网络安全与数据加密技术 期末模拟卷

一、简答题（共 4 题，共 20 分）

1.(5 分)对安全系统的攻击可以分为主动攻击和被动攻击，请描述两种攻击方式的特点并举例说明。

2.(5 分)DES(数据加密标准)加密方法采用了_____位的分组长度和_____位的密钥长度，一共进行_____轮变换。MD-5 算法的分组长度为_____位，消息摘要长度为_____位。SHA-512 算法的分组长度为_____位，消息摘要长度为_____位。

3. (5 分)请简述使用 Hash 函数检查数据完整性的过程。

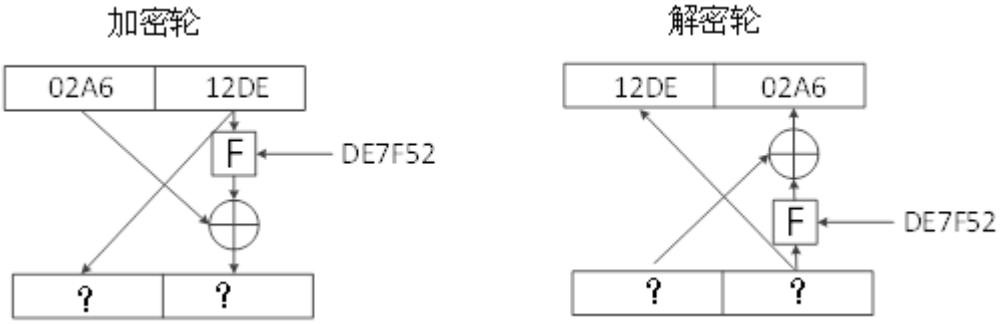
4. (5 分)请分别描述（1）公钥证书的获取过程和交换过程，（2）公钥证书的验证过程。

二、问答题（共 6 题，共 60 分）

1. (10 分) 请使用 Playfair 密码加密技术来完成对下列明文的加密，画出加密置换所需的字母矩阵并写出加密结果。

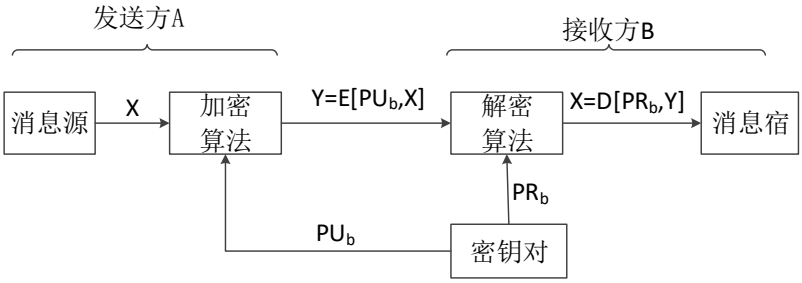
   明文为：Ilovecryptography，密钥词为 shmtu. (注：密文均为大写字母)

2. (10 分) 下图为 Feistel 密码结构在第 13 轮的加密示意图及与之对应的第 4 轮解密示意图，请写出该轮加密和对应解密的结果(即下图中“？”部分)，并简述该轮加密过程和对应的解密过程。

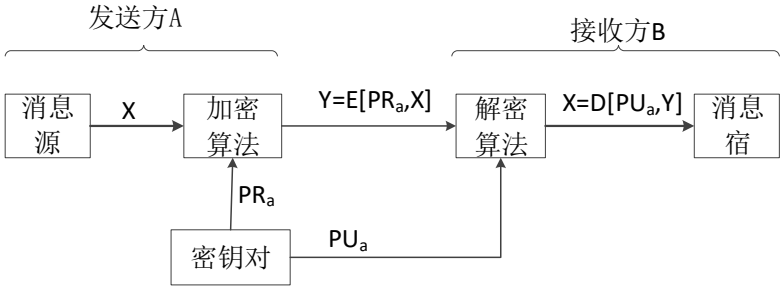


3.(10 分) 请描述基于生日悖论进行碰撞攻击的过程。

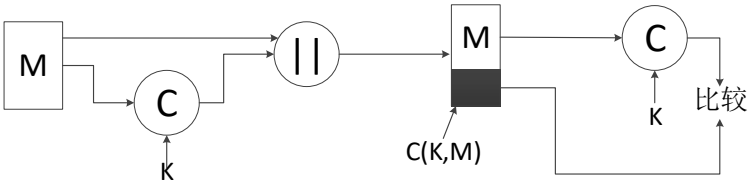
4.(10 分)下图分别描述了(a)公钥密码体制的保密性、(b)公钥密码体制的认证、(c)使用消息认证码进行消息认证、(d)对文件进行数字签名，请根据下图提示，用文字和公式分别进行描述和简要分析。



