海 军 工 程 大 学

2027 年硕士研究生招生考试自命题科目考试大纲

科目代码：834　　科目名称：密码学

一、考试要求

主要考查学生对密码学基本概念的理解与掌握；对序列密码、分组密码、公钥密码及其应用的理解与掌握；对数字签名与认证及其应用的理解与掌握；对密钥管理基本知识及其应用的理解与掌握；以及运用基本理论和方法，分析解决密码算法工程应用问题的能力。

二、考试内容

1. 密码学概论

密码体制，密码学研究的基本问题及主要应用，密码学研究现状及发展趋势。编制密码的基本原理和方法，置换密码、代替密码、转轮密码。

2. 对称密码

序列密码的原理及工作方式，线性反馈移位寄存器，m-序列，非线性前馈和非线性组合模型，典型序列密码算法。分组密码的原理和设计原则，分组密码的两种典型结构，分组密码的主要工作模式，DES 算法，AES 算法，及其它典型分组密码算法。

3. 非对称密码

非对称密码的基本思想、工作方式，RSA 公钥密码算法，RSA 算法的安全性分析及其实现要点，Elgamal 公钥密码算法和 ECC 公钥密码算法。

4. 密码算法应用

数字签名的概念、原理及其主要应用，RSA、Elgamal 数字签名方案，特殊作用的数字签名方案。Hash 函数的性质，MD5 和 SHA-1 算法，Hash 函数的典型应用，消息认证，认证协议和身份认证。

5. 密钥管理

密钥的分类、层次结构、密钥的分散管理及 Shamir 门限秘密分割方案、密钥的生命周期、传统密码体制和公钥密码体制的密钥管理、数字证书的基本原理及应用。

三、考试形式

考试形式为闭卷、笔试，考试时间为 3 小时，满分 150 分。

题型包括：选题题 30 分、填空题 20 分、判断题 20 分、简答题 20 分、计算题 40 分、综合题 20 分。

四、参考书目

《现代密码学》. 胡卫等主编. 国防工业出版社，2024 年 9 月，第 1 版。

全国硕士研究生招生考试海军工程大学

密码学　样卷

（科目代码 834）

注意事项：

1．本试卷共 3 页，满分 150 分；考试时间 180 分钟。

2．所有试题都作答在答题纸（卡）上，答在试卷上无效。

3．考试结束后，考生将答题纸（卡）和本试卷一同装入试卷袋后密封，并在密封签上签名。

一、不定项选择题（本大题共 15 小题，每小题 2 分，共 30 分）

在每小题列出的四个备选项中至少有一个是符合题目要求的，请将其代码填写在答题纸上对应题号内。少选、错选或未选均无分（全部选对得 2 分，少选、错选或未选得 0 分）。

