**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）**

***\*本卷依据网安流出18年试卷重制而成，以方便打印，感谢提供者！ — by xyz\****

**专业： 学号： 姓名：** 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 |

1. **简答题（共4小题，每小题6分，共24分）**
2. 请描述加密解密基本过程及密钥的作用。
3. 密码学中的‘对称’与‘非对称’的含义是什么？
4. 什么是认证？认证与数字签名的区别是什么？
5. 请解释什么是短块问题，列举常用处理方法，比较优缺点。
6. **计算题（共4小题，每小题10分，共40分）**
7. 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）

1. DES密码中第一个S盒为如下表所示（16进制表示），

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | | | | | | | | | | | | | | |
|  | 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 |

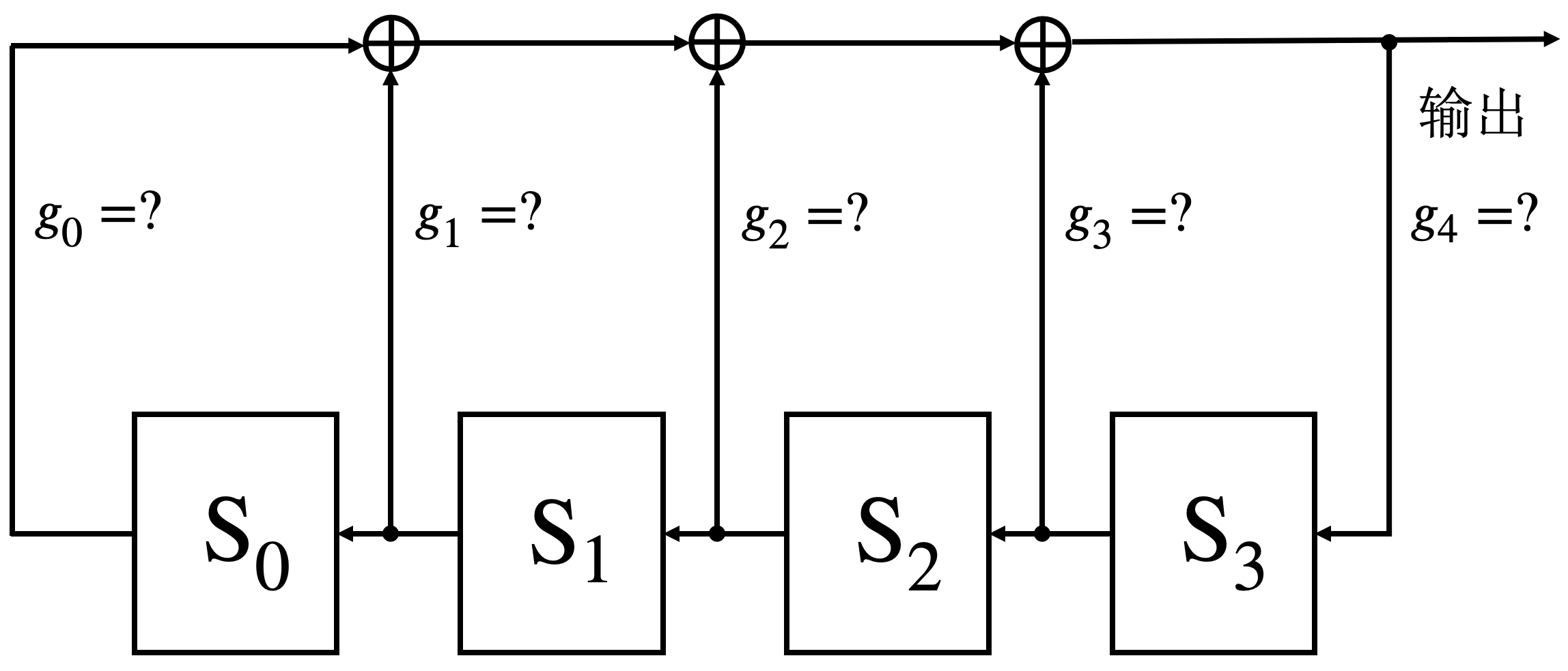
设S盒的输入为X，输出为Y。（X和Y都以二进制表示）

（1）对于已知输入值和，分别求出对应的输出值（3分）和（3分）。

（2）比较输出值和各位的异同，即按位计算。（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。

1. 已知为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）。

1. 已知素数域上椭圆曲线方程，参数，，。请求出该曲线在GF(p)上的全部解点。
2. **分析判断题（共2小题，每小题10分，共20分）**
3. 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”

1. 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改击实例：

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KeB进行加密，再用发送方自己的私钥进行签名，即用户A发送如下消息给B。

1. **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。