第二讲 密码学发展及其应用

白杨 alicepub@163.com

第二讲 密码学发展及其应用

① 密码学重要意义

② 密码学发展历史

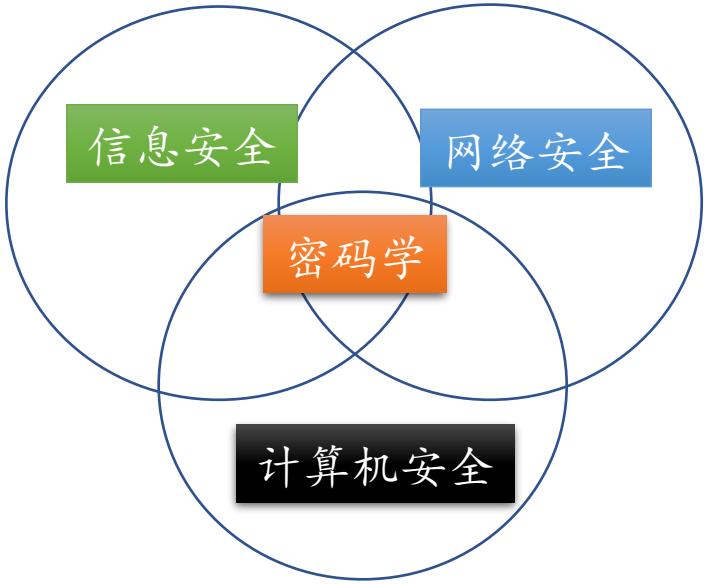
③ 密码学基本概念

④ 密码算法

⑤ 网络空间安全中的密码学应用

密码学与网络空间安全

密码学是实现网络空间安全的重要组成部分，是核心基础技术之一



信息论　系统论　...

计算机理论　控制论

数学（代数、数论、概率统计、组合数学、博弈论）

网络空间安全基础理论

应用安全

系统安全

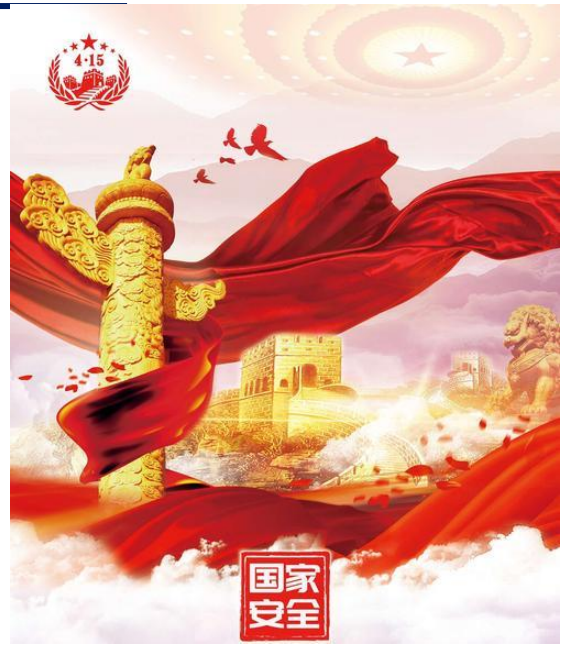
网络安全

密码学及应用

密码学是网络空间安全的核心基础技术

■网络空间安全的重要性

网络空间安全关乎国家战略层面的安全，是继陆、海、空、天后的第五疆域。没有网络安全就没有国家安全，没有信息化就没有现代化



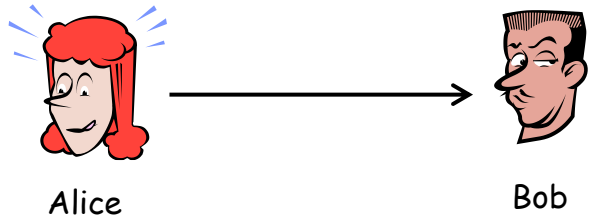
传统密码学主要用于保密通信，基本目的是使得两个在不安全信道中通信的实体，以一种使其敌手不能明白和理解通信内容的方式进行通信。

现代密码技术及应用已经涵盖数据处理过程的各个环节，如数据加密、密码分析、数字签名、身份识别、零知识证明、秘密分享等。以密码学为核心的理论与技术来保证数据的**机密性、完整性、可用性等安全属性。**

密码学是网络空间安全的核心基础技术

安全三大问

- Alice/Bob：和我通信的真的是Bob/Alice吗？**（数据原发性）**钓鱼网站伪装攻击
- Bob：我收到的信息是Alice发给我的原始信息吗？有没有被人篡改过？**（数据完整性）**信息内容被篡改
- Alice/Bob：我和Bob/Alice的通信内容有没有被别人窃听到？**（数据保密性）**信息内容被窃去



使用消息认证码或者数字签名技术可以解决问题1(数据源的认证)和问题2(数据完整性)

使用加密技术可以解决问题3(数据的保密性)

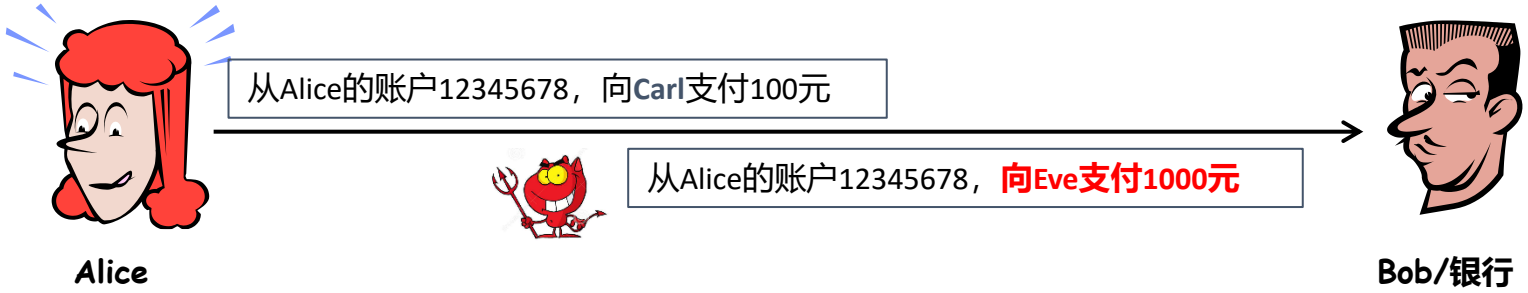
➢数据原发性

- 钓鱼网站或伪装攻击

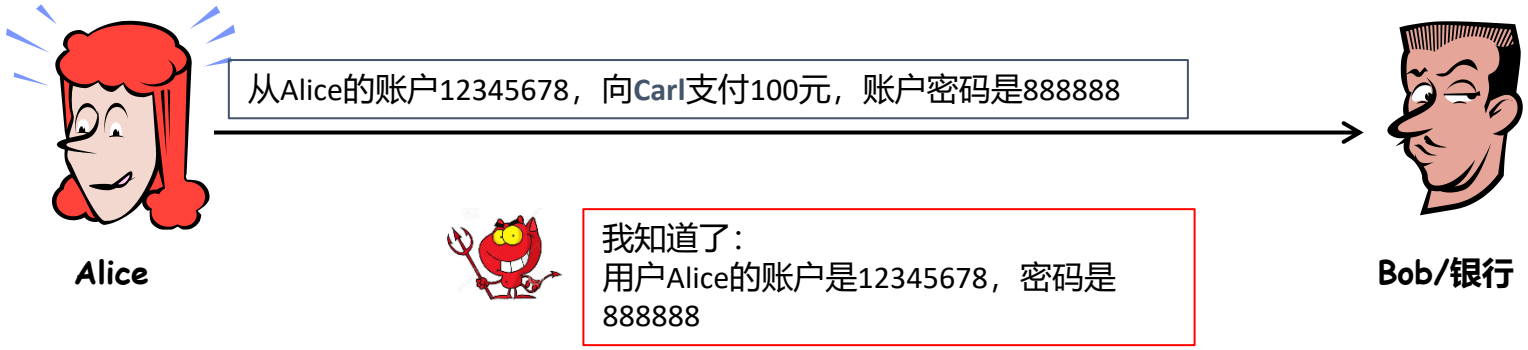
钓鱼网站示例（遨游浏览器）

➢数据完整性与保密性

- 攻击者修改消息内容



- 攻击者窃听获得消息内容



➢解决方法

一．数据保密性

使用加密技术可以解决

二．数据源与数据完整性认证（包含从某个声称的消息源到接收者的传输过程，该接收者在接收时会验证消息）

① 接收方执行消息验证的目的在于确认消息发送者的身份，防止冒充合法用户发送消息。

② 接收方执行消息验证的目的还在于确认收到的消息是否完整(离开消息源之后没有被篡改)。

③ 验证的进一步目的是验证消息的鲜活性(消息是否第一次从正确的消息源被发送出来的)。

④ 使用数字签名技术（非对称密码的应用）或消息认证码可解决。

密码学是网络空间安全的核心基础技术

■ 信息安全三要素

通过以密码学为核心的理论与技术来保证数据的机密性、完整性、可用性等安全属性。

信息安全三要素

- 机密性 confidentiality → **信息不泄漏给非授权的用户、实体或者过程；**
- 完整性 integrity → **数据未经授权不能被改变**，即信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等操作所破坏；
- 可用性 availability → 保证信息和信息系统**可被授权实体访问并按需求使用**的特性，即当需要时应能存取所需的信息。

第二讲 密码学发展及其应用

① 密码学重要意义

② 密码学发展历史

③ 密码学基本概念

④ 密码算法

⑤ 网络空间安全中的密码学应用

密码学是网络空间安全的核心基础技术

■ 密码学发展历史

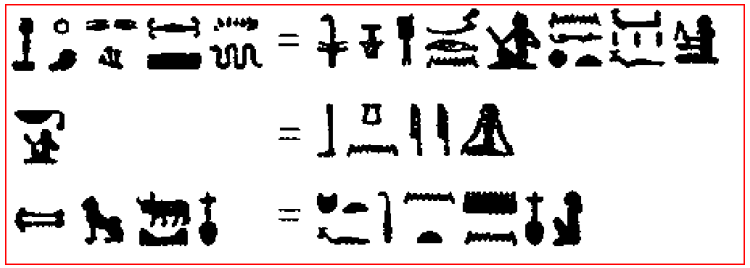
密码学（cryptology）是一门既古老又现代的学科。**作为数学、计算机、电子、通信、网络等领域的一门交叉学科**，从几千年前具有神秘性和艺术性的字谜，到广泛应用于军事、商业和现代社会人们生产、生活的方方面面的现代密码学，密码学逐步从艺术走向科学。

密码学发展经历了四个阶段：

- **古典密码**，从古代到19世纪末，“凯撒密码”、采用替代和置
- **近代密码**，20世纪初到1949年，机械密码机、机电密码机
- **现代密码早期**，从1949年到1975年，密码学从此开始成为一门科学
- **现代密码之公钥密码**，1976年开始一直延续至今，Diffie和Hellman提出了公钥密码的思想，数据加密标准（Data Encryption Standard，DES）

第一阶段：古典密码 —— 历史起点

大约在4000年以前，在古埃及的尼罗河畔，一位擅长书写者在贵族的基碑上书写铭文时有意用加以变形的象形文字而不是普通的象形文字来写铭文，从而揭开了有文字记载的密码史。这篇颇具神秘感的碑文，已具备了密码的基本特征：把一种符号(明文)用另一种符号(密文)代替。

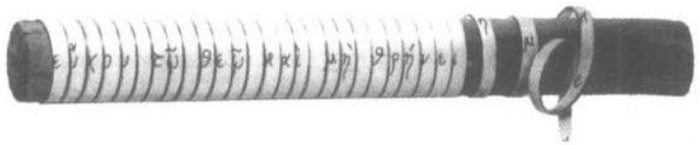


■ 有文字记载的最早密码

加密规则：

将纸带呈螺旋形地、无缝地缠绕在约定直径的圆筒上

将消息按正常顺序直接书写在圆筒上，取下纸带



解密规则：

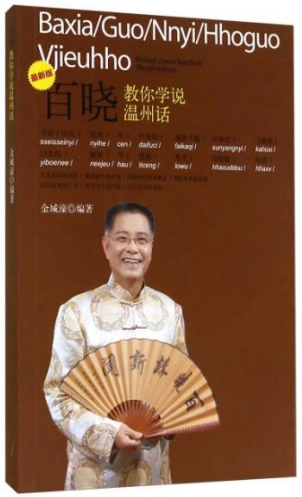
将纸带呈螺旋形地缠绕在约定直径的圆筒上，读出消息原文

第一阶段：古典密码 —— 中国3000年前

- 古中国周朝兵书《六韬．龙韬》也记载了密码学的运用，其中的《阴符》和《阴书》便记载了周武王问姜子牙关于征战时与主将通讯的方式

第一阶段：古典密码 —— 语言密码

- **其实，语言也是一种密码**
  - 印第安纳瓦霍族土语：太平洋战争中，印第安纳瓦霍族人用土语传递消息（《风语者》）
  - 江山话：二战中用江山话传递信息。
  - 温州话：越战中，我国军队采用温州话传递消息
  - 四川话？上海话？

