具体编码过程如表 13-1 所示。

表 13-1　RSA 公钥参数 e 和 n 编码过程

RSA 公钥参数	标识串	长度串	内容串
n=B4 F6…F7 F3	02	81 81	00 B4 F6…F7 F3
e=01 00 01	02	03	01 00 01

2．对 RSAPublicKey 进行 DER 编码

RSAPublicKey 为 SEQUENCE 结构类型，编码规则采用结构类型定长模式。

对于标识串，采用低标识编码方式，只需 1 个字节。SEQUENCE 的 tag 为 0x10；class 选择 universal，则位 8 和位 7 为 0，SEQUENCE 为结构类型，则位 6 为 1。因此，标识串=0x30。

对于长度串，采用长型编码方式，需要 2 个字节。

对于内容串，由 modulus 和 publicExponent 的 DER 编码值组成。

具体编码过程如表 13-2 所示。

表 13-2　RSAPublicKey 编码过程

RSA 公钥	标识串	长度串	内容串
RSAPublicKey	30	81 89	02 81 81 00 B4 F6…F7 F3 02 03 01 00 01

13.2　数字证书格式编码示例

13.2.1　ASN.1 描述与实例

以第 11 章中 ZHANG San 的数字证书为例，序列号=1174（0x0496），证书签发者 DN=“CN = Virtual CA，C = CN”，证书持有者 DN=“CN = ZHANG San，OU = Person，C = CN”，证书有效期=20140222000000-20160222000000。

1．TBSCertificate 的 ASN.1 描述与实例

TBSCertificate 格式用 ASN.1 描述如下：

```
TBSCertificate  ::=  SEQUENCE  {
    version              [0]  EXPLICIT Version DEFAULT v1,
    serialNumber              CertificateSerialNumber,
    signature                 AlgorithmIdentifier,
    issuer                    Name,
    validity                  Validity,
    subject                   Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID   [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                                  -- If present, version MUST be v2 or v3
```

```
        subjectUniqueID [2]    IMPLICIT UniqueIdentifier OPTIONAL,
                                    -- If present, version MUST be v2 or v3
        extensions             [3]  EXPLICIT Extensions OPTIONAL
                                    -- If present, version MUST be v3
    }
    Extensions   ::=   SEQUENCE SIZE (1..MAX) OF Extension
```

TBSCertificate 中各项内容具体值如表 13-3 所示。

表 13-3　TBSCertificate 内容值

TBSCertificate	值
version	02（十六进制）
serialNumber	04 96（十六进制）
signature	sha1WithRSAEncryption（1.2.840.113549.1.1.5）
issuer	“CN=Virtual CA，C=CN”
validity	notBefore=20140222000000、notAfter=20160222000000
subject	“CN=ZHANG San，OU=Person，C=CN”
subjectPublicKeyInfo	同 13.1 节
issuerUniqueID subjectUniqueID	空
extensions	包含 6 个扩展项（Extension）：basicContraints、subjectKeyIdentifier、keyUsage、extKeyUsage、netscapeCertType、authorityKeyIdentifier

2. Extension 的 ASN.1 描述与实例

Extension 格式用 ASN.1 描述如下：

```
Extension   ::=   SEQUENCE   {
    extnID        OBJECT IDENTIFIER,
    critical      BOOLEAN DEFAULT FALSE,
    extnValue     OCTET STRING   }
```

Extension 各扩展项值如表 13-4 所示。

表 13-4　Extension 各扩展项值

Extension	值
basicContraints	关键项，值为空（表示 cA=FALSE）
subjectKeyIdentifier	2C 04 87 10 60 FC 61 F6 2B 64 81 3D FB 66 30 DA F0 73 BC 08（SHA1 值，简写为：2C 04…BC 08）
keyUsage	关键项，值为 Digital Signature、Non-Repudiation、Key Encipherment、Data Encipherment、Key Agreement（F8）
extKeyUsage	客户端身份验证（1.3.6.1.5.5.7.3.2）、智能卡登录 （1.3.6.1.4.1.311.20.2.2）、安全电子邮件（1.3.6.1.5.5.7.3.4）
netscapeCertType	SSL 客户端身份验证、SMIME（A0）
authorityKeyIdentifier	96 F0 94 F8 49 8D 23 05 86 B0 CA B5 2D 7A 9A 60 32 FB B0 F9（简写为：96 F0…B0 F9）

3．Certificate 的 ASN.1 描述与实例

Certificate 格式用 ASN.1 描述如下：

```
Certificate ::=   SEQUENCE   {
    tbsCertificate              TBSCertificate,
    signatureAlgorithm          AlgorithmIdentifier,
    signatureValue              BIT STRING   }
```

Certificate 中各项内容的具体值如表 13-5 所示。

表 13-5　Certificate 内容值

Certificate	值
tbsCertificate	见 DER 编码过程
signatureAlgorithm	sha1WithRSAEncryption（1.2.840.113549.1.1.5）
signatureValue	8D 42 AD 5C DF C7 C7 90 FA 58 C0 74 15 C6 4F 20 9B F1 49 9C B8 3C 22 98 45 75 A6 0D 7C 02 9D 83 1D C4 5D CF 4F 8E 57 E7 0A 9B 67 02 33 23 59 76 B4 B5 B7 F3 27 36 6F F4 32 6C 1C E9 B3 4B 81 DC D0 CF 2E CF 07 4C 65 75 74 DF 23 9D 7D 2B E4 F1 15 0C 84 61 41 5F DC 67 92 A9 7C 39 A0 CA A9 58 6B ED 7D 94 08 F7 83 42 61 F8 62 D8 DC 3B 5D B7 69 5C D0 36 F2 99 A8 0C 99 6E B0 0C 21 E3 98 9F 12 6D D1 76 4E 0C 31 CB 7F 54 73 FE 96 83 76 35 22 2F BF F6 2B 11 04 3A A7 BE 33 3C D5 DA EE 56 7A C4 1A 67 3B 77 DE 52 C0 DA 09 CA 45 71 11 B2 D5 35 BF 44 54 08 C2 FA 0C 5C EF C0 EF 82 63 37 3C 4C AB 59 4C FD 6C 2A 9D 64 27 35 4E 4F D8 2E 2C 5C EB A1 99 DB FA 3A 53 54 13 92 91 5D 8F 38 DD 1C D8 AB 34 22 9A EF 8A E4 62 C2 23 9D 06 A5 D7 D8 58 B7 F4 98 CA 61 29 9D DE A8 F6 DA CC 81 （256 字节，简写为：8D 42…CC 81）

