第一部分 计算题

一、 RSA 的计算

基本原理：RSA 算法基于大数分解的数学问题。可用于加密和数字签名

01 密钥生成：

- 选择两个大质数 p 和 q，**计算 n = pq，φ(n) = (p-1)(q-1);**
- 选择一个整数 e , (1 < e < φ(n))且 e 与φ(n)互质.
- 根据等式：$(de) \bmod \varphi(n) = 1$ 计算 d .
- **公钥：** (e,n) **，私钥：** (d,n) **. (只写** e **或** d **都是正确的).**

02 加密：密文 C = M^e **mod n，消息 M** 是一个小于 n 的整数;

03 解密：消息 M = C^d **mod n。**

☆练习 1

若 $p = 3, q = 11, e = 7, M = 5$ **，求加解密过程.**

解答： $n = pq = 33, \varphi(n) = (p-1)(q-1) = 20$

由于$e = 7$,则公钥$pk = 7$

根据$7d \bmod 20 = 1$,计算得到$d = 3$,因此私钥$sk = 3$

密文：$C = 5^7 \bmod 33 = 14,$

解密：$M' = 14^3 \bmod 33 = 5$

☆练习 2

在使用 *RSA* **的公钥体制中，已截获发给某用户的密文** $C = 10$ **，该用户的公钥** $e = 5$ **，** $n = 35$ **，那么明文** M **是多少?**

解答：倘若直接根据 $M^5 \bmod 35 = 10,$ 额，似乎不太好计算，

注意到$n = pq = 35 = 5 \times 7$,不妨假设 $p = 5, q = 9$ ，因此 $\varphi(n) = 4 \times 6 = 24$

因此$5d \bmod 24 = 1,$ 则 $d = 5$

因此 $M = C^d \bmod 35 = 10^5 \bmod 35 = 5$

★关于模运算的技巧

Tips1：求高阶幂运算， $ab \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$ **，核心思想：递归拆分**

Q：求$3^{78} \bmod 7 = ?$

A：将3^{78}拆分成尽可能小的两部分进行计算(等分),按①－⑧顺序进行逐一计算

①$3^{78} \bmod 7 = (3^{39} \cdot 3^{39}) \bmod 7$⑧$= (6 \cdot 6) \bmod 7 = 1$

②$3^{39} \bmod 7 = (3^{19} \cdot 3^{19} \cdot 3) \bmod 7$⑦$= (3 \cdot 3 \cdot 3) \bmod 7 = 6$

③$3^{19} \bmod 7 = (3^{9} \cdot 3^{9} \cdot 3) \bmod 7$⑥$= (6 \cdot 6 \cdot 6) \bmod 7 = 3$

④$3^{9} \bmod 7 = (3^{4} \cdot 3^{4} \cdot 3) \bmod 7$⑤$= (4 \cdot 4 \cdot 3) \bmod 7 = 6$

按照这个思路，以上5^7是不是就相对更好计算了！

Tips2：已知私钥求公钥，已知 d 和φ(n)，根据$(de) \bmod \varphi(n) = 1$计算$d$.

Q：若$7d \bmod 20 = 1$,求d.

A：由于$7d \bmod 20 = 1$，则$7d = 20k + 1(k \in Z^+)$

$$7d = 21k + 1 - k(k \in Z^+), \text{则} d = 3k + \frac{1-k}{7}(k \in Z^+)$$

而$d \in Z^+$,则$\frac{1-k}{7} \in Z(k > 0)$,$k$可取1,则$d = 3$.

当然,k的解不唯一,通解为$k = 1 - 7t(t = 0,-1,-2,-3....)$

当时以上思路并不具有一般性，还得具体情况具体分析，如果能一下看出来，那就不用想那么复杂了，比如已知$7d = 24k + 1$，则应该化简成$d = 3k + 1 + \frac{3(k-2)}{7}$,则

$k = 7t + 2(t = 0,1,2....)$

二、 D-H 协议的计算

基本原理：基于求解离散对数问题的困难性

- 选择参数：参与方约定并公开两个大素数 P 和 G，其中 P 是素数，G 是模 P 的一个原根。
- 密钥生成：Alice 选择一个私密数 a 作为私钥，并计算 $A = G^a \bmod P$；

  Bob 选择一个私密数 b 作为私钥，并计算 $B = G^b \bmod P$。
- 交换信息：Alice 发送 A 给 Bob，Bob 发送 B 给 Alice。
- 计算共享密钥：Alice 计算 $S_1 = B^a \bmod P$，Bob 计算 $S_2 = A^b \bmod P$，共享密钥

$S = S_1 = S_2$

☆练习 1

已知$P = 71, G = 7, A$的私钥为$X_A = 5, B$的私钥$X_B = 12$.

求A、B的公钥以及共享密钥.

