中國科學院大學

听课报告

课程名称:	网络空间安全的密码学导引
学院:	计算机学院
专业:	计算机体系结构
姓名:	卞留念
学号:	201828013229131

2019 年 6 月 30 日

中國科學院大學 听课报告

专业：计算机体系结构
姓名：卞留念
学号：201828013229131
日期：2019 年 6 月 30 日

一、 课程简介

在信息化充分发达的今天，网络空间安全在国家安全中的重要性越来越大。

《网络空间安全的密码学导引》一课讲解了应用在网络空间安全领域的密码学理论。从密码学的基本概念讲起，结合文件加密、磁盘加密、软件保护、VPN、即时通信等密码技术应用实例，从原理上阐述利用密码手段解决网络空间安全中实际问题的思路和方法。

课程的主要内容包括密码学理论、信息隐藏与数字水印、文件系统加密、软件保护、互联网加密技术、操作系统安全简介、网络攻防技术简介等等。

二、 概念与模型

1. 基本概念

以下是密码学中的一些基本概念。

Definition 1 (明文)**.** 明文是指未经加密的文本或字符串。

Definition 2 (密文)**.** 密文是对明文进行加密后的报文。

Definition 3 (加密)**.** 加密是对明文按某种算法进行处理，使其成为不可读的一段代码，使其只能在输入相应的密钥之后才能显示出本来内容。

Definition 4 (解密)**.** 解密是加密的逆过程，即将该编码信息转化为其原来数据的过程。

Definition 5 (Hash)**.** *Hash*，把任意长度的输入（又叫做预映射 *pre-image*）通过散列算法变换成固定长度的输出，该输出就是散列值。

Definition 6 (异或运算)**.** 定义运算 $\oplus$ 如下

$$0 \oplus 0 = 0 \qquad 1 \oplus 1 = 0$$
$$0 \oplus 1 = 1 \qquad 1 \oplus 0 = 0$$

异或运算具有以下性质：

(1) 对于任意的 a，有 $a \oplus b \oplus b = a$

(2) 设 $a \oplus b = c$，如果 a 为 1 的概率是 50%，那么 c 为 1 的概率也是 50%

Kerckhoff's Principle. 一个安全保护系统的安全性不是建立在它的算法对于对手来说是保密的，而是建立在它所选择的密钥对于对手来说是保密的。

2. 密码学基本模型

Model 1. *密码学基本模型如图 1所示。明文通过密钥加密生成密文，密文通过不安全信道传输，密钥通过绝对安全信道传输，接收方使用密钥对密文进行解密后得到明文。*

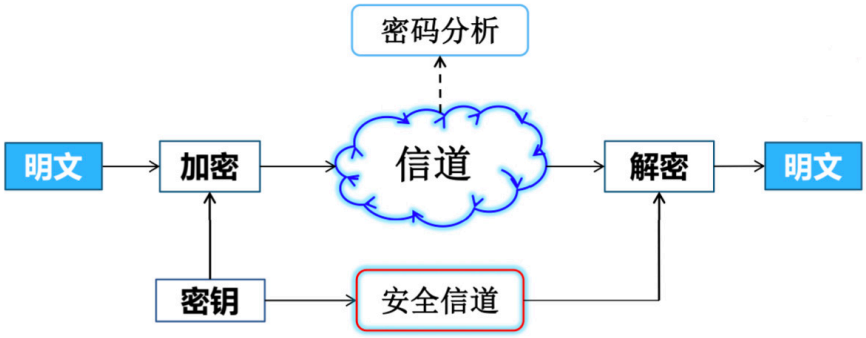

图 1: 密码学基本模型

观察图 1所示的密码学基本模型。在不考虑暴力破解时，整个系统安全性取决于安全信道是否安全，如果是，那么这样的加密是安全的；如果考虑暴力破解，即使安全信道安全，密钥也有被暴力猜解的风险。

在现实生活中，往往不存在绝对安全的信道，密钥也面临暴力猜解的威胁。根据 Kerckhoff 准则可知，密钥是系统安全的关键。基于此模型，出现了许多加密算法，统称为对称加密算法，典型的有：

(1) DES，主要思想在于数据位的置换与移位过程，通过 16 次的迭代加密与最终的逆置换得出最终的密文。安全性较差，但运算简单经济。

(2) AES，AES 加密过程涉及四种操作，分别是字节替代、行移位、列混淆和轮密钥加，解密过程分别为对应的逆操作，加解密中每轮的密钥分别由初始密钥扩展得到。安全性较强。

