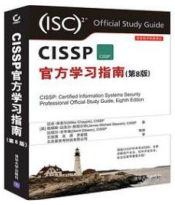


笔记二【OSG】6章：密码学和对称密钥算法

全书结构

本书的组织结构

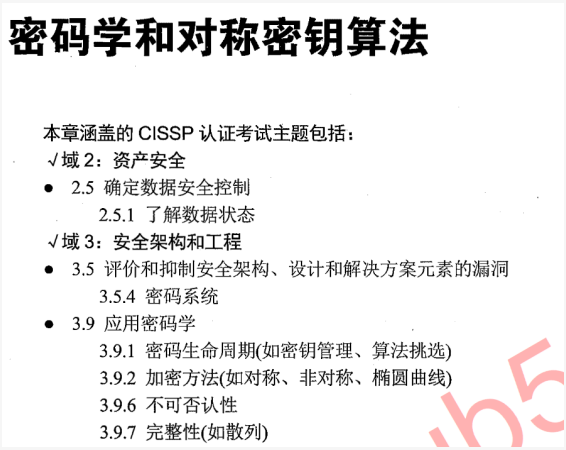
本书涵盖 CISSP 通用知识体系的 8 个域，其深度足以让你清晰掌握相关资料。本书的主体由 21 章构成。域和各章的关系说明如下。

第 1~4 章：安全与风险管理。
第 5 章：资产安全。
第 6~10 章：安全架构和工程。
第 11 章和第 12 章：通信与网络安全。
第 13 章和第 14 章：身份和访问管理(IAM)。
第 15 章：安全评估与测试。
第 16~19 章：安全运营。
第 20 章和第 21 章：软件开发安全。

每章包含的元素可帮助你归纳学习重点和检验你掌握的知识。有关每章所涵盖域主题的详情，请见本书目录和各章介绍。

笔记二【OSG】6章：密码学和对称密钥算法

本章覆盖CBK内容



1

密码可为敏感信息提供**保密性、完整性、身份验证和不可否认性**保护。

2

凯撒密码：古罗马时代征战欧洲的朱利叶斯·凯撒用来与身在罗马的西塞罗传递消息的密码。

> 加密一条消息时，你只需要将字母表上的**每个字母向右移三位**就可以了。例如， A 变成 D, B 变成 E，凯撒密码还被叫作 **ROT3 （或 Rotate 3, 轮转 3) 密码**。
>
> 变种：例如ROT12每次右移12位将A变为M，B变为N。
>
> 凯撒密码面对**"频率分析"攻击**时十分脆弱。

3

密码学的目标：

- **保密性** (Confidentiality) 确保数据在**静止、传输（也称"运动中的数据"）**和**使用**等三种不同状态下始终保待私密。

  > 有两大类密码系统专用千实现保密性：**对称密码系统、非对称密码系统**。

- **完整性** (Integrity) 确保数据没有被人未经授权更改。

  > 消息完整性通过使用加密的消息摘要实现；这个摘要叫"数字签名"，是在消息传输时创建的。

- **身份验证**（Authentication）用于验证系统用户所声称的身份。

  > 挑战-应答协议是执行身份验证的一种方案。对称和非对称密码都能执行身份验证。

- **不可否认性（Nonreputation）**向接受者保证：消息发自发送者，而且没有人冒充发送者。

  秘密密钥或对称密钥密码系统（例如简单的替换密码）不提供不可否认性保障。不可否认性由公钥或非对称密钥密码系统提供。

4

一些密码学基本概念：

一条消息进入编码形式之前，叫作**明文消息**，描述加密功能时用字母 P 表示。一条消息的发送者用一种密码算法给明文消息加密，生成一条**密文消息**，用字母 C 表示。

所有密码算法都**靠密钥维持安全**。多数情况下，**密钥是一个数，**通常是一个**极大的二进制数**。

每种算法都有一个特定**密钥空间**。密钥空间是一个特定的数值范围，而某一特定算法的密钥在这个范围内才有效。密钥空间由位大小决定，密钥空间为0到2^n，表示密钥为n位二进制数。

