现代密码学 Q&A

3.传统加密

3.1 对称密钥的五个基本要求?

明文、密文、密钥、加密、解密

3.2 密码算法中两个基本函数?

代替和替换

3.4 分组密码和流密码的区别是什么?

分组密码是明文块被视为一个整体，用来产生一个相同长度的密文块。

流密码是加密的数字数据流的一个位或一次一个字节。

3.5 攻击密码的两种一般方法是什么?

1.密码学分析攻击

2.穷举攻击

3.6 列出并简要的定义基于攻击者所知道信息的密码分析攻击类型?

1.唯密文攻击：只知道算法和密文

2.已知明文攻击：知道一些明文-密文对

3.选择明文攻击：选择一些明文得到密文

4.选择密文攻击：选择一些密文得到明文

5.选择攻击：选择明文/密文去加密/解密

3.7 无条件安全密码和计算上安全密码的区别?

1.无条件安全密码是指无论使用多少的计算机算力或时间，密码都不可被攻破

2.计算上安全密码是指在给定的计算机资源下，密码无法被攻破

3.8 为什么凯撒密码容易被穷举攻击攻破?

因为凯撒密码只有25种密钥

3.9 单表代替密码的密钥空间?

26!

3.10 Playfair密码的缺点?

保留了明文语言的结构特征，可以用统计学方法攻击

3.11 单表代替密码和多表代替密码的区别?

多表代替密码即是对每个字母进行一次单表代替。密钥空间为26^n

3.12 一次一密的两个问题?

1.产生大规模随机密钥很困难

2.密钥的分配和保护很困难

3.13 什么是置换密码?

对明文进行排列

3.14 隐写术的缺点?

需要许多额外的付出来隐藏较少的信息

4.分组加密和DES

4.3 为什么说使用任意可逆替代密码不可行?

因为对于n位的的分组密码，密钥长度为n * (2 ^ n)位

4.5 混淆和扩散的区别?

混淆：使密钥和密文的关系变得尽可能复杂

扩散：将明文的统计特征分散在密文中，即让每个明文数字尽可能影响多个密文数字

在扩散中，明文的统计结构被消散为密文的远程统计。 这是通过使每个明文数字位影响许多密文数字位的值来实现的，这等效于说每个密文数字位都受到许多明文数字位的影响。 混淆试图使密文的统计信息和加密密钥的值之间的关系尽可能复杂，以再次阻止发现密钥的尝试。 因此，即使攻击者可以对密文的统计信息有所了解，使用密钥生成密文的方式也非常复杂，以致于难以推断出密钥。 这是通过使用复杂的替换算法来实现的。

4.6 哪些参数与实际选择决定了实际的Feistel算法?

块长度、密钥长度、迭代轮次、子密钥产生算法、F函数算法

习题4.1

1.证明对于n个位的分组长度，理想分组密码的不同可逆映射个数为2 ^ n !个。

答：对于n位的分组，一共有2^n个密文分组，对于第一个明文，可以选择2^n中任意一个，对于第二个明文，可以选择2^n - 1中任意一个，则映射个数为2 ^ n !

2.理论上，密钥长度可以为log2（2^n）！ 位。 例如，为每个映射分配一个从1到（2^n）！ 的数字 并维护一个表格，其中显示了每个此类数字的映射。 然后，该密钥仅需要log2（2^n）！ 位，但我们也需要这个巨大的表。 定义密钥的一种更直接的方法是让密钥由每个明文块的密文值组成，并按顺序列出明文块0到2^(n –1)。这是表3.1所建议的。 在这种情况下，密钥大小为n*2^n，并且不需要巨大的表。

5.AES高级加密

5.1 为什么AES解密可以和加密使用一样的结构?

加密过程为：字节代替、行移位、列混淆、轮密钥加，原本解密过程为：逆向行移位、逆向字节代替、轮密钥加、逆向列混淆。

但是逆向行移位只改变字节的顺序，不改变字节的内容、逆向字节代替只改变字节的内容，不改变字节的顺序，故可以交换。

轮密钥加、逆向列混淆不改变状态中字节的顺序，但是两个操作对于列输入是线性的，即对于给定的状态S和轮密钥W

逆向列混淆（S + W） = [逆向列混淆 S] + [逆向列混淆 W]

6.工作模式

6.1 什么叫中间相遇攻击?