3. 公私钥密码模型

Model 2. *公私钥密码模型如图 2所示。此模型具有两种密钥，一种是公钥，一种是私钥，公钥可在网上公开传输，私钥仅保存在本地，不在网络上进行传输。*

公私钥密码模型安全性基于 NP 问题难解，基本过程如下：

(1) 选定大素数 p、q，$N = p \cdot q$

(2) $\varphi(N) = (p-1)(q-1)$

(3) 选择随机数 D，满足 $gcd(D, \varphi(N)) = 1$

(4) 取 E，满足 $E \cdot D \equiv 1 \ mod \ \varphi(N)$

(5) E 为公钥，x 为明文，y 为密文，加密算法为 $y \equiv x^E \ mod \ N$

(6) D 为私钥，x 为明文，y 为密文，解密算法为 $x \equiv y^D \ mod \ N$

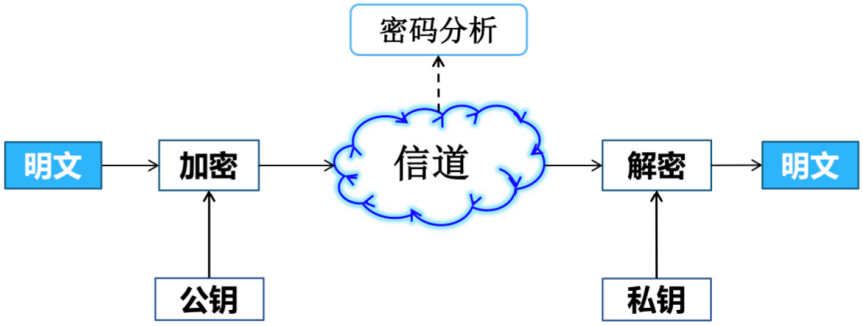

图 2: 公私钥密码模型

三、 密钥

1. 密钥的生命周期

密钥具有如下生命周期

(1) 密钥的生成，主密钥应是高质量的真随机数，加密密钥是根据主密钥和加密算法生成的密钥；

(2) 密钥的配送，通过安全信道传输密钥或者将其安装在保密系统的软硬件中；

(3) 密钥的更换，密钥使用一段时间后，泄露的风险就加大，需要产生新的密钥来代替旧的密钥；

(4) 密钥的保存，将密钥存储在一个独立的、安全的存储介质中；

(5) 密钥的销毁，一旦确定未来不会再需要该组密钥后，就可以从系统中注销该组密钥，并且消除与之相关的所有记录。

2. Diffe-Hellman 密钥协商

Diffe-Hellman. *Diffe-Hellman 密钥协商如图 3所示，该密钥协商机制主要解决如何在不安全信道上约定好密钥以达到保密通信的目的。*

协商过程如下：

(1) 双方约定 p 和 g，确定运算难度

(2) Alice 确定 a 的值

(3) Bob 确定 b 的值

(4) Alice 将 $G_a = g^a \ mod \ p$ 发送给 Bob

(5) Bob 将 $G_b = g^b \ mod \ p$ 发送给 Alice

(6) Alice 计算出密钥 $K_a \equiv G_b^a \ mod \ p$

(7) Bob 计算出密钥 $K_b \equiv G_a^b \ mod \ p$

(8) 由 $g^{ab} \equiv g^{ba}$ 可知 $K_a \equiv K_b$，协商完毕