13.2.2　DER 编码过程

1．对 Extension 进行 DER 编码

各扩展项具体内容用 ASN.1 描述如下：

```
BasicConstraints ::= SEQUENCE {
    cA                      BOOLEAN DEFAULT FALSE,
    pathLenConstraint       INTEGER (0..MAX) OPTIONAL }
SubjectKeyIdentifier ::= KeyIdentifier
（KeyIdentifier ::= OCTET STRING）
KeyUsage ::= BIT STRING
ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId
```

```
（KeyPurposeId ::= OBJECT IDENTIFIER）
NetscapeCertType ::= BIT STRING
AuthorityKeyIdentifier ::= SEQUENCE {
        keyIdentifier              [0] KeyIdentifier              OPTIONAL,
        authorityCertIssuer        [1] GeneralNames               OPTIONAL,
        authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL   }
（KeyIdentifier ::= OCTET STRING）
```

Extension 为 SEQUENCE 结构类型，不同扩展项 DER 编码值包含在 OCTET STRING 类型 extnValue 中，编码规则采用结构类型定长模式。各扩展项 DER 编码值用括号分隔。其中，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。

Extension 具体编码过程如表 13-6 所示。

表 13-6　Extension 编码过程

Extension	标识串	长度串	内　容　串
basicContraints	30	0C	06 03 55 1D 13 01 01 FF 04 02（30 00）
subjectKeyIdentifier	30	1D	06 03 55 1D 0E 04 16（04 14 2C 04…BC 08）
keyUsage	30	0E	06 03 55 1D 0F 01 01 FF 04 04（03 02 03 F8）
extKeyUsage	30	29	06 03 55 1D 25 04 22（30 20 06 08 2B 06 01 05 05 07 03 02 06 0A 2B 06 01 04 01 82 37 14 02 02 06 08 2B 06 01 05 05 07 03 04）
netscapeCertType	30	11	06 09 60 86 48 01 86 F8 42 01 01 04 04（03 02 05 A0）
authorityKeyIdentifier	30	1F	06 03 55 1D 23 04 18（30 16 80 14 96 F0…B0 F9）

2．对 TBSCertificate 进行 DER 编码

TBSCertificate 内容编码规则采用结构类型定长模式，具体编码过程如表 13-7 所示。

表 13-7　TBSCertificate 内容编码过程

TBSCertificate	标识串	长度串	内　容　串
version [0] EXPLICIT	A0	03	02 01 02
serialNumber	02	02	04 96
signature	30	0D	06 09 2A 86 48 86 F7 0D 01 01 05 05 00

（续表）

TBSCertificate	标识串	长度串	内　容　串
issuer	30	22	31 0B 30 09 06 03 55 04 06 13 02 43 4E 31 13 30 11 06 03 55 04 0313 0A 56 69 72 74 75 61 6C 20 43 41
validity	30	1E	17 0D 31 34 30 32 32 31 31 36 30 30 30 30 5A 17 0D 31 36 30 32 32 31 31 36 30 30 30 30 5A
subject	30	32	31 0B 30 09 06 03 55 04 06 13 02 43 4E 31 0F 30 0D 06 03 55 04 0B 13 06 50 65 72 73 6F 6E 31 12 30 10 06 03 55 04 03 13 09 5A 48 41 4E 47 20 53 61 6E
subjectPublicKeyInfo	30	81 9F	30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 81 8D 00 30 81 89 02 81 81 00 B4 F6 … F7 E3 02 03 01 00 01
extensions [3] EXPLICIT	A3	81 9F	30 81 9C 30 0C …30 00：basicContraints 30 1D…BC 08：subjectKeyIdentifier 30 0E…03 F8：keyUsage 30 29…03 04：extKeyUsage 30 11…05 A0：netscapeCertType 30 1F…b0 F9：authorityKeyIdentifier

TBSCertificate 为 SEQUENCE 结构类型，编码规则采用结构类型定长模式。TBSCertificate 具体编码过程如表 13-8 所示。

表 13-8　TBSCertificate 编码过程

TBSCertificate	标识串	长度串	内　容　串
TBSCertificate	30	82 01 D4	A0 03…01 02：version 02 02…04 96：serialNumber 30 0D…05 00：signature 30 22…43 41：issuer 30 1E…30 5A：validity 30 32…61 6E：subject 30 81…00 01：subjectPublicKeyInfo A3 81…B0 F9：extensions

3．对 Certificate 进行 DER 编码

Certificate 内容编码规则采用结构类型定长模式，具体编码过程如表 13-9 所示。

表 13-9　Certificate 内容编码过程

Certificate	标识串	长度串	内　容　串
tbsCertificate	30	82 01 D4	A0 03…B0 F9
signatureAlgorithm	30	0D	06 09 2A 86 48 86 F7 0D 01 01 05 05 00
signatureValue	03	82 01 01	00 8D 42…CC 81