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 A 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		总分
总分	30	30	40		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=10。
   （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_0b_5 \ $b_1b_2b_3b_4$	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	3	5	8
2	4	1	E	8	D	6	2	B	F	C	9	7	A	0	6	D
3	F	C	8	2	4	9	1	7	5	B	3	E	5	6	3	0

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= 101100 和 X_2= 100100，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. 在假设攻击者总能已知算法、获得密文的情况下，根据攻击者占有资源的角度分类，密码分析方法有哪些类别？

2. 为什么 AES 算法中的第一个加密步骤和最后一个加密步骤必须是 AddRoundKey？

3. 在使用 RSA 算法签名时，直接对消息进行签名而不用 hash 会有什么安全隐患？

三、 方案设计题（共 1 小题，每小题 40 分，共 40 分）

1. 请针对现有某种支付方式进行安全性分析，包括：潜在的威胁分析、支付流程分析等，重点对支付过程中的协议进行适当设计，以及密码学理论的运用。