中间相遇攻击 虽然双重 DES 对应的映射与单 DES 对应的映射不同，但是还有另外一种攻击方法，这种方法不依赖于 DES 的任何特殊性质，对所有分组密码都有效。

该算法称为中间相遇攻击，文献[DIFF77]首次对它进行了描述。它基于如下观察：假设

$$C = \mathrm{E}(K_2, \mathrm{E}(K_1, P))$$

则有［参见图 7.1(a)］

$$X = \mathrm{E}(K_1, P) = \mathrm{D}(K_2, C)$$

给定明密文对 (P, C)，攻击如下展开：首先，将 P 按所有可能的密钥 K_1 加密，得到的 2^{56} 个结果按 X 的值排序放在一个表内。然后将 C 用所有可能的密钥 K_2 解密，每解密一次就将解密结果与表中的值比较，如果有相等的，就用刚才测试的两个密钥对一个新的明密文对进行验证。如果两个密钥产生了正确的密文，就认定这两个密钥是正确的密钥。

7.密钥分发

7.1 解释为什么中间人攻击对图14.3中讨论的秘密密钥分发协议无效。

图14.3：

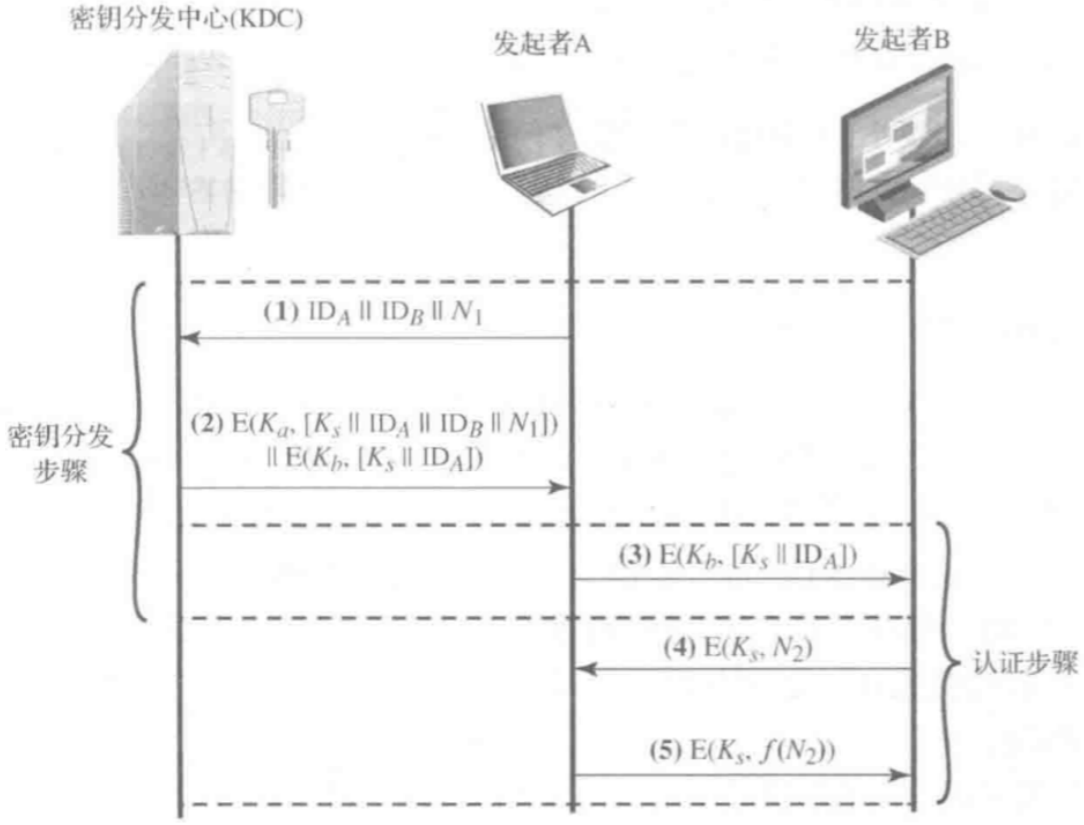

图 14.3 密钥分发方案

中间人就算截获到消息，但是由于不知道KDC与A B共享的主密钥，无法伪造消息。

7.2 端到端密钥分发的主要问题是什么？ 密钥层次结构的概念是如何解决该问题的?

需要的密钥个数太多。如果有N个端，则需要(N * (N - 1)) / 2个密钥。

每个用户和KDC之间有唯一的主密钥，用主密钥来分发会话密钥。这样只需要分发和保护N个密钥即可

7.3 什么是临时交互号(nonce)?

