陕西科技大学　试题纸 A

课程____密码学____　学期____2018—2019—2____

答案及评分标准：

一、（本题 20 分）

1、解：$M=3\times5\times7,\frac{M}{3}=35,\frac{M}{5}=21,\frac{M}{7}=15$，.....1 分

由$35e_1\equiv1\bmod3,21e_2\equiv1\bmod5,15e_3\equiv1\bmod7$，.....2 分

可得$e_1=2,e_2=1,e_3=1$，.....4 分

则$x=2\times2\times35+1\times1\times21+1\times1\times15=176\bmod105=71$。.....3 分

2、解：$f(x)+g(x)=x^6+x^4+x^2+x+1+x^7+x+1=x^7+x^6+x^4+x^2$，.....4 分

$$f(x)\times g(x)=x^{13}+x^{11}+x^9+x^8+x^7+x^7+x^5+x^3+x^2+x+x^6+x^4+x^2+x+1$$

$$=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1$$，.....3 分

$$f(x)\times g(x)\bmod m(x)=x^7+x^6+1$$。.....3 分

二、（本题 20 分）

解：加密变换为$c=11m+2\bmod26$，

对明文 puxm 加密为密文：love。.....20 分

三、（本题 15 分）

1、双重 DES 的加密算式$C=E(K_2,E(K_1,P))$；.....10 分

2、高级加密标准 AES 中每轮都经过字节代替、行移位、列混淆、轮密钥加变换。.....5 分

四、（本题 15 分）

解：取$p=5$，$q=11$，公钥$e=3$，$M=9$，$n=p\times q=5\times11=55$，

$\phi(n)=(p-1)\times(q-1)=4\times10=40$，.....3 分

由$3d\equiv1\bmod40$可得$d=27$，.....2 分

所以$PU=\{3,55\}$，$PR=\{27,55\}$，.....4 分

$C=M^e\bmod n=9^3\bmod55\equiv14$，.....3 分

$M=C^d\bmod n=14^{27}\bmod55\equiv9$。.....3 分

五、（本题 15 分）

解：$GF(23)$ 上的椭圆曲线 $E: y^2 = x^3 - 4x + 1$，$P = (4,7)$，$Q = (10,31)$，那么

$\lambda = \left(\frac{31-7}{10-4}\right) \bmod 23 = \left(\frac{24}{6}\right) \bmod 23 = 4$，.....5 分

$x_R = \left(4^2 - 4 - 10\right) \bmod 23 = 2 \bmod 23 = 2$，

$y_R = \left(4(4-2) - 7\right) \bmod 23 = 1 \bmod 23 = 1$，.....9 分

所以点 $R = P + Q$ 的坐标为 $R = (2,1)$。.....1 分

六、（本题 15 分）

解：$Y_A = \alpha^x \bmod 19 = 10^{16} \bmod 19 = 4$，

所以 A 的公钥是 $\{q, \alpha, Y_A\} = \{19,10,4\}$。.....3 分

签名者 A 对 $m = 14$ 的签名：

$S_1 = \alpha^k \bmod 19 = 10^5 \bmod 19 = 3$，

$k^{-1} \bmod (q-1) = 5^{-1} \bmod 18 = 11$，

$S_2 = k^{-1}(m - xS_1) \bmod (q-1) = 11(14 - 16 \times 3) \bmod 18 = -374 \bmod 18 = 4$，.....6 分

验证签名：

$V_1 = \alpha^m \bmod q = 10^{14} \bmod 19 = 16$，

$V_2 = (Y_A)^{S_1} (S_1)^{S_2} \bmod q = 4^3 \times 3^4 = \bmod 19 = 5184 \bmod 19 = 16$，

因为 $V_1 = V_2$，所以签名是合法的。.....6 分