

武汉大学国家网络安全学院
2018-2019 学年度第一学期
《密码学》期末考试试卷(A 卷)

专业: 信息安全 学号: 201801010101 姓名: 张子豪

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	总分
分值	24	40	20	16	100

一. 简答题 (共 4 小题, 每小题 6 分, 共 24 分)

1. 请描述加密解密基本过程及密钥的作用。
2. 密码学中的‘对称’与‘非对称’的含义是什么?
3. 什么是认证? 认证与数字签名的区别是什么?
4. 请解释什么是短块问题, 列举常用处理方法, 比较优缺点。

二. 计算题 (共 4 小题, 每小题 10 分, 共 40 分)

1. 以英文为例用加法密码, 取密钥常数 $k=5$ 。
(1) 写出密文字母表: (4 分)
(2) 对明文 WUHAN UNIVERSITY 进行加密, 求出密文。(6 分)
2. DES 密码中第一个 S 盒为如下表所示 (16 进制表示),

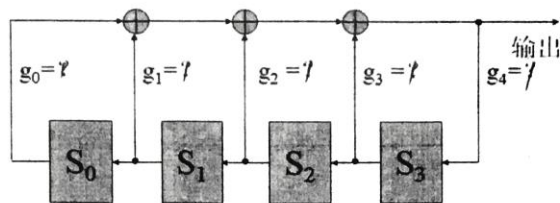
	$b_1b_2b_3b_4$															
b_0b_5	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
1	0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
2	4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
3	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D

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 $X_1=001010$ 和 $X_2=101010$, 分别求出对应的输出值 Y_1 (3 分) 和 Y_2 (3 分)。
- (2) 比较输出值 Y_1 和 Y_2 各位的异同, 即按位计算 $Y_1 \oplus Y_2$ 。(2 分) 该计算结果体现了 S 盒的什么特点? (2 分)

注: 要求答案以二进制表示。

3. 已知 $g(x)=x^4+x^3+x^2+x+1$ 为 GF(2) 上的多项式, 以其为连接多项式组成线性移位寄存器。



- (1) 求出反馈函数 (2 分), 并画出简化后的逻辑框图 (2 分);
 (2) 试穷举其所有非零状态 (2 分), 给出状态变迁 (2 分) 并求出其周期 (2 分)。

4. 已知素数域上椭圆曲线方程 $y^2 = x^3 + ax + b \pmod{p}$, 参数 $a=2, b=9, p=13$ 。请求出该曲线在 $GF(p)$ 上的全部解点。

三. 分析判断题 (共 2 小题, 每小题 10 分, 共 20 分)

1. 判断下列说法的正误, 并给出相应安全应用实例或者攻击实例:

“既然有安全隐蔽信道, 那么不需要密码算法也可以实现数据保密通信”

2. 判断下列说法的正误:

“对于公钥密码, 任何人都可以进行公钥操作, 即任何人都可以加密消息, 任何人都可以验证签名”。

根据你对于上述说法判断, 对下述加密和签名过程给出攻击实例:

用户 A 向用户 B 发送消息, 采用先加密再签名的方案——使用接受方 B 的公钥 K_{eB} 进行加密, 再用发送方自己的私钥 K_{dA} 进行签名, 即用户 A 发送如下消息给 B。

$$D(E(M, K_{eB}), K_{dA})$$

四. 综合设计题 (共 16 分)

请针对远程支付系统 (选择其中一种), 进行安全性分析与设计。分析设计时主要包括:

- (1) 应用问题描述;
- (2) 你认为其中的主要安全问题有哪些 (写主要问题 1—2 个即可);
- (3) 你觉得可以采用什么样的安全协议或密码学技术可以解决;
- (4) 若现有技术无法有效解决, 请提出你的观点。