《信息安全原理与技术》试题与答案

一、写出下面术语的中文名称

Block Cipher　分组密码

Ciphertext　密文　（密码：**Cipher**）

Known-Plaintext Attack　已知明文攻击

Encryption　加密

Non-Repudiation　不可否认性

Key Distribution Center　秘钥分配中心

Denial of Service　拒绝服务

Data Integrity　数据完整性

AES　高级加密标准（**Advanced encryption Standards**）

Authorization　认证；授权

Relpay Attack　重放攻击

One-way Function　单向函数

Brute Force Search　穷举攻击

Stream Cipher　流密码

Symmetric Encryption　对称加密

Asymmetric Encryption　非对称密码体制

Ciphertext-only Attack　唯密文攻击

Known-Plaintext Attack　已知明文攻击

Chosen-Plaintext Attack　选择明文攻击

Man-in-the-Middle Attack　中间人攻击

Message Authentication Code　消息认证码

Hashed Message Authentication Code　散列消息认证码

Digital Signature　数字签名

Secure Socket Layer　安全套接字层（**SSL**）

二、选择题

1. 如果 m 表示明文，c 表示密文，E 代表加密变换，D 代表解密变换，则下列表达式中描述加密过程的是（　A　）

A、 c=E(m)　　B、 c=D(m)

C、 m=E(c)　　D、 m=D(c)

2. 将获得的信息再次发送以在非授权情况下进行传输，这属于　（　D　）

A 窃听　　B 篡改

C 伪装　　D 重放

3. DES 加密过程用以下形式交换，其中正确的是（　B　）

A、Li-1=Ri-1　Ri-1=Li-1⊕f(R i,Ki)　　i=1,2,3,……16

B、Li=Ri-1　　Ri=Li-1⊕f(Ri-1,Ki)　　i=1,2,3,……16

C、Li-1=Ri+1 Ri=Li+1⊕f(Ri-1,Ki) i=1,2,3,……16
D、Li-1=Ri-1 Ri=Li+1⊕f(Ri-1,Ki) i=0,1,2,3,……15
4. 在不知道密钥的情况下，通过获取密文而恢复明文的方法是。(C)
A、密钥管理 B、数据加密解密算法
C、密码分析 D、密码编码
5. RSA 属于（ B ）
A、传统密码体制 B、非对称密码体制
C、现代密码体制 D、对称密码体制
6.下面哪个加密算法被选为 AES(B)
A MARS B Rijndael
C Twofish D E2
7. DES 中子密钥的位数是 （ B ）
A、32 B、48 C、56 D、64
8. 如果使用两密钥的 Triple-DES，则下面正确的是（ A ）
A C = EK1[DK2[EK1[P]]] B C = EK1[EK2[EK1[P]]]
C C = EK3[DK2[EK1[P]]] D C = EK1[DK2[DK1[P]]]
9. DES 中如果 S 盒输入为 110011，则对应输入位置为（ B ）
A、第 2 行第 9 列 B、第 4 行第 10 列
C、第 3 行第 10 列 D、第 3 行第 11 列
10 每次加密一位或者一个字节是 （ B ）
A、离散密码 B、流密码
C、随机密码 D、分组密码
11. 在下列密码体制中，加密密钥 k1 解密密钥 k2 是相同的。(A)
A、传统密码体制 B、非对称密码体制
C、现代密码体制 D、公开密码体制
12. DES 用多少位密钥加密 64 位明文（ C ）
A、16 B、32 C、56 D、64
13. 用公钥密码体制签名时，应该用什么加密消息 （ C ）
A、会话钥 B、公钥 C、私钥 D、共享钥
14. 防止发送方否认的方法是 （ D ）
A、消息认证 B、保密 C、日志 D、数字签名
15、一个数据包过滤系统被设计成允许你要求服务的数据包进入，而过滤掉不必要的服务。这属于（ A ）基本原则。
A、最小特权 B、阻塞点 C、失效保护状态 D、防御多样化
16、不属于安全策略所涉及的方面是（ D)。
A、物理安全策略 B、访问控制策略 C、信息加密策略 D、防火墙策略
17、(D ）协议主要用于加密机制
A、HTTP B、FTP C、TELNET D、SSL
18、不属于 WEB 服务器的安全措施的是（ B ）
A、保证注册帐户的时效性
B、删除死帐户
C、强制用户使用不易被破解的密码
D、所有用户使用一次性密码
19、为了防御网络监听，最常用的方法是（ B ）