参考答案：$Y_A = 51, Y_B = 4, S = 43$

☆练习 2

已知 $P = 11, G = 2, A$的公钥为$Y_A = 9, B$的公钥为$Y_B = 3$

(1) 证明：2 是 11 的本原根.**(扩展)**
(2) 求 A 和 B 的私钥以及共享密钥 S.

解答：(1) 证明：已知 $P = 2,$ 则 $\varphi(P) = (P-1)(G-1) = 10$，只要证明 $G^{\varphi(P)} = 1(\mathrm{mod}\, P)$ 即可.则 $2^{10} \bmod 11 = 1024 \bmod 11 = 1$，得证

(2)解答：

三、 替换密码

1. 单表替换密码

1.1 凯撒密码：相对于原文字母移动 3 位
1.2 广义凯撒密码：相对于原文字母移动 K 位.

☆练习 1

解决密钥分配问题的一个办法是使用收发双方都有的一本书中某行文字。至少在某些侦探小说中经常把一本书的第一句话作为密钥。

给定下列消息：

SIDKHKDMAF HCRKIABIE SHIMC KD LFEAILA

这段密文是用《沉默的背后》(The Other Side Silence)一书的第一句话和单表代替方法产生的，使用的是简单的代替密码，这句话是

The snow lay thick on the steps and the snowflakes driven by the wind looked black in the headlights of the cars.

(1) 根据以上密文和密钥求原文消息。
(2) 为了使密钥分配问题简单化，通信双方都同意使用一本书的第一句话或最后一句话作为密钥。要想改变密钥，他们只需更换一本书就行了。使用第一句话比使用最后一句话要好，为什么?

(1) 根据单表代换原理，可得代换表：

原文	a	b	c	d	e	f	g	h	i	j	k	l	m
代换	I	S	L	O	C	P	T	B	K		M	H	
原文	n	o	p	q	r	s	t	u	v	w	x	y	z
代换	E	F	N		Q	D	A		R		G	J	

原文：basilisk to leviathan is contact

(2) 使用最后一句作为密钥可能无法包含 26 个英文字母，如果使用第一句话无法包括所有字母时，可用第二句或随后的句子找出剩余的字母。

2. 多表替换密码-维吉尼亚密码

2.1 凯撒密码：相对于原文字母移动 3 位

2.2 广义凯撒密码：相对于原文字母移动 K 位.

☆练习 2

用维吉尼亚密码加密单词“cybersecurity”，密钥为“course”。

★ Tips：把每个英文字母的序号给列出来：

A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8	J 9
K 10	L 11	M 12	N 13	O 14	P 15	Q 16	R 17	S 18	T 19
U 20	V 21	W 22	X 23	Y 24	Z 25				

解答：

☆练习 3

采用维吉尼亚密码一次一密版本的用途。该方案中，密钥是位于 0～26 的随机数字。例如，如果密钥时 3 19 5，则明文的第一个字母使用 3 个字母的移位加密，第二个字母使用 19 个字母的移位加密，第三个字母使用 5 个字母的移位加密，以此类推。

(1) 使用密钥流 9 1 7 23 15 21 14 11 11 2 8 9 加密明文 sendmoremoney.

(2) 使用(1)中产生的密文找到一个密钥，以便该密文解密为 cashnotneeded.

参考答案：

(1) 密文为：beokjdmcxzpmh

(2) 密钥为：25 4 22 3 22 15 19 15 19 21 12 8 4

3. 多表替换密码-普莱费尔密码

☆练习 4

已知密钥为 occurrence，使用普莱费尔密码加密以下消息：

Must see you over Cadogan West.Coming at once

参考答案：

1. 明文分组：mu,st,se,ey,ou,ov,er,ca,do,ga,nw,es,tc,om,in,ga,to,nc,ex(X 为补位)

2. 构造矩阵：

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

3. 密文:

☆练习 5

已知密钥为 Tuesday，使用普莱费尔密码加密消息 M 得到如下密文：

FBIBXTSBTVGECV

求消息 M.

四、 置换密码

1. 栅格置换：自己设计一个栅格置换密码，对 This is cybersecurity exam 进行加密.

2. 使用列数为 3 的矩形换位，将明文消息 M 按从上往下、从左往右的顺序写入矩阵进行加密得到密文：taseaoytsydiud，求明文 M.

五、 DES 计算

1. 利用 DES 算法和全 0 密钥对输入 10000001 19600000 进行一圈加密的结果
参考答案：196000000 8cd89aaf

2. 假设密文和密钥的各位全为 1，计算 DES 解密时第一轮输出中的 1 位，16，33，48 位.