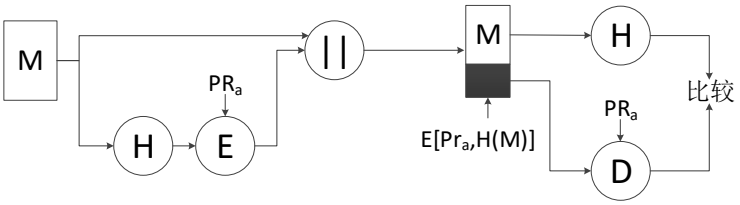
(a. 公钥密码体制的保密性)



(b. 公钥密码体制的认证)

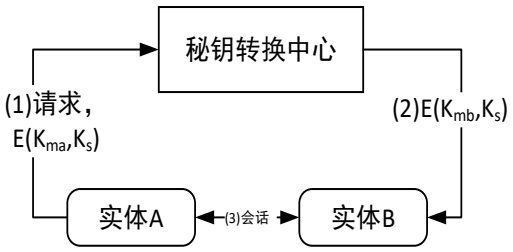


(c. 消息认证)

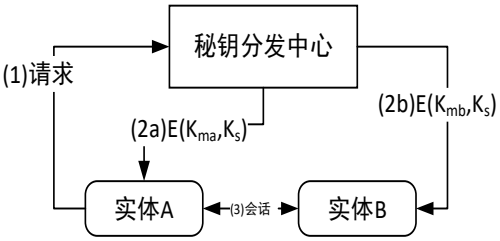


(d. 数字签名)

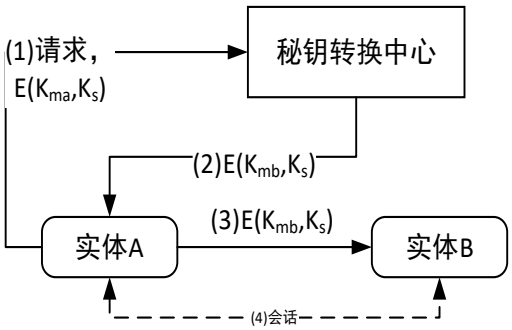
5. (10 分)下图两个通信实体之间的密钥分发方式，一共有两种不同的选项，每个选项都有两个变体。请分别描述四种不同的密钥分发方式的过程。



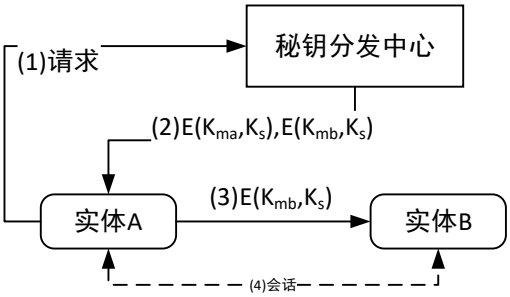
(a)密钥转换



(c)密钥分发



(b)带密钥转发的密钥转换



(d)带密钥转发的密钥分发

6.(10 分)对于基于非对称加密的单向认证中，签名的信息添加保密性的方法是A→B:$\mathbf{E}(\boldsymbol{PU_b}, [\boldsymbol{M}||\boldsymbol{E}(\boldsymbol{PR_a}, \boldsymbol{H}(\boldsymbol{M}))])$：

(1).请综合本课程所学的知识，找出上述方法的缺点是什么？

(2).请针对上述缺点进行改进，并写出改正思路及方法。

三、计算题（共 1 题，共 20 分）

1.请使用 RSA 算法完成如下计算，并写出计算过程：

(1). (10 分)请描述并计算基于 RSA 算法的公钥和私钥的过程，其中$\mathrm{p} = 5$，$\mathrm{q} = 17$，选择公钥中的$\mathrm{e} = 5$。