用于标识该次传输，可以是一个时间戳、计数器或随机数

习题14.1

14.1 本地网络向量提供一个密钥分发方案，如图 14.18 所示。

（a）描述该方案。

（b）相比图 14.3 的方案，有哪些优点和缺点。

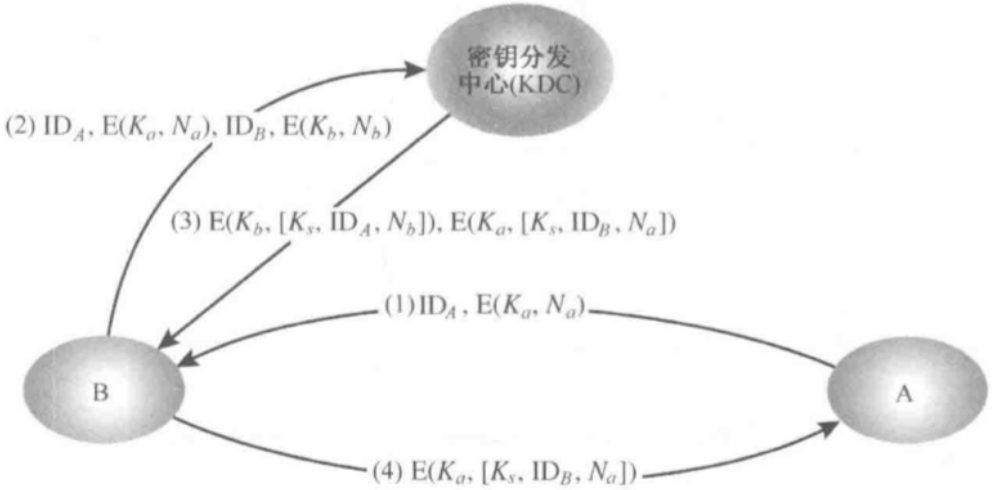

图 14.18 习题 14.1 的图

A使用B与A与KDC共享的密钥加密的事件标记或随机数（Na）向B发送连接请求。 如果B准备接受连接，它将向KDC发送请求以获取会话密钥，包括A的加密随机数以及B生成的随机数（Nb），并使用B与KDC共享的密钥进行加密。 KDC将两个加密的块返回给B。一个块供B使用，并包括会话密钥，A的标识符和B的现时。 为A准备了一个类似的块，并将其从KDC传递到B，然后传递到A。A和B现在已安全地获取了会话密钥，并且由于该随机数，可以确保另一个密钥是真实的。 b。 提议的方案似乎提供了与图14.3相同的安全等级。 所提出的方案的一个优点是，在B拒绝连接的情况下，避免了与KDC交互的开销。

习题14.2

14.2 “福尔摩斯，我们有很大的压力。”侦探 Lestrade 看起来很紧张。“我们已经知道，一些敏感的政府文件复印件出现在伦敦一个外国大使馆的电脑上，通常，这些文件一般以电子形式存放在少数几台政府计算机上，满足最严格的安全要求。有时要通过网络连接发给所有的政府计算机，但是这些消息是由我们最好的加密专家鉴定的绝密算法加密的，NSA 和 KGB 都无法破解。但是现在这些文件却出现在一个小的甚至是无关紧要的国家的外交官手里，我想不明白为什么会发生这种事情。”

“但是你已经有了嫌疑人，不是吗？”福尔摩斯问。

“是的，我们做了一些调查，有一个男人合法地访问过一台政府计算机，并且和那个外交官联系很频繁。但是他访问的不是那些文件通常存放的计算机，他是嫌疑犯，但我们不知道他是如何获得文件复印件的。即便他得到加密的文件，也不能解密。”

“请描述下，该网络使用的通信协议。”福尔摩斯睁开眼睛，以告诉 Lestrade 他虽然一脸睡意但是他还是在认真听着。

“协议如下，网络中的每个节点 N 都有唯一的密钥 K_n，用于节点和可信服务器之间的安全通信，即所有的密钥也在服务器中存放。用户 A 想要发送秘密消息 M 给 B 时，使用以下协议：