3. 假设明文和密文拥有相同的位模式：
十六进制：0 1 2 3 4 5 6 7 8 9 A B C D E F
二进制： 0000 0001 0010 0011 0100 0101 0110 0111
1000 1001 1010 1011 1100 1101 1110 1111

(1) 推导第一轮的子密钥 K_1

PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

(2) 推导 L_0，R_0

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(3) 扩展 R_0 得到 $E(R_0)$

E

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

(4) 计算 $A = E[R_0] \oplus K_1$

(5) 讲(4)中的 48 位结果分成 6 位数据一组得集合并求对应 S 盒代替的值

S₁

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

S₂

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

S₃

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

S₄

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

S_5

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

S_6

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

S_7

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

S_8

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

(6) 讲(5)中的结果连接起来获得一个 32 位的结果 B

(7) 应用置换获取 $P(B)$

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) 计算 $R_1 = P(B) \oplus L_0$

(9) 写出密文

六、 其余一些题目

1. 设实数域上的椭圆曲线为 $y^2 = x^3 - 36x$，令 $P = (3,9)$，$Q = (-2,8)$，计算 $P + Q$ 和 $2P$.

参考答案： $P + Q = (6,0)$， $2P = (6.25, -4.375)$，过程见 PPT29 页

2. 有两颗形状、大小完全一样的球：一颗红球、一颗绿球，X 是红绿色盲，Y 能够向 X 证明这两颗球是一红一绿吗？【零知识证明】

参考解答：

- X 左手拿着红球，右手拿着绿球，并在背后不让 Y 看到，进行交换(或者不交换)两只球；
- Y 能够根据颜色精准判断 X 是否进行了交换；
- 执行上述操作 N 次后，Y 都能精确判断，即能在 X 是色盲的情况下，Y 仍能够向 X 证明能这两颗球是一红一绿。

第二部分 简答题

一、密码学基础

1. 单表代换和多表代换密码的区别和各自的优缺点。
2. 为什么说一次一密具有理论上的安全性，以及在实际应用中存在什么问题。
3. 密码体制从原理上可以分为哪两大类，具体比较这两类密码体制的特点。
4. 简述数字签名和消息认证的区别。
5. 简述数字签名的五大特性
6. 什么是“扩散”，什么是“混淆”以及各自的实现方式。
7. **简述五种安全的作用点。**

• 实体安全

作用点：对计算机网络与计算机系统的物理装备的威胁，主要表现在自然灾害、电磁辐射与恶劣工作环境方面。

外显行为：通信干扰，危害信息注入，信号辐射，信号替换，恶劣操作环境。

防范措施：抗干扰系统，防辐射系统，隐身系统，加固系统，数据备份。

- **网络安全**

作用点：对计算机网络与计算机系统可用性与可控性进行攻击。

外显行为：网络被阻塞，黑客行为，非法使用资源等，计算机病毒，使得依赖于信息系统的管理或控制体系陷于瘫痪。

防范措施： 防止入侵，检测入侵，攻击反应，系统恢复。

- **系统安全**

作用点：对各种系统的使用进行的攻击威胁，主要表现在操作系统、数据库、Web 系统、电子商务等应用系统等的攻击威胁。

外显行为：冒充合法用户，篡改密码，信息抵赖。

防范措施：加密身份认证技术，系统加固技术，安全交易协议。

- **数据安全（信息安全）**

作用点：对所处理的信息机密性与完整性的威胁，主要体现在加解密、防篡改、数字产品产权等方面。

外显行为：窃取信息，篡改信息，冒充信息，信息抵赖。

防范措施：加解密，完整性技术，数字签名，数字水印。

- **内容安全**

作用点：有害信息的传播对我国的政治制度及传统文化的威胁，垃圾信息对人们日常生活的干扰。

外显行为：淫秽暴力信息泛滥、敌对的意识形态信息涌入、英语文化的“泛洪现象 ”

对民族文化的冲击，垃圾信息泛滥。

防范措施：监测、控管、信息过滤、隐私保护，法律法规

8. 什么是机密性、认证性、完整性和不可抵赖性，分别阐述。

保密性是指确保信息资源仅被合法的实体（如用户、进程等）访问，使信息不泄漏给未授权的实体。

这里所指的信息不但包括国家秘密，而且包括各种社会团体、企业组织的工作秘密及商业秘密，个人的秘密和个人隐私（如浏览习惯、购物习惯等）。保密性还包括保护数据的存在性，有时候存在性比数据本身更能暴露信息。实现保密性的方法一般是通过对信息加密，或是对信息划分密级并为访问者分配访问权限，系统根据用户的身份权限控制对不同密级信息的访问。

完整性是指信息资源只能由授权方或以授权的方式修改，在存储或传输过程中不被偶然或蓄意地修改、伪造等破坏。

不仅仅要考虑数据的完整性，还要考虑操作系统的逻辑正确性和可靠性，要实现保护机制的硬件和软件的逻辑完备性、数据结构和存储的一致性。实现完整性的方法一般分为预防和检测两种机制。

