# 第六章重点课后题参考答案

1．在 DSS 数字签名标准中，取 p=83=2×41+1，q＝41，h＝2，于是 g≡$2^2$≡4 mod 83，若取 x＝57，则 $y≡g^x≡4^{57}$＝77 mod 83。在对消息 M=56 签名时选择 k＝23,计算签名并进行验证。

解：这里忽略对消息 M 求杂凑值的处理

计算 $r＝(g^k \bmod p) \bmod q＝(4^{23} \bmod 83) \bmod 41=51 \bmod 41=10$

$k^{-1}$mod q=$23^{-1}$ mod 41=25

$s=k^{-1}(M+xr) \bmod q$=25(56+57*10) mod 41=29

所以签名为(*r*,*s*)=(10,29)

接收者对签名(*r*′,*s*′)=(10,29)做如下验证：

计算 w＝$(s')^{-1}$ mod *q*=$29^{-1}$ mod 41=17

u1＝[*M*′w] mod *q*=56*17 mod 41=9

u2＝*r*′w mod *q*＝10×17 mod 41＝6

v＝$(g^{u1}y^{u2} \bmod p) \bmod q$=($4^9$×$77^6$ mod 83) mod 41＝10

所以有 v＝*r*′，即验证通过。

2．在 DSA 签字算法中，参数 k 泄漏会产生什么后果？

解：如果攻击者获得了一个有效的签名(*r*,*s*)，并且知道了签名中采用的参数 k，那么由于在签名方程 $s=k^{-1}(M+xr) \bmod q$ 中只有一个未知数，即签名者的秘密钥 x，因而攻击者可以求得秘密钥 x＝$r^{-1}(sk－M) \bmod q$，即参数 k 的泄漏导致签名秘密钥的泄漏。