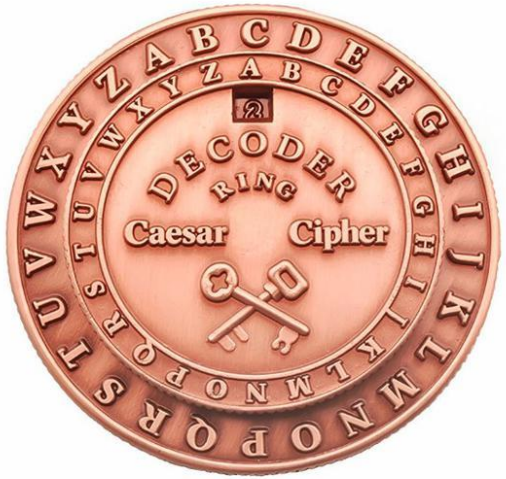


第一阶段：古典密码 – 凯撒密码

加密规则：

明文中的所有字母都在字母表上向后按照一个固定数目进行**偏移后**，被替换成密文移动位数是秘钥

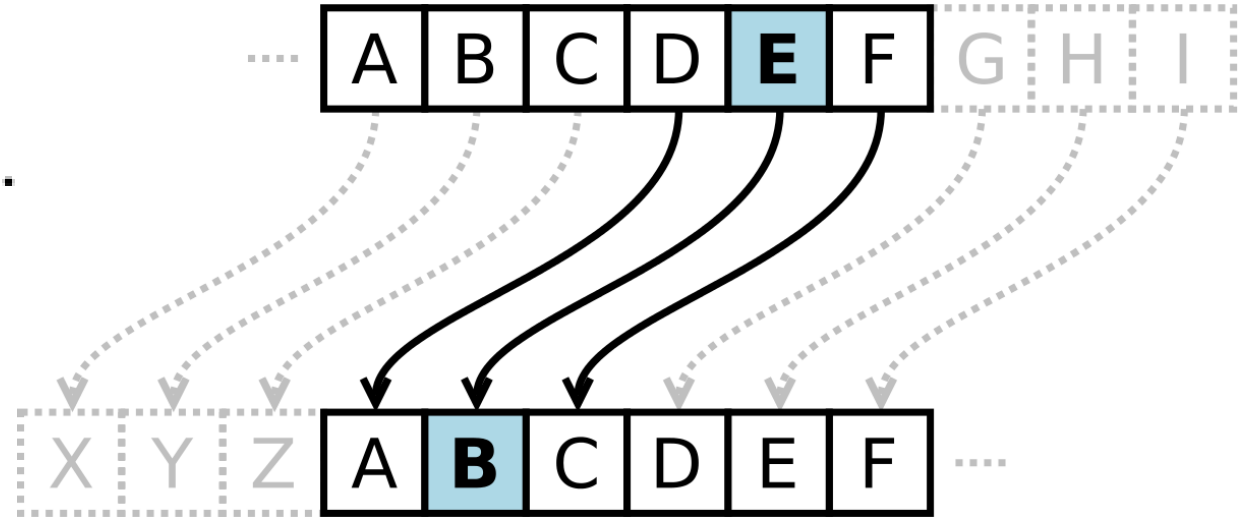
$$E_n(x) = (x + n) \mod 26.$$



解密规则：

将密文进行反方向偏移

$$D_n(x) = (x - n) \mod 26.$$



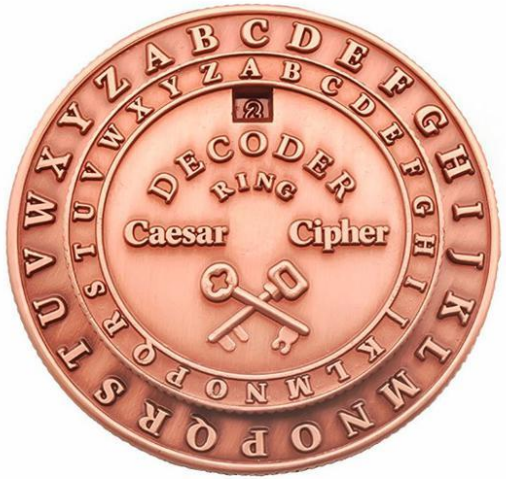
第一阶段：古典密码 – 凯撒密码

明文字母表：

ABCDEFGHIJKLMNOPQRSTUVWXYZ

密文字母表：

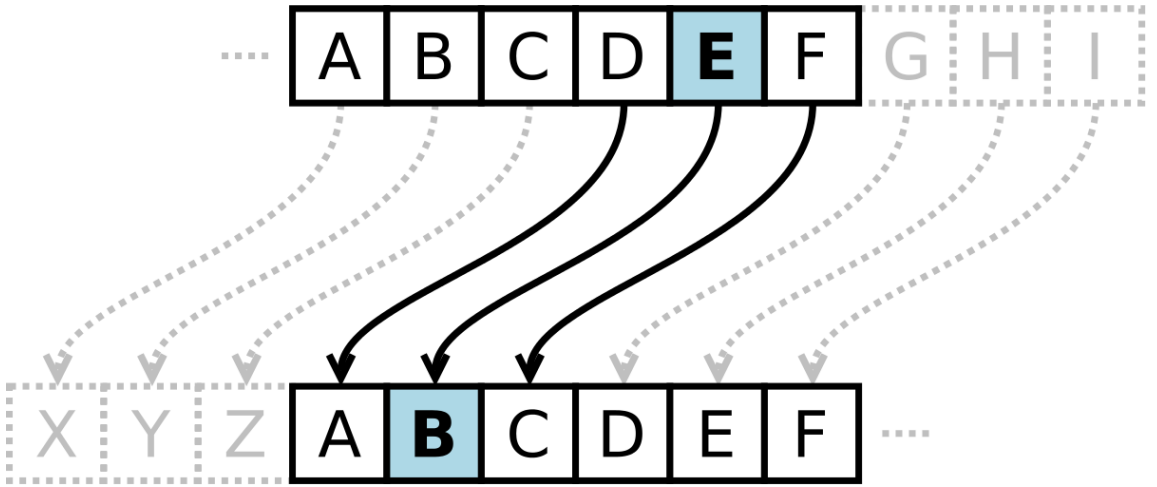
DEFGHIJKLMNOPQRSTUVWXYZABC



明文：FIGHTING

密文：？？？算算看

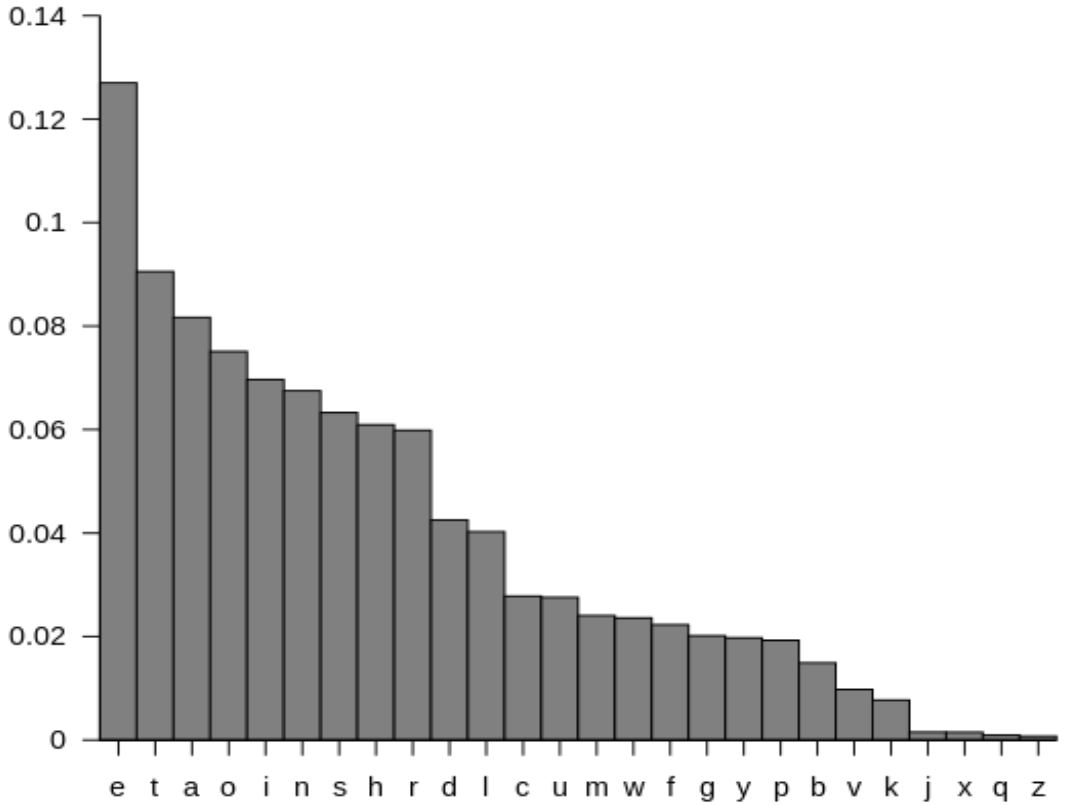
ILJKWLQJ



第一阶段：古典密码 – 凯撒密码

凯撒密码是一种比较简单的古典密码，仅仅将明文的每个字符偏移相同的偏移量，在密文较多的情况下，这种方式的加密破译起来非常简单。

可以通过字频统计找出每个字母出现的频率，然后根据对应的字频统计图直接找出密文字母对应的明文，然后计算出偏移量，对所有字符统一进行解密即可。

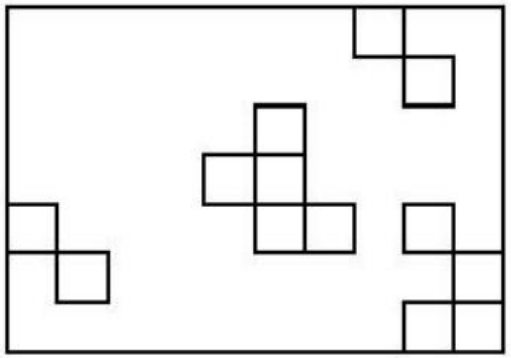


第一阶段：古典密码 —— 卡尔达诺漏格板

- 漏格板是一张用硬质材料(如硬纸、羊皮、金属等)做成的板，上面挖了一些长方形的孔，即漏格。
- 16世纪中期，意大利的卡尔达诺发明了卡尔达诺漏格板，覆盖在密文上，可从漏格中读出明文，这是较早的一种分置式密码

情书

I LOVE YOU
I HAVE YOU
DEEP UNDER
MY SKIN MY
LOVE LAST S
FOREVER IN
HYPERSPACE



追杀令：YOU KILL AT ONCE

I LOVE YOU
I HAVE YOU
DEEP UNDER
MY SKIN MY
LOVE LAST S
FOREVER IN
HYPERSPACE

自从人类有了战争，就有了密码。历史上的战争，特别是两次世界大战对于保密学的理论技术的发展起了巨大的推动作用。从手工加密，到机械加密，到计算机加密。从基于算法安全，到基于密钥安全，从面向贵族到面向平民。

第一阶段：古典密码 - 维吉尼亚密码

- 多表替换密码,抗击频率分析
- 意大利学者贝拉索1553年发明
- 维吉尼亚在1586年的改进（**久而久之，贝拉索密码就被叫成了维吉尼亚密码**）
  - 加密： $C_i \equiv P_i + K_i \pmod{26}$.
  - 解密： $P_i \equiv C_i - K_i \pmod{26}$.

  例如：

  明文：“Common sense is not so common.”

  密钥：“PIZZA”

  密文：“Rwlloc admst qr moi an bobunm.”

	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

- 查尔斯-巴比奇（Charles Babbage，1791-1871）英国数学家，于1854年成功破解了维吉尼亚密码，结束了维吉尼亚**200多年**的神话。

第一阶段：古典密码 – 维吉尼亚密码

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

设n=6，密钥是cipher,这相应于密钥k=(2,8,15,7,4,17),明文是“this cryptosystem is not secure”（明文用小写字母表示），试用（Vigenere）密码对其加密（密文用大写字母表示）。

t	h	i	s	c	r		y	p	t	o	s	y
19	7	8	18	2	17		24	15	19	14	18	24
2	8	15	7	4	17		2	8	15	7	4	17
21	15	23	25	6	8		0	23	8	21	22	15
V	P	X	Z	G	I		A	X	I	V	W	P

第一阶段：古典密码 – 维吉尼亚密码

s	t	e	m	i	s		n	o	t	s	e	c
18	19	4	12	8	18		13	14	19	18	4	2
2	**8**	**15**	**7**	**4**	**17**		**2**	**8**	**15**	**7**	**4**	**17**
20	1	19	19	12	9		15	22	8	25	8	19
U	**B**	**T**	**T**	**M**	**J**		**P**	**W**	**I**	**Z**	**I**	**T**

u	r	e										
20	17	4										
2	**8**	**15**										
22	25	19										
W	**Z**	**T**										

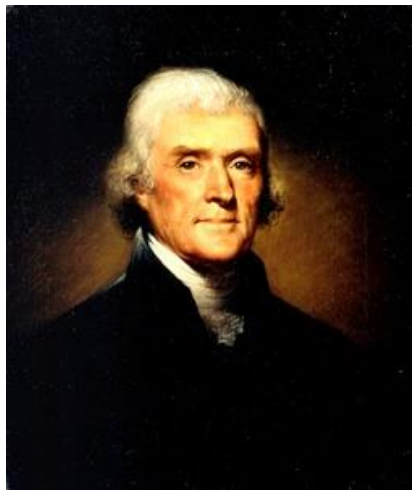
密文

VPXZGIAXIVWPUBTT
MJPWIZITWZT

第一阶段：古典密码 - 维吉尼亚密码

- 多表替换密码，意大利学者贝拉索1553年发明，维吉尼亚在1586年的改进（久而久之，贝拉索密码就被叫成了维吉尼亚密码）。
- 通过多套字符加密明文来混淆字母出现的频率，抗击频率分析。
- 查尔斯-巴比奇（Charles Babbage，1791-1871），英国数学家，于1854年成功破解了维吉尼亚密码，结束了维吉尼亚200多年的神话。在计算上，第一次提出完整破解维吉尼亚加密的方法，是在1863年，由弗里德里希·卡西斯基提出，这套方法也被成为卡西斯基试验。“相同的明文字母组，在明文序列中间隔的字母数为d（d是密钥的长度）的倍数时，则明文字母组对应的密文字母组也必相同. 反之则不一定，但相同的概率很大. 如果将密文中相同字母组找出来，并对其间隔的距离进行研究，找出它们的最大公因子，则该因子是密钥长度的概率是较大的。”寻找重复出现的字母序列，并求其长度的过程被称为Kasiski试验。
- https://zhuanlan.zhihu.com/p/386388707（如何破解维吉尼亚密码）

第二阶段：近代密码－机械密码



第三任美国总统杰弗逊对密码学很有研究，于1795年发明了一种加密装置，被称为“杰弗逊圆盘”，或叫做“杰弗逊转轮加密器”（Jefferson wheel cipher）。这个装置有36片同样大小的木制转轮，套在一根铁杆上，每片转轮上的圆周边缘上刻有乱序的26个英文字母表。进行秘密通信的双方必须各自拥有完全一样转轮加密器。

第二阶段：近代密码－机械密码

当要把一段文字（不超过36字）秘密通知对方时，只需转动加密器上的各片转轮，使这段文字正好出现在同一行上，这时转轮上排列的其他25行都是无意义的乱码；此时发信人抄写其中任意一行的乱码，关交给信使传送（加密）。对方收到乱码信后，只需拿出自己保存的同样的装置，转动上面各片转轮，让它们的排列使得这段乱码正好出现在同一行上，然后他查看其他25行上的内容，其中必然有一行会显示出真正的信息（解密）。