不可抵赖性通常又称为不可否认性，是指信息的发送者无法否认已发出的信息或信息的部分内容。信息的接收者无 法否认已经接收的信息或信息的部分内容。实现不可抵赖性的措施主要有：数字签名、可信第三方认证技术等。

可认证性是指，保证信息使用者和信息服务者都是真实声称者，防止冒充和重演的攻击。

二、信息隐藏

9. 简述信息隐藏和信息加密的区别，以及举例各自的实现方式有哪些。
10. 简述数字水印的嵌入过程和数字水印的特性。

三、安全漏洞

11. 简述网络安全扫描的过程以及各个过程通常采用的技术。
12. 简述 IP 源地址欺骗的步骤及防范措施。
13. 简述网络监听的防范措施。
14. 简述拒绝服务攻击的原理和防范措施。
15. 简述缓冲区溢出攻击的原理和直接防范措施。
16. 简述 SQL 注入攻击的一般步骤。
17. 简述计算机病毒的特性和常见的检测方法。

四、防火墙

18. 常见的防火墙的性能指标有哪些。
19. 简述包过滤技术的原理和局限性。
20. 简述防火墙的体系结构类型和各自的组成部分。
21. 简述入侵检测的需求特性。
22. 描述 CIDF 模型的组成部分。
23. 比较 NIDS 和 HIDS。

24. 简述误用检测和异常检测的区别。

五、安全体系

25. 比较 L2TP 和 PPTP 协议。
26. 描述 IPSec 安全协议建立的五个阶段。
27. 简述代理协议 sockets 的工作过程。
28. 简述 PGP 鉴别/保密服务的实现过程。
29. TCSEC 计算机安全系统分为几大安全等级。
30. ITSEC 安全保障分为几大等级。
31. 描述 ISMS 的实施过程。
32. ISO 27000 标准体系包含哪些内容。
33. 等级保护 2.0 分为哪几级。
34. 等级保护 2.0 的等保流程是什么。
35. 等级保护 2.0 的定级对象包括哪些。
36. 写出本学期网络空间安全概论的上课老师全名及本学期做过的四次实验。

01 加密解密算法　第五周周六晚
02 信息隐藏实验　第七周周六晚
03 拒绝服务攻击与防御仿真实验　第九周周六晚
04 SQL 注入实验　第 11 周周六晚
上课时间：周一、周三

第三部分 综合题

1. 假如你是单位WEB服务器管理员，试述你会采取哪些主要措施来保障WEB服务器安全。

（1） 访问控制（IP 地址限制、Windows 帐户、请求资源的 Web 权限、资源的 NTFS 权限）；
（2） 用虚拟目录隐藏真实的网站结构；
（3） 设置基于 SSL 的加密和证书服务，以保证传输安全；
（4） 完善定期审核机制；
（5） 安装防火墙及杀毒软件；
（6） 及时安装操作系统补丁，减少操作系统漏洞等等。

2. 试编写一个简单的口令管理策略。

（1）所有活动账号都必须有口令保护。
（2）生成账号时，系统管理员应分配给合法用户一个唯一的口令，用户在第一次登录时应该更改口令。
（3）口令必须至少要含有 8 个字符。
（4）口令必须同时含有字母和非字母字符。
（5）必须定期用监控工具检查口令的强度和长度是否合格。
（6）口令不能和用户名或者登录名相同。
（7）口令必须至少 60 天更改一次。

3. 假如你是一个网络管理员，请说明你会采取哪些措施来构建网络安全体系，这些措施各有什么作用。

（1） 保证物理安全，将重要设备放入专门房间，保持良好环境，有专入制度。
（2） 在网关出口使用防火墙，如果对网络安全要求较高，可以使用状态检测型防火墙，如果对速度要求高可以使用硬件防火墙。
（3） 在防火墙后面使用入侵检测系统 IDS，与防火墙配合使用，以加强内网安全。
（4） 做好操作系统、数据库系统、应用软件及时升级维护打补丁，消除漏洞；
（5） 做好数据备份，保障数据安全；
（6） 使用正版杀毒软件并及时升级；
（7） 对外通信采用 IPSec 或 SSL 等安全协议和技术，保障通信安全；
（8） 为系统和用户设置安全口令及权限，做好访问控制，保障系统使用安全；
（9） 建立完善的安全管理制度、审计制度、建立应急响应机构和机制；
（10） 做好内部安全监管、安全培训等。

4. 试论述目前造成计算机网络不安全的原因是什么?可采取哪些相应的安全措施？

不安全原因 1.网络自身的特性 2.网络技术的开放 3．网络协议的漏洞 4. 通信系统和信息系统的自身缺陷 5.系统"后门"6.黑客及病毒等恶意程序的攻击。

措施:制定安全策略：如采用什么样的安全保障体系、确定网络资源职责划分、制定使用规则、制定日常维护规程、确定在遇到安全问题时采取的措施；采取加密、数字签名、访问控制、数据完整性、鉴别、业务填充、路由控制、可信第三方证书等机制。具体技术措施如：1）设置 IP 限制，屏蔽有威胁的 IP 地址 2）设置身份验证，确保只有合法用户才能访问授权范围内的资源 3）设置资源的 WEB 权限 4）设置文件或目录的 NTFS 权限 5）用虚拟目录隐藏真实的网站结构 6）设置基于 SSL 的加密和证书服务，保证传输安全 7）完善定期审核机制 8）安装防火墙软件 9）安装杀毒软件 10）及时安装操作系统补丁，减少操作系统漏洞.