A、采用物理传输（非网络） B、信息加密 C、无线网 D、使用专线传输

20、使网络服务器中充斥着大量要求回复的信息，消耗带宽，导致网络或系统停止正常服务，这属于（ A ）漏洞

A、拒绝服务 B、文件共享 C、BIND 漏洞 D、远程过程调用

21、不属于计算机病毒防治的策略的是（ D ）

A、确认您手头常备一张真正“干净”的引导盘

B、及时、可靠升级反病毒产品

C、新购置的计算机软件也要进行病毒检测

D、整理磁盘

22、关于 RSA 算法下列说法不正确的是（ A ）

A、RSA 算法是一种对称加密算法。

B、RSA 算法的运算速度比 DES 慢。

C、RSA 算法可用于某种数字签名方案。

D、RSA 算法的安全性主要基于素因子分解的难度

23、下列属于非对称加密技术的是（ C ）

A、IDEA B、AES C、RSA D、DES

24、黑客在程序中设置了后门，这体现了黑客的（ A ）目的。

A、非法获取系统的访问权限 B、窃取信息

C、篡改数据 D、利用有关资源

25、软件驻留在用户计算机中，侦听目标计算机的操作，并可对目标计算机进行特定操作的黑客攻击手段是（ B ）

A、缓冲区溢出 B、木马 C、拒绝服务 D、暴力破解

26. 在防火墙技术中，内网这一概念通常指的是（ A ）

A. 受信网络 B. 非受信网络

C. 防火墙内的网络 D. 互联网

27. 信息安全技术的核心是（ A ）

A. PKI B. SET

C. SSL D. ECC

28. 通常为保证商务对象的认证性采用的手段是（ C ）

A. 信息加密和解密 B. 信息隐匿

C. 数字签名和身份认证技术 D. 数字水印

29. 关于 Diffie-Hellman 算法描述正确的是（ B ）

A. 它是一个安全的接入控制协议 B. 它是一个安全的密钥分配协议

C. 中间人看不到任何交换的信息 D. 它是由第三方来保证安全的

30. 以下哪一项不在证书数据的组成中？（ D ）

A. 版本信息 B. 有效使用期限

C. 签名算法 D. 版权信息

二、填空题：（每空 2 分，共 20 分）

1、计算机安全技术研究的内容包括**硬件实体安全、软件安全、数据安全、网络安全、病毒防治、防计算机犯罪**。

2、美国国防部发表的评估计算机系统安全等级，计算机安全等级划分为 4 类 8 级，由高到低依次是即 A2、A1、B3、B2、B1、C2、C1、D 级，其中 UNIX 系

统、XENIX、Novell、WindowsNT 属于 **C2 级**。在 A 级系统构成的部件来源必须有安全保证。我国计算机安全等级分五个等级从低到高依次是：**用户自主保护级、系统审计保护级、安全标记保护级、机构化保护级、访问验证保护级**。我国先后出台了一系列信息安全保护条例，如**《中华人民共和国计算机信息系统安全保护条例》**等。

3、常用的软件保护技术包括：**系列号方式、时间限制、NAG 窗口、KEYFile 保护、功能限制的程序、CD-check**。在进行软件的破解、解密工作中，一个首要的问题是对软件进行分析，常用的分析方法包括：**静态分析技术、动态分析技术**。