杰弗逊加密器属于“多表替换”型加密，很难被破解，除非能得到加密装置。据说美国军队直到上世纪60年代仍然在使用。当然，这种加密器的缺点也是很明显的，即它每次只能传送简单的信息（字长不能超过转轮的片数），而且参与通信的各方不能太多。

第二阶段：近代密码－电子机械密码

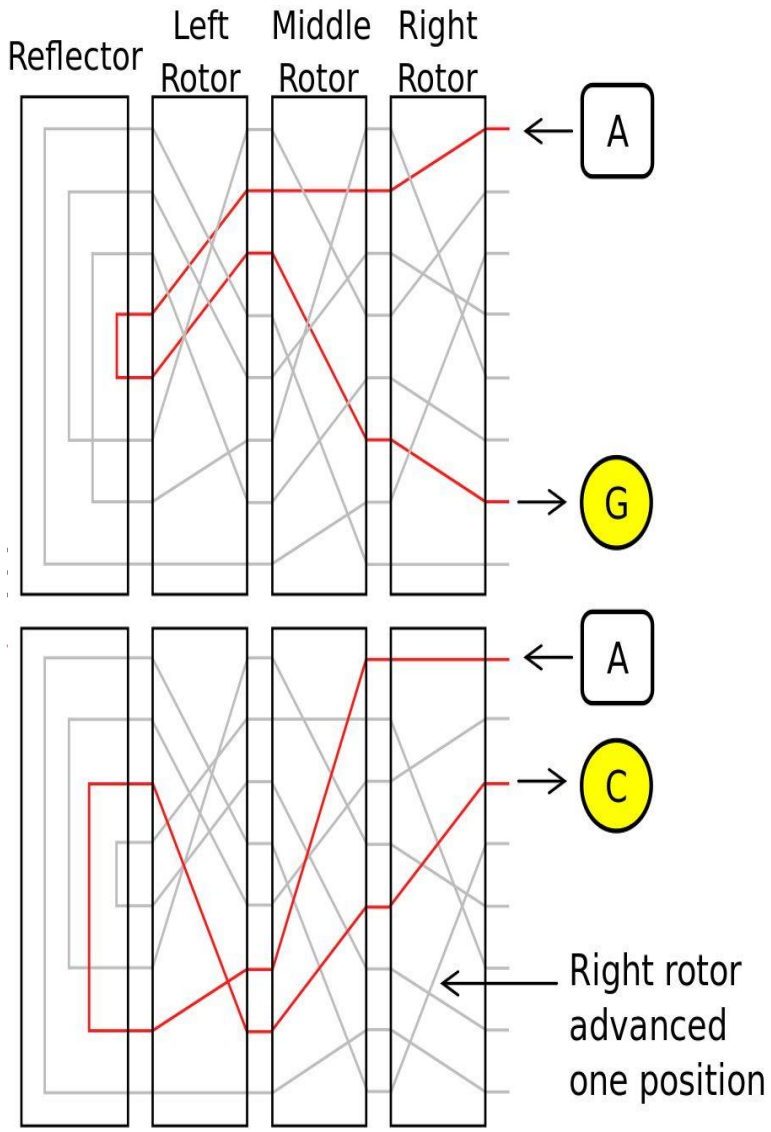
又称转轮密码，用一组转轮或接线编码轮所组成的机器，用以实现长周期的多表代换密码，最有名的的代表Enigma（恩尼格玛）。

1918年，德国发明家亚瑟•谢尔比乌斯和理查德•里特创办了一家新技术应用公司，谢尔比乌斯利用电气技术发明一种能够自动编码的机器，并给自己所发明的电气编码机械取名“恩尼格玛”（ENIGMA，意为哑谜）。

恩尼格玛在1920年代早期开始被用于商业，后来也被一些国家的军队与政府采用过，在这些国家中，最著名的是第二次世界大战时的纳粹德国。

https://www.bilibili.com/video/BV1eW411K7x7/

第二阶段：近代密码 - 电子机械密码



图显示了，当按下键盘的A键时，使灯盘D亮的电流示意图，电流从电池（1）通过双向键盘开关（2）进入插板（3）。接下来，它穿过**三个或四个已安装的转子**（5）的布线，并进入**反射器（6）**。**反射器通过完全不同的路径将电流返回**，通过转子（5）和进入轮（4），流经连接有电缆（8）的插头“ S”（7）和插头“ D”，再通过另一个双向开关（9）点亮相应的灯。

由于转子会随着按键的输入而转动，由此导致三个转子之间线路发生变化。例如，在下图中两次输入A的示例中，由于右侧转子的转动（反射器、左侧转子、中间转子都没有变化），导致最终输出结果不同。

第二阶段：近代密码－机电密码Enigma

从20世纪初到1949年，是近代密码发展阶段。由于机械工业的迅猛发展，这一阶段开始使用机械代替手工计算，发明了机械密码机和更进一步的机电密码机，但是密码算法的安全性仍然取决于对密码算法本身的保密。

机电密码又称转轮密码：用一组转轮或接线编码轮所组成的机器，用以实现长周期的多表代换密码，最有名的的代表：Enigma(恩尼格玛），Purple（紫密）

结构

键盘：使用键盘进行输入

转轮：代表26个字母的触点，形成换字表。一般三个转轮，随按键产生进位

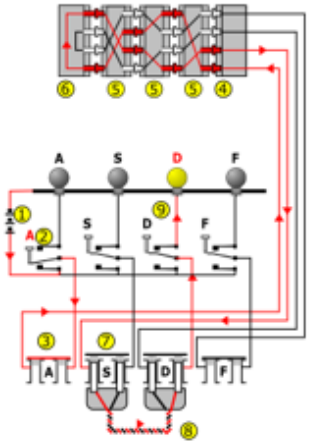
显示板：显示输出的字母

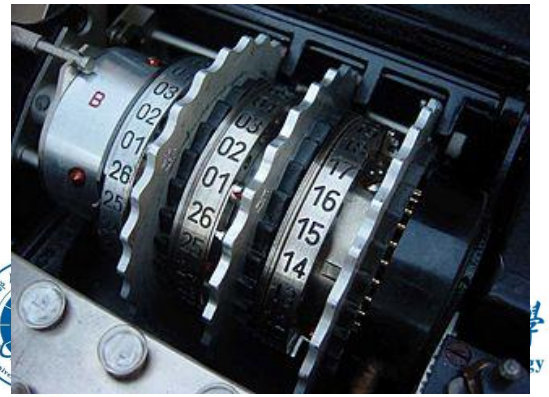
加密原理

输入字母，加密后的字母在显示器上显示

每输入一次，最右转轮转动一格，并逐位进位，产生不同替换表

一个转轮产生26种换字表，3个转轮一共有26*26*26=16900种可





第二阶段：近代密码－机电密码Enigma

使用“恩尼格玛”通讯时，发信人首先要调节三个转子的方向（**而这个转子的初始方向就是密匙，是收发双方必须预先约定好的**），然后依次键入明文，并把显示器上灯泡闪亮的字母依次记下来，闪亮字母按照顺序用正常的电报方式发送出去。收信方收到电文后，只要也使用一台“恩尼格玛”，按照原来的约定，把转子的方向调整到和发信方相同的初始方向上，**然后依次键入收到的密文，显示器上自动闪亮的字母就是明文了。加密和解密的过程完全一样，这就是反射器的作用**。

“恩尼格玛”加密的关键就在于**转子的初始方向**。当然如果敌人收到了完整的密文，还是可以通过不断试验转动转子方向来找到这个密匙，特别是如果破译者同时使用许多台机器同时进行这项工作，那么所需要的时间就会大大缩短。对付这样“暴力破译法”（即一个一个尝试所有可能性的方法），可以通过增加转子的数量来对付，因为只要每增加一个转子，就能使试验的数量乘上26倍。

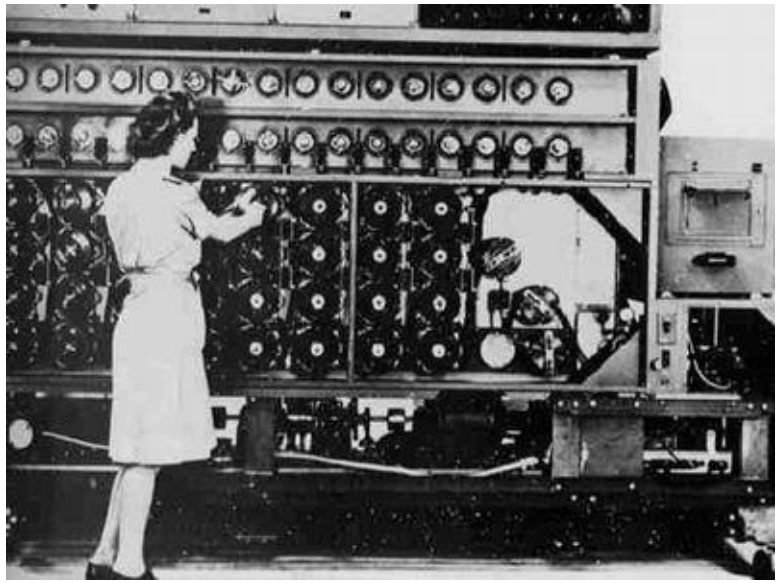
第二阶段：近代密码－机电密码Enigma

- Enigma 的破解

波兰情报部门截获德国恩尼格码密码机

三位基字辈数学家（亨里克·佐加尔斯基、杰尔兹·罗佐基和马里安·雷杰夫斯基）破译德军密码

图灵破解恩尼格码 （不依赖重复密钥的破解方法）



第二阶段：近代密码－机电密码Enigma

在德军全面使用Enigma传递军事情报后，很多人认为Enigma是一种无法破译的密码机。最初，英国和法国的间谍得到了德军的Enigma的构造，波兰密码学家雷耶夫斯基（Marina Rejewski）在得到法国共享的情报后，找出了破解Enigma的可行方法。但是由于担心德国入侵波兰，密码破译无法继续尽行下去，于是波兰决定将情报提供给英国和法国。果然不久后，第二次世界大战全面爆发，德国闪电战入侵波兰。

英国的密码学家们在布莱切利继续进行Enigma的破译研究，计算机之父**阿兰·图灵（Alan Turing）**就是这个破译团队的重要成员之一。图灵在之前众多密码学家的研究成果的基础上，终于在1940年找出能够破解Enigma的方法并制造了破译机器（bombe，炸弹）。

图灵图灵的思路：“用机器对抗机器”。

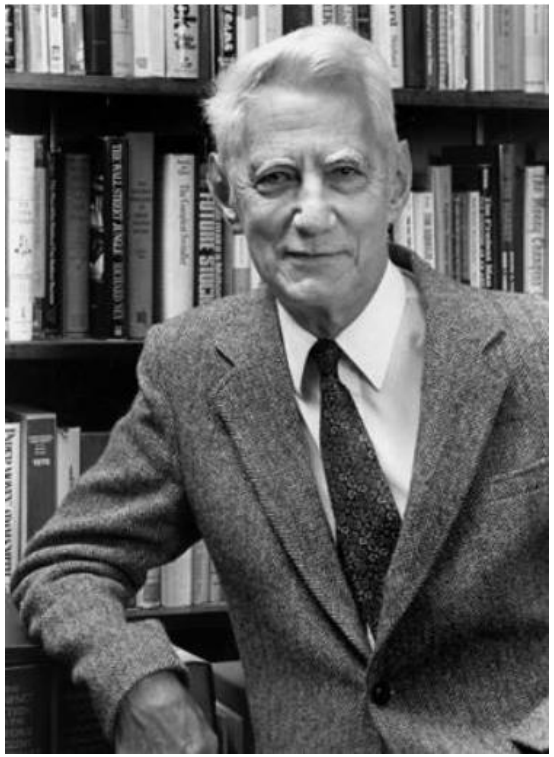
使用DigitalOcean公司的云服务器和来自Enigma Pattern的人工智能软件，一条在帝国战争博物馆内简短的德文信息在13分钟内被破解了。

第三阶段：现代密码学

从1949年到1975年，是现代密码学的早期发展时期。1949年，Shannon发表的划时代论文“保密系统的通信理论”（The Communication Theory of Secret Systems），为密码学奠定了理论基础，密码学从此开始成为一门科学。

1976年，Diffie和Hellman发表了题为“密码学的新方向”（New Directions in Cryptography）的文章，提出了公钥密码的思想，引发了密码学历史上的一次变革，标志着密码学进入公钥密码学的新时代。

1977年，美国制定了数据加密标准（Data Encryption Standard，DES），公开密码算法的细节，并准许用于非机密单位和商业应用。这个时期密码得到广泛应用，密码标准化工作和实际应用得到各国政府、学术界和产业界的空前关注，推动了密码学的研究与应用。



香农

小结

古典密码：保证机密性

- 数据完整性？
- 认证性？
- 不可否认性？
- 防重放攻击？

现代密码学

- 对称密码（单钥密码）：分组密码，流密码
- 非对称密码（公钥密码）：公钥加密、数字签名

第二讲 密码学发展及其应用

① 密码学重要意义

② 密码学发展历史

③ 密码学基本概念

④ 密码算法

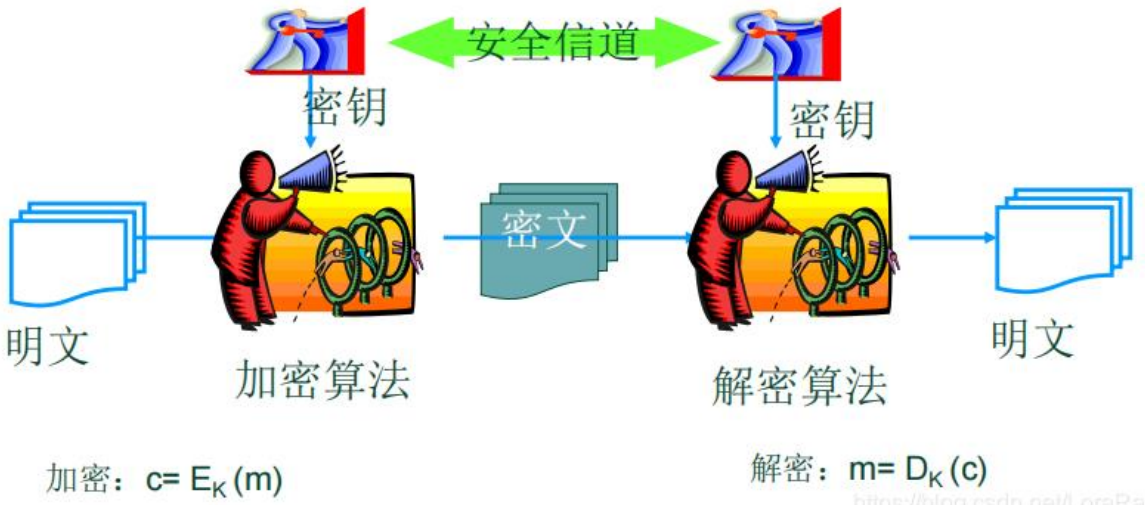
⑤ 网络空间安全中的密码学应用

密码学基本概念

密码学包括：密码编码学（cryptography）和密码分析学（cryptanalysis）两部分。

密码编码学--主要研究信息的编码，构建各种安全有效的密码算法和协议，用于消息的加密、认证等方面

密码分析学--是研究破译密码获得消息，或对消息进行伪造。



- **消息**

  消息被称为明文(Plaintext)

