南 京 航 空 航 天 大 学

二〇一九 ～ 二〇二〇 学年 第 I 学期 **《密码学》考试试题**

考试日期： 2020 年 1 月 日 试卷类型： 试卷代号：

班号			学号			姓名				
题号	一	二	三	四	五	六	七	八	九	十	总分
得分											

一、 单项选择题：在下列各题中，将唯一正确的答案代码填入括号内
(本大题共 10 小题，总计 10 分)

1、加密和解密都是在（ a ）控制下进行的。

(a) 密钥 (b) 人 (c) 计算机

2、设 $X=X_1X_2\cdots X_n$ 是一个长度为 n 的可读明文的英文字母串，则 X 的重合指数 $I_c(x)$ 的大小接近于（ c ）。

(a) 0.038 (b) 1 (c) 0.065

3、跟公钥密码体制相比，对称密码体制具有加解密（ a ）的特点。

(a) 速度快 (b) 速度慢 (c) 速度不确定

4、三重 DES 的有效密钥长度为（b）。

(a) 56 位 (b) 112 位 (c) 64 位

5、尽管双重 DES 不等价于使用一个 56 位密钥的单重 DES，但有一种被称为（c）的破译方法会对它构成威胁。

(a) 中途差分攻击 (b) 随机碰撞攻击 (c) 中途相遇攻击

6、EIGamal 公钥密码体制的安全性是基于（ c ）问题的难解性。

(a) 椭圆曲线上的离散对数(ECC) (b) 大整数的素数分解(RSA) (c) 有限域上的离散对数

7、公钥密码体制的理论基础是（a）。

(a) 陷门单向函数 (b) 大数的素数分解 (c) 有限域上的离散对数

8、产生序列密码中的密钥序列的一种主要工具是（ c ）。

(a) 指令寄存器 (b) 数据寄存器 (c) 移位寄存器

9、设计序列密码体制的关键就是要设计一种产生（c）的方法。

（a）随机数　　（b）伪随机数　　（c） 密钥序列

10、下列不能使 DES 的 S 盒能够实现较好的混淆的是（a）

（a）S 盒的输出都是其输入的线性或仿射函数。

（b）改变 S 盒的一个输入比特，其输出至少有两比特产生变化，即近一半产生变化。

（c）当 S 盒的任一输入位保持不变，其它 5 位输入变化时(共有 2^5 =32 种情况)，输出数字中的 0 和 1 的总数近于相等。

二、是非题：在下列各题中，表述正确的在括号内划（∨），表述错误的在括号内划（╳）
(本大题共 10 小题，总计 10 分，每小题 1 分)

1、流密码是将明文划分成字符(如单个字母)，或其编码的基本单元(如 0, 1 数字)，字符分别与密钥流作用进行加密，解密时以同步产生的同样的密钥流实现。（∨）

2、在数学课上老师进行的定理证明是一个最大泄漏证明。（∨）

3、RSA 算法本质上是一种多表映射的加密算法。（╳）

4、对合密码是加密用的一种加密函数 f(x, k)，满足条件 f(x, k)2 =I (恒等置换)。（∨）

5、以一个本原 f(x)函数为特征多项式的 LFSR 的输出序列一定是 m 序列。（∨）

6、与 DES 算法相比，RSA 算法计算速度较快，适用对大量数据的加密。（╳）

7、分组密码的安全性不但依赖于密钥，也依赖于对加密算法和解密算法的保密。（╳）

8、Hash 函数是一种消息摘要函数，它适合应用于数字签名。（∨）

9、零知识最小泄露证明必须满足验证者从示证者那里得不到全部有关证明的知识。（╳）

10、SHA－1 的输出的长度为 160 位。（∨）

三、设 n=2，密钥为 $K=\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}$，将明文 CIST 用 Hill 加密，求其密文。**(本题计 10 分)**

解: 计算得 $K=\begin{pmatrix}7 & 18\\ 23 & 11\end{pmatrix}$（解密用）

明文为 CIST，则相应的明文向量为（2，8）和（18，19）。于是，相应的密文向量分别为

（2，8）$\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}$= (22+24, 16+56)= (20,20)（所有值 Mod26）

$$(18,19)\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}=(198+57,144+133)=(21,17)$$

因此，明文 CIST 的密文为 UUVR 。

四、设英文字母 a, b, c, …, z 分别编码为 0, 1, 2, …, 25. 已知 Hill 密码中的明文分组长度为 2，密钥 K 是 Z_{26} 上的一个 2 阶可逆方阵，假设明文 Friday 所对应的密文为 pqcfku，求出密钥 K。**(本题计 10 分)**

解：设 K= $\begin{pmatrix}a & c\\ b & d\end{pmatrix}$

明文相应的明文向量为（5, 17），(8, 3)和(0, 24)