（1）A 产生临时交互号 R，发送自己的名字 A、目的地 B 和 $E(K_a,R)$ 给服务器。

（2）服务器回复消息 $E(K_b,R)$ 给 A。

（3）A 发送 $E(R,M)$ 和 $E(K_b,R)$ 给 B。

（4）B 使用 K_b 解密 $E(K_b,R)$ 得到 R，随后应用 R 解密 $E(R,M)$ 得到消息 M。

“我相信你有你的道理，Lestrade。这个协议是不安全，因为服务器不能鉴定谁发的请求。明显地，协议设计者相信发送 $E(K_x,R)$ 就可以鉴定发送者为用户 X，因为只有 X 知道 K_x，但是你也知道 $E(K_x,R)$ 可能被截获然后重放。只要知道漏洞在哪里，通过监控该男子对访问计算机的使用，可以得到更多的证据。他最有可能是这么做的：截获 $E(K_a,R)$ 和 $E(R,M)$ 后，我们称该男子为 Z，会假装 A，然后……”

完成福尔摩斯的话。

8.公钥体制

8.1 什么是公钥证书?

认证机构将用户的姓名和公钥绑定在一起， 用户用自己的私钥对数字文件签名后，可以通过证书识别签名者，因为签名者是唯一拥有与证书上对应的私钥的用户。

证书允许密钥交换，而无需实时访问公钥授权。

8.2 公钥和私钥的角色分别是什么?

8.3 公钥密码体制的三种应用是什么?

数据保密、密钥分配、数字签名

8.4 为得到安全算法，公钥密码体制应满足哪些要求?

对于公钥，无法推出私钥。两个密钥都可用于加密/解密

8.5 什么是单向函数?

每个函数值都存在唯一的逆，求出函数值很容易，但是无法求出逆。

8.6 什么是单向陷门函数?

一个函数，若计算函数值很容易，并且在缺少一些附加信息时计算函数的逆是不可行的，但是已知这些附加信息时，可在多项式时间内计算出函数的逆，那么称这样的函数为单向陷门函数。

习题

9.11

9.11 “我想告诉你，福尔摩斯，”华生激动地说，“你最近进行的网络安全活动让我对密码学产生了浓厚的兴趣，就在昨天，我发现一次一密的加密方法是可行的。”

“噢？真的吗？”福尔摩斯从睡意蒙眬中醒过来。“这么说，你找到了一种生成强密码序列的确定性方法了？”

“千真万确，福尔摩斯。这个想法倒是挺简单的。对给定的单向函数 F，通过将 F 应用于某标准的变量参数序列，我就产生了一个长伪随机数序列。假使密码分析者知道了 F 和序列的一般性质，这个性质可能很简单，比如 S，$S+1$，$S+2$，...，而不知道 S，由于 F 的单向性，没人能够对某 i，从 $F(S+i)$推出 S，即使他得到了序列的一段，他也不能确定其他部分。”

“华生，我担心你的想法并非无懈可击，至少它要求 F 满足一些附加条件。我们考虑一下。例如，RSA 加密函数 $F(M)=M^K \bmod N$，K 是保密的，这个函数被认为是单向的，但是我不赞成将这种方法用于类似 $M=2$，3，4，5，6，…这样的序列。”

“为什么，福尔摩斯？”华生大惑不解，“为什么你认为，如果 K 是保密的，那么像 $2^K \bmod N$, $3^K \bmod N$, $4^K \bmod N$, …这样的序列不适合于一次一密？”

“因为它至少是部分可预测的，亲爱的华生，即使 K 是保密的，如你刚才所说，假定密码分析者知道了 F 和序列的一般性质，再假设他能截获一小段输出序列，在密码学界这种假设是可行的。对于该输出序列，已知最前面的两个元素，即使他不能预测出所有元素，但他可预测出该序列中后续的许多元素。因此这样的序列在密码学上不能被认为是强序列。利用预测出的较长的序列段，他可预测出序列中更多的元素。瞧，已知序列的一般性质和序列的前面两个元素：$2^K \bmod N$, $3^K \bmod N$，就很容易计算出后续元素……”

请说明这是如何做到的？

9.15

9.15 “这是一个非常有趣的案例，华生。”福尔摩斯说，“这个年轻人爱上了一个女孩，这个女孩也爱他。但是女孩的父亲非常怪，他坚持要求他未来的女婿以公钥密码体制为基础设计一个简单安全的协议，以便他在公司的计算机网络中使用。这个年轻人提出了下列两方通信协议：假设用户 A 要将消息 M 发送给用户 B［交换的消息形为(发送方的姓名，消息正文，接收方的姓名)］”