- **加密**

  用某种方法伪装消息以隐藏它的内容的过程称为加密(Encrtption)

- **密文**

  被加密的消息称为密文(Ciphertext)

- **解密**

  把密文转变为明文的过程称为解密(Decryption)

- **加密算法**

  对明文进行加密操作时所采用的一组规则称作加密算法(Encryption Algorithm)

- **解密算法**

  接收者对密文解密所采用的一组规则称为解密算法(Decryption Algorithm)

第二讲 密码学发展及其应用

① 密码学重要意义

② 密码学发展历史

③ 密码学基本概念

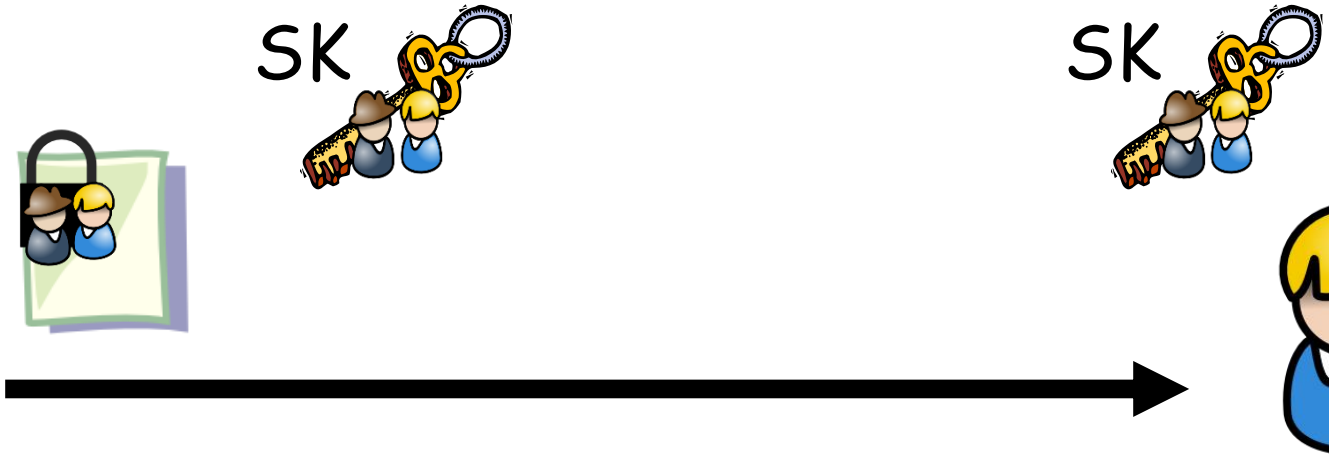
④ 密码算法

⑤ 网络空间安全中的密码学应用

对称密码(Symmetric Key Encryption)

基本机制：加密与解密密钥相同（例如：DES[Data Encryption Standard]等）

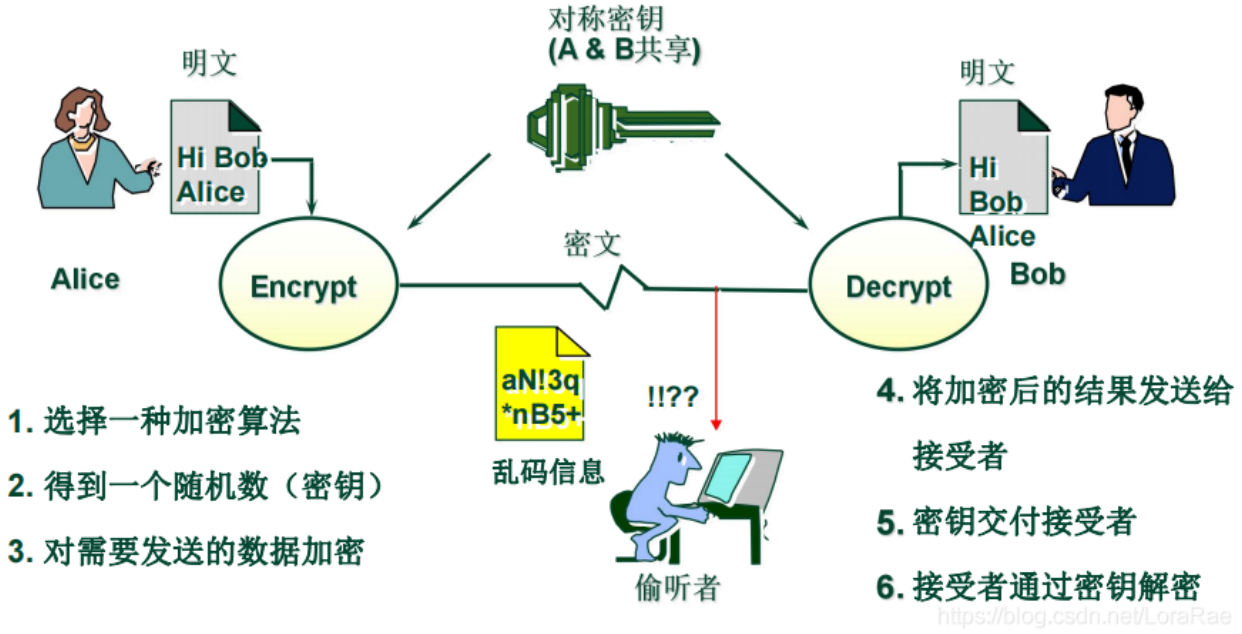
- 密钥交换：建立一个共享的密钥sk
- 加密：CT ← Enc(M, sk)
- 解密：M ← Dec(CT, sk)



分组密码

也叫块加密(block cyphers)，一次加密明文中的一个分组/块。是将明文按一定的位长分组，明文组经过加密运算得到密文组，密文组经过解密运算（加密运算的逆运算），还原成明文组。且通常情况是密文、明文等长。

- 加密步骤一：将明文拆分为 N 个固定长度的明文块
- 加密步骤二：用相同的秘钥和算法对每个明文块加密得到 N 个等长的密文块
- 加密步骤三：然后将 N 个密文块按照顺序组合起来得到密文



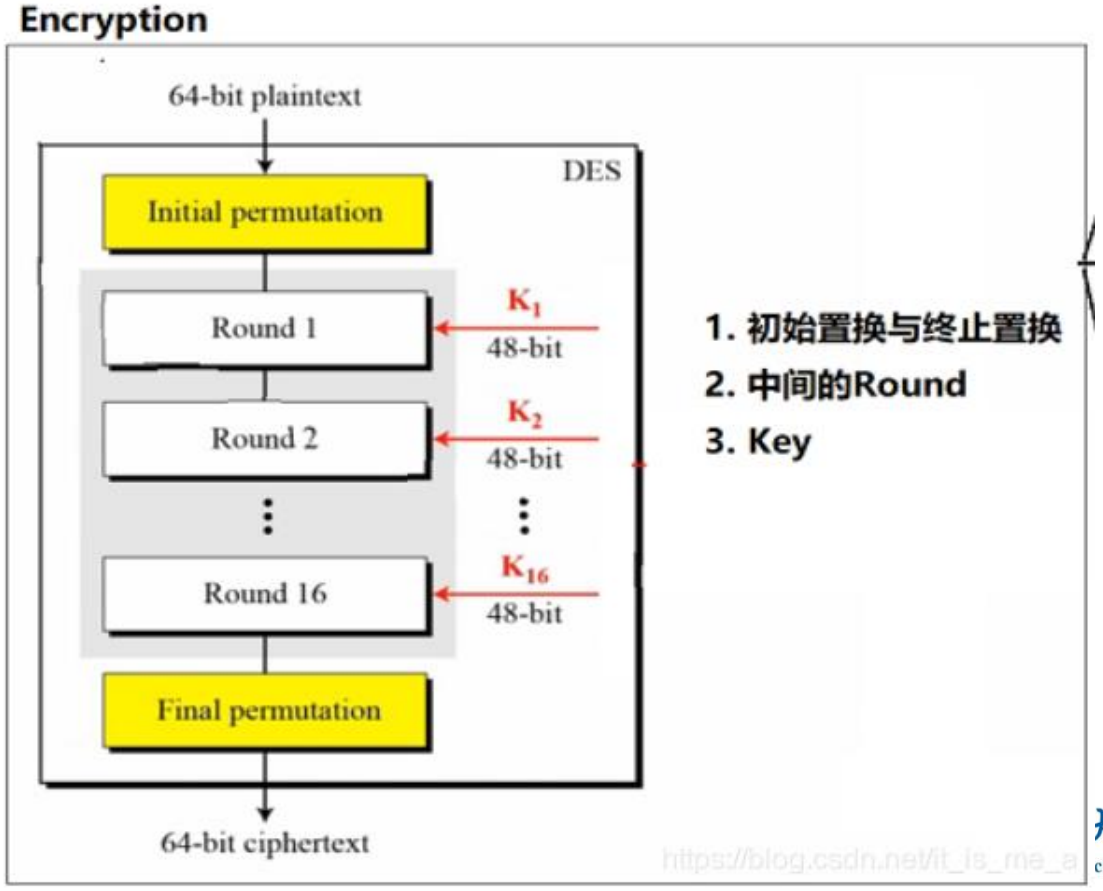
常见的分组密码算法包括 AES、SM1（国密）、SM4（国密）、DES、3DES、IDEA、RC2 等；

分组密码-DES算法

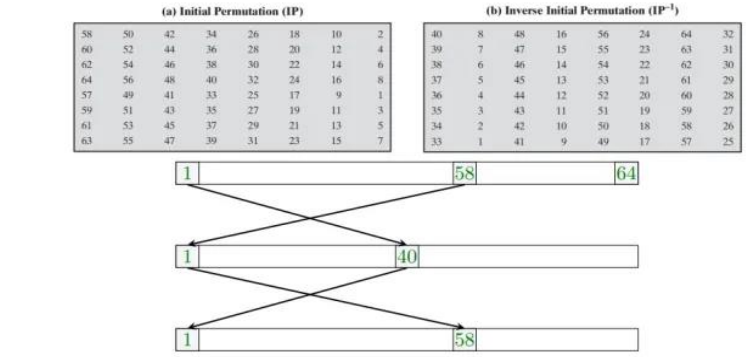
1977年美国数据加密标准（**DES**）作为第一个公开应用的加密标准，是一种最有代表性的对称分组密码算法。

- 1973年美国国家标准局NBS公开征求国家密码标准方案
- 1975年IBM公司首次提出方案
- 1977年被NIST确定为联邦信息处理标准并命名为DES
- 输入：64位明文分组、64位密钥(8位校验位)
- 输出：64位密文分组解密算法与加密算法相同

DES算法的基本思想是对明文进行分组，然后利用用户秘钥对明文分组进行16轮的移位和循环移位、置换、扩展、压缩、异或等位运算，利用复杂运算把明文编码彻底打乱。



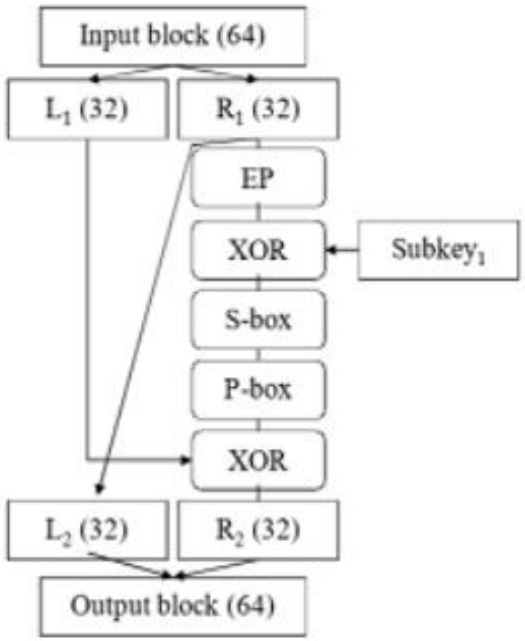
初始置换 IP 和逆置换 IP^{-1}



初始置换和结尾逆置换并不是为了增强安全性，而是为了方便硬件电路实现
(https://crypto.stackexchange.com/a/6)

分组密码-DES算法

2. 中间的Round



2.1 EP 拓展置换

2.2 XOR 异或运算

2.3 S-box S盒压缩

2.4 P-box P盒置换

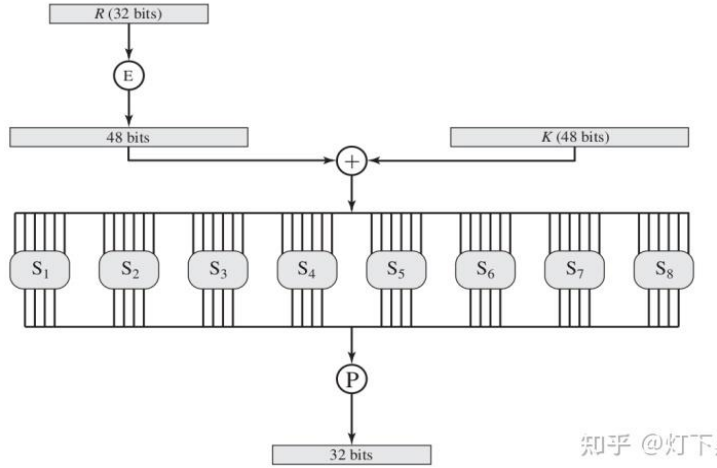
- 64-bit output from round 1 is input for round 2
- Output from round 2 is input for round 3