(2). (5 分)使用(1)中已经计算出的公钥对明文$\mathrm{M} = 11$进行加密，并描述加密的计算过程。

(3). (5 分)对(2)中所得的密文使用(1)中已计算出的私钥进行解密，并描述解密的计算过程。

参考答案及评分标准（供参考）

一、简答题：(每题 5 分，共 20 分)

1.（5 分）主动攻击包括对数据流进行修改或伪造数据流，可分为四类：伪装、重播、消息修改和拒绝服务。

被动攻击的特性是对传输进行窃听和监测。攻击者的目标是获得传输的信息。信息内容的泄露和流量分析是两种被动攻击。

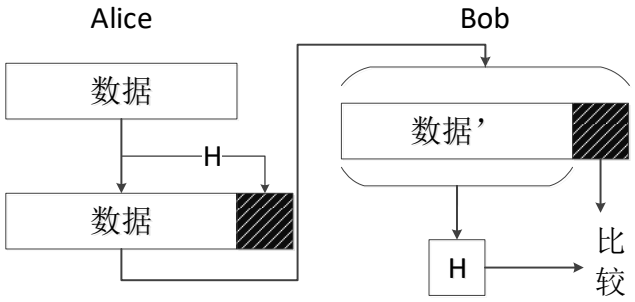
2.（5 分）

64 56 16

512 128

1024 512

3.（5 分）发送者根据待发送的消息使用该函数计算一组 Hash 值，然后将 Hash 值和消息一起发送过去。接收者收到后对于消息执行同样的 Hash 计算，并将结果与收到的 Hash 值进行对比。如果不匹配，则接收者推断出消息(也有可能是 Hash 值)遭受了篡改。



4.（5 分）

（1）a. 公钥证书的获取：

通信方向 A 证书管理员提供一个公钥请求证书，申请者以某种安全的认

证通信方式发送其公钥PU_a，管理员提供如下形式的证书：

$$C_A = E(PR_{auth}, T||ID_A||PU_a])$$

通信方向 B 以同样的方式获取证书C_B.

b. 公钥证书的交换：

在通信之前，A 和 B 分别将自己的证书C_A和C_B发送给对方。

（2）公钥证书的验证过程：

后者通过以下方式读取和验证证书：

$$D((PU_{auth}, C_A) = D(PU_{auth}, E(PR_{auth}, [T||ID_A||PU_a]) = (T||ID_A||PU_a)$$

因为证书只有使用管理员的公钥才能读取证书，因此接收方可验证证书确实是来自于证书管理员。ID_A和PU_a向接收方提供证书持有者的名字和公钥，时间戳 T 验证证书的时效性。

二、问答题(每题 10 分，共 60 分)

1. 答：(共 10 分)

首先构造置换表为：

S	H	M	T	U
A	B	C	D	E
F	G	I/J	K	L
N	O	P	Q	R
V	W	X	Y	Z

然后对明文进行分组和填充，从而使明文变为如下形式：

Il ov ec ry pt og ra ph yx。

每一个双字母明文对应的密文如下：

KF NW AD QZ QM WO NE OM ZY.

2.答：(共 10 分)

$12DE\ \ 02A6 \oplus F(DE7F52,12DE)\ \ 02A6 \oplus F(DE7F52,12DE)\ \ 12DE$

加密过程：

对于加密第 14 轮，设其LE_{13}和RE_{13}表示第14轮加密输入的左半部分和右半部分，则第 14 轮的输出，$LE_{14} = RE_{13}$，$RE_{14} = LE_{13} \oplus F(RE_{13}, K_{14})$，因为$RE_{13} = 12DE$，$LE_{13} = 02A6$，则$LE_{14} = RE_{13} = 12DE$，$RE_{14} = LE_{13} \oplus F(RE_{13}, K_{14}) = 03A6 \oplus F(DE7F52,12DE)$。

解密过程：

对于解密第 3 轮，逆序使用子密钥K_i。也就是说，第一轮使用$K_n(K_{16})$，第二轮使用$K_{n-1}(K_{15})$，直到最后一轮使用K_1。

第 3 轮输入，$LD_2 = RE_{14}, RD_3 = LE_{14}$，其左部分输出为：$LD_3 = RD_2$，其右部分输出为：$RD_3 = LD_2 \oplus F(RD_2, K_{14})$，因为$LD_2 = 02A6 \oplus F(DE7F52,12DE)$，$RD_2 = 12DE$则$LD_3 = 12DE$，$RD_3 = F(DE7F52,12DE) \oplus 02A6 \oplus F(DE7F52,12DE) = 02A6$

