网络道德安全教育

总主编 李 辛
本册主编 李 辛

高二

下册

中国出版集团
世界图书出版公司

网络道德安全教育

高二

下册

总主编　李　辛
本册主编　李　辛
编　　者　李　靖　梁　萌　蒋　帅　李　欣

中国出版集团
世界图书出版公司

图书在版编目(CIP)数据

网络道德安全教育. 高二. 下册/李辛主编. —西安:世界图书出版西安有限公司,2016.1

ISBN 978-7-5192-0718-2

Ⅰ. ①网… Ⅱ. ①李… Ⅲ. ①计算机网络—道德规范—高中—教学参考资料 ②计算机网络—安全技术—高中—教学参考资料 Ⅳ. ①G631.6 ②G634.673

中国版本图书馆 CIP 数据核字(2016)第 024791 号

网络道德安全教育——高二 下册

策　　划	霍小燕
总 主 编	李　辛
本册主编	李　辛
责任编辑	李志刚
封面设计	新纪元文化传播
出版发行	世界图书出版西安有限公司
地　　址	西安市北大街 85 号
邮　　编	710003
电　　话	87233647(市场营销部) 029-87235105(总编室)
传　　真	029-87279675　87279676
经　　销	全国各地新华书店
印　　刷	西安金鼎包装设计制作印务有限公司
成品尺寸	185mm×260mm　1/16
印　　张	6
字　　数	80 千
版　　次	2016 年 1 月第 1 版　2016 年 1 月第 1 次印刷
书　　号	ISBN 978-7-5192-0718-2
定　　价	12.00 元

前言
PREFACE

写给同学们的话

亲爱的同学们：

时间总是过得很快，你们已经成为了高中学生。岁月增添的不仅仅是年龄，更应该是阅历、视野与知识。

在数字时代，上网已经成为人们常态化的生活方式。对于互联网，作为高中生的你，不应是小学时的懵懂和好奇，也不应是初中时的幼稚和盲从，而应该是成熟、理性和智慧。

是的，网络为我们提供了张扬个性、发展自我的舞台；提供了触摸科学、增长知识的窗口；提供了高效交流、便捷生活的平台……遥不可及的远方，已经成为近在咫尺的比邻；危险抽象的化学实验，已变成眼前绚丽绽放的视频；空洞宽泛的理论，已建构成生动形象的模型……

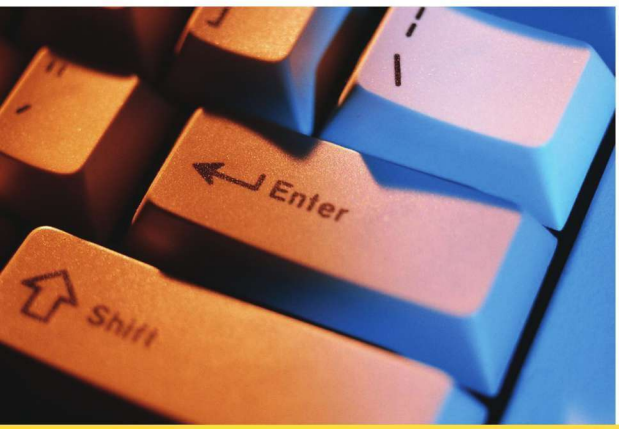
快速发展的信息技术，为我们的数字生活增添了无以伦比的新体验，等待着我们去了解、去学习、去掌握。密码学为我们展现了人类的非凡智慧，云计算和大数据开阔了我们的思维天地，电子商务、物联网、可穿戴设备则构成了现代化社会的基本组成。

然而，绝对美好而又无害的事物是不存在的。科技的发展也同步带来了种种弊端，而网络安全与道德则首当其冲。面对这些新问题、新矛盾，没有科学、没有技术则没有安全。我们要通过学习和实践，了解网络技术的科学原理，掌握网络应用的技术方法，做一个有知识、有能力，维护网络安全与文明的践行者和维护者，成为符合网络社会要求、有责任意识的新时代公民。

这些，你们能做到吗？

编者

2015 年 9 月



第一单元

信息安全的核心：密码技术

第一节 古典密码

神秘的古代圆盘

在人类历史上，对信息保护的需求与对信息本身一样久远。右图是在克里特岛的一间小破屋里发现的 Phaistos 圆盘，一个直径约为 160mm 的黏土圆盘，表面有明显字间空格的字母。虽然它被很多科学家研究过，但至今还是无法破译它上面的那些象形文字。专家们只能大致推论出它的时间大约在公元前 1700 ~ 公元前 1600 年之间。