科克霍夫原则（也叫**科克霍夫假设**）：即便有关密码系统的一起人尽皆知，只要密钥不被别人掌握，密码系统也应该是安全的。“随敌人去了解我们的系统。”

> 算法公布于众可以带来更多活力，更容易暴露出更多弱点，最终导致放弃不够强力的算法，更快采用合适的算法。

创建和执行秘密代码和密码的技艺叫**密码术**（也叫**加密法**）。而**密码分析**研究的是打败代码和密码的方法。密码术和密码分析合在一起，就是我们通常说的**密码学**。

一种代码或密码在硬件和软件中的具体执行叫**密码系统**。

> 联邦信息处理标准 (FIPS)140-2“ 密码模块的安全要求”定义了可供联邦政府使用的密码模块的硬件和软件要求。

私钥密码系统、秘密密钥密码系统、对称密码系统：参与者使用一个共享密钥。

> *注：本书提到了表示对称密码的多种术语，在日常工作中“私钥密码”、“秘密密钥密码”并不常用，需要注意考试中遇到，尤其是“私钥密码”。*

公钥密码系统、非对称密码系统：每个参与者都有一个密钥对。

5

密码数学：

布尔数学：FALSE or TRUE。

逻辑运算：AND、OR、NOT、Exclusive OR，按位进行的“与”、“或”、“非”、“异或”运算。

模函数：一次除法运算后的余数，如8 mod 6 = 2，mod运算有时也使用“%”表示。

单向函数 (One-Way Function) 是便于为输入的每种可能组合生成输出值的一种数学运算，但这一运算会导致无法恢复输入值。

> 实践又从来没有证明，任何具体的已知单向函数确实是单向的。这些函数被未来的密码分析者破解的可能性始终存在。

Nonce：是一个**随机数**，可在数学函数中充当占位符变量。比较有名的Nonce例子之一是**初始化向量(IV)**。

零知识证明：你向某个第三方证明，你确实知道一个事实，但同时不把这个事实本身披露给第三方；这样的机制借助密码学形成，通常通过口令和其它秘密鉴别符实现。零知识证明是一种通信概念。

分割知识：把职责分离和双人控制融于一个解决方案的做法叫"分割知识"。"密钥托管"概念是体现分割知识的最佳例子。**N 分之 M 控制**要求操办人总数(N）中至少要有 M 个操办人同时在场才能执行高安全级任务。因此，**八分之三控制**要求，在被指派可执行密钥托管恢复任务的8 个操办人中，要有 3 个同时在场才能从密钥托管数据库中提取一个密钥（其中 M 永远要小于或等于 N) 。

代价函数：对一个加密系统实施一次完整蛮力攻击所需付出的时间和精力，通常是代价函数所代表的内容。挑选密码系统的安全专业人员除了了解数据具有价值的时间长度外，还必须了解新涌现的技术可能对破解密码的努力产生什么影响。一个密码系统提供的保护与它的代价函数／因子值呈正比例关系。

6

密码的定义：

> **代码**是由代表单词和短语的符号构成的密码系统（*注：类似于代号、暗语*）；代码尽管有时是保密的，但它们并不一定提供保密性保护。
>
> **密码**通过各种技术手段更改和／或重新排列消息的字符或位，以达到实现保密性的目的。密码始终要隐藏消息的真实含义。密码以位、字符或块（即消息的一个固定片段，通常以位数表示）为单位将消息从明文转变成密文。

> **移位密码**：移位密码(transposition cipher)通过一种加密算法重新安排明文消息的字母，形成密文消息（*注：仅位置变化*）。解密算法只需要逆向执行加密转换便可恢复原始消息。

替换密码："替换密码 "(substitution cipher) 通过加密算法用一个不同的字符替换明文消息的每个字符或位。

> **凯撒密码(ROT3密码)就是替换密码**的一个例子。结合模函数运算，ROT3密码的加密过程可表示为：C = (P + 3) mod 26，解密为：P = (C - 3) mod 26。
>
> **多表替换密码（如Vigenere密码系统）**是一个更为复杂的替换密码例子。