5. 答(共 10 分)

(1). 发送方 A 准备对文本消息 x 进行签名，其使用的方法是：用 A 的私钥对 m 位的 Hash 码加密并将加密后的 Hash 码附于消息之后。

(2).攻击者产生该(合法)x 的$2^{m/2}$种变式 x’，且每一种变式表达相同的意义，将这些消息以及对应的 Hash 值存储起来。

(3).攻击者准备伪造一条消息 y，并想获取 A 的签名。

(4).攻击者再产生该伪造(非法)消息 y 的消息变式 y’，每个变式 y’与 y 表达相同的意义。对于每个 y’，攻击者计算 H(y’)，并与任意的 H(x’)进行比对，重复这一过程直到碰撞出现。即这一过程直到找到一个 y’与某个 x’具有相同的 Hash 值。

(5).攻击者将该合法消息变式 x’提供给 A 签名，将该签名附于伪造消息的有效变式 y’后并发送给预期的接收方。因为上述两个变式的 Hash 码相同，所以他们产生的签名也相同，因此攻击者即使不知道加密秘钥也能攻击成功。

4. 答(共 10 分)

a.公钥密码体制的保密性：

发送方 A 的消息源产生消息 X，A 欲将消息 X 发送给 B。B 产生公钥PU_b和私钥PR_b,其中只有 B 知道PR_b，而PU_b则是公开可访问的，所以 A 也可以访问PU_b。

为了实现保密性,A 使用作为输入的消息 X 和加密密钥PU_b,生成密文Y，其中$Y = E(PU_b, X)$，期望的接收方 B 因为拥有相应的私钥，所以可以进行逆变换$X = D(PU_b, Y)$。攻击者可以观察到Y并且可访问PU_b，但是他不能访问PR_b，从而无法得知消息X，从而实现了公钥密码体制的保密性。

b.公钥密码体制的认证：

A 向 B 发送消息前，先用 A 的私钥对消息加密($Y = E(PR_a, X)$)，B 则用 A 的公钥对消息解密($X = D(PU_a, Y)$)。由于是用 A 的私钥对消息加密，所以只有 A 可以加密消息，因此，整个加密后的消息就是数字签名。

c.消息认证：

假定通信双方比如 A 和 B，共享密钥 K。若 A 向 B 发送消息时，则 A 计算 MAC，它是消息和密钥的函数，即$MAC = C(K, M)$，其中 M 为输入消息，C 为 MAC 函数，K 为共享的密钥，MAC 为消息认证码。

消息和 MAC 一起被发送给接收方。接收方对收到的消息用相同的密钥进行相同的计算，得出新的 MAC，并将接收到的 MAC 与其计算出的 MAC 进行比较，如果假设只有收发双方知道该密钥，那么如果消息未被修改，则接收到的 MAC 与计算得出的 MAC 相等。

d. 数字签名：

A 对一个消息 M 进行数字签名，首先计算该消息的 Hash 值（$H(M)$），然后用自己的私钥（PR_a）进行加密得签名$\mathrm{X} = \mathrm{E}(PR_a, H(M))$,最后将消息 M 与签名一起发送给验证方。验证方 B 将签名X使用签名方 A 的公钥PU_a进行解密得该消息的 Hash 值$H(M) = \mathrm{D}(PU_a, \mathrm{X})$,然后计算接收到的消息$M'$的 Hash 值（$H(M')$），若$H(M) = H(M')$，说明该消息确实是由签名方 A 签名的。由于只有签名方 A 有私钥PR_a，所以改签名肯定是 A 生成的。

