密码学基础-作业4

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共享的密钥为K多少?

(a):

计算:

$2\ mod\ 11=2$

$2^2\ mod\ 11=4$

$2^3\ mod\ 11=8$

$2^4\ mod\ 11=5$

$2^5\ mod\ 11=10$

$2^6\ mod\ 11=9$

$2^7\ mod\ 11=7$

$2^8\ mod\ 11=3$

$2^9\ mod\ 11=6$

$2^{10}\ mod\ 11=1$

生成了群中所有元素，所以2是11的本原根

(b):

依题意得:

$\alpha^{X_A}\ mod\ q=Y_A$

即$2^{X_A}\ mod\ 11 = 9$

由(a)得，$X_A = 6$

(c):

由DH密钥交换协议的规则知，共享密钥K为：

$K = Y_B^{X_A}\ mod\ q = 3^6\ mod\ 11 = 3^3\ mod\ 11 \times 3^3\ mod\ 11$

$= 5\ mod\ 11 \times 5\ mod\ 11 = 25\ mod\ 11 = 3$

所以$K = 3$

---

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?

   可以完成，中间人只需要在每次截取后，将自己的公钥发送给对应的一方即可。

   设中间人生成的私钥为p，原通信双方生成的私钥为x和y，本原根为g，则经中间人攻击，通信双方分别持有密钥g^{py}和g^{px}，而中间持有g^x、g^y和p，显然可以生成这两个密钥

---

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

$-P = (5, -8\ mod\ 17) = (5,9)$

$-Q = (3, -0\ mod\ 17) = (3,0)$

$-R = (0, -6\ mod\ 17) = (0,11)$

---

4. 12.6节的开头，当给定一个单分组消息X的CBC MAX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 MAX值，因为该值仍然是T。请证明上述结论。

由CBC和MAC加密规则，对两个分组消息加密过程为：

$MAC(K, X||(X \oplus T)) = MAC(K, MAC(X) \oplus (X \oplus T)) = MAC(K, X)$

注：第二个等于号是因为相当于对X加密再解密

所以上述结论成立

5.

6. 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，α<q且α是q的本原根
   私钥　　X，X < q
   公钥　　$Y = \alpha^X mod q$
   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×h=X(mod q-1)的Z,并将α^Z作为对该消息的签名。验证签名即是验证$Y = (\alpha^Z)^h = \alpha^X mod q$
   (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。

(a)：

因为
$Z \times h - X = X(mod\ q-1) - X = X + n(q-1) - X = n(q-1)$

所以$a^{Zh-X} = a^{n(q-1)}$

由欧拉定理：$a^{n(q-1)} \equiv 1\ mod\ q$

所以$a^{Zh-X} \equiv 1\ mod\ q$

即：$(a^Z)^h = a^X\ mod\ q$

(b)：

由于哈希函数是公开的，所以对于密文M，可以求h=H(M)，进而可以求出h^{-1}

而公钥PK=$a^x\ mod\ q$，所以可以伪造签名$Ya^{h^{-1}}$，

那么PK'=$(Ya^{h^{-1}})^h$=PK=$a^x\ mod\ q$，伪造成功

---

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（ 512 ）位
   （2）若消息长度为2048位，需要填充（ 448）位
   （3）SHA1算法最终得到的消息摘要长度是（ 160 ）位