  :
- Output from round 16 is passed through a final permutation

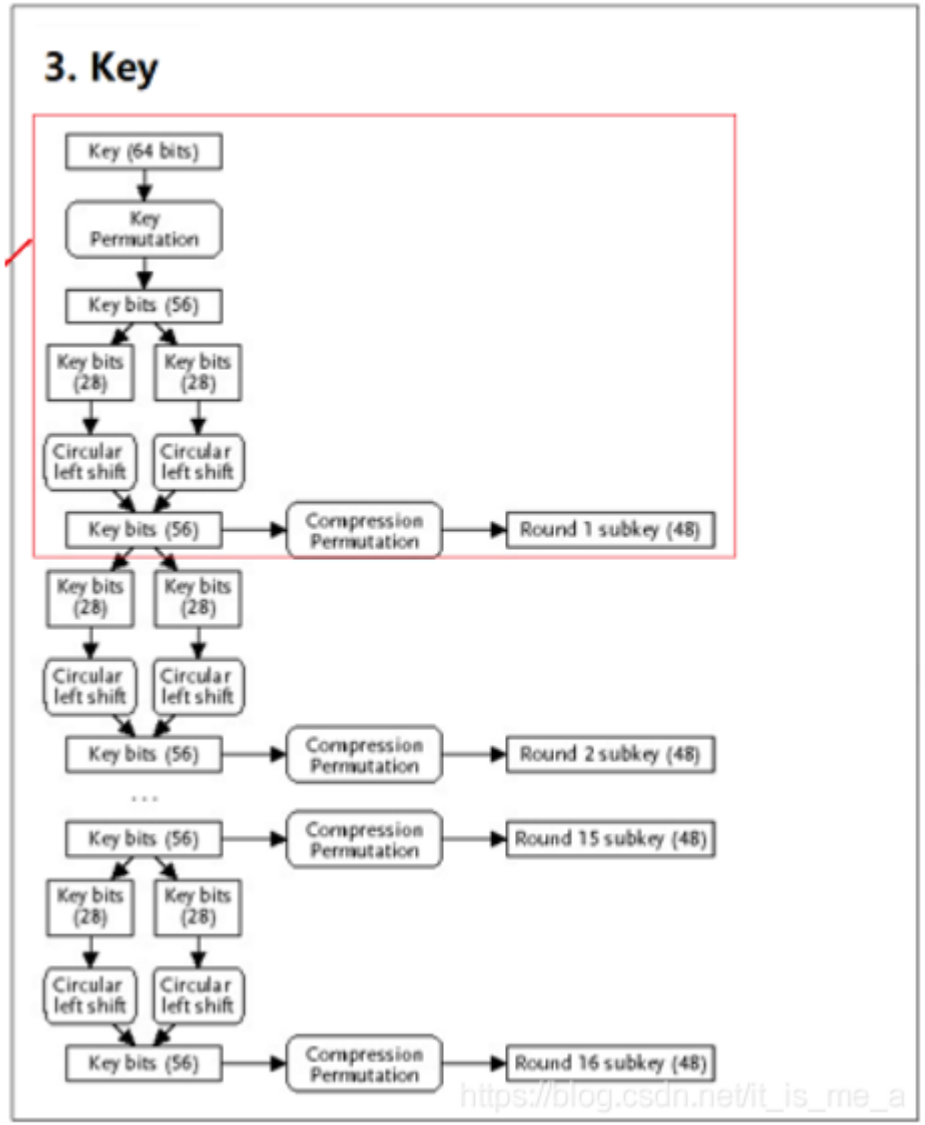
2.1 EP 拓展置换

扩展置换表

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01



分组密码-DES算法



3.1 Key Permutation

- A **key permutation** removes eight parity bits and

57,	49,	41,	33,	25,	17,	9,	1,
58,	50,	42,	34,	26,	18,	10,	2,
59,	51,	43,	35,	27,	19,	11,	3,
60,	52,	44,	36,	63,	55,	47,	39,
31,	23,	15,	7,	62,	54,	46,	38,
30,	22,	14,	6,	61,	53,	45,	37,
29,	21,	13,	5,	28,	20,	12,	4

- The 57th bit is moved to position 1
- The 49th bit is moved to position 2

3.2 Circular left shift

- 56 key bits (after permutation) divided into two 28-bit halves
- Each half circularly shifted left by one bit (rounds 1,2,9 and 16) or 2 bits (all other rounds)
- Halves recombined into 56 bit string

3.3 Compression Perm

14,	17,	11,	24,	1,	5,	3,	28,
15,	6,	21,	10,	23,	19,	12,	4,
26,	8,	16,	7,	27,	20,	13,	2,
41,	52,	31,	37,	47,	55,	30,	40,
51,	45,	33,	48,	44,	49,	39,	56,
34,	53,	46,	42,	50,	36,	29,	32

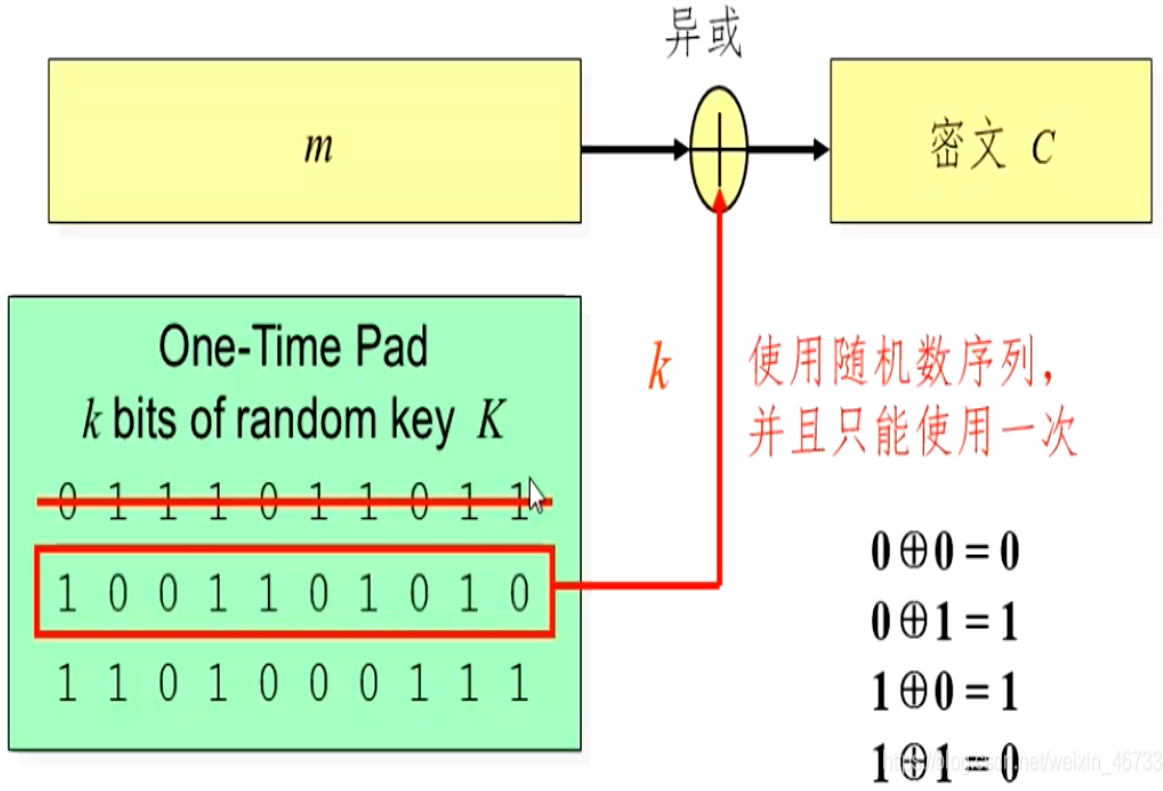
- 14th bit goes to output 1
- 17th bit goes to output 2

DES的解密过程和加密过程几乎完全相同：相同的算法和密钥，区别在于：

1. Subkey16用在第一轮；
2. Subkey15用在第二轮…

流密码

将密钥、明文表示成连续的二进制流或字符，一位一位的对应进行加密。加密和解密双方使用相同密钥，明文数据每次与密钥数据流顺次对应加密，得到密文数据流。实践中数据通常是一个位（bit）并用异或（xor）操作加密。



1949年Shannon证明了只有**一次一密的密码体制**是绝对安全的，这给序列密码技术的研究以强大的支持，序列密码方案的发展是模仿一次一密系统的尝试，或者说“一次一密”的密码方案是序列密码的雏形。

如果序列密码所使用的是真正随机方式的、与消息流长度相同的密钥流，则此时的序列密码就是一次一密的密码体制。

流密码

一次性密码和本身含义一样，为只能使用一次的密码，也称为动态密码或单次有效密码，简称OTP。

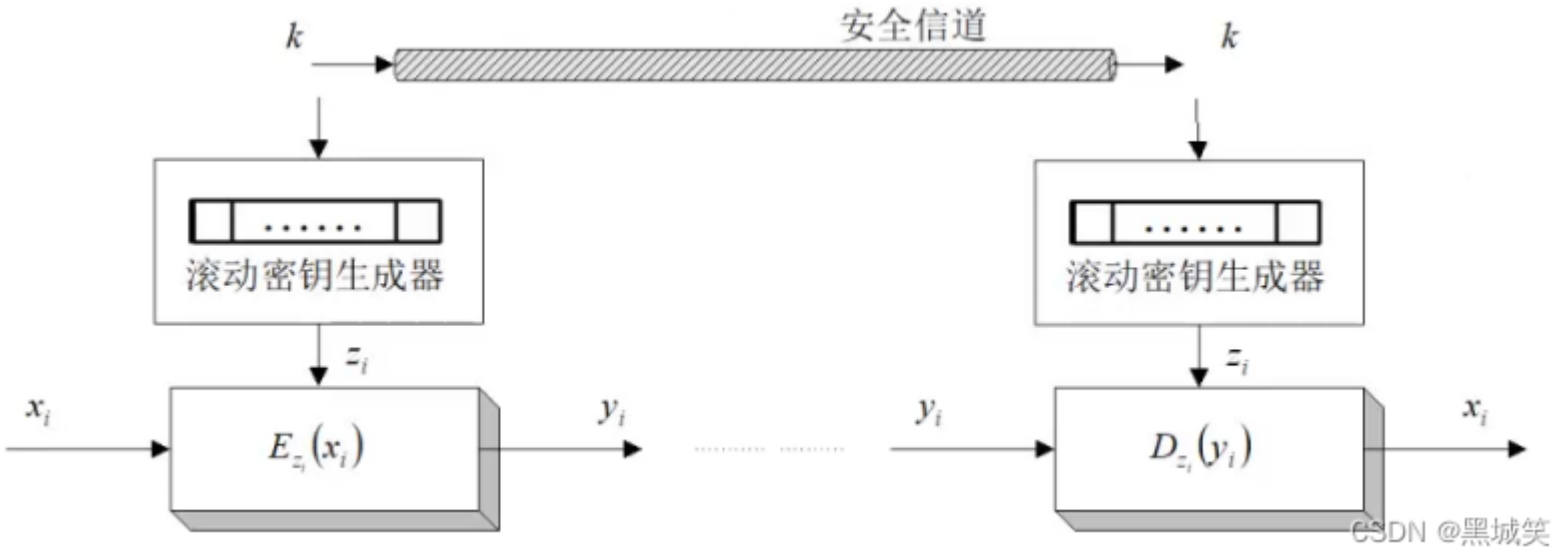
OTP不容易遭到重放攻击，需要使用到大于自身长度的密钥流，密钥流必须完全随机生成，并且密钥不能重复使用。**完全随机的无限长的密钥流的生成、分发和存储是非常困难的，而且，既然能安全交换密钥，为什么不直接安全交换同样长度的明文呢？**

我们需要使用有限长的种子密钥（易生成、分发、存储），来生成无限长的随机密钥序列——我们称拥有这种功能的算法为伪随机序列发生器。如何设计高效而又安全的**伪随机数发生器**，是流密码的核心研究内容。

同步流密码

在流密码产生密钥序列时，如果密钥序列的产生与之前明文字符、密文字符均无关，也即密钥序列的产生可以完全独立于明文加密，则将这种流密码称为同步流密码。

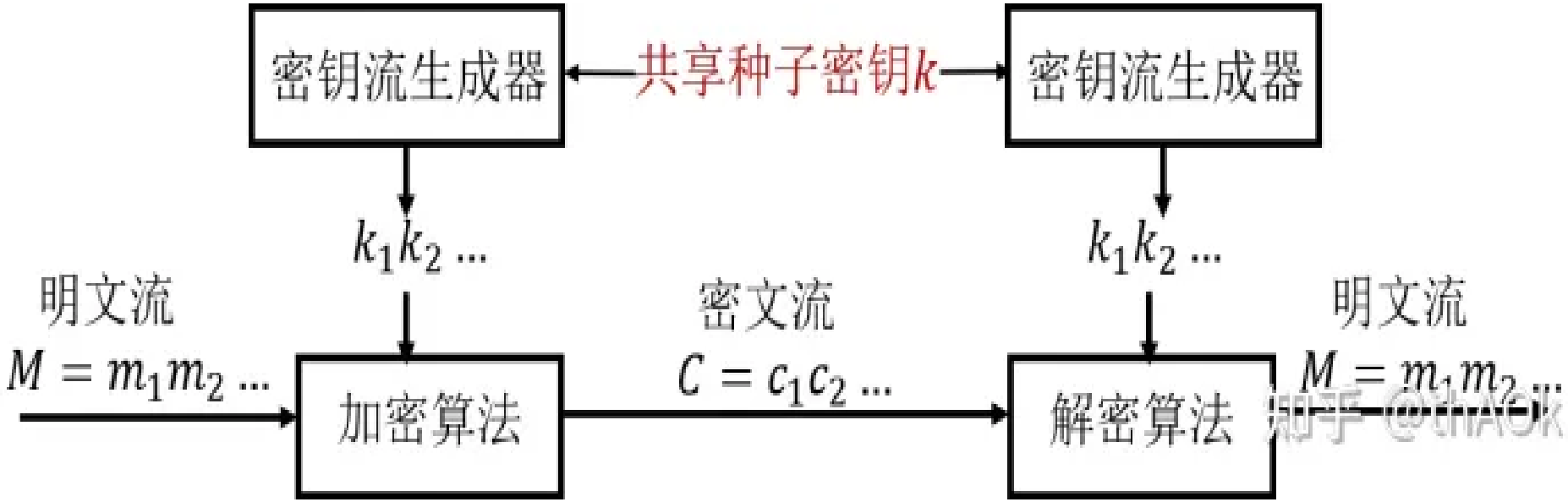
同步流密码在加密或解密时，需要使两者密钥流生成器的状态一致（这里的状态可以决定密钥流生成器产生的密钥），否则会导致加解密密钥不一致，使解密失败。当两者密钥流生成器的状态不一致时，必须借助外接手段来同步。



k是密钥流的第一个数，同步流密码只需传递一个数k，因为有同样的滚动密钥生成器，所以只由密钥流的第一个数可推出整个密钥流。

自同步流密码

在流密码产生密钥序列时，如果密钥序列的产生与以往的密文序列有关，即密钥产生算法是密钥和以往密文序列的函数，则称这种流密码为自同步流密码。自同步流密码中，密钥序列的产生与明文的加密是不独立的，也是不能分割的。很多情况下，明文或者密文都需要给密钥序列的产生提供反馈。