● 凯撒大帝的制胜法宝——凯撒密码

古典密码也可以称为“凯撒密码”，它是古罗马凯撒大帝在传递重要军事情报时，所使用的一种加密方法。

在加密过程中，需要发送的信息原文称为明文，明文经过加密后形成的不被识别的信息称为密文。

古典密码采用的是简单的“字符换位”加密技术。它是将明文中的每个字母，用其后面的字母来替换，产生字面上没有任何意义的密文。

比如，凯撒大帝向正在前线作战的部队发出了密文“VWRSDWWDFNLQJ”，同时附带另一条指令：“前进 3 步。”这条密文代表什么意思呢?

“前进 3 步”非常重要，它的含义是把密文中的每个字母按字母表的顺序向

后移动 3 个字母进行对位。即有如下的对应关系：

明	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
密	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

因此，我们可以推算出，凯撒命令的明文是“STOPATTACKING”（停止进攻）。

若给每个字母一个整数编号，就可以得到一个数字密码本：

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

“前进 3 步”中的“3”，指明了明文字母与密文字母的错位数。实际上，只要有了“3”，通过上述的整数编号，就可以用一个“取模运算”来表示整个密码本：

密文字母 =（明文字母 +3）mod 26

mod 运算称为取模运算，即求余数的运算，它的表示形式是“n mod p”，其运算结果是一个整数 n 除以另一个整数 p 的余数，且不考虑运算的商。因此，上述算式的含义是：将代表明文字母的数字加上 3，再除以 26，就得到了代表密文字母的数字，反推出字母。

例如，表示明文字母 S 的数字是 19，加 3 后再除以 26，商为 0，余数为 22，即（19+3）mod 26 = 22，因此，S 的密文字母应该是数字为 22 的 V。

根据数字密码本，可以先将明文的文字串“STOPATTACKING”置换成数字串“19 20 15 16 1 20 20 1 3 11 9 14 7”，再按照运算公式对这个数字串进行加密，得到密文“22 23 18 19 4 23 23 4 6 14 12 17 10”。

● “芝麻开门”开启藏宝秘洞——密钥

如果将上式中的错位数“3”用变量 K 表示，就会得到凯撒密码的通式：

密文字母 =（明文字母 +K）mod 26

很显然，通式中的 K 非常关键，它像一把“钥匙”，用来进行加密和解密，

因此，我们将 K 称为“密钥”。

凯撒密码的核心是建立一个置换表。加密时，通过查表将明文中的字符置换为对应的密文字符。在加密过程中只使用了一个置换表，因此可称为“单表置换”。在单表置换中，同一个明文字母总是对应着同一个密文字母。因此，它结构单一，非常容易被人破译，安全性很差。

随后，产生了古典密码中的另外一种类型——维吉尼亚密码。

● 闪转腾挪匿影藏形——维吉尼亚密码

维吉尼亚密码是一种多表置换密码。多表置换密码是对单表置换密码的改进，把密钥由一位整数换成了一个单词，并且同一个字母在明文中的不同位置，会对应不同的密文字母。比如，字母 E 在一个位置可能被 M 所置换，而在另一个位置则有可能被 K 所置换。这样就增加了密钥的复杂度，提高了密码的安全性。下图是一个维吉尼亚密码表。

比如有明文“DATE SECURITY”，密钥为“BEST”。加密时，先根据密钥的长度，将明文分解成“DATE SECU RITY”三组，然后用密钥“BEST”分别对每一组进行加密。加密时，以明文字母做行、密钥字母做列，查阅维吉尼亚密码表，得出密文。

比如第一组明文“DATE”，行上的明文字母“D”，对应列上的密钥字母“B”，可得到密文“E”；行上的明文字母“A”，对应列上的密钥字

	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	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
b	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
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
d	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
e	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
f	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
g	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
h	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
i	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
j	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
k	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
l	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
m	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
n	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
o	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
p	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
q	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
r	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
s	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
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
u	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
v	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
w	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
x	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
y	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
z	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