5. 分析讨论信息系统所面临的安全威胁（至少 5 种）。

（1） 软硬件故障：由于设备硬件故障、通信链接中断、信息系统或软件 Bug 导致对业务、高效稳定运行的影响。

（2） 物理环境威胁：断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境条件和自然灾害。

（3） 无作为或操作失误：由于应该执行而没有执行相应的操作，或无意的执行了错误的操作，对系统造成影响。

（4） 管理不到位：安全管理无法落实，不到位，造成安全管理不规范，或者管理混乱，从而破坏信息系统正常有序运行。

（5） 恶意代码和病毒：具有自我复制、自我传播能力，对信息系统构成破坏的程序代码。

（6） 越权或滥用：通过采用一些，超越自己的权限访问了本来无权访问的资源；或者滥用自己的职权，做出破坏信息系统的行为。

（7） 黑客攻击技术：利用黑客工具和技术，例如，侦察、密码猜测攻击、缓冲区溢出攻击、安装后门、嗅探、伪造和欺骗、拒绝服务攻击等手段对信息系统进行攻击和入侵。

（8） 物理攻击：物理接触、物理破坏、盗窃

6. 请利用加密技术设计一套机制，用于实现商品的真伪查询。

系统产生一随机数并存储此数，然后对其加密，再将密文贴在商品上。当客户购买到此件商品并拨打电话查询时，系统将客户输入的编码(即密文)解密，并将所得的明文与存储在系统中的明文比较，若匹配则提示客户商品是真货，并从系统中删了此明文；若不匹配则提示客户商品是假货。

7. 请利用认证技术设计一套机制，用于防止电脑彩票伪造问题。

首先，系统给彩票编好码，习惯称之为条形码；然后，将条形码通过 Hash 运算，得到相应的消息摘要；接着，对消息摘要进行加密，得到相应密文；最后，系统将条形码与密文绑定在一起并存储，若需要查询时只要查看条形码与密文是否相关联即可。这样，即可实现电脑彩票防伪，因为伪造者是无法伪造密文的。

8. 请说明数字签名的主要流程。

(1) 采用 Hash 算法对原始报文进行运算，得到一个固定长度的消息摘要(Message Digest)，消息摘要具有单向性、散列性和无碰撞性。

(2) 发送方用目己的私有密钥对摘要进行加密来形成数字签名。

(3) 这个数字签名将作为报文的附件和报文一起发送给接收方。

(4) 接收方首先对接收到的原始报文用同样的算法计算出新的报文摘要，再用发送方的公开密钥对报文附件的数字签名进行解密，比较两个报文摘要，如果值相同，接收方就能确认该数字签名是发送方的，否则就认为收到的报文是伪造的或者中途被篡改。

9. 用户 A 需要通过计算机网络安全地将一份的机密文件传送给用户 B，B 希望 A 今后对该份机密文件无法抵赖，请问如何实现。

假定通信双方分别为 Alice 和 Bob，（1）双方选用一个公开密钥密码系统；（2）双方把自己的公开密钥通过 PKI 证书传送给对方；（3）加密方 Alice 将用自己的私钥加密文件，再用 Bob 的公钥加密文件，然后发送给 Bob；（4）解密方 Bob 收到后用自己的私钥解密，再用 Alice 的公钥解密，就可以得到原机密文件。

10. 简述公钥密码体制的基本思想。

答：①公钥密码体制的基本思想是把密钥分成两个部分：公开密钥和私有密钥（简称公钥和私钥），公钥可以向外公布，私钥则是保密的；密钥中的任何一个可以用来加密，另一个可以用来解密；公钥和私钥必须配对使用，否则不能打开加密文件；已知密码算法和密钥中的一个，求解另一个在计算上是不可行的。②相对于传统密码体制来说，公钥密码体制中的公钥可被记录在一个公共数据库里或以某种可信的方式公开发放，而私有密钥由持有者妥善地秘密保存。这样，任何人都可以通过某种公开的途径获得一个用户的公开密要，然后进行保密通信，而解密者只能是知道私钥的密钥持有者，该体制简化了密钥的分配与分发；同时因为公钥密码体制密钥的非对称性以及私钥只能由持有者一个人私人持有的特性，使得公钥密码体制不仅能像传统密码体制那样用于消息加密，实现秘密通信，还可以广泛应用于数字签名、认证等领域。