该密钥协商机制无法抵御中间人攻击。

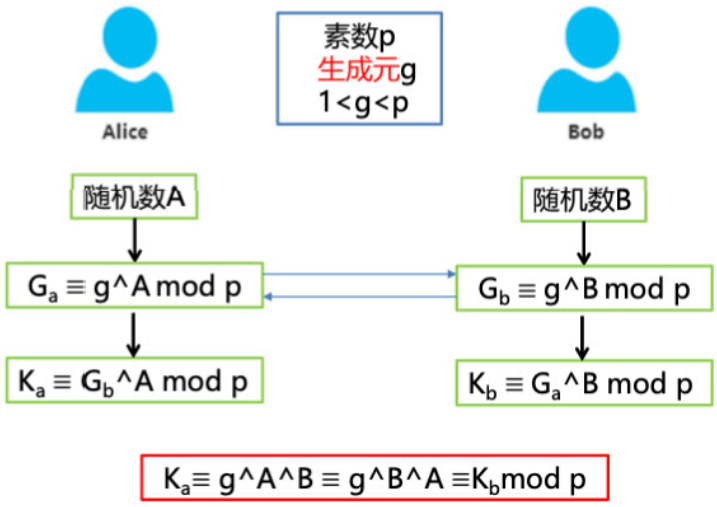

图 3: Diffe-Hellman 密钥协商

3. 盐

密钥生成过程中，加盐与不加盐的情况如图 4所示。

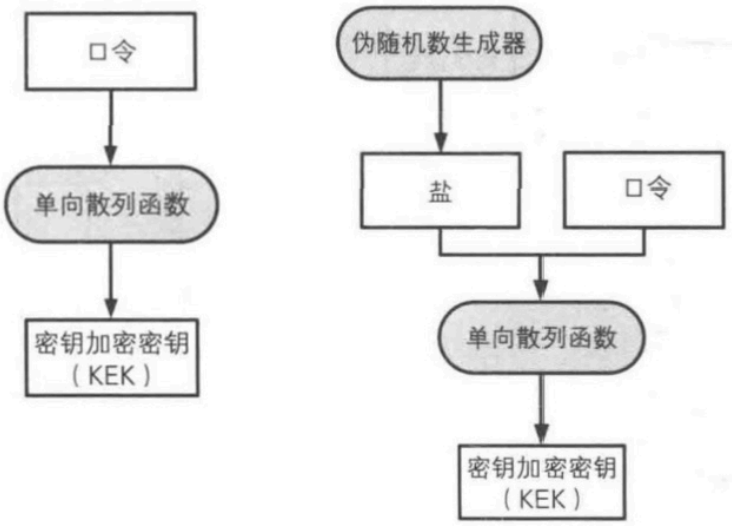

图 4: 加盐与不加盐对比

如图 5所示，不加盐时，由于相同口令对应的密钥值相同，攻击者可能进行字典攻击来暴力猜解。
如图 6所示，加盐时，即便口令相同，只要盐值不同，密钥值也不同，因此无法进行字典攻击。

口令	对应的KEK值
abc	02 E3 29 13 2A D0
abcde	F5 21 62 FE 72 77
abcxyz	81 75 8E B2 9F 66
hello	3E F3 C7 06 DF B7
pass	18 1C 48 22 E6 EF
...	...

图 5: 不加盐示意表

盐	口令	对应的KEK值
5B94E7	abc	4D 58 FD 69 87 38
E5AB9D	abc	EB 4D CB A9 C3 A4
F8DC3B	abc	09 70 F0 7D AC 20
C6541B	abc	44 40 32 6F AB 16
F6C109	abc	1F C5 3C 14 DF D8
...	...	...

图 6: 加盐示意表

四、 随机数

Definition 1 (伪随机数). 伪随机数是按照一定算法模拟产生的，其结果是确定的。

伪随机数又分为强伪随机数和弱伪随机数，其中弱伪随机数只具备随机性，而强伪随机数不仅有随机性，还有不可预测性。

Definition 2 (真随机数). 真随机数是使用物理现象产生的：比如掷钱币、骰子、转轮、使用电子元件的噪音、核裂变等等，这样的随机数发生器叫做物理性随机数发生器，它们的缺点是技术要求比较高。

真随机数具有以下性质：

(1) 随机性

(2) 不可预测性

(3) 不可重现性

五、 密码技术的应用

1. 数字签名

数字签名，就是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

数字签名有两种功效：一是能确定消息确实是由发送方签名并发出来的，因为别人假冒不了发送方的签名。二是数字签名能确定消息的完整性。因为数字签名的特点是它代表了文件的特征，文件如果发生改变，数字摘要的值也将发生变化。