维吉尼亚密码表

母“E”，得到密文“E”。以此类推，得到明文“DATE”的密文是“EELT”，“SECU”的密文是“TIUN”……最后的密文是“EELTTIUNSMLR”。

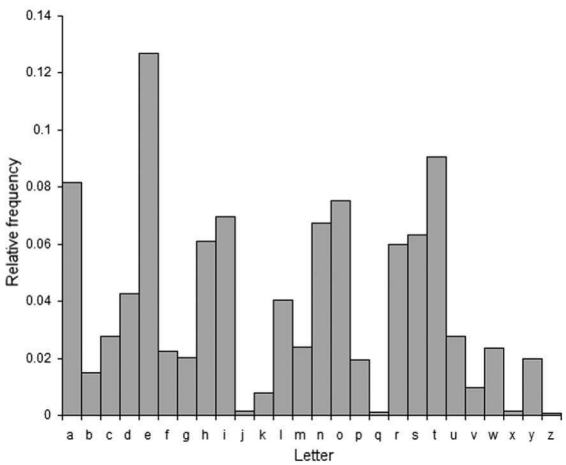
可以看出，古典密码的核心思想是“置换”，也就是构造明文与密文之间的变换关系。

● 古典密码的克星——统计分析方法

古典密码非常容易利用统计分析的方法进行破解。

在凯撒密码中，同一个明文字母总是对应着同一个密文字母，也就是说，明文字母与密文字母的出现频率是相同的。由于英文中字母出现的频率相对稳定，因此，可以从大量密文中统计出各个字母出现的频率，与英文统计频率表相比较，推断出明文字母。

比如，在密文中出现次数最多的字母，极有可能代表了字母“E”；第二多的应该是“T”……这样，只需找出几个字母，便能够分析出密文的密钥。



英文字母频率

对于维吉尼亚密码，可以通过寻找重复的“字母段”来进行分析。因为在任何比密钥要长得多的密文中，都会不可避免地出现字母段的重复。

比如明文“BETTER TO DO WELL THAN TO SAY WELL”，如果用密钥“FOREST”加密，可得到密文“GSKXWKYCUSOXQZKLSGYCJEQPJZC”。

可以发现，密文中“YC”共出现了两次，从第一个 YC 出现后到第二个 YC 的结尾，共有 12 个字母（USOXQZKLSGYC），那么可以认定密钥的长度是 12

的整除数。换句话，这表示 12 是密钥长度的约数，即密钥长度应该是 1，2，3，4，6，12 中的一个。当得到大量的此类信息后，经过频率分析，就会知道密钥的确切长度，而一旦知道了密钥长度，就可以破译密文。

概念巧记忆

密码 密码是一种用来混淆的技术，它希望将正常的（可识别的）信息转变为无法识别的信息。当然，对一小部分人来说，这种无法识别的信息是可以再加工并恢复的。密码按特定法则编成，用以对通信双方的信息进行明密变换。换言之，密码是隐蔽了真实内容的的符号序列。就是把用公开的、标准的信息编码表示的信息通过一种变换手段，将其变为除通信双方以外其他人所不能读懂的信息编码，这种独特的信息编码就是密码。

探索应用

试着用凯撒加密技术发送信息“Network security”。

第二节 对称分组密码

如果说古典密码只是一种“小聪明”的话，那么现代密码则体现了人类的非凡智慧。依靠高深的数学工具与先进的计算机技术，现代密码已经广泛应用于军事、外交、政务、商务、通信等各个领域，在信息安全方面具有不可替代的作用。

● 一把钥匙　两种用途——对称密码

对称密码属于现代密码中的一种，它的加密与解密都使用了相同的密钥，该密钥必须保密，发送方用该密钥对明文进行加密，然后将密文传输至接收方，接收方再用相同的密钥对收到的密文进行解密。

对称密码的解密密钥可以从加密密钥中推算出来的，反过来也成立。因此，它要求发送者和接收者在安全通信之前，共同商定一个密钥。对称算法的安全性依赖于密钥，密钥一旦被泄漏，就意味着任何人都能对消息进行加密和解密。

对称密码的目标是“扩散”和“混淆”。扩散是让明文中的单个字符影响密文中的多个字符，从而使明文的统计特征在密文中消失，相当于明文的统计结构被扩散；混淆是让密钥与密文之间的关系变得复杂多变，从而增加利用统计方法

进行破解的难度。

对称密码也利用“置换”来进行加密，但这种置换比古典密码的置换要复杂很多。比如，可以按照分组来进行，即“分组密码”。举例如下：

假如有明文“The night gives me black eyes, but I will use it to find the light”，我们可以把整个句子按字母分组，每组 4 个字母，最后一组若不足 4 个则填入空格。然后在每组内按预先设计的密钥（3，1，4，2）进行置换，即组内的第 1 个字母用本组的第 3 个字母置换，第 2 个字母用第 1 个字母置换，第 3 个字母用第 4 个字母置换，最后一个字母用第 2 个字母置换。具体步骤如下：

