[1. 安全技术 2](#_Toc16065)

[1.1. 计算机安全 2](#_Toc6353)

[1.2. 目标 2](#_Toc22167)

[1.3. 其他目标 2](#_Toc7823)

[2. OSI安全体系结构 2](#_Toc21306)

[2.1. OSI参考模型 2](#_Toc7726)

[2.2. 五类安全服务 2](#_Toc5734)

[2.3. 八类安全机制 2](#_Toc9908)

[3. TCP/IP安全体系结构 2](#_Toc15961)

[3.1. TCP/IP参考模型 2](#_Toc17265)

[3.2. 安全体系 3](#_Toc7940)

[4. 密码学 3](#_Toc7914)

[4.1. 定义 3](#_Toc11724)

[4.2. 密码编码学 3](#_Toc16924)

[4.3. 密码分析学 3](#_Toc15418)

[4.4. 常用术语 3](#_Toc31457)

[4.5. 保密通信模型 4](#_Toc337)

[4.6. 对称密码体系 4](#_Toc2690)

[5. Base64 4](#_Toc11870)

[5.1. 字符映射表 4](#_Toc1456)

[5.2. 编码原理 5](#_Toc29564)

[5.3. 实例 5](#_Toc22912)

[5.4. RFC 2045 5](#_Toc14639)

[5.5. Bouncy Castle和Commons Codec 5](#_Toc17698)

[6. Url Base64 5](#_Toc16309)

[6.1. 差别 5](#_Toc22120)

[7. 消息摘要算法 6](#_Toc6656)

[7.1. 简述 6](#_Toc10065)

[7.2. MD 6](#_Toc27008)

[7.3. SHA 6](#_Toc19774)

[7.4. MAC 6](#_Toc10521)

[8. 对称加密算法 6](#_Toc11895)

[8.1. DES 6](#_Toc2305)

[8.2. DESede（三重DES） 6](#_Toc22823)

[8.3. AES 6](#_Toc10842)

[8.4. IDEA 6](#_Toc3840)

[8.5. PBE 6](#_Toc16575)

[9. 非对称加密算法 6](#_Toc4894)

[9.1. DH 6](#_Toc4385)

[密钥交换算法（diffie-hellman），目的在于让消息的收发双方可以在安全的条件下交换密钥，以备后续加密/解密使用。DH算法仅能用于密钥分配，不能用于加密或解密消息。 6](#_Toc29668)

1. 安全技术
   1. 计算机安全

为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄漏。

* 1. 目标
* 保密性(Confidentiality)：数据不能被未授权的第三方使用。
* 完整性(Integrity)：数据在传输过程中不能被未授权方修改。
* 可用性(Availability)：确保所有数据仅在适当的时候可以由授权方访问。
* 可靠性(Reliability)：确保系统能在规定条件下、规定时间内、完成规定功能时具有稳定的概率。
* 抗否认性(Non-Repudiation)：确保发送方与接收方在执行各自操作后，对所做的操作不可否认。
  1. 其他目标
* 可控性：对信息及信息系统实施安全监控。
* 可审查性：通过审计、监控、抗否认性等安全机制，确保数据访问者的行为有证可查。
* 认证：确保数据访问者和信息访问者的身份真实有效。
* 访问控制：确保数据不被非授权方或以未授权方式使用。

1. OSI安全体系结构
   1. OSI参考模型

物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。

* 1. 五类安全服务
* 认证服务：在网络交互过程中，对收发双方的身份及数据来源进行验证。
* 访问控制服务：防止非授权用户非法访问资源。
* 数据保密性服务：防止数据在传输过程中被破解、泄漏。
* 数据完整性服务：防止数据在传输过程中被篡改。
* 抗否认性服务：防止发送方与接受方双方在执行各自操作后，否认各自所做的操作。
  1. 八类安全机制
* 加密机制：对应数据加密性服务
* 数字签名机制：对应认证服务
* 访问控制机制：对应访问控制服务
* 数据完整性机制：对应数据完整性服务
* 认证机制：对应认证服务
* 业务流填充机制：对应数据加密型服务。通过在数据传输过程中传送随机数的方式，混淆真实的数据，加大数据破解的难度，提高数据的保密性。
* 路由控制机制：对应访问控制服务。为数据发送方选择安全网络通信路径，避免发送方使用不安全路径发送数据，提高数据的安全性。
* 公证机制：对应抗否认性服务

