武汉大学国家网络安全学院
2019 -2020 学年度第 一 学期
《密码学》期末考试试卷 B 卷（开卷）

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。

未经主考教师同意，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
总分							100

一. **算法分析题**（共 2 小题，每小题 15 分，共 30 分）

1. 以英文为例用加法密码，取密钥常数 k=8。

（1）写出密文字母表；

（2） 对明文 WUHAN UNIVERSITY 进行加密，求出密文。

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	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= 010101 和 X_2= 010111，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）结合以上计算结果，说明 S 盒在 DES 算法中的作用。

二. **简答题（共 3 小题，每小题 10 分，共 30 分）**

1. 密码分析是研究密码体制的破译问题，根据密码分析者所获得的数据资源，有哪些密码分析方法？

2. 以 DES 为例，画出分组密码的密码分组链接（CBC）模式的加密/解密示意图，假设加密时明文一个比特错误，对密文造成什么影响？

3. 简述公钥密码体制的基本思想，以及相对于传统密码体制的优势？

三. **方案设计题（共 1 小题，每小题 40 分，共 40 分）**

1. 请针对现有某种信息系统进行安全性分析，包括：潜在的威胁分析、操作流程分析等，重点信息系统运行过程中的安全协议进行适当设计，以及密码学理论的运用。