武汉大学国家网络安全学院
2020-2021 学年度第 1 学期
《密码学》期末考试试卷 A 卷（开卷）

专业：信息安全　　学号：2018302180069　　姓名：郭占占

说明：答案请全部写在答题纸上，写在试卷上无效。
考试试卷、答题纸、草稿纸均不得带离考场，否则视为违规。

题号	一	二	三	四	五			总分
分值	32	50	18					100

一. 简答题（共 4 小题，每小题 8 分，共 32 分）

1、我国首个公开的商用密码算法标准是？该算法使用了哪些基本密码部件？

2、根据密码分析者可利用的数据资源来分类，密码攻击有哪些类型？

3、简述非对称（公钥）密码的基本思想，并比较对称密码与公钥密码体制的主要特点。

4、什么是认证？认证和数字签名的联系和区别是什么？

二. 计算题（共 5 小题，每小题 10 分，共 50 分）

1、在某通信加密场景中，已知明密文编码都是普通的英文字母，使用的算法是古典加法密码。目前截获到密文是：**ECPIV CVQDMZAQBG**，经过分析其中的前 5 个字符对应的明文是 **WUHAN**。

（1） 根据上述信息，计算密钥 k=？；

（2） 给出完整的明文/密文字母对照表；

（3） 试对于上述密文，恢复出完整的明文。

2、DES 密码中第一个 S 盒为如下表所示（16 进制表示），

	$b_1b_2b_3b_4$															
b_0b_5	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	E	4	D	1	2	F	B	8	3	A	6	C	B	9	5	3	8
1	0	F	7	4	E	2	D	1	A	6	C	B	9	3	A	5	0
2	4	1	E	8	D	6	2	B	F	C	9	7	3	A	0	6	D
3	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D	

设 S 盒的输入为 X，输出为 Y。（X 和 Y 都以二进制表示）

（1）对于已知输入值 X_1= 011111 和 X_2= 011011，分别求出对应的输出值 Y_1 和 Y_2。

（2）比较输出值 Y_1 和 Y_2 各位的异同，即按位计算 $Y_1 \oplus Y_2$。

3、已知有限域 GF（2）上的本原多项式 $g(x)=x^4+x^3+1$，以其为连接多项式组成线性移位寄存器。

（1）画出其中的逻辑框图（2 分），并求出反馈函数（2 分）；

（2）设初始状态为（0, 0, 0, 1），给出其周期（2 分）、状态变迁（2 分）及输出序列（2 分）。

4、已知 RSA 密码体制的公开密钥为 $n=143$，$e=13$。

（1） 试加密明文 $M_1=103$。

（2） 通过分解 n 破译该密码，并对密文 $C_2=141$ 解密。

5、完成如下 ElGamal 型椭圆曲线密码的相关计算，其中椭圆曲线为 $y^2=x^3+x-5 \bmod 11$，基点 G=(3,5)。

（1）设私钥 d=5，计算公钥 P=dG；

（2）已知明文 M=7，假如加密过程中随机数选取 k=9，计算相应的密文。

三、 **应用题**（共 1 小题，每小题 18 分，共 18 分）

请针对电子支付中至少两类支付方式的安全性进行比较和分析，运用密码学知识综合分析不同支付方式在实际应用中潜在的风险和规避方法。