密码学基础-作业 4 答案

提交方式：通过HITsz Grade平台提交　　提交截止时间：以系统上公布时间为准
提交格式：pdf文件　　文件命名规则：学号_姓名_作业4.pdf
注：若包含照片或插图，请旋转至适合阅读的方向

1. 设在$Diffie-Hellman$方法中，公用素数$q=11$,本原根$\alpha=2$。

   (a)证明2是11的本原根。

   (b)若用户A的公钥$Y_A=9$,则A的私钥X_A为多少？

   (c)若用户B的公钥$Y_B=3$,则与A共享的密钥K为多少？

ANSWER：

(a) 证明：
由于11为素数，故$\phi(11)=10$，且$2^{10}=1024\equiv 1 \ mod\ 11$，进而验证有$2^1\equiv 2 \ mod\ 11$，
$2^2\equiv 4 \ mod 11$，$2^3\equiv 8 \ mod\ 11$，$2^4\equiv 5 \ mod 11$，$2^5\equiv 10 \ mod 11$，$2^6\equiv 9 \ mod 11$，
$2^7\equiv 7 \ mod 11$，$2^8\equiv 3 \ mod 11$，$2^9\equiv 6 \ mod 11$
综上所述，2是11的本原根

(b) 由(a)可知，$2^6 \ mod 11=9$，故A的私钥$X_A=6$

(c) $K=3^6 \ mod 11=3$

2. 10.1节中介绍了针对$Diffie-Hellman$密钥交换协议的中间人攻击。敌手生成了两个公钥-私钥对。如果只生成一个公钥-私钥对，那么能够完成攻击吗？

ANSWER：

1. Darth 通过生成随机私有X_D然后计算相应的公共Y_D来准备攻击。
2. Alice 发送 Y_A给 Bob.
3. Darth 拦截 Y_A并发送 $Y_D$to Bob. Darth 还计算 $K2=Y_A{}^{X_D} mod\ q$.
4. Bob 收到Y_D并计算$K1=Y_D{}^{X_B} mod\ q$.
5. Bob 发送 X_A 给 Alice.
6. Darth 拦截 X_A 并发送 Y_D to Alice. Darth 计算 $K1=Y_B{}^{X_D} mod\ q$.
7. Alice 接收 Y_D 并计算 $K2=Y_D{}^{X_A} mod\ q$.

3. 下列Z_{17}上的椭圆曲线的点的负数是多少？$P(5,8)$；$Q(3,0)$；$R=(0,6)$。

ANSWER：

The negative of a point $P=(X_p,Y_p)$ is the point $-P=(X_p,-Y_p \ mod\ p)$.

Thus

$$-P=(5,9);\ -Q=(3,0);\ -R=(0,11)$$

4. 12.6节的开头，当给定一个单分组消息X的$CBC\ MAC$值$T=MAC(K,X)$时，敌手立

即就知道两个分组消息$X||(X \oplus T)$的$CBC\ MAC$值，因为该值仍然是T。请证明上述结论。

ANSWER:

我们使用第 12.6 节中的定义。对于单块消息，使用CBC-MAC的MAC是 $T = E(K, X)$，其中 K 是键，X 是消息块。现在考虑两个块消息，其中第一个块是 X，第二个块是 $X \oplus T$。那么 MAC 是$E(K, [T \oplus (X \oplus T)]) = E(K, X) = T$.

5. 设计$Diffie-Hellman$算法的一个变体作为数字签名是有意义的。下面的方法比DSA更简单，它只需要私钥而不需要秘密随机数：

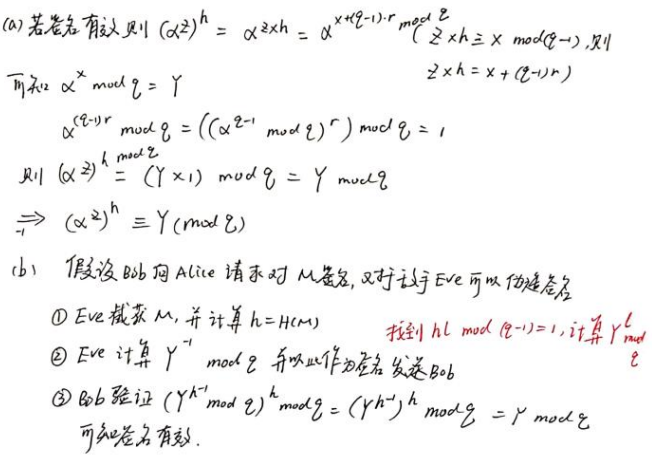
公开素数	q，素数
	α，$\alpha < q$且α是q的本原根
私钥	X，$X < q$
公钥	$Y = \alpha^X \bmod q$

要对消息M签名，则先计算该消息的$Hash$码$h = H(M)$。我们要求$gcd(h, q-1) = 1$,若不等于1,则将该哈希码附在消息后再计算哈希码，继续该过程直至产生的哈希码与$q-1$互素：然后计算满足$Z \times h = X (mod\ q-1)$的$Z$,并将$\alpha^Z$作为对该消息的签名。验证签名即是验证$Y = (\alpha^Z)^h = \alpha^X \bmod q$。

(a)证明该方案能够正确运行。即证明若签名是有效的，则在验证过程中将有上述等式成立。

(b)给出一种简单的方法对任意消息伪造用户签名，以证明这种体制是不可接受的。

ANSWER:



6. $SHA1$预处理要进行消息填充：在消息原文后面需要填充第一位为1其余为0的消息X，末尾64位要填充上原文消息的长度。请计算待填充消息X的长度。

（1）若消息长度为1472位，需要填充（　）位

（2）若消息长度为2048位，需要填充（　）位

（3）$SHA1$算法最终得到的消息摘要长度是（　）位

ANSWER:

(1) 512

(2) 448

(3) 160