流密码小结

流密码是一个随时间变化的加密变换，具有转换速度快、低错误传播的优点，硬件实现电路更简单；

其缺点是：低扩散（意味着混乱不够）、插入及修改的不敏感性。

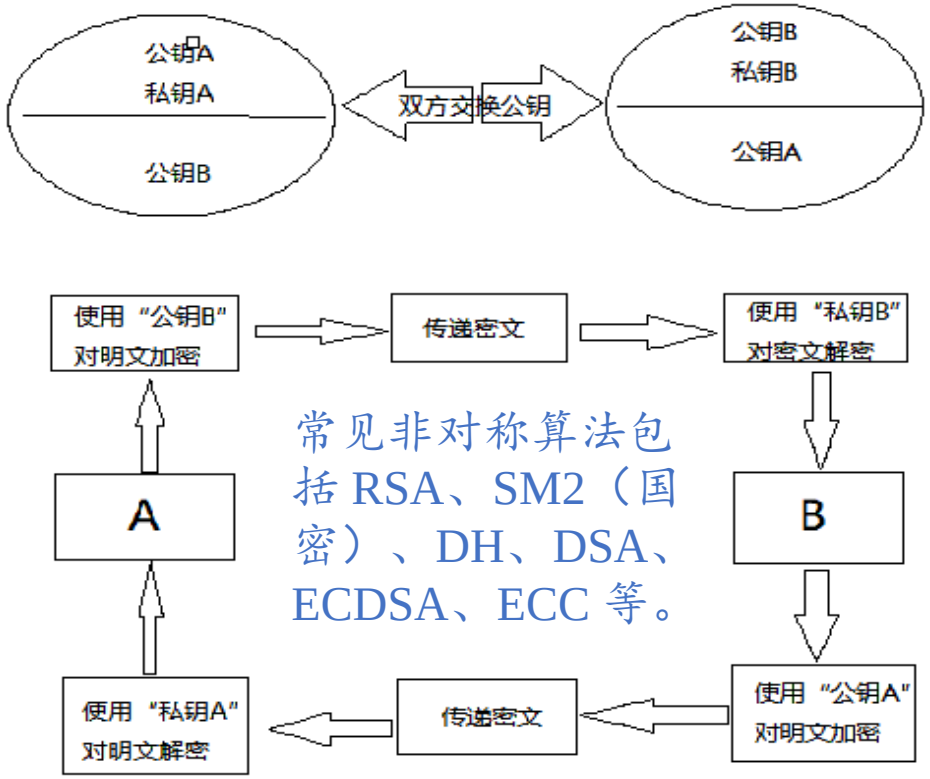
流密码涉及到大量的理论知识，提出了众多的设计原理，也得到了广泛的分析，但许多研究成果并没有完全公开，这也许是因为序列密码目前主要应用于军事和外交等机密部门的缘故。目前，公开的序列密码算法主要有RC4、SEAL等。

祖冲之算法（ZUC），属于同步序列密码，其也是中国第一个成为国际密码标准的密码算法。

2011年9月19-21日，在日本福冈召开的第53次第三代合作伙伴（3GPP）系统架构组（SA）会议上，我国设计的祖冲之密码算法（ZUC）被批准成为新一代宽带无线移动通信系统（LTE）国际标准，即4G的国际标准。

非对称加密(Asymmetric Key Encryption)

非对称加密需要两把密钥：公钥和私钥，他们是一对，如果用公钥对数据加密，那么只能用对应的私钥解密。如果用私钥对数据加密，只能用对应的公钥进行解密。因为加密和解密用的是不同的密钥，所以称为非对称加密。

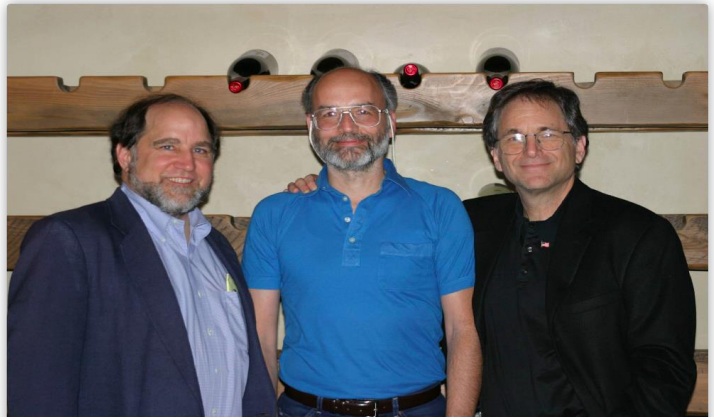


常见非对称算法包括 RSA、SM2（国密）、DH、DSA、ECDSA、ECC 等。

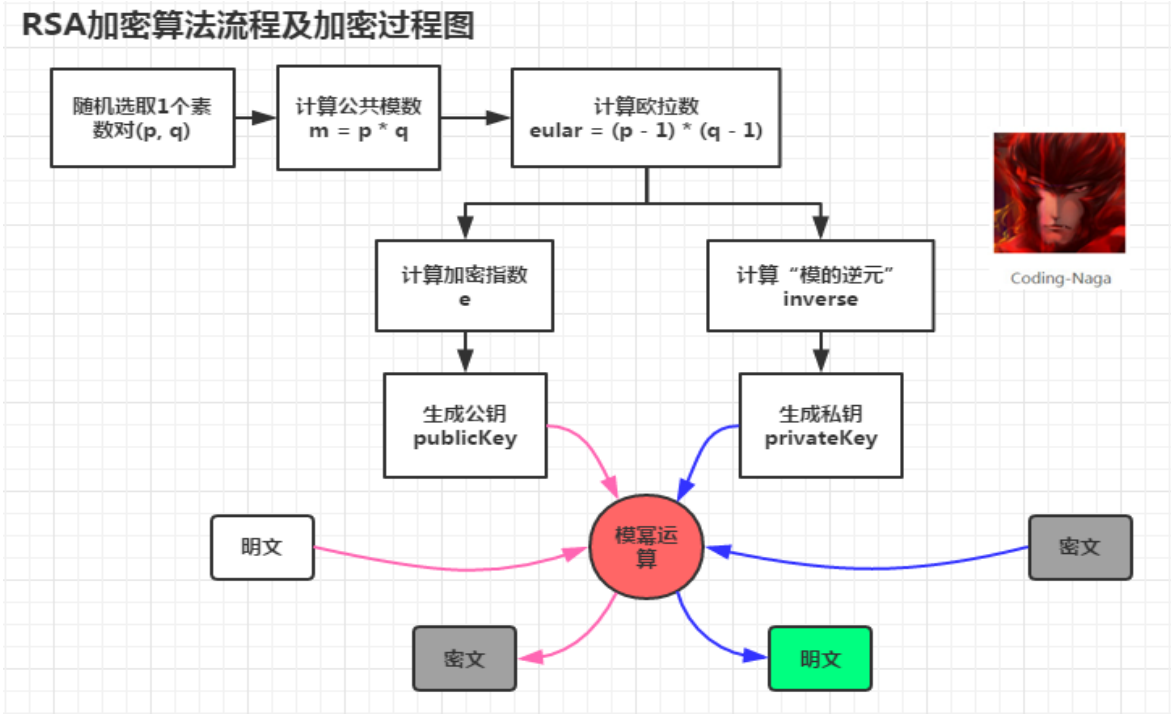
(1) A要向B发送信息，A和B都要产生一对用于加密和解密的公钥和私钥。
(2) A 的私钥保密，A 的公钥告诉 B；B 的私钥保密，B 的公钥告诉 A。
(3) A 要给 B 发送信息时，A 用 B 的公钥加密信息，因为 A 知道 B 的公钥。
(4) A 将这个消息发给 B（已经用 B 的公钥加密消息）。
(5) B 收到这个消息后，B 用自己的私钥解密 A 的消息。其他所有收到这个报文的人都无法解密，因为只有 B 才有 B 的私钥。

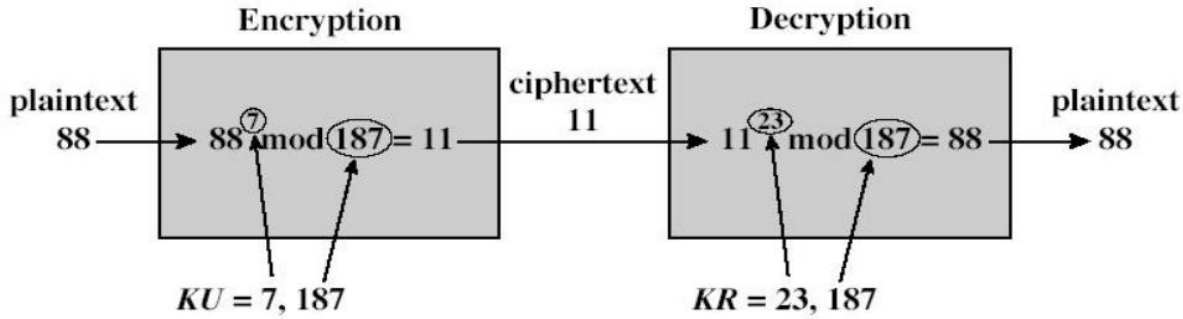
RSA算法简介

1977年，三位数学家Rivest、Shamir 和 Adleman 设计了一种算法，可以实现非对称加密。这种算法用他们三个人的名字命名，叫做RSA算法，RSA是目前最有影响力的公钥加密运算。



根据数论，寻求两个大素数比较简单，而将它们的乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥，即公钥。而两个大素数组合成私钥。公钥是可发布的供任何人使用，私钥则为自己所有。





优点：一对多的加密机制，任何人都可以使用公钥与该用户进行安全通信；解决秘钥分配问题

缺点：速度慢，需要大量数学计算

使用：用以进行密钥交换，产生临时会话秘钥，具体的数据加密使用会话秘钥和对称加密算法进行加密

密码算法 -- 摘要算法

摘要算法所产生的固定长度的输出数据称为摘要值 、散列值或哈希值，摘要算法无秘钥。有几个重要特性：

（1）哈希函数是将任意有限长度比特串映射为固定长度的串，公式表示如下：

$$h=H（M）$$

（2）Hash值计算速度快

（3）防碰撞特性

（4）**隐藏性（Hiding）**或者叫做**单向性（one-way）**

MD（Message Digest，消息摘要算法）、SHA-1（Secure Hash Algorithm，安全散列算法）和 MAC（Message Authentication Code，消息认证码算法）；另国密标准 SM3 也属于摘要算法。

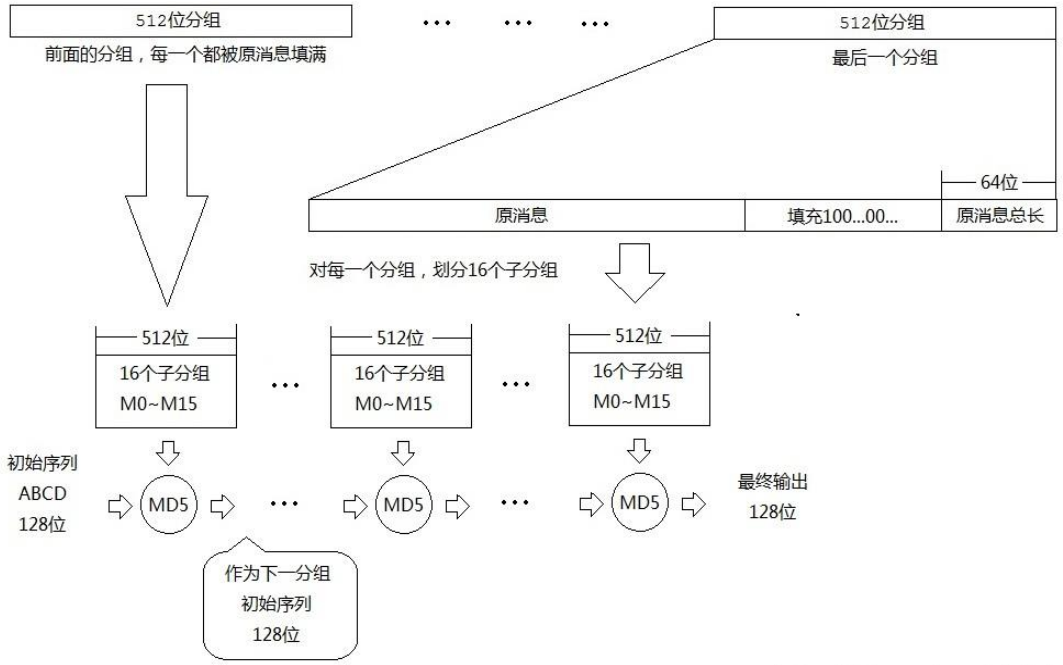
密码算法 – Hash算法MD4 MD5

- 1990年，MD4 由Ron Rivest设计

对任意长度的输入，产生128位输出；其安全性不依赖任何假设，适合高速实现。MD4公布不久，一些密码学家发现，如果去掉MD4算法的第一轮和最后一轮，则算法是不安全的，但他们并没有证明整个算法是不安全的。