11. 高级持续性威胁 APT 攻击案例分析：

①对谷歌等公司的激光攻击事件。

②对伊朗核设施的攻击事件。

③对韩国农协银行的攻击事件。

12. 包过滤技术的局限

•定义包过滤路由器，可能是一项复杂的工作。因为网络管理员需要详细地了解 Internet（因特网）的各种服务、包头格式以及希望在每个域查找的特定的值。

•路由器信息包的吞吐量，随包过滤路由器数量的增加而减少。

•不能彻底防止地址欺骗。大多数包过滤路由器都是基于“源 IP 地址、目的 IP 地址”进行过滤的，而 IP 地址的伪造，是很容易、很普遍的。

•一些应用协议不适合于数据包过滤。即使是完美的数据包过滤，也会发现一些协议并不适合于经由数据包过滤安全保护。如 RPC（远程过程调用）、X- Window 和 FTP（文件传输协议）。

•正常的过滤路由器无法执行某些安全策略。例如，数据包说它们来自什么主机，而不是什么用户，因此，我们不能强行限制特殊的用户。

•一些包过滤路由器不提供任何日志能力，直到闯入发生后，危险的封包才可能检测出来。

13. 军事作战中，A 需要通过计算机网络给 B 发送大量资料，A 应该如何和 B 进行安全的信息传送，请说明具体步骤

• 数据加密：使用强加密算法（例如 AES）对资料进行加密。这确保即使数据被截获，也无法被未经授权的人读取。

• 建立安全通道：利用安全协议（如 SSL 或 TLS）建立安全的通信通道。这种通道保护数据在传输过程中免受窃听或篡改。

• 强制访问控制：实施强制访问控制模型，为数据设定明确的访问权限，确保只有授权的用户才能够访问和接收数据。

• 数字签名：对数据进行数字签名以验证数据的完整性和来源。这确保接收方能够确认数据未被篡改，并验证发送方的身份。

• 物理安全措施：除了网络安全措施外，确保在物理上保护计算机设备和网络设施，防止未经授权的人员接触到这些设备。

• 分段传输与重组：将大量资料分割成小块，并通过安全通道单独传输，最后在接收端重组。这有助于降低传输过程中的风险。

• 实时监控和审计：在传输过程中实时监控数据流，记录访问记录和操作路径，及时发现异常行为或攻击。
• 安全性审查和更新：定期对安全措施进行审查和更新，确保与最新威胁和需求保持同步，及时调整和改进安全措施。

14. 一家公司，只使用了防火墙安全技术，请说服主管外加一个入侵检测技术。

当谈到网络安全时，防火墙是保护系统免受未经授权访问的重要工具，但它并不能完全保证网络免受所有威胁。加入入侵检测技术可以提供额外的安全层面，让我为您列举几点：
• **实时威胁检测：**入侵检测系统能够监控网络流量和系统活动，及时发现异常行为或潜在攻击，迅速做出反应。这种实时检测可以大大降低潜在攻击造成的损害。
• **综合防御：**单独依赖防火墙可能无法完全拦截所有攻击。入侵检测技术可以通过分析多种数据源，识别新型威胁和攻击模式，提供更全面的安全保护。
• **合规性要求：**许多行业和法规要求公司采取特定的安全措施来保护数据和网络。入侵检测技术常常是符合这些合规性要求的重要手段之一。
• **攻击后分析：**如果出现了安全漏洞或者遭受攻击，入侵检测系统可以帮助公司进行事后分析，找出攻击源头和漏洞，从而改善安全策略，避免未来类似事件的发生。
• **增强安全意识：**引入入侵检测技术可以提高公司对安全威胁的认识和了解，促进员工更积极地参与安全培训和实践，从而加强整体安全文化。
• 将入侵检测技术与防火墙结合使用可以建立更强大的安全防线，提高对抗各种安全威胁的能力，确保公司网络和数据的安全。

