网络信息安全 2017 年考题野生答案

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

一、 单项选择题

1	2	3	4	5	6	7	8
A	C	C	B	D	C	A	C

二、 证明题

1. 解：

（1）

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

（2）

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

（3）

$$\begin{aligned}
&n = pq = 33 \\
&\phi(n) = \phi(p)\phi(q) = (p-1)(q-1) = 20 \\
&\because 3e \mod \phi(n) = 3 \times 7 \mod 20 = 1 \\
&\therefore d = 3
\end{aligned}$$

（4）

$$E(pk, 7) = 7^7 \bmod 33 = 28$$

2. 解：

- 通信双方约定一个大素数(或多项式)p, 和模p的一个素根**α**
- 各方产生公开密钥
  - 选择一个秘密钥(数值)，如$x_A < p$， $x_B < p$
  - 计算公钥, 如$y_A = \alpha^{x_A} \bmod p$, $y_B = \alpha^{x_B} \bmod p$, 并相互交换
- 双方共享的会话密钥K_{AB}可以如下算出
  $K_{AB} = \alpha^{x_A . x_B} \bmod p$
  $= y_A^{x_B} \bmod p$ (which **B** can compute)
  $= y_B^{x_A} \bmod p$ (which **A** can compute)
- K_{AB}是双方用对称密码通信时共享的密钥
- 如果双方继续通信，可以继续使用这个密钥，除非他们要选择新的密钥
- 攻击者如果想要获得x, 则必须解决DLP问题

中间人攻击

假定A和B希望交换密钥，而D是攻击者，攻击过程如下：

(1)为了进行攻击，D先生成两个随机的私钥 X_{D1}和 X_{D2}，然后计算相应的公钥 Y_{D1}和 Y_{D2}

(2)$Alice$将Y_A传递给Bob。

(3)D截获了Y_A，将Y_{D1}传给B。D同时计算 $K_2 = (Y_A)^{X_{D2}} \bmod q$。

(4)B收到Y_{D1}，计算$K_1 = (Y_{D1})^{X_B} \bmod q$。

(5)B将Y_B传给A。

(6)D截获了Y_B，将Y_{D2}传给A。D计算 $K_1 = (Y_B)^{X_{D1}} \bmod q$。

(7)A收到Y_{D2}，计算$K_2 = (Y_{D2})^{X_A} \bmod q$。

此时，B和A想，他们已共享了密钥，但实际上，B和 D共享了密钥 K_1 而 A和 D共享了密钥K_2。接下来，B和 A之间的通信以下列方式泄密：

(1)A发了一份加了密的消息 M：$E(K_2, M)$。

(2)D截获了该秘密消息，解密，恢复出 M。

(3)D将$E(K_1, M)$或$E(K_1, M')$发给B，其中M'是任意的消息。

3. 解：

（1）

$D(sk, Z) = V(U^X \mod P)^{-1} \mod P$，证明如下：

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

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

（2）

$M^* = M^8 \mod p$，证明如下：

$\because U = g^r \bmod p$， 密文的 U 变为 U^8

$\therefore$此时随机数 r 变为 $8r$

此时 $V =((M^8 \bmod P)Y^{8r}) \bmod P = M^8 Y^{8r} \bmod P = (MY^r)^8 \bmod P$

$=(MY^r \bmod P)^8 = V^8$

三、 计算题

1. 解：

（1） $(130 \times 5) \bmod 2^8 = 138$

（2）

$f(x) = x^8 + x^4 + x^3 + x^2 + 1 = 100011101$

$f(x) \oplus (2^8 - 1) = 100011101 \oplus 011111111 = 111100010$

去除最高位，得到 11100010

$\therefore$该多项式为 $x^7 + x^6 + x^5 + x$

本题涉及知识参见 https://zhuanlan.zhihu.com/p/262267121

2. 解：

（1）

$a = g^k \bmod p = 10^5 \bmod 19 = 3$

$\because 5 \times 11 \bmod 18 = 1$

$\therefore k^{-1} = 11$

$\therefore b = (M - xa)k^{-1} \bmod (p-1) = (14 - 16 \times 3) \cdot 11 \bmod 18 = 4$

（2）

$$
\begin{aligned}
\text{左边} &= y^a a^b \bmod p \\
&= y^a (g^k \bmod p)^{(M-xa)k^{-1} \bmod (p-1)} \bmod p \\
&= (g^x)^a g^{k(M-xa)k^{-1} \bmod (p-1)} \bmod p \\
&= g^{xa} g^{(M-xa) \bmod (p-1)} \bmod p \\
&= g^{M \bmod (p-1)} \bmod p \\
&= g^M \bmod p \\
&= \text{右边}
\end{aligned}
$$