对一个 ASN.1 对象的 BER 编码有三种模式，使用哪一种模式取决于该对象的类型和该类型数据的长度是否已知，不同模式下编码信息中每个组成部分的编码规则不同。

4.2.2.1　基本类型定长模式

基本类型定长模式编码主要应用于基本类型和从基本类型通过隐式派生得到的类型，同时需要已知编码值的长度。各部分的 BER 编码规则如下。

1．标识串编码

标识串编码分为低标识编码和高标识编码两种形式。

（1）低标识编码。

① 适用于类型标识值小于 30 的类型。

② 编码结果只有 1 个字节。

③ 其中第 8 位和第 7 位表示 Class 类型，第 8 位和第 7 位的赋值规则参见表 4-2。

表 4-2　第 8 位和第 7 位的赋值规则

Class	第 8 位	第 7 位	Class	第 8 位	第 7 位
Universal	0	0	Context-Specific	1	0
Application	0	1	Private	1	1

④ 第 6 位置为 0 表示是基本类型的编码。

⑤ 第 5 位到第 1 位填充数据类型标识的值。

（2）高标识编码。

① 适用于类型标识值大于 30 的类型。

② 编码结果至少有 2 个字节。

③ 除了将第 5 到第 1 位置为 1，第一个字节与低标识编码获得的标识串的构成相同。

④ 第 2 个字节以后（包含第 2 个字节）的字节填充类型标识的值，基数是 128，每个字节的第 8 位作为结束标志，除了最后一个字节外其他都置为 1。

2．长度串编码

长度串编码分为短型和长型两种形式。

（1）短型长度串编码。

① 适用于内容长度小于 127 的类型。

② 编码只有一个字节。

③ 第 8 位置为 0，其他 7 位填充长度的值（是内容串的长度）。

（2）长型长度串编码。

① 适用于内容长度大于 127 的类型。

② 编码由 2～127 个字节组成。

③ 第 1 个字节的第 8 位置为 1，其他 7 位填充后面填充长度值所有的字节数。

④ 第 2 个字节以后（包含第 2 个字节）的字节，填充内容串的长度值。

3．内容串编码

表示基本类型具体的编码值。

对于 OBJECT IDENTIFIER 类型，假设 OID=V1.V2.V3.….V*n*，则其编码规则为：第 1 个字节=40×V1+V2（V1 取值范围为 0、1 或 2，V2 取值范围为 0～39）；对于 V3…V*n* 中的每个 V*x*，以 128 为基数将 V*x* 分解为多个数，除最后一个数外其余数的最高位（第 8 位）置为 1 后，成为编码后的多个字节。如 1.2.840.113549，第 1 个字节为 40×1+2=2A（十六进制）；840=6×128+48（十六进制），则编码后为 2 个字节 86 48；113549=6×128×128+77×128+0D（十六进制），则编码后为 3 个字节 86 F7 0D。因此 1.2.840.113549 编码后为 06 06 2A 86 48 86 F7 0D。

对于 BIT STRING 类型，编码后第 1 个字节表示填充位数或未使用位数。如 keyUsage=11111，编码后为 03 F8。

对于 INTEGER 类型，由于 DER 编码后第 1 字节第 8 位表示正负整数，因此如果正整数第 1 字节第 8 位为 1 时，在前填充 1 个字节 0x00。如十进制 128（十六进制为 80），编码后为 00 80。

对于 BOOLEAN 类型，TRUE 编码为 0xFF，FALSE 编码为 0x00。

4．内容结束串编码

无内容结束串编码。

4.2.2.2 结构类型定长模式

结构类型定长模式编码，主要应用于基本字符串类型、结构类型、从基本字符串类型和结构类型通过隐式派生得到的类型、从任意类型通过显式派生得到的类型，也需要已知编码值的长度。各个部分的 BER 编码规则如下：

