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：_____ **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	五			总分
分值								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？

答：我国首个公开的商用密码算法是 2006 年发布的 SM4 分组密码算法。（2 分）

SM4 算法使用了以下基本密码部件：

该题只写了4种部件没有解释的共-2分

（1）S 盒（2 分）

SMS4 的 S 盒是一种以字节为单位的非线性代替变换，其密码学的作用在于起到混淆的作用。S 盒的输入和输出都是 8 位的字节。它本质上是 8 位的非线性置换。设输入字节为 a，输出字节为 b，则 S 盒的运算可表示为：b=S_Box（a）

（2）非线性变换τ（2 分）

SMS4 的非线性变换τ是一种以字为单位的非线性代替变换。它由 4 个 S 盒并置构成。本质上它是 S 盒的一种并行应用。设输入字为 $A=(a_0,a_1,a_2,a_3)$，输出字为 $B=(b_0,b_1,b_2,b_3)$，则

$B=\tau(A)=(S\_box(a_0), S\_box(a_1), S\_box(a_2), S\_box(a_3))$。

（3）线性变换部件 L （1 分）

线性变换部件 L 是以字为处理单位的线性变换部件，其输入输出都是 32 位的字。其密码学的作用在于起到扩散的作用。设 L 的输入为字 B，输出为字 C，则 $C=L(B)=B\oplus(B<<<2)\oplus(B<<<10)\oplus(B<<<18)\oplus(B<<<24)$ 。

（4）合成变换 T（1 分）

合成变换 T 由非线性变换 τ 和线性变换 L 复合而成，数据处理的单位是字。设输入为字 X，则先对 X 进行非线性 τ 变换，再进行线性 L 变换。记为 $T(X)=L(\tau(X))$。

只写了密码攻击类型没有解释的每题-1

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？

答：⑴仅知密文攻击（Ciphertext-only attack）所谓仅知密文攻击是指密码分析者仅根据截获的密文来破译密码。因为密码分析者所能利用的数据资源仅为密文，因此这是对密码分析者最不利的情况。（2 分）

⑵已知明文攻击（Known-plaintext attack）所谓已知明文攻击是指密码分析者根据已经知道的某些明文-密文对来破译密码。例如，密码分析者可能知道从用户终端送到计算机的密文数据从一个标准词“LOGIN”开头。又例如，加密成密文的计算机程序文件特别容易受到这种攻击。这是因为诸如“BEGIN”、“END”、“IF”、“THEN”、“ELSE”等词的密文有规律地在密文中出现，密码分析者可以合理的猜测它们。再例如，加密成密文的数据库文件也特别容易受到这种攻击。这是因为对于特定类型的数据库文件的字段及其取值往往具有规律性，密码分析者可以合理的猜测它们。如学生成绩数据库文件一定会包含诸如姓名、学号、成绩等字段，而且成绩的取值范围在 0-100 之间。近代密码学认为，一个密码仅当它能经得起已知明文攻击时才是可取的。（2 分）

⑶选择明文攻击（Chosen-plaintext attack）所谓选择明文攻击是指密码分析者能够选择明文并获得相应

的密文。这是对密码分析者十分有利的情况。计算机文件系统和数据库系统特别容易受到这种攻击，这是因为用户可以随意选择明文，并获得相应的密文文件和密文数据库。如果分析者能够选择明文并获得密文，那么他将会特意选择那些最有可能恢复出密钥的明文。（2 分）

⑷选择密文攻击（Chosen-ciphertext attack）所谓选择密文攻击是指密码分析者能够选择密文并获得相应的明文。这也是对密码分析者十分有利的情况。这种攻击主要攻击公开密钥密码体制，特别是攻击其数字签名。（2 分）

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。

答：公开密钥密码的基本思想是将传统密码的密钥 k 一分为二，分为加密钥 K_e 和解密钥 K_d ，用加密钥 K_e 控制加密，用解密钥 K_d 控制解密，而且由计算复杂性确保由加密钥 K_e 在计算上不能推出解密钥 K_d 。这样，即使是将 K_e 公开也不会暴露 K_d ,也不会损害密码的安全。于是便可将 K_e 公开，而只对 K_d 保密。由于 K_e 是公开的，只有 K_d 是保密的，所以便从根本上克服了传统密码在密钥分配上的困难，也适合各种需要数字签名的应用。（4 分）

对称密码与公钥密码体制的优缺点比较：（1）对称密码：加解密密钥相同；加解密实现效率快，算法安全性高；密钥传输及管理困难，保密通信系统开放性差；难于完成数字签名等公钥密码的功能。（2 分）（2）公钥密码：加解密密钥不同；密钥分配简答、便于管理；系统开放性好；加解密实现效率低。（2 分）

4、什么是认证？认证和数字签名的联系和区别是什么？

第4题按8分给分，因卷面总计只有98分的题目

答：认证（Authentication）又称鉴别，确认，它是证实某事是否名符其实或是否有效的一个过程。认证和数字签名技术都是确保数据真实性的措施，但两者有着明显的区别。（3 分）