15. 举 3 个例，说明在日常社交网络平台中容易出现的信息安全问题，并给予改进建议。
• **个人隐私泄露：**

问题：用户可能过度分享个人信息，如生日、地址、电话号码等，导致隐私泄露。

建议：用户应该谨慎分享个人信息，并定期审查和更新隐私设置，限制谁可以看到自己的信息。
• **恶意链接和欺诈活动：**

问题：用户可能受到欺诈性链接或信息欺诈的威胁，如虚假广告、诱导点击等。

建议：警惕点击不明链接，安装反欺诈软件，对于可疑信息保持警惕，并报告可疑行为给平台。
• **账号被盗：**

问题：弱密码或不安全的登录方式可能导致账号被盗。

建议：使用强密码并定期更换，启用两步验证，避免使用相同的密码在多个平台上，定期审查登录活动。
• **虚假信息和网络欺凌：**

问题：虚假信息、恶意评论、网络欺凌等可能伤害用户感情和声誉。

建议：确保对社交平台上的信息进行验证和审查，避免敏感话题，及时举报和屏蔽恶意行为。
• **数据隐私问题：**

问题：平台可能收集和分享用户的个人数据，存在隐私泄露风险。

建议：定期审查隐私政策，了解平台对数据的使用和分享方式，控制个人数据的共享范围。

16. 企业内部员工在公司网络上访问敏感数据时，可能存在哪些安全风险？列举并提出相应的安全措施和建议

- 未授权访问：员工可能在未经授权的情况下访问敏感数据，例如使用其他员工的凭证或绕过权限。
- 安全措施：实施强制访问控制（MAC）和基于角色的访问控制（RBAC），限制员工仅能访问其职责所需的数据；启用身份验证和严格的账户管理。
- 数据泄露：员工可能意外或故意泄露敏感信息，例如将数据发送到错误的收件人或通过不安全的通信渠道传输数据。
- 安全措施：加强员工的安全意识培训，教育他们识别敏感信息并正确处理；实施数据分类和加密，限制敏感信息的传输方式。
- 内部威胁：内部员工可能有恶意行为，例如窃取数据、篡改信息或故意破坏系统。
- 安全措施：实施行为监控和异常检测系统，定期审计员工访问记录；建立内部报告机制，让员工能够匿名举报可疑行为。
- 弱密码和凭证共享：使用弱密码或共享凭证可能导致未经授权的访问。
- 安全措施：强制员工使用复杂密码，并定期更改；启用多因素身份验证（MFA）以增强账户安全性。
- 社会工程攻击：员工可能成为社会工程攻击的目标，被诱骗提供凭证或敏感信息。
- 安全措施：提高员工的安全意识，教育他们如何识别和应对社会工程攻击；建立流程，确保敏感信息只在特定安全环境中共享。

17. 一个政府部门需要将机密文件传输给另一个部门，如何确保文件在传输过程中的安全性？详细描述具体步骤和技术手段。

- 加密文件：使用强加密算法（如 AES）对机密文件进行加密。确保只有授权人员能够解密文件。
- 建立安全通道：使用安全协议（如 SSL/TLS）建立加密的安全通道，保护数据在传输过程中的隐私和完整性。
- 使用安全传输协议：选择安全的文件传输协议，如 SFTP（Secure File Transfer Protocol）或 FTPS（FTP over SSL/TLS），以确保数据在传输时受到保护。
- 数字签名验证：对机密文件进行数字签名，并确保接收方可以验证文件的完整性和来源。
- 访问控制和权限设置：设定适当的访问控制和权限，确保只有授权人员能够访问和下载这些文件。
- 分割和加密传输：将大文件分割成小块，然后分别加密和传输，减少单个文件传输的风险，同时增加数据安全性。
- 双因素身份验证：在文件传输的过程中，要求双方进行身份验证，使用多因素身份验证（如用户名密码配合短信验证码或硬件令牌）确保身份的真实性。
- 实时监控和审计：在传输过程中实时监控数据流，记录传输活动和访问日志，及时发现异常行为。
- 端到端的安全性：确保整个传输链路的每个环节都是安全可信的，从发送方到接收方，每个环节都需要严格控制和保护。
- 定期审查和更新：定期审查安全策略和技术措施，确保与最新的安全标准和威胁情报保持一致，并不断优化安全性。

