网络信息安全试题答案补充（软 191 级队自编）

说明：本文档由软件学院 191 级队同学自行编写，如有错误，请及时联系原作者，原作者 QQ：2208853487，如需添加好友请备注来意

1. 选择填空题

略，其中(11)第 2 空正确答案为 9

2. 证明题

（1） 略

（2） 略

（3）

$\because 3$ 与 11 互素

$\therefore 3^{201} \mod 11 = 3^{20\times 10+1} \mod 11 = 3 \times (3^{10} \mod 11)^{20} \mod 11 = 3$

3. 证明题

（1） $D(sk, Z) = V(U^X \mod P)^{-1} \mod P$（这题其实就是 ElGamal 算法）

证明：

$$
\begin{aligned}
U^X \mod P &= (g^r \mod P)^X \mod P \\
&= g^{rX} \mod P \\
&= (g^X)^r \mod P \\
&= (g^X \mod P)^r \mod P \\
&= Y^r \mod P
\end{aligned}
$$

$$
\begin{aligned}
\therefore V(U^X \mod P)^{-1} \mod P &= (MY^r \mod P)(Y^r \mod P)^{-1} \mod P \\
&= M \mod P \\
&= M(M \le P-1)
\end{aligned}
$$

（2） $M^* = 10M \mod p$，证明直接代（U相同则r必相同）

（3） $M^* = M^8 \mod p$，证明直接代（注意r是随机数，此时$r^* = 8r$）

4. 计算题

略

5. 计算题

（1）

$n = pq = 33$
$\phi(n) = \phi(p)\phi(q) = (p-1)(q-1) = 20$
$\because 3e \mod \phi(n) = 3 \times 7 \mod 20 = 1$
$\therefore d = 3$

（2） 略

（3） 略

6. 计算题

（1）

$D(sk, y) = y^d \mod N$

（2）

$D(sk, E(pk, M)) = (M^e \mod N)^d \mod N = M^{ed} \mod N$
$\because ed \mod \phi(N) = 1$
$\therefore ed = k\phi(N) + 1 (k \in \mathbb{N})$
$\therefore D(sk, E(pk, M)) = M^{k\phi(N)+1} \mod N = (M^{\phi(N)} \mod N)^k \cdot M \mod N = M$

（3） 用中国剩余定理可算出，具体过程略

（1） $D(sk, (Y, W)) = \dfrac{W}{Y^x}$，证明如下：

$$D(sk, (Y, W)) = \frac{W}{Y^x} = \frac{TM}{(g^r)^x} = \frac{TM}{(g^x)^r} = \frac{TM}{X^r} = \frac{TM}{T} = M$$