- 1991年，MD5 由Ron Rivest设计

输入分组 512bit，输出 128bit。



王小云教授带领的研究小组于2004年、2005年先后破解了被广泛应用于计算机安全系统的MD5和SHA-1两大密码算法

第二讲 密码学发展及其应用

① 密码学重要意义

② 密码学发展历史

③ 密码学基本概念

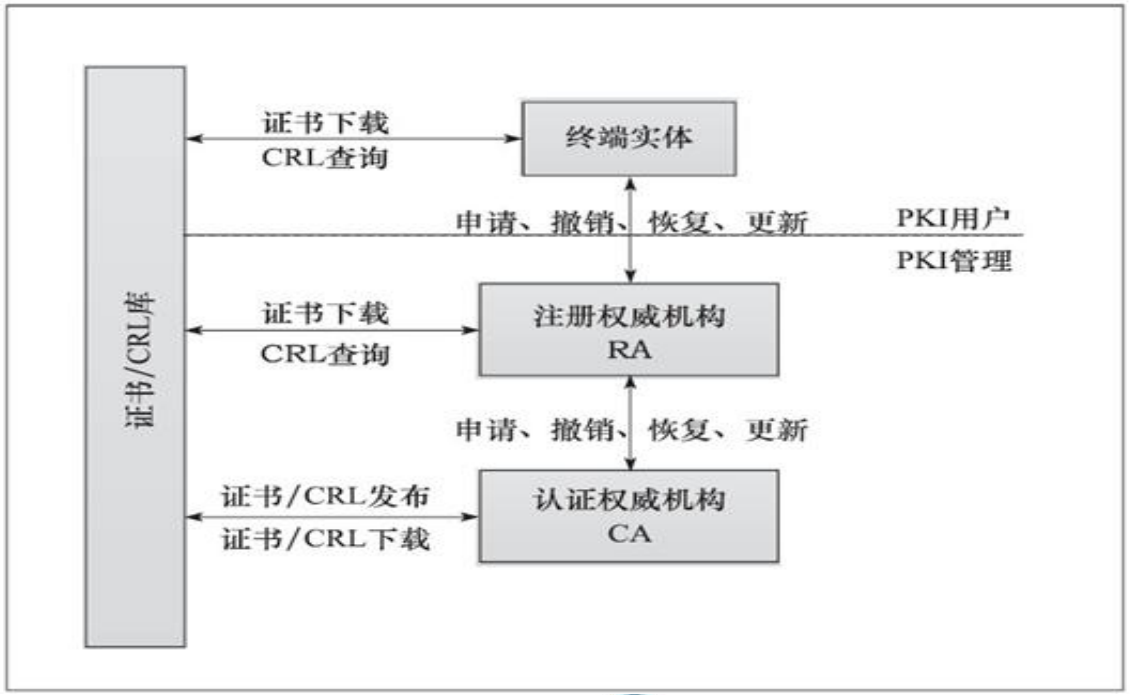
④ 密码算法

⑤ 网络空间安全中的密码学应用

公钥基础设施-PKI

- 为了使用户在不可靠的网络环境中得到真实的公钥，同时避免集中存放密钥和在线查询产生的瓶颈问题，PKI引入数字证书（也称公钥证书）的概念。通过可信第三方——认证权威机构（**Certification Authority，CA**）或称为认证中心把用户公钥和用户的真实身份绑定在一起，产生数字证书。PKI解决了大规模网络中的公钥分发和信任建立问题。
- 通过数字证书，用户能方便安全地获取对方公钥可以**离线验证公钥**的真实性。

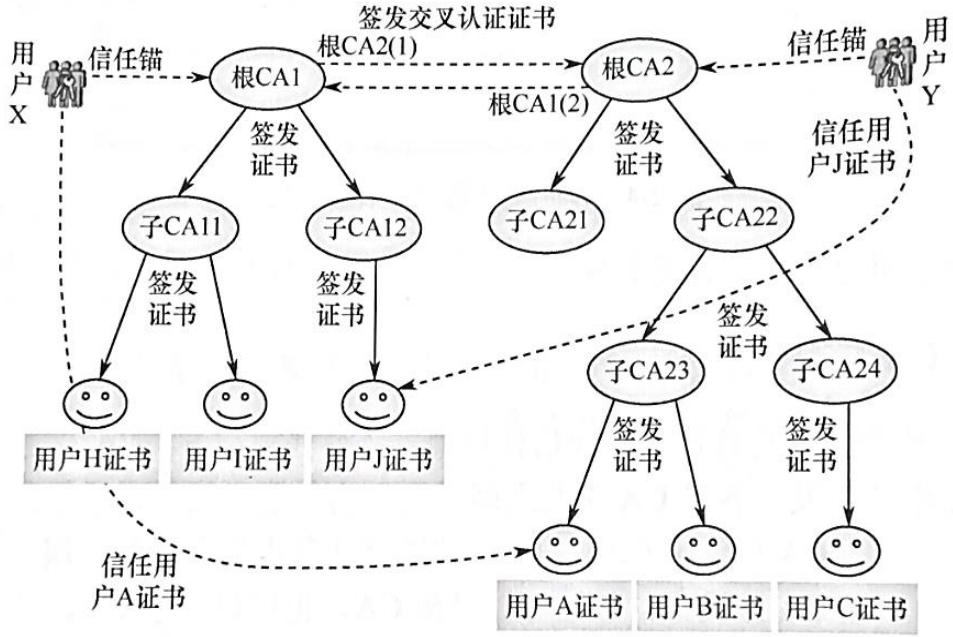
- PKI体系一般由CA、注册权威机构（Registration Authority，RA）、数字证书、证书/CRL库和终端实体等部分组成。



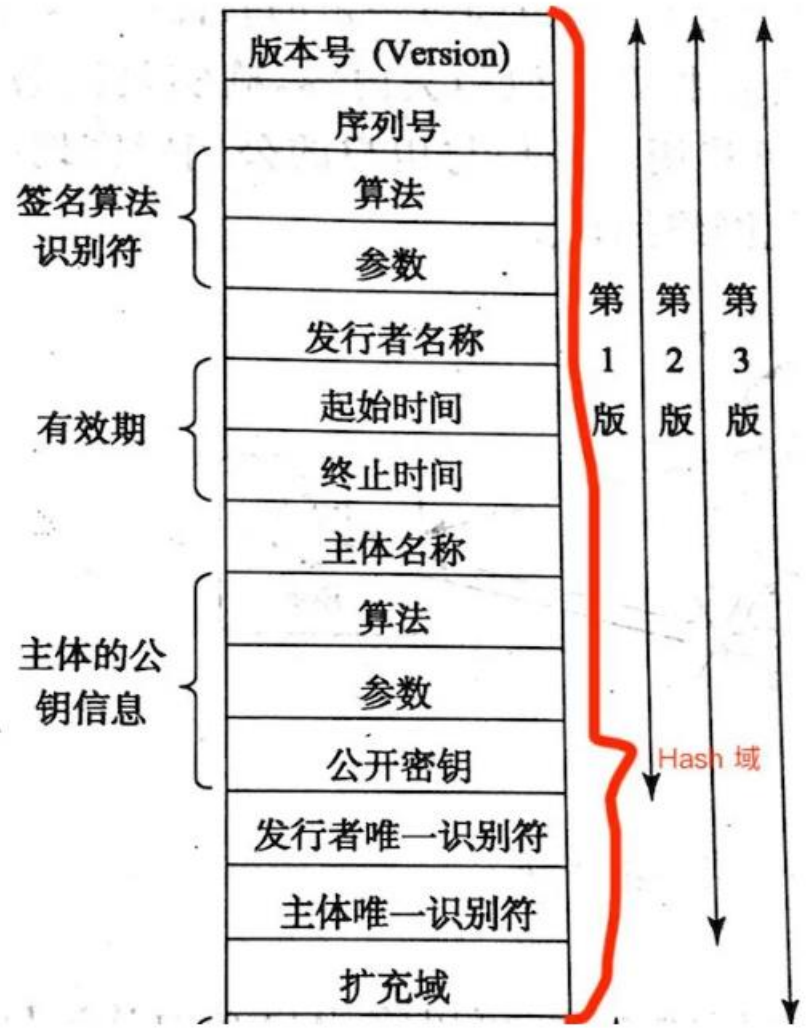
公钥基础设施 -- 数字证书

■数字证书的作用：

- 信息的保密性。
- 交易者身份的确定性
- 不可否认性
- 不可修改性



数字证书链

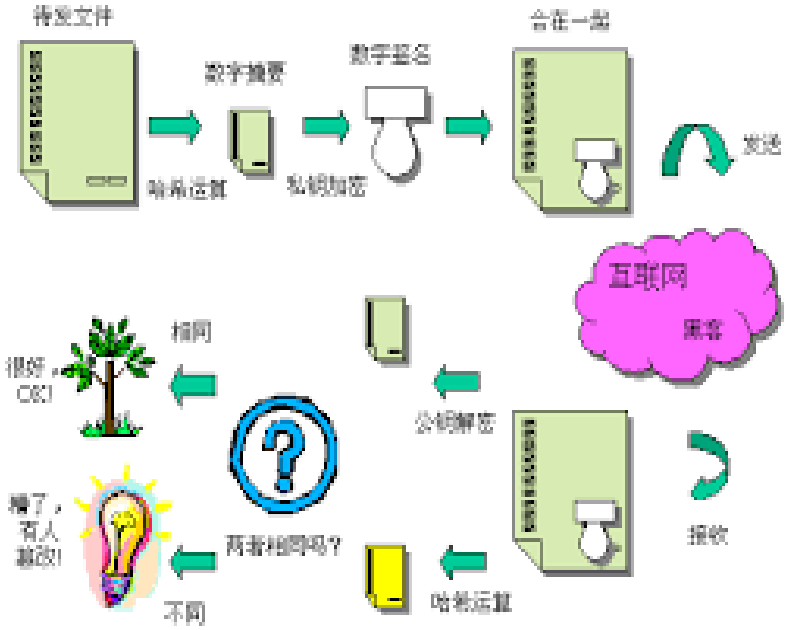


X.509 数字证书结构图

基于密码算法的身份认证

数字签名

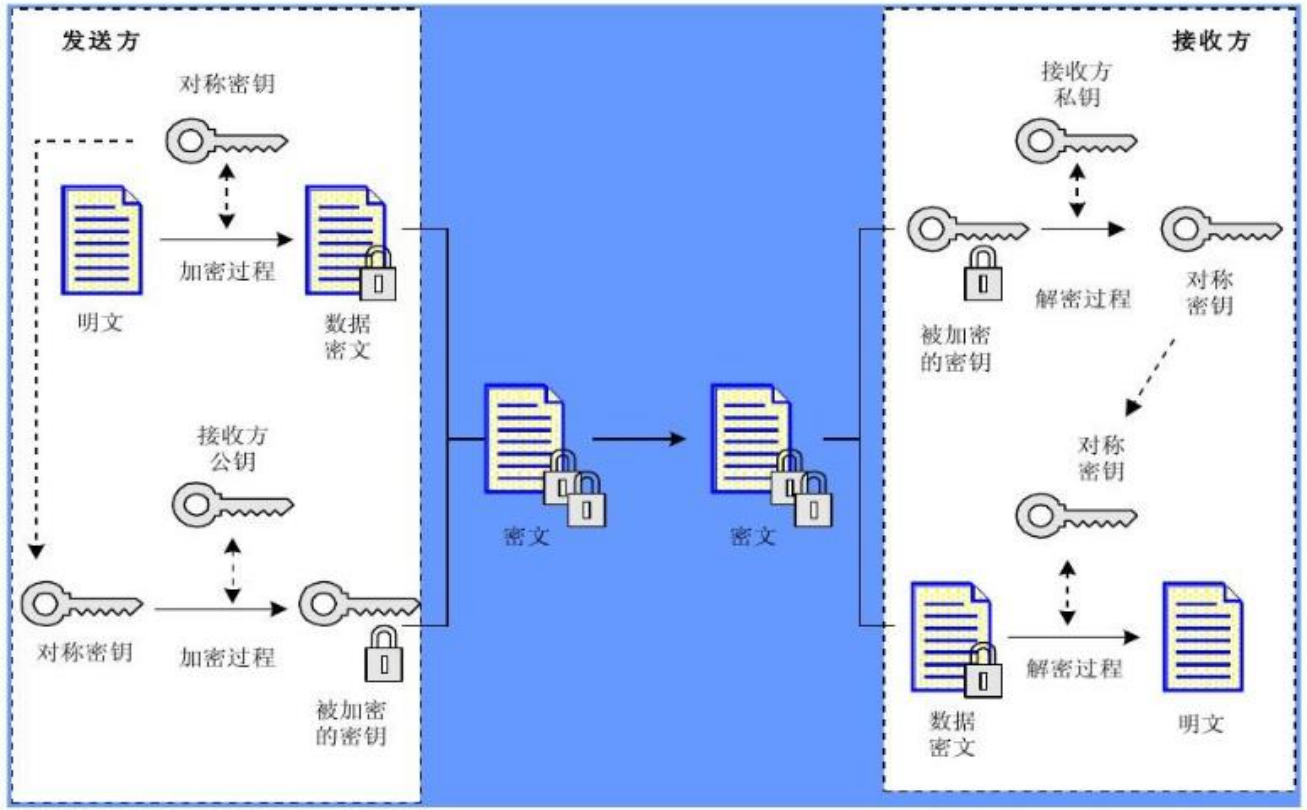
- **目的：**保证信息传输的完整性，发送者的身份，防止抵赖
- 发送方用**哈希函数**从报文文本中生成报文摘要，并用**私人密钥**对摘要进行加密，作为数字签名
- 发送方把**数字签名**和**报文文本**一起发给接收方
- 接收方用同样的哈希函数对报文进行计算，用**公用秘钥**对数字签名进行解密
- **如果两者相同**，说明数字签名有效



基于公钥加密算法的数字信封

数字信封是将**对称密钥**通过非对称加密（即：有公钥和私钥两个）的结果分发的方法。数字信封是实现信息**保密性**验证的技术。

1）A准备要传送的数字信息(明文)
2）A随机产生一个加密钥**(DES密钥)**，并用此密钥对要发送的信息(明文)进行加密，形成密文。（对称加密）
3）A用B的**公钥**对刚才随机产生的加密密钥进行加密，将加密后的DES密钥连同密文一起传送给B。（数字信封）