> **单次密本(one-time pad)**：是极其强力的一种**替换密码**。单次密本为明文消息中的**每个字母使用一个不同的替换字母表**。C = (P + K) mod 26。单次密本也叫**Vernam密码**，以发明者AT&T贝尔实验室的Gilbert Sandford Vernam命名。
>
> - 单次密本必须随机生成。
> - 单次密本必须处于物理保护之下，以防泄露。
> - 每个单次密本必须只使用一次。
> - 密钥必须至少与将被加密的消息一样长。
>
> 单次密本的优势在于使用得当，能够不可破解；劣势在于生成、分发和保护所要求的冗长密钥实在太难。
>
> 凯撒密码、 Vigenere 密码和单次密本彼此很像。它们之间的**唯一区别是密钥长度**。凯撒移位密码所用密钥的长度为 1, Vigenere 密码使用的密钥要长一些（通常是一个词或一句话），而单次密本使用的密钥与消息本身一样长。
>
> **运动密钥密码(running key cipher)**，也可称为**书密码**：加密密钥与消息本书一样长，而且往往选自一本普通书籍。本质上仍是一种替换密码，C = (P + K) mod 26。

块密码：块密码 (**block cipher**) 在消息“块“上运算，在同一时间对整个消息执行加密算法。**移位密码是块密码的例子。**

流密码：流密码 (**stream cipher**) 一次在消息（或消息流）的一个字符或一个位上运行。凯撒密码和单次密本都是流密码的例子。

混淆与扩散：密码算法依靠两种基本运算来隐藏明文消息——混淆 (confusion) 和扩散 (diffusion) 。**明文和密钥之间有着极复杂的关系**，迫使攻击者放弃只靠改动明文和分析结果密文来确定密钥——这就是**混淆**。**明文发生一点变化，会导致多个变化在整个密文中传播**——这就是**扩散**。

> 一个例子：一种密码算法首先进行一次复杂的替换，然后通过移位重新安排被替换密文的字符位置。在这个例中，替换带来的是混淆，移位带来的是扩散。

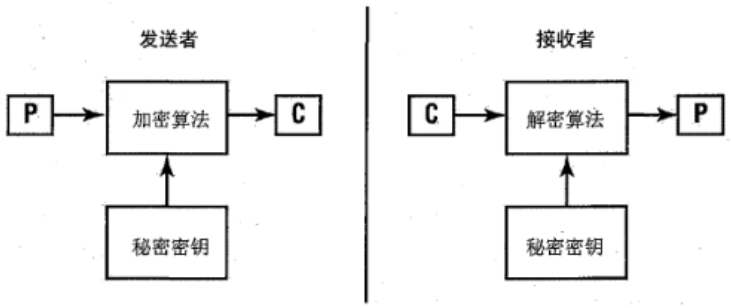
7

现代密码系统通过计算机化复杂算法和长密码密钥来实现密码学的保密性、完整性、身份验证和不可否认性目标。现代密码系统不依靠算法的保密性，所依靠的是为一个或多个密码密钥保密。密钥越长，破解密码系统越难。

对称密钥算法：对称密钥算法依靠一个分发给所有通信参与方的“共享秘密“加密密钥。也叫**秘密密钥加密法**和**私钥加密法**。

> 弱点：密钥分发是主要问题；不提供不可否认性；缺乏可伸缩性；密钥必须经常重新生成。

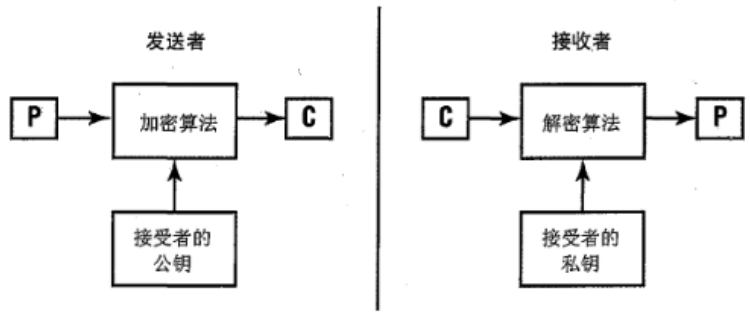
> 优势：运算速度非常快，对比非对称密码算法快1000至10000倍。
>
> 密钥数量要求：**密钥数** = n(n-1) / 2。n为用户数量，因此当用户数规模较大时，需要的大量密钥，缺乏可伸缩性。