18. 一家银行的 ATM 系统可能面临哪些安全挑战？提出解决方案以保护 ATM 系统免受潜在威胁。

• **卡片复制和欺诈：**黑客可能尝试复制银行卡信息，制作伪造卡片，并通过 ATM 系统进行欺诈性取款。

解决方案：使用 EMV 芯片技术替代磁条卡，采用动态加密和验证，增强卡片的安全性；实施欺诈检测系统，监控异常取款行为。

• 恶意软件攻击：针对 ATM 系统的恶意软件可能导致信息窃取、卡号盗取或恶意控制 ATM 机。

解决方案：定期更新 ATM 系统软件和操作系统，安装最新的安全补丁；使用防病毒软件和行为检测系统进行实时监控和防御。

• **物理攻击和钓鱼：**黑客可能尝试物理攻击 ATM 机，例如使用假面板或钓鱼设备窃取卡片信息或窃取现金。

解决方案：安装物理安全设备，如监控摄像头和钞箱破坏检测器；对 ATM 机进行定期巡检和维护，防止物理攻击。

• **网络攻击和数据泄露：**针对 ATM 系统的网络攻击可能导致数据泄露和服务中断。

解决方案：建立强固的防火墙和入侵检测系统，实施网络分段和加密通信，保护 ATM 系统免受网络攻击。

• 未经授权的访问和内部威胁：内部员工或授权者可能滥用权限，窃取客户信息或篡改 ATM 系统。

解决方案： 实施严格的访问控制和权限管理，定期审计员工访问记录，确保仅授权人员能够访问敏感数据。

19. 一家跨国公司在不同地区有分支机构，如何确保公司内部通信的安全性和保密性？列出解决方案。

• 加密通信：使用端到端加密的通信工具，如加密邮件服务、安全即时通讯应用程序或 VPN（虚拟专用网络），确保通信内容在传输过程中得到加密。

• 严格的访问控制：建立基于角色的访问控制，限制员工只能访问其需要的信息和资源，确保敏感信息仅对有权访问者可见。

• 使用安全的通信协议：鼓励或强制使用安全的通信协议，如 TLS/SSL，确保数据在传输时得到保护。

• 安全培训和意识提升：为员工提供安全意识培训，教育他们识别和应对网络钓鱼、恶意软件等安全威胁，确保他们在通信中遵循最佳安全实践。

• 加强设备和网络安全：在各分支机构部署防火墙、入侵检测系统和反病毒软件，确保网络和设备安全；同时定期进行安全审计和漏洞扫描。

• 加密存储和备份：对敏感数据进行加密存储，并定期备份数据，以防止数据丢失或泄露。

• 多重身份验证：强制启用多因素身份验证（MFA）来保护账户安全，确保只有授权人员可以访问敏感信息。

• 严格审查和监控：对公司内部通信进行严格的监控和审计，记录访问和通信日志，及时发现异常行为和潜在的安全风险。

• 合规性和法律规定：遵守各地区的合规性要求和隐私法律规定，确保公司内部通信符合当地法律法规。

• 安全文化建设：建立和促进安全文化，使员工意识到安全是每个人的责任，并鼓励报告安全漏洞和问题。

20. 一所学校的学生使用公共 Wi-Fi 上网，可能遇到的安全风险是什么？给予学生使用公共 Wi-Fi 时的安全建议。

安全风险：

• 窃听和数据泄露：公共 Wi-Fi 网络可能存在安全漏洞，黑客可以窃听数据流量，导致个人信息泄露。

• 恶意热点：黑客可能设立假的 Wi-Fi 热点，冒充公共网络，吸引用户连接并窃取信息。

• 恶意软件攻击：学生可能受到恶意软件的攻击，如间谍软件或恶意代码，导致设备感染病毒或个人信息泄露。

安全建议：

• 使用加密网络：尽量连接加密的 Wi-Fi 网络，如 WPA2/WPA3 加密，以确保数据在传输时被加密。

• 使用 VPN：使用虚拟专用网络（VPN），它可以加密网络流量，增强数据安全性，并避免窃听。

• 更新设备和应用：确保设备和应用程序都是最新版本，以修复已知漏洞，并避免被利用

• 禁用自动连接：禁用设备上的自动连接功能，避免随意连接未知的 Wi-Fi 网络。

• 启用防火墙：启用设备上的防火墙功能，增加对不明来源的连接的阻挡。

• 谨慎访问敏感网站和输入个人信息：避免在公共 Wi-Fi 上访问银行账户、输入密码或其他敏感个人信息。

• 使用 HTTPS 网站：尽可能访问使用 HTTPS 加密的网站，这些网站提供更高级别的安全性。

• 退出网络后及时断开连接：在使用完毕后及时断开连接，避免长时间保持连接公共 Wi-Fi

• 开启设备锁定功能：开启设备锁定功能（PIN 码、指纹或面部识别），以保护设备在连接过程中的安全。

21. 一个小型初创企业没有专门的安全团队，如何建立基本的安全基础设施？列出切实可行的安全措施和建议。

• 安全培训和意识提升：为员工提供基本的安全意识培训，教育他们识别和应对常见的网络威胁和风险。

• 设备安全和更新：定期更新所有设备的操作系统和应用程序，确保设备安全漏洞得到修复

• 强化账户安全：强制使用强密码，并定期更改密码；启用双因素身份验证（MFA）以增强账户安全性。

• 备份和恢复：定期备份重要数据，并测试恢复流程，以防止数据丢失或损坏时的灾难。

• 网络安全基础设施：部署基本的网络安全措施，如防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）和安全网关，保护网络不受攻击。

• 安全更新和漏洞管理：定期检查和安装安全补丁，保持系统和应用程序处于最新状态，并实施漏洞管理策略。

• 访问控制和权限管理：确保对公司资源的访问控制，限制员工访问敏感信息的权限。

• 制定安全政策：制定适合公司规模的安全政策，包括使用政策、数据备份政策、密码政策等，确保员工遵守最佳安全实践。

• 监控和日志记录：部署基本的监控系统，记录网络活动和安全事件，及时发现异常行为。

• 外部支持和咨询：考虑与安全服务提供商或专业咨询公司合作，获得安全建议和支持，填补安全团队的缺失。

Arranged By mzq　2024.06.16 23:50.