1. TCP/IP安全体系结构
   1. TCP/IP参考模型

网络接口层、网络层、传输层和应用层

* 1. 安全体系
* 网络接口层安全
* 网络层安全
* 传输层安全
* 应用层安全

1. 密码学
   1. 定义

主要是研究保密通信和信息保密的问题，包括信息保密传输和信息加密存储等。

密码学包括密码编码学和密码分析学两个分支。

* 1. 密码编码学

主要研究对信息进行编码，实现对信息的隐蔽，是密码学理论的基础，也是保密系统设计的基础。

* 1. 密码分析学

主要研究加密消息的破译或消息的伪造，是检验密码体制安全性最为直接的手段，只有通过实际密码分析考验的密码体制，才是真正可用的。

* 1. 常用术语
* 明文(Plaintext)：待加密信息
* 密文(Ciphertext)：经过加密后的明文
* 发送者(Sender)：发送消息的人
* 接收者(Receiver)：接收消息的人
* 加密(Encryption)：将明文转换为密文的过程
* 加密算法(Encryption Algorithm)：将明文变化为密文的转换算法
* 加密密钥(Encryption Key)：通过加密算法进行加密操作用的密钥
* 解密(Decryption)：将密文转换为明文的过程
* 解密算法(Decryption Algorithm)：将密文变化为明文的转换算法
* 解密密钥(Decryption Key)：通过解密算法进行解密操作用的密钥
* 密码分析(Cryptanalysis)：试图通过分析截获的密文从而推断出原来的密文或密钥的过程
* 密码分析者(Cryptanalyst)：从事密码分析的人
* 被动攻击(Passive Attack)：对一个保密系统采取截获密文并对其进行分析和攻击。这种攻击对密文没有破坏作用。
* 主动攻击(Active Attack)：攻击者非法入侵密码系统，采用伪造、修改、删除等手段向系统注入假消息进行欺骗。这种攻击对密文具有破坏作用。
* 密码体制(Cipher System)：由明文空间、密文空间、密钥空间、加密算法和解密算法五部分构成。
* 密码协议(Cryptographic Protocol)：以密码学为基础的消息交换的通信协议，目的是在网络环境中提供各种安全服务。
* 密码系统(Cryptography)：用于加密和解密的系统。由信源、加密变换、解密变化、信宿和攻击者组成。
* 柯克霍夫原则(Kerckhoffs’ Principle)：数据的安全基于密钥而不是算法的保密。系统的安全性取决于密钥，对密钥保密，对算法公开。
  1. 保密通信模型



图表 1

* 1. 对称密码体系



图表 2

1. Base64
   1. 字符映射表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Value** | **Encoding** | **Value** | **Encoding** | **Value** | **Encoding** | **Value** | **Encoding** |
| **0** | A | 17 | R | 34 | i | 51 | z |
| **1** | B | 18 | S | 35 | j | 52 | 0 |
| **2** | C | 19 | T | 36 | k | 53 | 1 |
| **3** | D | 20 | U | 37 | l | 54 | 2 |
| **4** | E | 21 | V | 38 | m | 55 | 3 |
| **5** | F | 22 | W | 39 | n | 56 | 4 |
| **6** | G | 23 | X | 40 | o | 57 | 5 |
| **7** | H | 24 | Y | 41 | p | 58 | 6 |
| **8** | I | 25 | Z | 42 | q | 59 | 7 |
| **9** | J | 26 | a | 43 | r | 60 | 8 |
| **10** | K | 27 | b | 44 | s | 61 | 9 |
| **11** | L | 28 | c | 45 | t | 62 | + |
| **12** | M | 29 | d | 46 | u | 63 | / |
| **13** | N | 30 | e | 47 | v |  | = |
| **14** | O | 31 | f | 48 | w |  |  |
| **15** | P | 32 | g | 49 | x |  |  |
| **16** | Q | 33 | h | 50 | y |  |  |