（1）认证总是基于某种收发双方共享的保密数据来认证被鉴别对象的真实性，而数字签名中用于验证签名的数据是公开的。（1 分）

（2）认证允许收发双方互相验证其真实性，不准许第三者验证，而数字签名允许收发双方和第三者都能验证。（1 分）

（3）数字签名具有发送方不能抵赖、接收方不能伪造和具有在公证人前解决纠纷的能力，而认证则不一定具备。（1 分）

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。

(1)(2)写错，(3) 正确仍有4分

答：（1）k=8（3 分）

（2）明文字母表{ABCDEFGHIJKLMNOPQRSTUVWXYZ}

密文字母表{IJKLMNOPQRSTUVWXYZABCDEFGH}（3 分）

（3）密文= ECPIV CVQDMZAQBG

明文=WUHAN UNIVERSITY（4 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= 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 $Y_1 \oplus Y_2$。

答：（1）$Y_1=(8)_{16}=(1000)_2$ （3 分） $Y_2=(5)_{16}=(0101)_2$ （3 分）；

（2）$Y_1 \oplus Y_2=(1101)_2$ ，即 Y_1 和 Y_2 有三位不同；（4 分）

本题没有写2进制的，没有写3位不同的都没有扣分

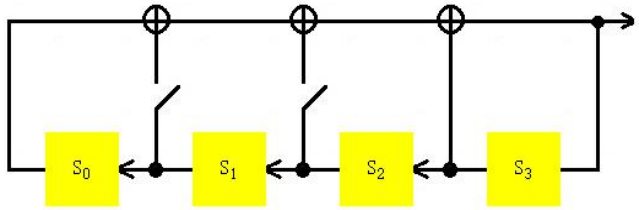
注：S 盒输出不是输入的线性和仿射函数；任意改变输入中的一位，输出至少有两位发生改变。S 盒是 DES 的非线性运算部件。

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）。

答：逻辑图如下（2 分）：



没有画两个断开处的没有分，反馈函数没有写异或的没有分

反馈函数为 $F(S_0, S_1, S_2, S_3)=S_0 \oplus S_3$ （2 分）

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

T=15 （2 分）

0001->0011->0111->1111->1110->1101->1010->0101->

1011->0110->1100->1001->0010->0100->1000->0001->...（2 分）

注：未按初始状态（0, 0, 0, 1）开始推导状态变迁，扣 2 分

输出序列：1110101100100001.... （2 分）

输出序列答案有误，多了一个0.正确答案是111010110010001.批改时按正确答案给分

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。

答：（1）方法一（反复平方）：令 $a = b^n = 103^{13} \bmod 143$， $n = 13 = (1101)_2$，（1 分）则

① $n_0 = 1, a_0 = 103, b_1 = 103^2 = 27$ （1 分）

② $n_1 = 0, a_1 = a_0 = 103, b_2 = b_1^2 = 14$ （1 分）

③ $n_2 = 1, a_2 = a_1 b_2 = 12, b_3 = b_2^2 = 53$ （1 分）

④ $n_3=1, a_3=a_2b_3=12\times53=64$（1 分）

方法二（CRT）：令

$$\begin{cases} x=103^{13} \bmod 11=9 \\ x=103^{13} \bmod 13=12 \end{cases}$$，（2 分）

没算出结果的，过程正确者过程分1-3分

则 $M_1=13, M_1'=13^{-1} \bmod 11=6, M_2=11, M_2'=11^{-1} \bmod 13=6$，（2 分）于是有

$x=9\times13\times6+12\times11\times6 \bmod 143=64$（1 分）

没算出结果的过程正确者过程分1-3分

(2) 计算 $143=11\times13$，$\varphi(143)=(11-1)(13-1)=120$，（1 分）由贝祖公式得

$(120,13)=-4\times120+37\times13$，（2 分）

故私钥 $d=37$，于是相应明文 $M_2=C_2^d=141^{37}=(-2)^{37}=37$（2 分）

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 k=9，计算相应的密文。

只写了公式没有计算的0分

答：（1）$P=5G=(2,7)$，计算过程如下：

①计算 $2G=(8,3)$：$\lambda=\dfrac{3x_1^2+a}{2y_1}=5$，$x_3=\lambda^2-2x_1=5$，$y_3=\lambda(x_1-x_3)-y_1=3$（2 分）

②计算 $4G=2G+2G=(7,9)$：$\lambda=1$，$x_3=7$，$y_3=9$（2 分）

③计算 $5G=G+4G=(2,7)$：$\lambda=1$，$x_3=2$，$y_3=7$（1 分）

（2）计算所有的点，得到 n=13;（2 分）

计算 kG=(7,2);（1 分） kP=(10,9);（1 分） x2=M*10mod13=2,（1 分）所以密文为（（7,2）,2）。

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，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。

本题支付方式（2）（3）（4）任意一个点完全没有的卷子酌情给了11-13分。支付方式答成支付协议的9分

答：(1)攻击模型和风险评估：3 分

(2)两类支付方式的支付流程说明与分析：5 分

(3)数据保密性与身份认证方法：5 分

(3)两种支付方式的比较较全面合理：5 分

有流程2分，有分析1分，分析合理2分