对称密钥加密法

非对称密钥算法：也叫**公钥算法**。每个用户都有**两个密钥**：一个是所有用户共享的**公钥**，另一个是只有用户自己知道
并保守秘密的**私钥**。如果 Alice 想用公钥加密法给 Bob 发一条消息，她首先创建这条消息，然后用 Bob 的公钥给消息加密。

> 优势：添加新用户只需要生成一对新的密钥对；便于从非对称系统中移除用户；只需要在用户私钥失信的情况下重新生成密钥；可提供完整性、身份验证、不可否认；密钥分发简便易行；不需要预先建立通信关联。
>
> 弱点：运算速度缓慢。



非对称密钥加密法

对称密码	**非对称密码**	
单个共享密钥	密钥对集	
带外交换	带内交换	共享密钥交换往往需要另一个安全的密钥分发方法，如线下（即带外交换）
不可扩展	可扩展	
速度快	速度慢	
大批量加密	少量数据、数字签名、数字封装、数字	*注：书中的数字封装，可能为"数字信封"*

	证书	
保密性	保密性、完整性、身份验证、不可否认性	可实现的密码学目标

散列算法：

> 用于对消息进行单向地归纳；对于理想的散列函数，逆向推导出消息即便不是完全不可能，也极其困难。
>
> 一个散列函数为两种不同消息产生相同的值的情况叫做**冲突（也叫碰撞）**，冲突的存在会导致散列算法贬值。
>
> 散列算法常与非对称密码一起使用提供数字签名能力，用于提供完整性和不可否认性目标。

8

常用的几种对称密码系统：数据加密标准（DES）、国家数据加密算法（IDEA）、Blowfish、Skipjack、高级加密标准（AES）。

数据加密标准（Data Encryption Standard, DES）：美国政府于 1977 年发布数据加密标准，提议将其用作所有政府通信的标准密码系统；由于算法存在缺陷与2001年12月被高级加密标准取代。

> DES 是一种 **64 位块密码（通过一些列异或运算生成密文）**，共有 5 种**运算模式**：**电子密码本**（Electronic Code Book，**ECB**）、**密码块链接**（Cipher Block Chaining，**CBC**）、**密码反馈**（Cipher Feedback，**CFB**）、**输出反馈**（Output Feedback，**OFB**）、**计数器**（Counter，**CTR**）。
>
> > 关于DES算法的密钥，虽然长度为64位，但**实际用于加密解密运算的位数为56位**，剩余8位用于奇偶校验。
>
> 由于DES不再安全，导致**3DES（三重DES）**算法的诞生，其存在4个版本。
>
> - **3DES-EEE3：C = E(K1, E(K2, E(K3, P)))**，使用3个不同的密钥对明文加密3次，有效密钥长度为56*3=168位；
> - **3DES-EDE3：C = E(K1, D(K2, E(K3, P)))**，依然使用3个不同密钥，区别在于第二次采用解密运算而不再是加密运算；
> - **3DES-EEE2：C = E(K1, E(K2, E(K1, P)))**，只是有2个密钥，有效密钥长度为112位；
> - **3DES-EDE2：C = E(K1, D(K2, E(K1, P)))**，同样只是有2个密钥；
>
> 既然有3DES，也曾出现**2DES**，但由于被证明（一种**"中间相遇"攻击**）其**安全性还不如标准DES**，就很快被抛弃了。

加密模式：**电子密码本**（Electronic Code Book，**ECB**）、**密码块链接**（Cipher Block Chaining，**CBC**）、**密码反馈**（Cipher Feedback，**CFB**）、**输出反馈**（Output Feedback，**OFB**）、**计数器**（Counter，**CTR**）