常用的数字签名方案如图 7所示。

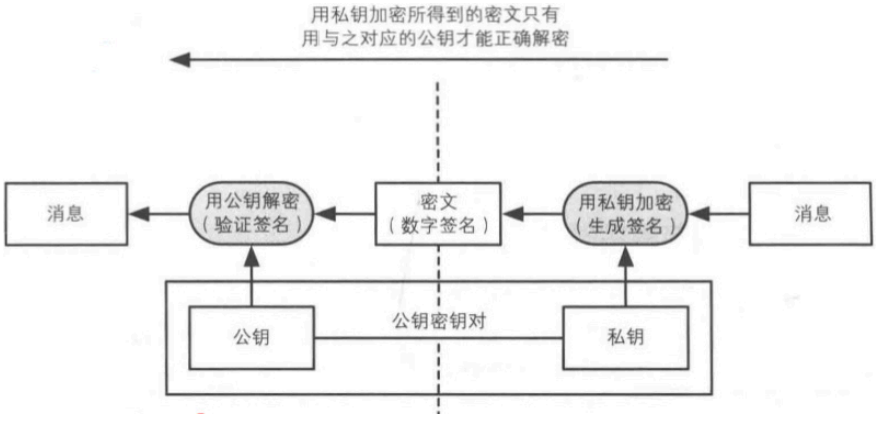

图 7: 数字签名方案

2. 数字证书

若通信双方直接交换信息，容易遭受中间人攻击。由此引入了数字证书的概念，数字证书是通过引入通信双方都信任的第三方机构，第三方机构负责担保消息接受的公钥是合法的。

数字证书工作原理如图 8所示。

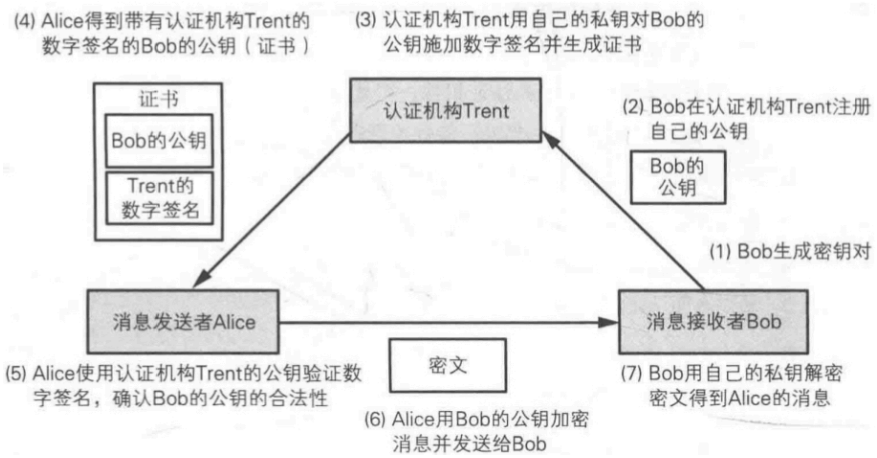

图 8: 数字证书工作原理

3. 软件防篡改

软件保护的一般手段是加壳，在原程序包裹一层程序，也就是壳程序，壳程序加载到内存运行后才会解密释放原程序到内存中运行。

加壳的目的是隐藏程序真正的入口点，这样就难以对程序进行动态分析，以达到保护壳内原始程序以及软件不被外部程序破坏，保证原始程序正常运行。

4. HTTPS

HTTP 在传输数据时使用的是明文，是不安全的，为了解决这一隐患，网景公司推出了 SSL 安全套接字协议层，SSL 是基于 HTTP 之下 TCP 之上的一个协议层，是基于 HTTP 标准并对 TCP 传输数据时进行加密，所以 HTTPS 是 HTTP+SSL/TCP 的简称。

TLS 是更为安全的升级版 SSL。由于 SSL 这一术语更为常用，因此我们仍然将我们的安全证书称作 SSL。

TLS/SSL 是一种加密通道的规范，它利用对称加密、公私钥不对称加密及其密钥交换算法，CA 系统进行数据加密从而进行安全的数据传输。

5. VPN

VPN 架构中采用了多种安全机制，如隧道技术、加解密技术、密钥管理技术、身份认证技术等，通过上述的各项网络安全技术，确保资料在公众网络中传输时不被窃取，或是即使被窃取了，对方亦无法读取数据包内所传送的资料。

