表 7-5 RDNSequence 编码过程

RDNSequence	标 识 串	长 度 串	内 容 串
countryName ="US"	30	42	31 0B 30 09 06 03 55 04 06 13 02 55 53 31 1D 30 1B 06 03 55 04 0A 13 14 45 78 ... 6F 6E 31 14 30 12 06 03 55 04 03 13 0B 54 65 ... 20 31

6. Name 编码

Name 为 CHOICE 类型，其 DER 编码值与 RDNSequence 相同。

用户 Test User 1 最终 DER 编码值如表 7-6 所示。

表 7-6 用户 Test User 1 最终 DER 编码值

DER 编码值	ASN.1 描述
30 42	
31 0B	
30 09	
06 03 55 04 06	attributeType = countryName
13 02 55 53	attributeValue = "US"
31 1D	
30 1B	
06 03 55 04 0A	attributeType = organizationName
13 14	attributeValue = "Example Organization"
45 78 61 6D 70 6C 65 20 4F 72 67	
67 61 6E 69 7A 61 74 69 6F 6E	
31 14	
30 12	
06 03 55 04 03	attributeType = commonName
13 0B	attributeValue = "Test User 1"
54 65 73 74 20 55 73 65 72 20 31	

7.2 RSA 算法示例

7.2.1 密钥产生

1. 计算 n

算法：选择两个大素数 p 和 q，计算出 $n=pq$。

示例：选择 2 个素数：$p=7$，$q=17$。$n=pq=7\times17=119$。

2．计算 $\varphi(n)$

算法：计算出 n 的欧拉函数 $\varphi(n)=(p-1)(q-1)$。

示例：$\varphi(n)=(7-1)\times(17-1)=96$。

3．选择 e

算法：从[0, $\varphi(n)-1$]中选择一个与 $\varphi(n)$互素的数 e 作为公开的加密指数。

示例：从[0, 95]中选择一个与 96 互素的数 $e=5$。

4．计算 d

算法：计算出满足公式 $ed=1 \bmod \varphi(n)$的 d 作为解密指数。

示例：根据 $5d=1 \bmod 96$，得出 $d=77$。（$ed=5\times77=385=4\times96+1=1 \bmod 96$）

5．获得公钥和私钥

算法：公钥 PK={e，n}，私钥 SK={d，n}

示例：公钥 PK={5, 119}，私钥 SK={77, 119}

7.2.2 加密解密

若用整数 X 表示明文，用整数 Y 表示密文（X 和 Y 均小于 n）。

1．公钥加密

算法：$Y=X^e \bmod n$，PK={e，n}

示例：设 $X=19$，PK={5, 119}

$Y=19^5 \bmod 119 = 2476099 \bmod 119 = (119\times20807+66) \bmod 119=66$。

即：明文 $X=19$，密文 $Y=66$。

2．私钥解密

算法：$X=Y^d \bmod n$，SK={d，n}

示例：设 $Y=66$，SK={77, 119}

$X=66^{77} \bmod 119=1.27\cdots x10^{140} \bmod 119= (1.06\cdots x10^{138}+19) \bmod 119=19$。

即：密文 $Y=66$，明文 $X=19$。

第三部分

PKI之数字证书与私钥：网络身份证

第 8 章　公/私钥格式

8.1　RSA

PKCS #1 中规定了 RSA 公钥/私钥的具体格式。

1. RSA 公钥格式

RSA 公钥格式用 ASN.1 描述如下：

```
RSAPublicKey ::= SEQUENCE {
    modulus             INTEGER,   -- n
    publicExponent      INTEGER    -- e
}
```

其中，n 和 e 为 RSA 公钥参数。

2. RSA 私钥格式

RSA 私钥格式用 ASN.1 描述如下：

```
RSAPrivateKey ::= SEQUENCE {
    version             Version,
    modulus             INTEGER,   -- n
    publicExponent      INTEGER,   -- e
    privateExponent     INTEGER,   -- d
    prime1              INTEGER,   -- p
    prime2              INTEGER,   -- q
    exponent1           INTEGER,   -- d mod (p-1)
    exponent2           INTEGER,   -- d mod (q-1)
    coefficient         INTEGER,   -- (inverse of q) mod p
}
version ::= INTEGER
```

其中，version 用于区分格式版本，缺省值为 0。

3. RSA 加密格式

RSA 公钥和私钥均可进行加密和解密操作。

假设使用公钥 pk（RSAPublicKey 类型）或私钥 vk（RSAPrivateKey 类型）对明文数据 D（字符串类型）进行加密计算。具体计算步骤如下：

① 构造加密块（encryption block）：EB = 00 || BT || PS || 00 || D。EB 长度为 k。

其中，BT 为块类型，OCTET STRING 类型，长度=1，值可以为 00、01 或 02。私钥加密/解密时，BT=00 或 01，公钥加密/解密时，BT=02。

PS 为填充字符串，为 OCTET STRING 类型，长度=$k-3-\|D\|$。当 BT=00 时，PS 值全为 00。当 BT=01 时，PS 值全为 FF。当 BT=02 时，PS 值不能为 0，随机产生。

② 格式转换：将 OCTET STRING 类型 EB 转换成 Integer 类型 x。

③ RSA 加密：使用 RSA 公钥或私钥对 Integer 类型 x 进行加密后获得 Integer 类型密文 y。

④ 格式转换：将 Integer 类型密文 y 转换成 OCTET STRING 类型密文 ED，长度为 k。

假设使用公钥 pk（RSAPublicKey 类型）或私钥 vk（RSAPrivateKey 类型）对密文数据 ED（OCTET STRING 类型）进行解密计算。具体计算步骤如下：

① 将 OCTET STRING 类型 ED 转换成 Integer 类型密文 y。

② RSA 解密：使用 RSA 公钥或私钥对 Integer 类型密文 y 进行解密后获得 Integer 类型明文 x。

③ 格式转换：将 Integer 类型明文 x 转换成 OCTET STRING 类型明文 EB，长度为 k。

④ 加密块分拆（encryption block）：将明文 EB 分拆成 BT、PS 和 D，即可获得明文数据 D。

4．RSA 签名格式

RSA 签名时摘要格式用 ASN.1 描述如下：

```
DigestInfo ::= SEQUENCE {
    digestAlgorithm DigestAlgorithmIdentifier,
    digest Digest }
DigestAlgorithmIdentifier ::= AlgorithmIdentifier
Digest ::= OCTET STRING
AlgorithmIdentifier  ::=  SEQUENCE  {
    Algorithm           OBJECT IDENTIFIER,
    Parameters          ANY DEFINED BY algorithm OPTIONAL  }
```

其中，DigestAlgorithm 为摘要算法，Digest 为摘要值。

假设使用私钥 vk（RSAPrivateKey 类型）对待签名数据 M（字符串类型）进行签名计算。具体计算步骤如下：

① 计算摘要值：MD = HASH（M）。

② 数据编码：将摘要算法 ID 和摘要值 MD 按照 DigestInfo 类型进行编码，获得摘要数据 D。

③ RSA 加密：使用私钥 vk 对摘要数据 D 进行加密后获得密文 ED（OCTET STRING 类型），其中 BT=0x01。

④ 格式转换：将密文 ED 转换成比特字符串 S（BIT STRING 类型）。其中 S 采用 MSB（most significant bit）方式。S 即为签名结果。

假设使用公钥 pk（RSAPublicKey 类型）对待签名数据 M（字符串类型）和待签名结果 S（BIT STRING 类型）进行签名验证。具体计算步骤如下：

① 格式转换：将签名结果 S（BIT STRING 类型）转换成密文 ED（OCTET STRING 类型）。