4、凯撒密码加密是将密文字母相对明文字母循环左移了三位，I will wait you at the zoo afternoon.用凯撒密码加密后 **l zloo zdlw arx dw wkh crr diwhvqrrq** 。

5、数字签名可保证数据的**机密性、完整性和不可抵赖性**。哈希函数可将任意长度的报文产生固定长度的比特串，其两个重要的特性是**混肴特性和抗碰撞特性**。

6、数据库中并发控制不当会造成数据的不一致，其并发控制是以事务为单位，通常使用**封锁技术**实现。

7、计算机病毒的众多特征中，**传染性、潜伏性、触发性和破坏性**是它的基本特征。计算机完整的工作过程包括以下几个环节：**传染源、传染介质、病毒触发、病毒表现、传染**。

8、病毒软件寄生在其它文件中，可以自我复制、可以感染其它文件，其目的是破坏文件和系统，可分为**引导型病毒、文件型病毒、混合型病毒**；黑客软件能寄生，**不可复制和感染文件**，黑客通过 **Email 或冒充可供下载的文件**被用户不经意下载运行。该用户的启动文件和注册表会被修改，黑客会通过网络找到它，盗取用户密码和监控系统。

9、网络安全的目标：**可靠性、可用性、保密性、完整性、不可抵赖性**。实现的安全服务有**鉴别服务、访问控制服务、数据机密性服务、数据完整性服务、抗抵赖服务**。常用的网络安全技术**数据加密技术、防火墙技术、网络安全扫描技术、网络入侵检测技术、黑客诱骗技术、无线局域网安全技术**；

10、防火墙是设置在不同网络或网络安全域之间的一系列部件的组合。它通过检测、限制、更改跨越防火墙的数据流，尽可能地对外部**屏蔽网络内部信息、结构和运行情况**，以此实现网络的保护。其对数据的处理方法大致分为两类：**包过滤防火墙和代理防火墙**。

11 攻击 UNIX 的方法有：（ **FTP 攻击** ）、（ **RPC 攻击** ）和用 **Sendmail** 攻击。

13、Web 服务器是驻留在服务器上的一个程序，它和用户浏览器之间使用（ **HTTP** ）进行相互通信。

14、根据检测方式来分类，入侵检测系统可分为（**异常检测**）和（**误用检测** ）

15、（**包过滤防火墙** ）是最简单的防火墙，只包括对源和目的 IP 地址及端口进行检查。

16、（ **扫描器** ）是自动检测远程或本地主机安全性漏洞的程序包。

17. MD-5 散列算法中输入消息可以任意长度，但要进行分组，其分组的位数是（ **512** ）

18. SHA 的含义是（ **安全散列算法** ）

19. 阻止非法用户进入系统使用（ **接入控制技术** ）

20. 以下不是数据库加密方法的是（ **信息隐藏** ）

三、计算题

1. 用流密码加密二进制数据 m=011001001 加密密钥为 k=110011001

（1）解密密钥是多少?

（2）密文为多少？

解：（1）流密码加密中加密解密密钥一样，故解密密钥为：110011001

（2）密文是密钥与明文的异或运算：101010000

2.使用 Playfair 密码的加密明文 good，密钥关键词是 monarchy，计算加密后的密文。

解：构成的密钥矩阵是：

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

将明文按照两个字母分组：

go od

密文是：

FN RH

3.设密钥字是 cipher, 使用维吉尼亚密码加密明文串是 this cryptosystem is not secure, 求密文

解：在明文下面重复写密钥字，组成密钥。

明文M： thiscryptosystemisnotsecure

密钥K： ciphercipherciphercipherciphercip

将明文和密钥转化为数字

M=(19,7,8,18,2,17,24,15,19,14,18,24,18,19,4,12,8,18,13,14,19,18,4,2,20,17,4)

K=(2,8,15,7,4,17,2,8,15,7,4,17,2,8,15,7,4,17,2,8,15,7,4,17,2,8,15)