6. 文件加密

各种存储设备往往是证据被发现的地方，文件加密是指文件在硬盘上是密文，在内存中是明文，以此来保证在存储设备泄露的情况下，文件内容不会泄露出去。

六、 信息隐藏

1. 信息隐藏与密码学的区别

加密是对信息本身进行保护，但是信息的传递过程是暴露的。信息隐藏是研究如何掩盖信息存在的事实。密码学保护的是通信的内容，信息隐藏保护的是通信的存在。

2. 基于图像位平面的数字信息隐藏

在古代，有各种各样的隐写术存在，下面介绍一种基于图像位平面的数字信息隐藏方法。

数字图像是由一个一个的像素点组成，每个像素的颜色都可以用 rgb 表示法表示为一个三元组，如图 9所示，三元组具有三个 8 比特长的二进制串。

(207, 137, 130)	(220, 179, 163)	(215, 169, 161)	(210, 179, 172)	(210, 179, 172)
(207, 154, 146)	(217, 124, 121)	(226, 144, 133)	(226, 144, 133)	(224, 137, 124)
(227, 151, 136)	(227, 151, 136)	(226, 159, 142)	(227, 151, 136)	(230, 170, 154)
(231, 178, 163)	(231, 178, 163)	(231, 178, 163)	(236, 187, 171)	(236, 187, 171)
(239, 195, 176)	(239, 195, 176)	(240, 205, 187)	(239, 195, 176)	(231, 138, 123)
(217, 124, 121)	(215, 169, 161)	(216, 179, 170)	(216, 179, 170)	(207, 137, 120)
(159, 51, 71)	(189, 89, 101)	(216, 111, 110)	(217, 124, 121)	(227, 151, 136)
(227, 151, 136)	(226, 159, 142)	(226, 159, 142)	(237, 159, 135)	(237, 159, 135)
(231, 178, 163)	(236, 187, 171)	(231, 178, 163)	(236, 187, 171)	(236, 187, 171)
(236, 187, 171)	(239, 195, 176)	(239, 195, 176)	(236, 187, 171)	(227, 133, 118)
(213, 142, 135)	(216, 179, 170)	(221, 184, 170)	(190, 89, 89)	(204, 109, 113)
(204, 115, 118)	(189, 85, 97)	(159, 60, 78)	(136, 38, 65)	(160, 56, 75)
(204, 109, 113)	(227, 151, 136)	(226, 159, 142)	(237, 159, 135)	(227, 151, 136)

图 9: 图像的三元组表示

由 rgb 表示法可知，修改每个二进制串的最低位的值，对图像影响最小，修改每个二进制串最高位的值，对图像影响最大。根据这一性质，我们将二进制串的 8 个比特位分成 8 个位平面，称每个二进制串最低位所含数据是第 1 个位平面，称每个二进制串最高位所含数据是第 8 个位平面。

下面是一个删去位平面的例子。如图所示 10是原始 Lena 图像。

如图 11所示是去掉第 1 个位平面的 Lena 图像和第 1 个位平面。

如图 12所示是去掉第 1-7 个位平面的 Lena 图像（即第 8 个位平面）和第 1-7 个位平面。

由此例可以发现，人肉眼几乎无法分辨第 1 个位平面的存在，所以可将数字信息隐藏在第 1 个位平面中以达到信息隐藏的目的。

图 10: 原始 Lena 图像

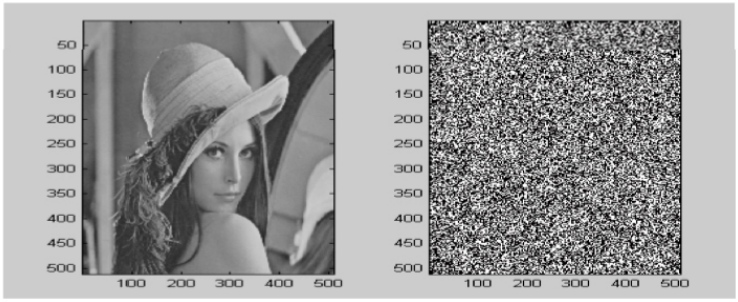

图 11: 去掉第 1 个位平面的 Lena 图像和第 1 个位平面

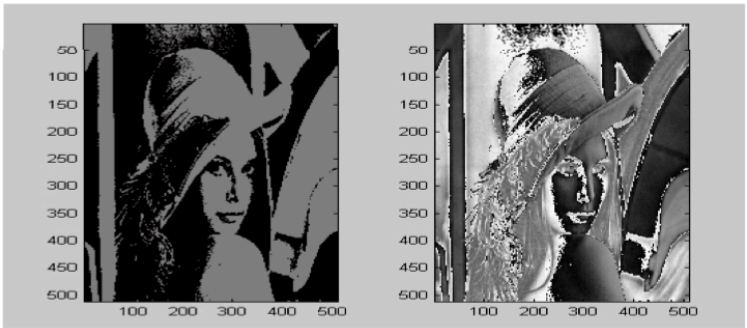

图 12: 去掉第 1-7 个位平面的 Lena 图像和第 1-7 个位平面