1．编制古典密码的基本方法主要有（　　）。

A．置换　B．代替　C．代数　D．迭代

2．以下（　　）行为是主动攻击。

A．中断　B．篡改　C．伪造　D．监听

3．下面哪些算法属于分组密码算法（　　）。

A．RC4　B．DES　C．AES　D．IDEA

4．编码类型主要可分为如下几种（　　）。

A．对称型　B．压缩型　C．扩展型　D．代替型

5．若 Alice 想向 Bob 分发一个会话密钥，采用 ELGamal 公钥加密算法，那么 Alice 应该选用的密钥是（　　）。

A．Alice 的公钥　B．Alice 的私钥　C．Bob 的公钥　D．Bob 的私钥

6．通信中仅仅使用数字签名技术，不能保证的服务是（　　）。

A．认证服务　B．完整性服务　C．保密性服务　D．不可否认服务

7．下面（　　）不是 Hash 函数具有的特性。

A．单向性　B．可逆性　C．压缩性　D．抗碰撞性

8．无记名投票系统主要采用（　　）签名技术。

A．不可否认签名　B．盲签名　C．多重签名　D．批量签名

9．Alice 收到 Bob 发给她的一个文件的签名，并要验证这个签名的有效性，那么签名验证算法需要 Alice 选用的密钥是（　　）。

A．Alice 的公钥　B．Alice 的私钥　C．Bob 的公钥　D．Bob 的私钥

10．MD5Hash 算法以（　　）位分组来处理输入文本。

A．64　B．128　C．256　D．512

11．解决软件共享问题主要应用（　　）技术。

A．不可否认签名　B．盲签名　C．多重签名　D．批量签名

12．密码类型根据对明文消息加密方式的不同分为（　　）。

A．序列密码　B．分组密码　C．公开密钥密码　D．传统密码

13．序列密码的工作方式主要包括（　　）。

A．同步　B．异步　C．自同步　D．跨步

14．分组密码的主要的工作模式有哪几种（　　）。

A．电码本模式　B．密文链接模式　C．密码反馈模式　D．输出反馈模式

15．报文认证包括哪几个方面（　　）。

A．报文的发送方　B．报文的接收方　C．报文的内容　D．报文的时间性

二、填空题（本大题共 10 个空，每空 2 分，共 20 分）

16．密码体制的安全应当只取决于_____的安全，而不取决于对_____的保密。

17．密码体制根据加解密时使用的密钥是否相同分为_____、_____。

18．分组密码的工作模式中可用于认证是_____、_____。

19．ELGamal 密码是一种基于_____困难性的公开密钥密码。

20．C.E.Shannon 提出的设计密码体制的两种基本原则是_____和_____。

21．设维吉尼亚密码的密钥为 class，对明文 wfahe 加密，则密文为_____。

三、判断题（本大题共 10 个小题，每小题 2 分，共 20 分）

22．网络安全应具有以下四个方面的特征：保密性、完整性、可用性、可查性。（　　）

23．没有一种密码系统是无懈可击的，仅仅是一个时间 / 空间复杂性问题。（　　）

24．加密程度越高，算法越复杂，系统性能会降低。（　　）

25．为了保证安全性，密码算法应该进行保密。（　　）

26．DES 算法中对明文的处理过程分 3 个阶段：首先是一个初始置换 IP，用于重排明文分组的 64 比特数据。然后是具有相同功能的 64 轮变换，每轮中都有置换和代换运算。最后是一个逆初始置换从而产生 64 比特的密文。（　　）

27．一次一密体制即使用量子计算机也不能攻破。（　　）

28.我的公钥证书是不能在网络上公开的，否则其他人可能假冒我的身份或伪造我的数字签名。（　　）

29．公开密钥密码体制比对称密钥密码体制更为安全。（　　）

30．日常所见的校园饭卡是利用的身份认证的单因素认证。（　　）

31．Diffie-Hellman 算法的安全性在于离散对数计算的困难性，可以实现密钥交换。（　　）

四、简答题（本大题共 4 小题，每小题 5 分，共 20 分）

32．请解释“一次一密”密码体制的基本思想。

33．为什么要引入非对称密码体制。

34．一种完善的签名应满足哪几个条件。

35．简述密钥分层管理的基本思想及其必要性。

五、计算题（本大题共 4 小题，每小题 10 分，共 40 分）

36．4-级的 LFSR，抽头位为 X_4 和 X_1，初态为 1001，试画出对应的反馈移位寄存器结构图，写出反馈逻辑函数，并求出从初态开始的一个周期的输出序列。

37．已知 DES 分组密码算法第一圈的输入为 L_0= 83D67FEB，R_0= 97A4F8ED，子密钥为 K_1= C4127AD42B45，求第一圈的加密结果 L_1 和 R_1（数据均为 16 进制表示，DES 工作原理见题 37 图）。

38．通信双方采用 RSA 公钥密码体制通信，发送方的公开密钥是(e_1, n_1)=（23，55）。接收方的公开密钥是（e_2, n_2）=(13，33)，试求用户 A 通过 RSA 算法向用户 B 发送的对消息 m=6 的带签名的保密信息。

39．设 p=19，g=2，私钥 x=8。消息 m 的 Hash 值为 7，选择随机数 k=5，试用 ElGamal 签名方案对消息 m 的 Hash 值进行签名，并用公钥验证签名。

六、综合题（本大题共 1 小题，每小题 20 分，共 20 分）

40．设 Alice 的标识为 ID_A，公私钥对为（K_{eA}，K_{dA}），模数为 N_A。Bob 的标识为 ID_B，公私钥对为

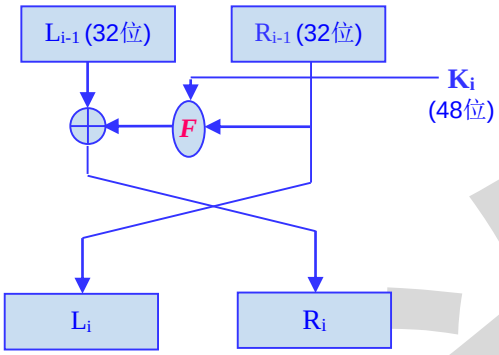
（K_{eB}，K_{dB}），模数为 N_B，设 $N_A<N_B$。Alice 想和 Bob 通过网络进行通信，设他们采用公开密钥密码体制，加密算法为 E，解密算法为 D，明文为 M，明文的 HASH 值表示为 H(M)。试根据下面要求设计相应的密码通信方案。

（1）仅确保数据来源的真实性（4 分）。

（2）在确保数据来源的真实性的基础上，确保数据的秘密性（6 分）。

（3）由于明文 M 相对较大，在传输过程中拟采用分组密码算法 AES 对数据进行加密，请设计会话密钥协商方案，同时实现认证、秘密性和报文真实性（10 分）。

题 37 图 DES 工作原理图



P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

8个6进4出S盒

输出行 \ 列	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1 0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
S_1 1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
S_1 2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
S_1 3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2 0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
S_2 1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
S_2 2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
S_2 3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3 0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
S_3 1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
S_3 2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
S_3 3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4 0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
S_4 1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
S_4 2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
S_4 3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5 0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
S_5 1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
S_5 2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
S_5 3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6 0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
S_6 1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
S_6 2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
S_6 3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7 0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
S_7 1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
S_7 2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
S_7 3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8 0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
S_8 1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
S_8 2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
S_8 3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11