第一步，将明文每 4 个字母分为一组，得到：

then ight give smeb lack eyes ,but Iwil luse itto find thel ight

第二步，按置换规则（3，1，4，2）进行置换，得到密文：

etnh hitg vgei esbm clka eesy u,tb iilw sleu tiot nfdi etlh hitg

将密文发送后，对方可以利用从加密密钥中推算出的解密密钥（2，4，1，3）对密文进行逆置换，得到明文。

在实际使用中，分组密码并不是只进行一次置换，而是要连续进行多次置换，每一次置换都在前一次的基础上进行，因此，它具有较高的密码强度。分组密码的最大特点是只要明文有微小的改动，都会引起密文的极大变化，也就是说，密文中的每一位依赖于明文中的若干位，这个特性称为“雪崩特性”。

● 重重叠叠　反复搅拌——迭代运算

在分组密码中，明文 M 总是被转换成二进制数，按定长的 2w 位进行分组，然后进行多次的“循环加密”，也就是说，每组的加密将进行 n 轮，每一轮都在上一轮加密的基础上重复运算，并且在每一轮加密中，都将产生新的密钥——子密钥，最终得到密文 E。这个过程称为“迭代”。

为增强扩散与混淆的程度，分组密码采用了复杂的算法：明文被转成二进

制数，将其分成左、右两半 L0 和 R0，进行 n 轮迭代，第 i–1 轮迭代的结果为第 i 轮迭代的起始，即 i–1 轮的输出为第 i 轮的输入，每迭代一次都将 L0 和 R0 的内容进行交换。迭代完成后，将左、右两部分合并到一起，就是最终的密文。

凯撒密码轮

在加密过程中，密钥也参与了迭代运算，每 i 轮迭代使用子密钥 ki，而 ki 则由初始密钥 k0 经过迭代生成。只要初始密钥不被泄露，即便公开加密算法，别人也无法得到密钥。

● 成竹在胸　一招制胜——DES 算法

典型的分组密码算法是 DES 算法。DES 使用了 16 轮迭代，运用了异或、置换、移位等基本运算方法。其大致过程为：首先将明文转成二进制数，再以 64 bit 为长度进行分组，按置换规则对每组进行初始置换，再将 64 bit 分割成 L0 和 R0 两半，通过特定的算法对 L0 和 R0 进行运算，接着交换 L0 和 R0，以此结果作为下一轮的起始，对第 2 轮到第 16 轮进行相同的运算，最后进行与初始置换相反的逆置换，两部分合并后得到密文。

在开始运算时，需要为 DES 算法提供初始密钥，密钥可以是长度为 56 位的任意数。每一轮迭代都将产生一个与上一轮不同的子密钥，作为这一轮迭代的新密钥。

与以往的加密算法不同的是，DES 的解密算法并不是加密算法的逆运算，而是与加密算法完全相同，只不过是密钥的次序恰好相反。如果各轮迭代中加

密密钥分别是 K1，K2，K3，……，K16，那么解密的密钥就依次是 K16，K15，K14，……，K1。

DES 的特点是加密速度较快，适用于加密大量数据的场合。

以前的密码体制，算法和密钥都是需要高度保密的，算法设计者总是千方百计地掩盖具体的加密过程，而 DES 的置换规则和加密算法则是公开的。因为到目前为止，除了穷举法以外，还没有发现其他更有效的攻击方法。对于密钥的 56 位长二进制数，其穷举空间是 256，根据当今计算机的处理速度和能力，56 位长度的密钥已经有可能被破解，而 128 位的密钥则被认为是安全的，但随着时间的推移，这个数字也迟早会被突破。

除了 DES 算法以外，属于对称分组密码的还有 AES 算法，它的设计思路与 DES 基本相同，也要经过 n 轮迭代，但每轮的处理算法不一样，并且分组长度与密钥长度可以灵活组合，因此，AES 具有比 DES 更高的安全性。

● 简便灵巧　随处可用——轻量级分组密码

可以看出，无论是 DES 还是 AES，都属于计算复杂、规模较大的密码算法。而手机、无线射频（RIFD）、无线传感器、U 盾、智能卡等微型便携设备，其计算能力、蓄电能力、内存空间是非常有限的，因此，需要设计简便、高效的密码算法，使其能在消耗极小的硬软件资源和能耗的前提下，达到期望的安全值。这种算法就是所谓的“轻量级分组密码”。

轻量级分组密码仍然保持了分组密码的设计思路，但它的显著特征是密钥的长度相对较短，算法结构简单。轻量级分组密码采用了“折中”的设计思想，目标是在安全性和执行效率之间找到最佳平衡点，应用于计算能力弱、存储空间小、能耗低和安全级别适中的环境，并且主要通过硬件来实现。