> - **电子密码本（EBC）**：是最容易理解的简单模式，也最不安全。算法每次处理一个 64 位块，它只用选好的秘密密钥给块加密，意味着对于同样的明文块将得到相同的密文块。由于这一特性，ECB模式变得几乎无法使用（面对密码分析手段较为脆弱），只用于交换少量数据。
> - **密码块链接（CBC）**：每块未加密文本在通过算法加密前，先要借助前面刚生成的密文块接受异或 (XOR)

> 运算。CBC使用一个初始化向量 (IV) 并用第一个消息块进行异或运算，每次运算生成一个唯一的输出。IV必须发送给接受者，否则将无法解密消息。
>
> 使用 CBC 模式时，错误传播是需要考虑的一个重要问题：如果一个块在传输过程中毁坏，这个块以及其后的块将无法解密。

- **密码反馈模式（CFB）**：是 CBC 模式的流密码版。使用与块大小相同的存储缓冲区，在缓冲区填满时给数据加密。与CBC一样，CFB模式也使用IV，也存在错误传播。
- **输出反馈模式（OFB）**：与CFB类似的流密码。但先后加密的密文块不存在链接（这里与CBC和CFB存在根本差异），OFB使用一个IV创建初始种子值，后面通过密码算法计算出一个种子值序列，种子值会与待加密的明文块进行异或运算。
- **计数器模式（CTR）**：也是一种流密码。区别于OFB，CTR的的种子来源于一个简单的计数器。与OFB一样，CTR不会传播错误。

> *注：“加密模式”不仅在DES算法中使用，也在包括下面介绍的IDEA、AES等在内的多数对称密码算法中使用。*

国际数据加密算法（IDEA），也是一种块密码。与DES一样运算在64位数据块上，但IDEA使用128位密钥。

> 在Phil Zimmerman 颇受欢迎的 PGP(Pretty Good Privacy, 良好隐私）安全邮件软件包中，可以看到IDEA 的一种盛行执行方案。

Blowfish块密码，是对DES和IDEA的一种替代方案。与前者相同，运行在64位数据块上，但其密钥长度可变，从32位~448位。

Skipjack密码，是一种运行在64位数据块上，密钥长度为80位的块密码。

> 被美国政府在联邦信息处理标准 (FIPS)185 EES 中批准使用。
>
> 由于其支持加密秘钥托管，及美国现行的托管规程，导致其不受密码界欢迎。

RC5（Rivest Cipher 5），是一种块大小可变（32/64/128位），密钥大小在0到2040位之间的块算法。

> 旧版RC2已被认定为不再安全。
>
> 新版的RC6还未被广泛采用。

高级加密标准（AES），2000 年 10 月， NIST 宣布， Rijndael 块密码已被选择用来代替 DES 。2001 年 11 月，NIST 发布 FIPS 197, 强制规定美国政府用 AES/Rijndael 加密所有敏感但未分类的数据。

> AES允许使用128/192/256位3种密钥长强度。
>
> AES只允许处理128位数据块。*原始Rijndael 算法支持使用与密钥长度相等的数据块大小*。
>
> 加密轮数取决于密钥长度：128位密钥要求10轮加密，192位密钥要求12轮加密，256位密钥要求14轮加密。

Twofish，Bruce Schneier （也是 Blowfish 的创造者）开发的 Twofish 算法是 AES 的另一个终极品。与Rijndael一样， Twofish 是一种块密码。它在 128 位数据块上运行，能够使用最长达 256 位的密码密钥。