密文相应的密文向量为（15, 16），(2, 5)和(10, 20)

得 ① (5a+17b) mod 26=15　② (5c+17d) mod 26=16

③ (8a+3b) mod 26= 2　④ (8c+3d) mod 26=5

⑤ (0a+24b) mod 26=10　⑥ (0c+24d) mod 26=20

由①③⑤得　a=7　b=8

由②④⑥得　c=19　d=3

求得 K= $\begin{pmatrix}7 & 19\\ 8 & 3\end{pmatrix}$

五、设 P=11，E 是由 $y^2 \equiv x^3 + x + 6 (\mathrm{mod}\ 11)$ 所确定的有限域 Z_{11} 上的椭圆曲线，设 α =（2，7），保密的解密密钥 d=7，① 计算 2 α = α + α ；② 若 β =7 α =（7，2），假设明文 x=（5，6），计算对应的密文。**(本题计 15 分)**

解：① $\lambda=(3\times2^2+1)(2\times7)^{-1}\bmod 11=2\times3^{-1}\bmod 11=2\times4\bmod 11=8$ **(2,7)点得斜率**

（分数模运算：a/b=k(mod p)⇔a=b*k(mod p)）

$$x_3=8^2-2-2\bmod 11=5$$
$$y_3=8\times(2-5)-7\bmod 11=2$$

得 2α=(5, 2)

② 随机选取 k=6，计算

$$y_0 = k\alpha = 6(2,7) = (7,9)$$

$$(c_1, c_2) = k\beta = 6(7,2) = (8,3)$$

$$y_1 = c_1 x_1 \bmod p = 8 \times 5 \bmod 11 = 7$$

$$y_2 = c_2 x_2 \bmod p = 3 \times 6 \bmod 11 = 7$$

所以密文 y=((7,9),7,7)

六、下列示意图为 DES 的四种工作模式中的两种模式，请在示意图下面写出此示意图是属于哪种工作模式及其表达式，并写出它们之间的差异。

其中，密文为 $Y=(Y_1Y_2\cdots Y_n)$，其密钥为 k_i，明文分组为 $x=(x_1x_2\cdots x_n)$，选取一个 64 位的初始向量 IV。

(本题总计 15 分)

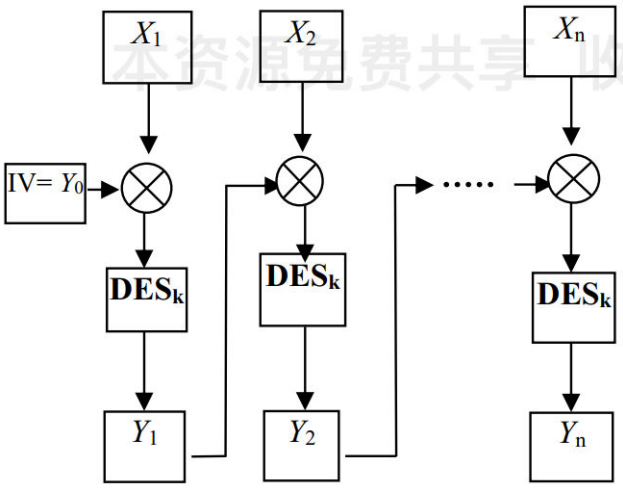


图 1

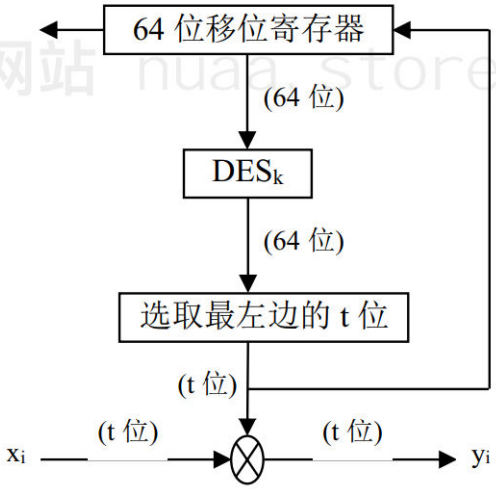


图 2

图 1 表达式：Y0＝IV，$y_i=DES_k(x_i \oplus y_{i-1})$，$1 \leqslant i \leqslant n$

图 2 的表达式：$z_0=IV$，$z_i=DES_k(z_{i-1})$，$y_i=x_i \oplus z_i$，$1 \leqslant i \leqslant n$