（1）A 将$(A, E(PU_b, [M, A]), B)$发送给 B；

（2）B 发送应答$(B, E(PU_a, [M, B]), A)$给 A；

“这个协议确实很简单，但是女孩的父亲还是认为该协议不够简单，因为这种协议中存在一些冗余，可进一步简化为

（1）A 将$(A, E(PU_b, M), B)$发送给 B；

（2）B 发送应答$(B, E(PU_a, M), A)$给 A；

由于这个原因，女孩的父亲不许他的女儿与年轻人结婚，这使得他们非常不愉快，因此年轻人来我这里请求我的帮助。”

“嗯，我不知道你会怎样帮助他。”华生想到年轻人要失去他心爱的人，显得有些不快。

“我想我可以帮助他，你知道，华生，冗余有时候对保证协议的安全性是有好处的，因此女孩父亲简化后的协议容易受到一种攻击，而年轻人设计的协议能够抗这种攻击。”福尔摩斯若有所思地说，“有办法了，华生。瞧，攻击者必须是网络用户中的一员，且能够截获 A 和 B 交换的消息。因为

是网络中的用户，所以他自己也有公钥，并且他可以发消息给 A 或 B，也可以接收 A 或 B 发出的消息。如果使用这个简化后的协议，那么他可以按下述过程得出 A 以前发送给 B 的消息 M，……”请完成上述的过程。

9.18

9.18 这个习题说明了选择密文攻击的简单应用。Bob 截获了一份发给 Alice 的密文 C，该密文是用 Alice 的公钥 e 加密的。Bob 想获得原始消息 $M=C^d \bmod n$。Bob 选择一个小于 n 的随机数 r，并计算

$$Z = r^e \bmod n$$
$$X = ZC \bmod n$$
$$t = r^{-1} \bmod n$$

接着，Bob 让 Alice 用她的私钥对 X 进行认证（如图 9.3 所示），从而对 X 进行解密。Alice 返回 $Y=X^d \bmod n$。请说明 Bob 如何利用获得的信息去求取 M。

11.Hash函数

11.1 安全Hash函数需要具有哪些特性?

输入长度可变、输出长度固定、效率、抗原像攻击(单向性)、抗第二原像攻击(抗弱碰撞性)、抗碰撞攻击(抗强碰撞性)

11.2 抗弱碰撞和抗强碰撞之间的区别是什么??

抗弱碰撞性：对于给定的x，找到y使得 H(x) = H(y)在计算上是不可行的

抗强碰撞性：找到任何满足H(x) = H(y)在计算上是不可行的

11.3 Hash函数中的压缩函数的作用是什么??

使得任意输入长度的消息可以产生固定长度的HASH值

11.5 SHA中使用的基本算术和逻辑函数是什么??

异或

12.消息认证码MAC

12.1 消息认证可解决哪些类型的攻击?

伪装、内容修改、顺序修改、计时修改

12.2 消息认证或数字签名机制中有哪两层功能?

1.验证消息完整性的函数

2.认证消息的函数

12.3 产生消息认证的方法有哪些?

Hash函数、消息加密、MAC

12.4 当将对称加密和错误控制码结合使用进行消息身份验证时，必须按什么顺序执行这两个功能?

先错误控制，再加密。

12.5 什么是消息认证码?

利用密钥来生成一个固定长度的数据块，并将该数据块附加在消息之后。

12.6 消息认证码和单向Hash函数有什么区别?

单向Hash函数不需要key。

12.8 为了攻击MAC算法，必须要恢复密钥吗?

不是必要。穷举攻击可以直接攻击MAC而不试图找出密钥。这种攻击是对给定的消息产生有效的MAC或者对给定的MAC产生对应的消息。

使用DAA生成消息身份验证代码是否安全，为什么?

不安全。如果T = MAC(K,X)，攻击者可构造X || (X⊕T)，得到的MAC还是T

使用Hash（Message || Pad（M）|| key）生成消息认证码是否安全，为什么?

不安全

使用Hash（key || Message）生成消息认证码是否安全，为什么?

不安全

13.数字签名

13.1列出在消息身份验证中可能引起的两个争议。

13.2数字签名应具有哪些性质?

1.它必须能验证签名者、签名日期和时间
2.它必须能认证被签的消息内容。
3.签名应能由第三方仲裁，以解决争执。

13.5应该以什么顺序将签名函数和保密函数应用于消息，为什么?

先签名，再保密

13.6直接数字签名方案有哪些威胁?