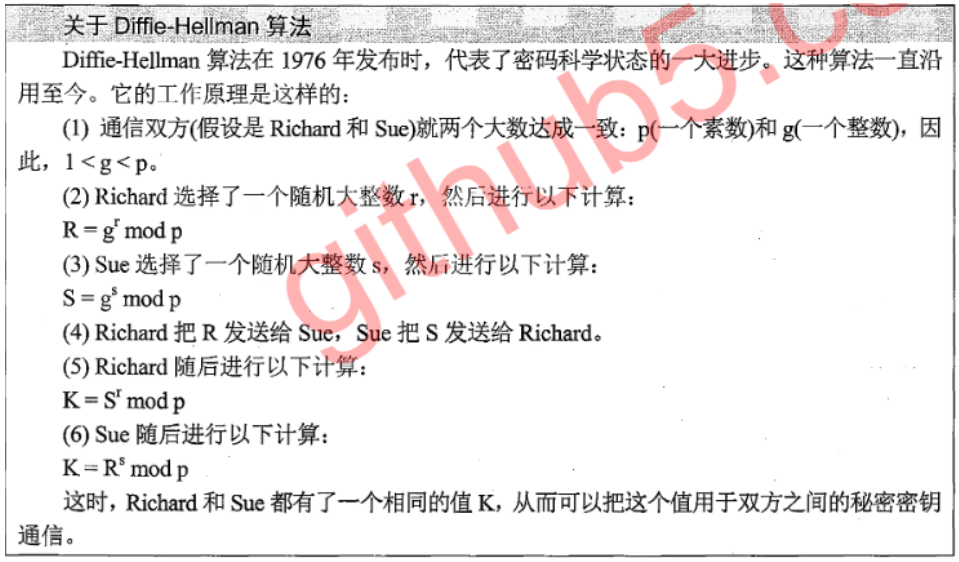
> Twofish 使用的两项技术是在其他算法中找不到的：
>
> > 预白化处理 (prewhitening) 指第 1 轮加密前用一个单独的子密钥对明文进行异或运算；
> >
> > 白化后处理 (postwhitening) 指第 16 轮加密后执行同样的运算。

算法	块大小	密钥强度	
AES	128	128/192/256	
Rijndael	可变，与密钥长度相同	128/192/256	
Blowfish（常用于SSH）	64	32~448	
DES	64	**56**	64位减去8位校验位
IEDA（用于PGP）	64	128	
RC2	64	128	
RC5	32/64/128	0~2040	
Skipjack	64	80	
3DES	64	**112或168**	3DES-EEE3 和 EDE3使用3个不同密钥，总强度为56*3； EEE2 和 EDE2使用2个不同密钥，总强度为56*2。
Twofish	128	1~256	

9

对称密钥管理，包括涉及秘密密钥创建、分发、存储、销毁、恢复和托管的防护手段。

> **创建与分发**，主要有三种方法：**线下分发**、**公钥加密**和 **Diffie-Helhnan 密钥交换算法**。
>
> > 当没有可用的线下物理手段，且没有现成可用的公钥基础设施的情况下，DH密钥交换算法被证明是最实用的机制。



关于 Diffie-Hellman 算法

Diffie-Hellman 算法在 1976 年发布时，代表了密码科学状态的一大进步。这种算法一直沿用至今。它的工作原理是这样的：

(1) 通信双方(假设是 Richard 和 Sue)就两个大数达成一致：p(一个素数)和 g(一个整数)，因此，$1 < g < p$。

(2) Richard 选择了一个随机大整数 r，然后进行以下计算：

$R = g^r \bmod p$

(3) Sue 选择了一个随机大整数 s，然后进行以下计算：

$S = g^s \bmod p$

(4) Richard 把 R 发送给 Sue，Sue 把 S 发送给 Richard。

(5) Richard 随后进行以下计算：

$K = S^r \bmod p$

(6) Sue 随后进行以下计算：

$K = R^s \bmod p$

这时，Richard 和 Sue 都有了一个相同的值 K，从而可以把这个值用于双方之间的秘密密钥通信。

注：DH算法在TLS/SSL、蓝牙协议中均有应用。

存储和销毁对称密钥，确保密钥安全的最佳实践：

- [存储] 绝不将加密秘钥与被加密的数据保存在同一个系统里；
- [存储] 对于敏感密钥，考虑诸如安排两个人各持有一半片段的方案（知识分割原则）；
- [销毁] 当掌握密钥的用户离职或取消授权后，应该销毁并替换密钥，并使用新密钥重新加密数据。