* 1. 编码原理

1)将给定的字符串以字符为单位，转化为对应的字符编码（如ASCII）

2)将获取的字符编码转化为二进制码

3)对获取的二进制码进行分组，每3个8位二进制码为一组，不足低位补0

4)将获取的3个8位二进制码转化为4个6位二进制码

5)对6位二进制码进行高位补0，组成4个8位二进制码

6)将获取的4个8位二进制码转化为十进制码

7)将获取的十进制码参照base64位字符表转换为对应的字符

解码原理过程相反

* 1. 实例

以AB为例

A=>65=>01000001,B=>66=>01000010 得到二进制妈

01000001 01000010 00000000 不足3个，低位补0

010000 010100 001000 000000 3\*8转化为4\*6

00010000 00010100 00001000 00000000 高位补0

16 20 8 = 转化为十进制

Q U I = 参照映射表一一转化

* 1. RFC 2045

根据RFC 2045定义，每行为76个字符，行末加入一个回车换行符。但并不是当每行够了76个字符才需要在行末加入一个回车换行符，每行不管够不够76个字符都要加入一个回车换行符。

* 1. Bouncy Castle和Commons Codec

Bouncy Castle遵循一般Base64算法编码。

Commons Codec提供了两种实现标准：一种是遵循一般Base64算法编码，另一种遵循RFC 2045定义。此外，还可以自定每行字符数和行末符号。同时提供了输入输出流的实现。

1. Url Base64
   1. 差别

符号“+”和“/”是不允许出现在URL中的，RFC 4648给出了相应的替代符号“-”和“\_”。同样，符号“=”用做参数分隔符，也不允许出现在URL中。符号“=”在Base64用做填充符，如果需要定长的Base64编码串，就需要相应的替代符号。

根据RFC 4648的建议，“~”和“.”符都有可能替代“=”符号。但“~”与文件系统相冲突，不能使用；某些文件系统认为“.”连续出现两次则为错误。

Bouncy Castle使用“.”填充，而Commons Codec直接放弃填充符，使用不定长Url Base64编码。

1. 消息摘要算法
   1. 简述

消息摘要算法包括MD（Message Digest，消息摘要算法）、SHA（Secure Hash Algorithm，安全散列算法）和MAC（Message Authentication Code，消息认证码算法）共3大系列，常用于检验数据的完整性，是数字签名算法的核心算法。

* 1. MD

不管是哪一种MD算法，都需要获取一个随机长度的信息并生成一个128位的信息摘要。如果将这个128位的二进制摘要信息换算成十六进制，可以得到一个32位（每4位二进制数转化为1位十六进制数）的字符串。

* 1. SHA

SHA算法基于MD4算法基础之上。

* 1. MAC

MAC结合了MD5和SHA的算法优势，并加入密钥的支持。因此，我们常把MAC称为HMAC(Keyed-Hash Message Authentication Code)。

1. 对称加密算法
   1. DES

数据加密标准（data encryption standard）,密钥偏短，仅56位，迭代次数偏少。

* 1. DESede（三重DES）

DESede算法针对密钥长度偏短和迭代次数偏少等问题做了相应改进，提高安全强度。

但DESede算法处理速度较慢，密钥计算时间较长，加密效率不高。

* 1. AES

高级数据加密标准（advanced encryption standard）,支持128、192和256位密钥长度。

具有密钥建立时间短、灵敏性好、内存需求低等优点。

* 1. IDEA

国际数据加密算法（international data encryption algorithm），使用128位的密钥，需要

使用bouncycastle实现。

* 1. PBE

基于口令加密（password based encryption）,综合了对称加密算法和消息摘要算法。PBE算法没有密钥的概念，使用口令代替密钥。但口令本身不可能很长，容易通过穷举攻击方式破译。于是，引入了盐。盐本身是随机信息，将盐附加在口令上，通过消息算法经过迭代计算获得构建密钥/初始化向量的基本材料，使得破译加密信息的难度加大。

1. 非对称加密算法
   1. DH

密钥交换算法（diffie-hellman），目的在于让消息的收发双方可以在安全的条件下交换密钥，以备后续加密/解密使用。DH算法仅能用于密钥分配，不能用于加密或解密消息。