概念巧记忆

异或运算 异或是一个数学运算符。它应用于逻辑运算。异或的数学符号为“⊕”，计算机符号为“xor”。其运算法则为：如果 a、b 两个值不相同，则异或结果为 1；如果 a、b 两个值相同，异或结果为 0。即：

a	b	异或值
0	0	0
1	0	1
1	1	0
0	1	1

移位运算 移位运算就是在二进制的基础上对数字进行平移。运算规则为：当向左移动时，高位移出（舍弃），低位的空位补零；当向右移动时，低位移出（舍弃），高位的空位补充符号位，即正数补零，负数补 1。

探索应用

在对称密码中，密钥只能由加密者和解密者所知晓。如果有 100 个人，你能算出他们两两之间需要多少个互不相同的密钥吗？

第三节 公开密钥密码

在对称密码中，如果在两个用户之间进行通信，只需要 1 把密钥，如果在三个用户间两两通信而又不能使用相同的密钥，则需要 3 把密钥，同样的道理，若用户数是四个，则需要 6 把密钥……

假如用户数为 n，则需要的密钥数可由排列组合公式得出：

$$C_n^2=\frac{n(n-1)}{2}$$

由计算得知，当 n=100 时，需要 4950 个密钥，当 n=1000 时，密钥数增加到 499500 个。可以想象，随着用户数的增多，密钥的数量会急剧增大，使得密钥的产生、分配和管理都出现问题。

● 两把钥匙　各司其职——公钥与私钥

我们来看这样一个假设：如果有两个人需要用电子邮箱进行通信，而这个邮箱不需要任何密码就能够直接进入，这两个人该怎样保证邮箱里的信件不被第三个人看到呢？

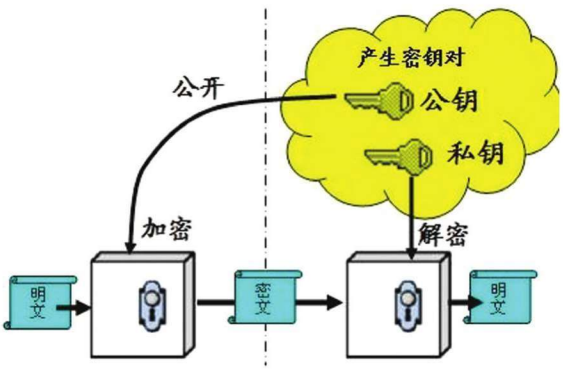
在这种情况下，为保证通信安全，邮箱的地址就不能被第三个人知道。因此，可以把邮箱地址看作双方共有的密钥。照此方法，我们与每一位联系人都要单独建立一个邮箱，这种情形显然是不可思议的。

实际上，无论与多少人通信，我们只需要一个邮箱就可以了，邮箱地址可以对外公开，任何人都可以向邮箱内发送邮件，而打开邮箱则需要一个私人密码，这个密码只有邮箱的主人知道。

因此，对于一个邮箱来说，我们相当于拥有两个密钥，一个是可以公开的邮箱地址，另一个是需要保密的私人密码。

邮箱地址类似于公开密钥，而私人密码则类似于私密密钥。这种密码体系称为“公开密钥密码体系”。

与对称密码不同的是，公钥密码要求密钥必须成对出现，一个为加密密钥，另一个为解密密钥，且不可能从其中一个推导出另一个。私钥由拥有者自己秘密保存，而公钥则可以公布于众。



公钥与私钥的不同作用

公钥与私钥有着紧密的联系，任何用公钥加密的信息，只能通过与其对应的私钥进行解密，反过来也一样。当用公钥加密时，可用于信息保密，当用私钥加密时，可实现“数字签名”的功能。

假设有合法用户 A、B、C 三人和一名非法“窃听者”E，并且 A 利用算法生成了自己的公钥和私钥，则可以有以下使用方法：

1. A 可以将公钥分发给其他可信任的人，比如 B 和 C；

2. A 可以使用私钥对信息进行加密，将密文发送给 B 和 C，由于 A 是唯一拥有私钥的人，因此，B 和 C 用收到的公钥解密出来的任何信息，都可以确认其一定来自 A，这就是“数字签名”；

3. B 可用收到的公钥解密 A 发出的密文，如果他想给 A 和 C 发送信息，可以使用该公钥进行加密。此时，A 可以用私钥对密文进行解密，但 C 由于没有与