陕西科技大学　试题纸 A

课程____密码学____　学期____2019—2020—2____

班级 _____　学号 _____　姓名 _____

题号	一	二	三	四	五	六	七	八	九	十	总分
得分											
阅卷人											

一、（本题 20 分）

1、利用中国剩余定理求解同余方程组 $\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases}$；

2、选择 $m(x) = x^8 + x^4 + x^3 + x + 1$ 来构造的有限域 $GF(2^8)$ 中，多项式 $f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$，$g(x) = x^3 + x + 1$，试计算 $f(x) + g(x)$，$f(x) \times g(x)$。

二、（本题 20 分）

1、使用 Caesar 密码算法（密钥 $k = 3$）对“pexkhbax”进行加密，对“zhqol”进行解密；

2、用 Vigenere 密码加密单词“explanation”，密钥为“leg”。

三、（本题 15 分）

1、高级加密标准 AES 中每轮都经过哪些变换？

2、公钥密码体制的主要成分是什么？什么是单向陷门函数？

3、什么是消息认证码？消息认证码的基本用途？

四、（本题 20 分）

1、使用公钥密码算法 RSA，若取 $p = 3$，$q = 11$，公钥 $e = 7$，对 $M = 5$ 进行加密，并对所得的密文进行解密。

2、在 ELGamal 加密体制中，设素数 $p = 71$，本原根 $g = 7$，

（1）如果接收方 B 的公开钥是 $y_B = 3$，发送方 A 选择的随机整数 $k = 2$，求

明文$M=30$所对应的密文。

（2）如果 A 选择另一个随机数k，使得明文$M=30$加密后的密文是$C=(59,C_2)$，求C_2。

五、（本题 15 分）

1、考虑$GF(23)$上的椭圆曲线$E:y^2=x^3+11x+18$，令$P=(6,1)$，$Q=(9,15)$，试计算点$R=P+Q$的坐标及点$2P$的坐标。

2、椭圆曲线$E_{11}(1,6)$表示$y^2\equiv x^3+x+6 \bmod 11$，确定$E_{11}(1,6)$中所有第一象限的点。

六、（本题 10 分）

在 ElGamal 数字签名方案中，假设$q=19$，$\alpha=10$。如果签名者 A 选取的私钥为$X_A=16$，试计算公钥。设签名者 A 要对消息$m=14$进行签名，且选取随机数$K=5$，求签名者 A 对$m=14$的签名。并验证该数字签名的合法性。（$10^{16} \bmod 19=4$，$10^5 \bmod 19=3$）