5. (共 10 分)

a 密钥转换：实体 A 生成或获取一个对称密钥，作为与 B 进行通信的会话密钥。A 使用与 KTC 共享的主密钥对密钥进行加密，并将加密后的密钥发送给 KTC。KTC 解密会话密钥，将其与 B 共享的主密钥中的会话密钥重新加密，KTC 直接将其发送给 B。

b 带密钥转发的密钥转换：实体 A 生成或获取一个对称密钥，作为与 B 进行通信的会话密钥。A 使用与 KTC 共享的主密钥对密钥进行加密，并将加密后的密钥发送给 KTC。KTC 解密会话密钥，将其与 B 共享的主密钥中的会话密钥重新加密，然后将重新加密的会话密钥发送给 A，让 A 转发给 B。

c 密钥分发：实体 A 向 KDC 发送一个对称密钥的请求，该对称密钥用作与 B 进行通信的会话密钥。KDC 生成一个对称会话密钥，然后使用与 A 共享的主密钥加密该会话密钥并将其发送给 A。KDC 用与 B 共享的主密钥对会话密钥进行加密，并将其发送给 B。

d 带密钥转发的密钥分发：实体 A 向 KDC 发送一个对称密钥的请求，该对称密钥用作与 B 进行通信的会话密钥。KDC 生成一个对称会话密钥，然后使用与 A 共享的主密钥加密该会话密钥并将其发送给 A。KDC 还是用与 B 共享的主密钥对会话密钥进行加密后，KDC 中心将两个加密的密钥都发送到 A，然后 A 把用 KDC 和 B 共享的主密钥加密的会话密钥转发给 B。

6. （共 10 分）

（1）上述方法的缺点，使用公钥加密算法对$\boldsymbol{M||E(PR_a, H(M))}$加密，由于消

息 M 可能会很长，而公钥加密算法对长消息加密解密的运算开销太大，使的该方法实际运行开销过大。

（2）改正思路：对于$\boldsymbol{M}||\boldsymbol{E}\left(\boldsymbol{PR_a}, \boldsymbol{H}(\boldsymbol{M})\right)$消息使用对称加密算法进行加密，将加密的秘钥由接收方的公钥进行加密，由于只有接收方能够读取会话秘钥，从而实现消息的保密。A→B:$\mathbf{E}(\boldsymbol{PU_b}, K_s)||\mathrm{E}(K_s, [\boldsymbol{M}||\boldsymbol{E}\left(\boldsymbol{PR_a}, \boldsymbol{H}(\boldsymbol{M})\right)])$.

三、问答题(共 20 分)

(1)（共 10 分）

按照题目给定的两个素数$\mathrm{p}=5$，$\mathrm{q}=17$，

计算$n=pq=5\times17=85.$

计算$\phi(n)=(p-1)(q-1)=4\times16=64.$

选定 e 使其与$\phi(n)=64$互素且小于$\phi(n)$，本题目给定为的$\mathrm{e}=5$。

确定 d 使得$de\equiv1\ (mod\ 65)$且$d<65$。因$5\times13=65=1\times64+1$，所以$d=13$。

所得的公钥$PU=\{5,85\}$，私钥$PR=\{13,85\}.$

(2)．（共 5 分）

加密时，计算$C=11^5\ (\mathrm{mod}\ 85)$。利用模算术的性质，可如下计算：

$11^5\ (\mathrm{mod}\ \ 85)=[11^4\ (\mathrm{mod}\ \ 85)\times11^1\ (\mathrm{mod}\ \ 85)]\ mod\ \ 85$

其中：

$11^1\ (\mathrm{mod}\ \ 85)=11$

$11^2\ (\mathrm{mod}\ 85)=121\ (\mathrm{mod}\ \ 85)=36$

$$11^4 \pmod{85} = (11^2 \pmod{85})^2 \pmod{85} = (36)^2 \pmod{85} = 21$$

所以，$11^5 \pmod{85} = [21 \times 11]\ mod\ 85 = 231 mod\ 85 = 61.$

得到密文$C = 61$。

(3)．（共 5 分）

解密时，计算$M = C^{13} \pmod{85} = 61^{13} \pmod{85}$

$61^{13} \pmod{85} = [61^8 \pmod{85} \times 61^4 \pmod{85} \times 61^1 \pmod{85}] \pmod{85}$

其中

$$61^1 \pmod{85} = 61$$

$$61^2 \pmod{85} = 3721 \pmod{85} = 66$$

$$61^4 \pmod{85} = (61^2 \pmod{85})^2 \pmod{85} = 66^2 \pmod{85} = 21$$

$$61^8 \pmod{85} = (61^4 \pmod{85})^2 \pmod{85} = 21^2 \pmod{85} = 16$$

则，

$37^{13} \pmod{85} = [16 \times 21 \times 61] \pmod{85} = 11$。

得到明文$M = 11$。