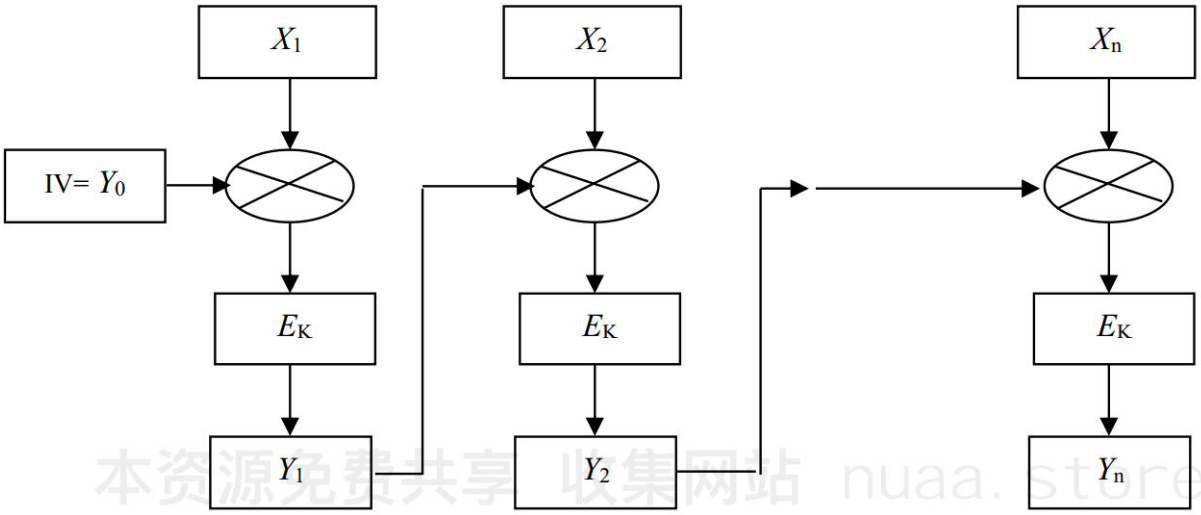
特点：在 OFB 模式中，一个密文块 yi（或明文块 xi）的改变在解密（或加密）时只会引起相应的明文块 x_i（或密文块 yi）的改变，不会引起其他密文块的改变。

在 CBC 模式中，一个密文块 yi 的改变在解密时时只会引起相应的相应的明文块 xi 和 xi+1. 的改

变，不会引起其他明文块的改变。而一个明文块 xi 的改变，在加密时将会相应的密文块 yi 以及其后的所有密文块的改变。

七、设一个分组密码体制有 $y=E_k(x)$，其密钥为 k，明文分组为 $x=(x_1x_2\cdots x_n)$，请画出其密码分组链接模式（CBC）示意图，并进行适当的文字说明。 **(本题总计 15 分)**

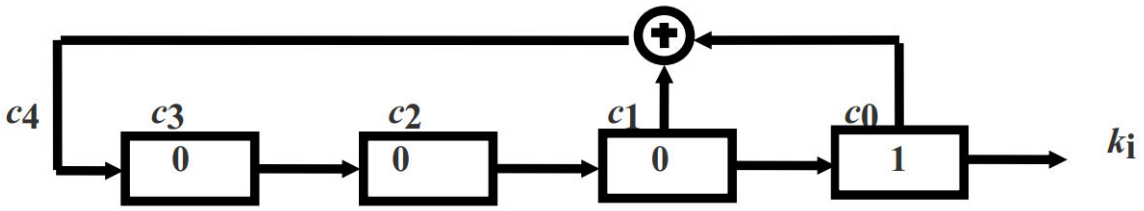
解：



CBC 模式的加密操作

在 CBC 模式下，首先选取一个初始向量 IV，定义 Y_0=IV。每个明文组 X_i 加密之前，先与反馈至输入端的前一组密文 Y_{i-1} 按位模 2 求和后，再送至 E_K 加密。第一组明文 X_1 加密时尚无反馈密文，为此需要选取一个初始向量 IV，定义 Y_0=IV。各密文组 Y_i 不仅与当前明文组 X_i 有关，而且通过反馈作用还与以前的明文组 X_1，X_2，…，X_{i-1}，有关。最后有 $Y_i = E_k(X_i \oplus Y_{i-1})$.

八、设 n=4 的 LFSR，输出序列满足 $k_{i-4}+k_{i-3}+k_i=0$。初始状态为 1000。
序列的周期为 $15=2^4-1$。图如下：



请写出状态转移序列及相应输出。**(本题总计 15 分)**

时刻	状态				输出
	3	2	1	0	0
0	0	0	0	1	1
1	1	0	0	0	0
2	0	1	0	0	0
3	0	0	1	0	0
4	1	0	0	1	1
5	1	1	0	0	0
6	0	1	1	0	0
7	1	0	1	1	1
8	0	1	0	1	1
9	1	0	1	0	0
10	1	1	0	1	1
11	1	1	1	0	0
12	1	1	1	1	1
13	0	1	1	1	1
14	0	0	1	1	1
15	0	0	0	1	1