① 标识串编码，与基本类型定长模式编码中的标识串编码规则基本相同，除了将第 1 个字节的第 6 位置为 1，表示结构类型编码。

② 长度串编码，与基本类型定长模式编码中的长度串编码规则完全相同。

③ 内容串编码，与基本类型定长模式编码中的内容串编码规则完全相同；需要根据结构类型对象的不同类型而采用不同的编码。

④ 内容结束串编码，无。

4.2.2.3 结构类型非定长模式

结构类型非定长模式编码，主要应用于基本字符串类型、结构类型、从基本字符串类型和结构类型通过隐式派生得到的类型、从任意类型通过显式派生得到的类型，不需要知道编码值的长度。各个部分的 BER 编码规则如下：

① 标识串编码，与结构类型定长模式编码中的标识串编码规则完全相同。

② 长度串编码，只有 1 个字节，赋值为 0x80，表示该数据编码是非定长模式编码。

③ 内容串编码，与结构类型定长模式编码中内容串编码规则完全相同。

④ 内容结构串编码，由 2 个字节组成，赋值为 0x0000。

4.2.3 DER 定长编码规则

DER 编码是 ASN.1 数据类型中具有唯一编码的编码规则。DER 编码是 BER 编码的子集，是将每一个 ASN.1 抽象对象类型表示成唯一的 1 和 0 码字符串的编码规则。这种编码

规则是为需要编码成唯一比特串的应用系统而制定的，特别是在应用安全技术的应用系统中，由于安全加密技术要求输入数据是字节流的形式，并且是与原数据唯一对应的字节流，因此需要使用 DER 编码来实现数据结构的编码。

DER 编码称为有关安全技术的应用系统的最佳选择。它基本上继承了 BER 编码规则，同样，也有三种编码方法。但为了保证编码结果的唯一性，DER 编码在 BER 编码规则的基础上又附加了一些规则：

① 必须使用定长模式编码。

② 对于内容长度小于 127 的类型值，长度串编码必须采用短型。

③ 对于内容长度大于 128 的类型值，长度串编码必须采用长型，同时长度串编码的字节个数必须是最少的。

④ 对于简单字符串类型和从简单字符串类型通过隐式派生得到的类型，必须使用基本类型定长模式编码方法。

⑤ 对于结构类型、从结构类型通过隐式派生得到的类型，以及从任何类型通过显示派生得到的类型，必须使用结构类型定长模式编码方法。

第5章 密码技术

5.1 密码算法

5.1.1 算法分类

按照技术特征分类，密码算法可以分为以下三类。

1. 对称算法

对称算法是指加密密钥和解密密钥相同的密码算法，又称秘密密钥算法或单密钥算法。该类算法又分为流密码算法和分组密码算法。

流密码算法又称序列密码算法，每次加密或解密一位或一字节的明文或密文。

分组密码算法将明文（密文）分成固定长度的数据块（比特块或字节块），用同一密钥和算法对每一明文（密文）块加密（解密）后得到等长的密文（明文）块，然后将密文（明文）块按照顺序组合起来最终得到明文（密文）。

常见的流密码算法包括 RC4；常见的分组密码算法包括 DES、IDEA、RC2、AES、SM4 等。

2. 非对称算法

非对称算法是指加密密钥和解密密钥不相同的密码算法，从一个密钥很难推导出另一个密钥，又称公开密钥算法或公钥算法。该算法使用一个密钥进行加密，用另一个密钥进行解密。其中加密密钥可以公开，又称公开密钥或公钥；解密密钥必须保密，又称私有密钥或私钥。

常见的非对称算法包括 RSA、DH、DSA、ECDSA、ECC、SM2 等。

3. 摘要算法

摘要算法是指把任意长的输入消息数据转化成固定长度的输出数据的一种密码算法，又称散列函数、哈希函数或杂凑函数、单向函数等。摘要算法所产生的固定长度的输出数据称作摘要值、散列值或哈希值。摘要算法没有密钥。

