‘D’->’k’,’P;->’l’;
13.密文中出现”RKZZEKYFLFF”由上已知为”s _ r r o _ n d e d”,，推测为”surrounded”, ‘K’->’u’;
14.密文中出现”TIRRUEZF”由上已知为”_assword”,，推测为”password”, ‘T’->’p’;
最后经过统计得出未被采用的字母为b,c,d,j,q,v,x,y,z ,其中“GH”，推测为”by”, ‘G’->’b’,’H’->’y’;

MAL	TIRRUEZF	CR	MAL	RKZYIOL	EX	MAL	OIY	UAE	RICF	"MAL	ACWALRM	DYEUPLFWL	CR	ME	DYEU	MAIM	UL	IZL	RKZZEKYFLF	GH	OHRMLZH
the			the	_____t		the		_h_		"the	h_he_t	_____e__e		t_		tb_t	_e	__e	_____e_		___te__
the	_a_____		the	____a_t		the	_a_	_h_	_a__	"the	h_he_t	_____e__e		t_		that	_e	a_e	_____e_		___te__
the	_a____r_		the	__r_a_t		the	_a_	_h_	_a__	"the	h_he_t	_____e__e		t_		that	_e	are	__rr____e_		___ter_
the	_a__w_r_		the	__r_a_t		the	_a_	wh_	_a__	"the	h_he_t	___w_e__e		t_	___w	that	we	are	__rr____e_		___ter_
the	_a__wor_		the	__r_a_t	o_	the	_a_	who	_a__	"the	h_he_t	__ow_e__e		to	__ow	that	we	are	__rro___e_		___ter_
the	_a__wor_		the	__r_a_t	of	the	_a_	who	_a__	"the	h_he_t	__ow_e__e		to	__ow	that	we	are	__rro___e_		___ter_
the	_asswor_	is	the	s_r_a_t	of	the	_a_	who	saj_	"the	h_hest	__ow_e__e	is	to	__ow	that	we	are	s_rro___e_		__ster_
the	_assword	is	the	s_r_a_t	of	the	_a_	who	said	"the	hi_hest	__ow_ed_e	is	to	__ow	that	we	are	s_rro__ded		__ster_
the	password	is	the	s_r_a_t	of	the	_a_	who	said	"the	hi_hest	__ow_ed_e	is	to	__ow	that	we	are	s_rro__ded		__ster_
the	password	is	the	s_rnamt	of	the	man	who	said	"the	hi_hest	_now_ed_e	is	to	_now	that	we	are	s_rro_nded		m_ster_
the	password	is	the	s_rnamt	of	the	man	who	said	"the	highest	_now_edge	is	to	_now	that	we	are	s_rro_nded		m_ster_
the	password	is	the	s_rnamt	of	the	man	who	said	"the	highest	knowledge	is	to	know	that	we	are	s_rro_nded		m_ster_
the	password	is	the	surnamt	of	the	man	who	said	"the	highest	knowledge	is	to	know	that	we	are	surrounded		m_ster_
the	password	is	the	surnamt	of	the	man	who	said	"the	highest	knowledge	is	to	know	that	we	are	surrounded	by	mystery

MAL	TIRRUEZF	CR	MAL	RKZYIOL	EX	MAL	OIY	UAE	RICF	"MAL	ACWALRM
the			the	_____t		the		_h_		"the	h__he_t
the	_a_____		the	____a_t		the	_a_	_h_	_a__	"the	h__he_t
the	_a____r_		the	__r_a_t		the	_a_	_h_	_a__	"the	h__he_t
the	_a__w_r_		the	__r_a_t		the	_a_	wh_	_a__	"the	h__he_t
the	_a__wor_		the	__r_a_t	o_	the	_a_	who	_a__	"the	h__he_t
the	_a__wor_		the	__r_a_t	of	the	_a_	who	_a__	"the	h__he_t
the	_assword_	is	the	s_r_a_t	of	the	_a_	who	saj_	"the	h__hest
the	_assword	is	the	s_r_a_t	of	the	_a_	who	sajd	"the	hi_hest
the	password	is	the	s_r_a_t	of	the	_a_	who	sajd	"the	hi_hest
the	password	is	the	s_rnamt	of	the	man	who	sajd	"the	hi_hest
the	password	is	the	s_rnamt	of	the	man	who	sajd	"the	highest
the	password	is	the	s_rnamt	of	the	man	who	sajd	"the	highest
the	password	is	the	surnamt	of	the	man	who	sajd	"the	highest
the	password	is	the	surnamt	of	the	man	who	sajd	"the	highest

DYEUPLFWL	CR	ME	DYEU	MAIM	UL	IZL	RKZZEKYFLF	GH	OHRMLZH
_____e__e		t_		th_t	_e	__e	_____e_		___te__
_____e__e		t_		that	_e	a_e	_____e_		___te__
_____e__e		t_		that	_e	are	__r_____e_		___ter_
___w_e__e		t_	___w	that	we	are	__r_____e_		___ter_
__ow_e__e		to	__ow	that	we	are	__rro___e_		___ter_
__ow_e__e		to	__ow	that	we	are	__rro___e_		___ter_
__ow_e__e	is	to	__ow	that	we	are	s_rro___e_		__ster_
__ow_ed_e	is	to	__ow	that	we	are	s_rro__ded		__ster_
__ow_ed_e	is	to	__ow	that	we	are	s_rro__ded		__ster_
_now_ed_e	is	to	_now	that	we	are	s_rro_nded		m _ster_
_now_edge	is	to	_now	that	we	are	s_rro_nded		m _ster_
knowledge	is	to	know	that	we	are	s_rro_nded		m _ster_
knowledge	is	to	know	that	we	are	surrounded		m _ster_
knowledge	is	to	know	that	we	are	surrounded	by	mystery

3.2 破解结果

明文: the password is the surname of the man who said “the highest knowledge is to know that we are surrounded by mystery”.
结果: Schweitzer (the surname of Albert Schweitzer)