密钥托管和恢复，主要存在2中方法：

公平密码系统：密钥被分解为两个或以上的片段，分别交由一个独立的第三方保管。

受托加密标准：这种托管方法向政府提供了解密密文的技术手段。该标准是Skipjack 算法的基础。

注：书中此处介绍的密钥托管，更多是在"长期保存敏感数据"场景下。常规的应用系统，如加密保护用户隐私数据或商业数据时，通常采用分级密钥机制，并可借助硬件安全模块（HSM）进行密钥托管（与密钥安全存储采用类似的方案）。

10

密码生命周期

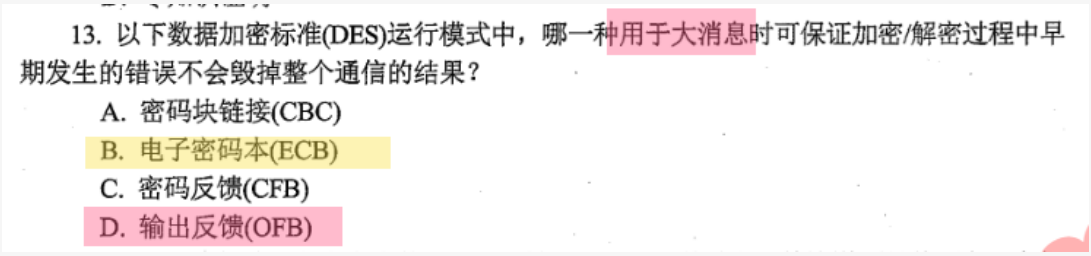
除了单次密本外，所有的密码系统的使用寿命都是有限的。

挑选密码算法时，需要适当的管控，确保选择的算法、协议、密钥长度足以保持密码系统的完整性：

- 规定可接受的密码算法；
- 根据信息的敏感性识别可以与每种算法配套使用的可接受的密钥长度；
- 枚举可接受的安全协议。

11

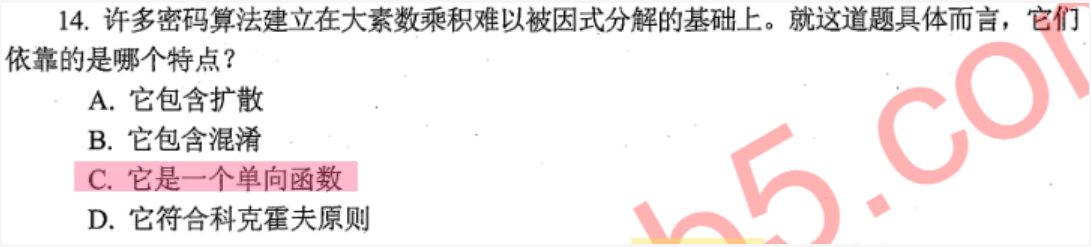
书后系统易错分析



13. 以下数据加密标准(DES)运行模式中，哪一种用于大消息时可保证加密/解密过程中早期发生的错误不会毁掉整个通信的结果？

A. 密码块链接(CBC)
B. 电子密码本(ECB)
C. 密码反馈(CFB)
D. 输出反馈(OFB)

> 虽然OFB和ECB都不会传播错误，但是题目中明确需要用于加密大消息，回顾加密模式相关内容，ECB模式显然不符合要求。



14. 许多密码算法建立在大素数乘积难以被因式分解的基础上。就这道题具体而言，它们依靠的是哪个特点？

A. 它包含扩散
B. 它包含混淆
C. 它是一个单向函数
D. 它符合科克霍夫原则

> 记住它。另外回忆一下混淆 (confusion) 和扩散 (diffusion)的概念，替换带来混淆、移位带来扩散。

注："易错"其实指的是我第一次做错了。

参考文献

整个项目主要来自于《CISSP官方学习指南(OSG)》系列和《CISSP权威指南(AIO)》系列。

本章笔记主要来源于：

[1]. 《CISSP官方学习指南(第8版)》。