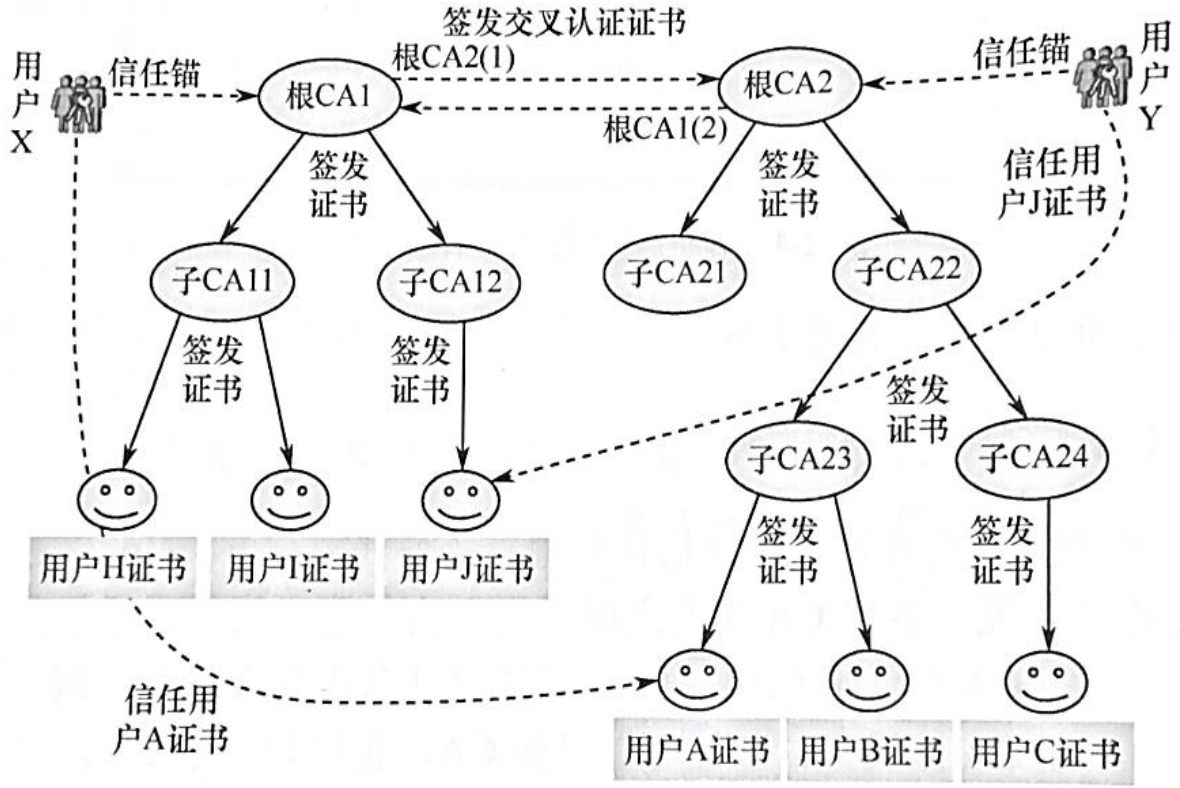


1）B收到A传送过来的密文和加过密的DES密钥，先用自己的**私钥(SK)**对加密的DES密钥进行解密，**得到DES密钥**。
2）B然后用DES密钥对受到的密文进行**解密**，得到明文的数字信息，然后将DES密钥抛弃(即DES密钥作废)。

公钥基础设施-PKI

但是有一 所谓假的证明书，
比如说有一 是史提芬的公开
密钥。那么， 北尔自己不能解
密。

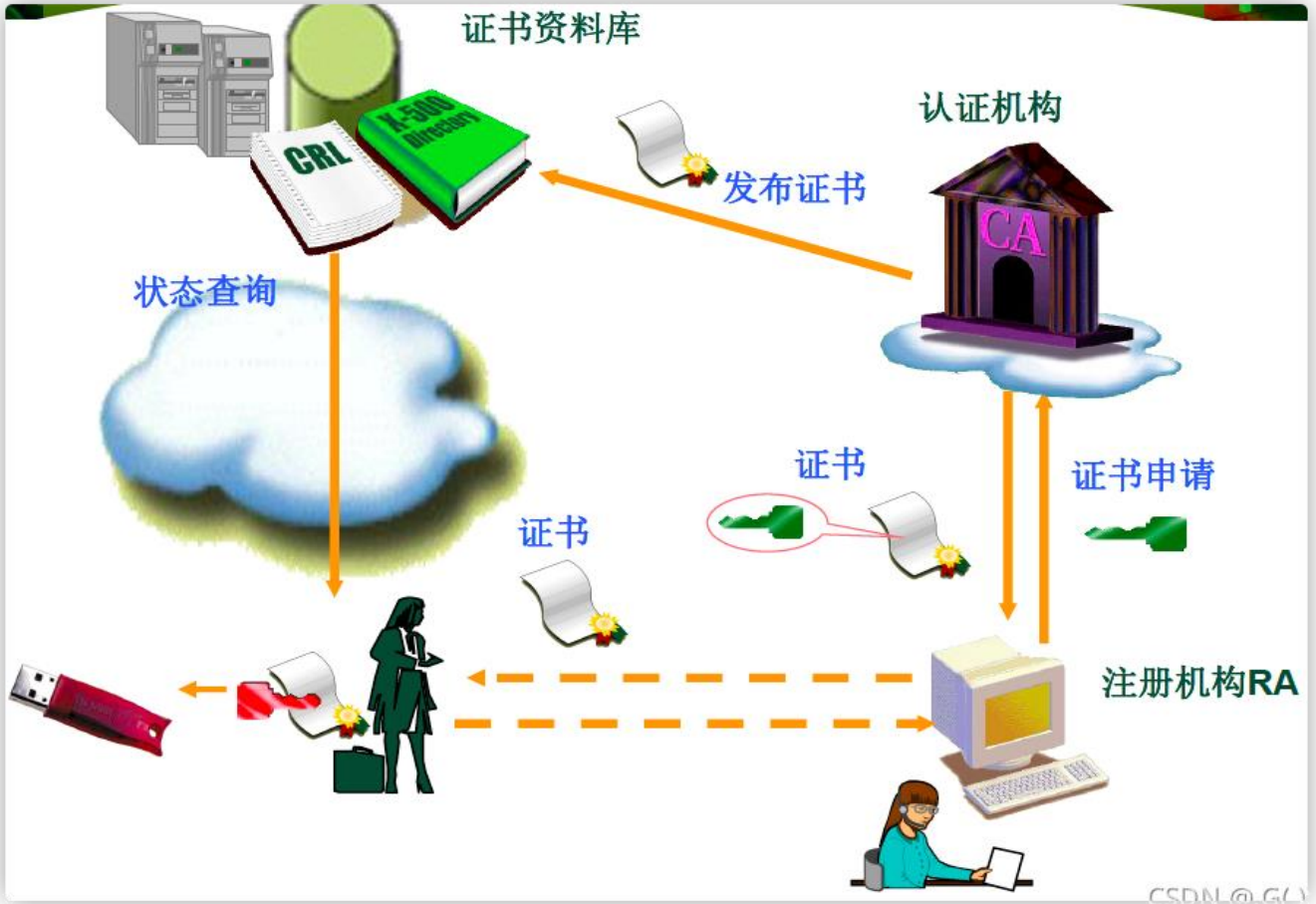
这样看来 度，直接与证书
的可信度挂 实是一个社会基
础设施建设



为了使用 可信第三方——
认证权威机 证中心，把用户
公钥和用户的真实身份绑定在一起，产生形成证明书（数字证书）。公钥基础设施，PKI（Public Key Infrastructure）解决了大规模网络中的公钥分发和信任建立问题。

公钥基础设施-PKI

PKI体系一般由CA、注册权威机构（Registration Authority，RA）、数字证书、证书/CRL库和终端实体等部分组成。



PKI的应用场景

①电子商务PKI技术可以确保电子商务交易的安全性，防止交易中的信息泄露和欺诈行为。

②网络通信PKI技术可以确保网络通信的安全性，防止网络攻击和数据泄露。

③数字签名PKI技术可以为数字签名提供安全保障，确保签名的真实性和完整性。

PMI概述

当用户访问应用系统时必须能控制：**访问者是谁、能访问哪些资源，而且这两项控制检查措施必须在用户进入应用系统时进行。**

- “访问者是谁”对应的是用户的身份认证问题；
- “能访问哪些资源”对应的是授权权限问题。

为了解决后一个问题，特权管理基础设施（Privilege Management Infrastructure，PMI）应运而生，**它提供了一种在多应用环境中的权限管理和访问控制机制，将权限管理和访问控制从具体应用系统中分离出来，使得访问控制机制和应用系统之间能灵活且方便地结合。**

PMI的主要功能包括对**权限管理进行系统的定义和描述**，建立起**用户身份到应用授权的映射**，支持应用访问控制。简单地说，它能提供一种独立于应用资源、用户身份及访问权限的对应关系，保证用户能够获取授权信息。

PMI的组成

PMI是属性证书（Attribute Certificate，AC）、属性权威机构（AA）和AC库等部件的集合，用来完成权限和AC的产生、管理、存储、分发和撤销等功能，下面分别介绍下这三部分：

1.属性证书

2.属性权威机构

3.证书库(AC库)

PMI应用结构

PMI建立在PKI提供的可信的身份认证服务的基础上，采用基于属性证书的授权模式，提供用户身份到应用权限的映射。PMI和PKI之间的主要区别是：

1.PMI主要进行授权管理，证明用户有什么权限、能干什么？

2.PKI主要进行身份鉴别，证明用户身份；

3.两者之间的关系类似于护照和签证，护照是身份证明，可以用来唯一标识个人，同一个护照可以有多个国家的签证，能在指定时间进入相应的国家。

◆当然两者之间的架构也有很多相似之处，例如：

1.为用户数字证书签名的实体被称为CA，签名AC的实体被称为AA

2.PKI信任源被称为根CA，PMI的信任源被称为SOA

3.CA可以有它们信任的次级CA，次级CA可以代理鉴别和认证，SOA可以授权给次级AA

4.如果用户需要废除其签名密钥，则CA将签发CRL。与之类似，如果用户需要废除授权允许（authorization permissions），AA将签发一个AC撤销列表。

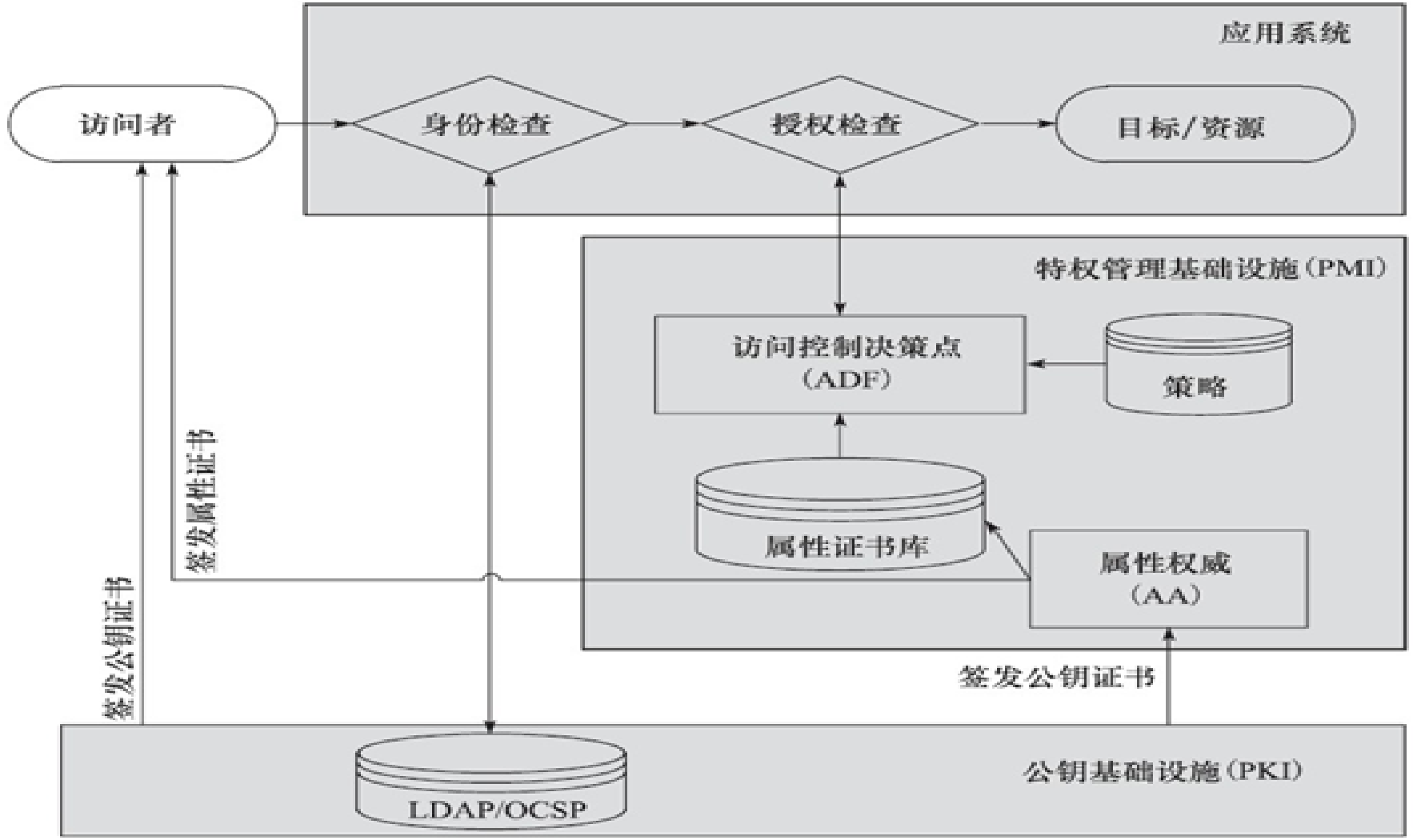


图 2-16　PKI/PMI 应用逻辑结构

第一次作业

- 作业1："XXXX安全问题与目前发展趋势及研究热点"，小报告，字数2000左右。 内容：学生自主选择网络空间安全体系/领域中某一类安全问题，针对此问题查阅资料，介绍该问题的主要关键技术以及相关发展的趋势或研究热点。

  评价标准：1. 格式清爽、文字行距、段落干净整齐 2. 论点清晰，具有一定的逻辑性 3. 论据充分，结论明确 4. 语言运用较好

- **提交到“课程中心”，截止时间4月30日**

THE END