常见的摘要算法包括 MD5、SHA1、SM3 等。

5.1.2 对称密码算法

本节主要介绍 DES、3DES、AES、SM4 算法。

1. DES

对称算法最具代表性的是 IBM 公司提出的 DES 算法，该算法自 1977 年被美国国家标准局（NBS）颁布为商用数据加密标准后，得到了广泛应用。

DES 算法是一个分组算法，它以 64 位为分组对数据进行加解密。其密钥长度为 56 位，

由8个字节组成，每个字节的第8位用作奇偶校验。密钥可以是任意的56位比特块，且可在任意时间改变，其中极少数56位比特块被认为是弱密钥，在使用中需要避开这些弱密钥。所有的保密性依赖于密钥。

DES算法的一般过程如图5-1所示。

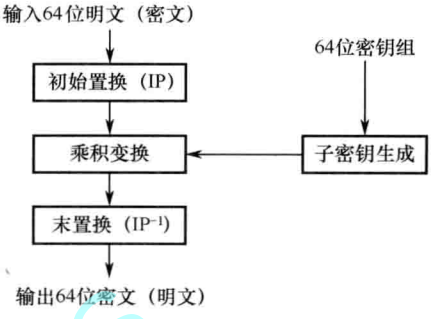

图5-1 DES算法的一般过程

① 初始置换：是按照固定的矩阵进行换位，此部分与密钥无关。初始置换将明文（密文）分组分成左半部分和右半部分，各32位长。

② 子密钥生成：外部输入的56位密钥（64位中去掉8个校验位）通过置换和位移操作生成加密和解密需要的16个48位的子密钥。该16个子密钥分别用于乘积变换中的16轮运算。

③ 乘积变换：该过程与密钥有关，且比较复杂，是加密/解密过程的关键。该过程包括线性变换和非线性变换。该过程通过多次复杂的替代和置换方法，打乱原输入数据组，加大了非规律性，增加了系统分析的难度。乘积变换将进行16轮完全相同的运算，在运算过程中数据与密钥结合，最终生成32位长的左半部分和右半部分。

④ 末置换：是初始置换的逆变换，与密钥无关。乘积变换生成的左半部分和右半部分合在一起，经过末置换后生成64位的密文（明文）。

DES算法最主要的优点是：可靠性较高、加密解密速度快、算法容易实现、通用性强。其主要的缺点是：密钥位数少、算法具有对称性、容易被穷尽法攻击、密钥管理复杂。

有些密钥会导致生成相同的16个子密钥，这些密钥叫作弱密钥。当密钥是全0、全1或一半是全0、一半是全1时，会发生这种情况。4种弱密钥（十六进制编码，带奇偶校验位）参见表5-1。

表5-1 弱密钥列表

弱密钥（十六进制，带奇偶校验位）	
01 01 01 01 01 01 01 01	1F 1F 1F 1F 0E 0E 0E 0E
E0 E0 E0 E0 F1 F1 F1 F1	FE FE FE FE FE FE FE FE

有些密钥把明文加密成相同的密文，这些密钥只产生2个不同的子密钥，而不是生成16个不同的子密钥，这些密钥叫作半弱密钥，参见表5-2。

表5-2 半弱密钥列表

半弱密钥（十六进制，带奇偶校验位）	
01 FE 01 FE 01 FE 01 FE	FE 01 FE 01 FE 01 FE 01
1F E0 1F E0 0E F1 0E F1	E0 1F E0 1F F1 0E F1 0E
01 E0 01 E0 01 F1 01 F1	E0 01 E0 01 F1 01 F1 01
1F FE 1F FE 0E FE 0E FE	FE 1F FE 1F FE 0E FE 0E
01 1F 01 1F 01 0E 01 0E	1F 01 1F 01 0E 01 0E 01
E0 FE E0 FE F1 FE F1 FE	FE E0 FE E0 FE F1 FE F1