对每个明文数字和对应的密钥数字，使用ci=(mi+ki)mod 26加密
得到密文数字为：
C=(21,15,23,25,6,8,0,23,8,21,22,15,21,1,19,19,12,9,15,22,8,25,8,19,22,25,19)
于是密文为：
VPXZGIAXIVWPUBTTMJPWIZITWZT

4.利用 RSA 算法运算，如果 p=11，q=13, e=103,对明文 3 进行加密.求 d 及密文

解：Φ（n）=（p-1）*(q-1)=10*12=120

e*d≡1 modΦ（n），而 e=103 故可解出 d=7

n=p*q=11*13=143

c= me mod n=3103 mod 143=16

5. 在 Diffice—Hellman 密钥管理方法，计算 A 和 B 双方共同的密钥。设 a=3，p=720，其中 A 的秘密信息为 X_a=6， B 的秘密信息 X_B=11。

解：

$Y_A=a^{XB}$ mod p = 3^{11} mod 720 = 9

$K_B = Y_A^{XB}$ mod p = 377

6.下面是 DES 的一个 S 盒，如果输入为 011001，求输出。

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

解：

输入六位数的第一位与最后一位组合所对应的十进制数确定行，剩余四位对应的十进制数确定列，因此确定输出数为 2 行 13 列交叉，对应十进制数为 1，因此输出为：0001.

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

解：n=p*q (p 和 q 都是素数)，n=35 故解出 p=5 ，q=7 ；

Φ（n）=（p-1）*(q-1)=24 ；

又因为 e*d≡1 modΦ（n），而 e=5 故可解出 d=5；

m= cd mod n=105 mod 35=5 。

8.在 Diffie-Hellman 方法中，公共素数 p = 11，本原根 α = 2

(1). 如果用户 A 的公钥 Y_A = 9，则 A 的私钥 X_A 为多少？

(2). 如果用户 B 的公钥 Y_B = 3，则共享密钥 K 为多少？

解：（1）$YA=a^{XA}$mod p,则 X_A=6；

（2）$K=Y_B^{XA}$mod p=36 mod 11=3。

8.用列置换加密明文 permutation cipher hide the message by rearranging the letter order。假如用密钥 network。

解：将明文按照密钥的长度一行一行地写成一个矩阵，然后按照密钥字母对应的数值从小到大，按照列读出即为密文

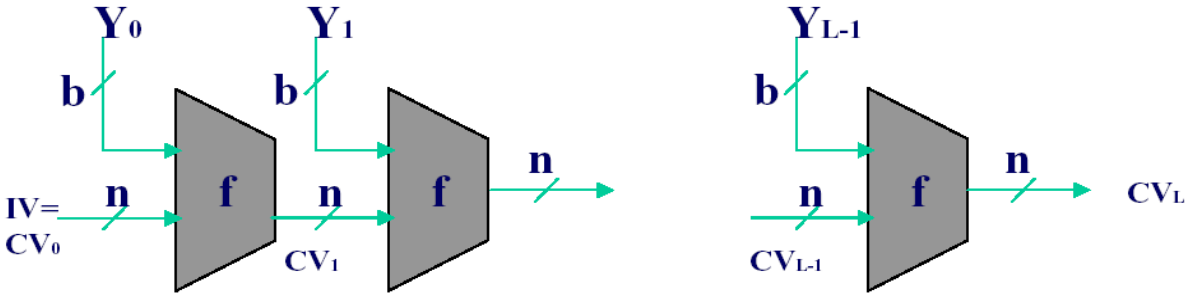
密钥	n	e	t	w	o	r	k
明文	p	e	r	m	u	t	a
	t	i	o	n	c	i	p
	h	e	r	h	i	d	e
	t	h	e	m	e	s	s
	a	g	e	b	y	r	e
	a	r	r	a	n	g	i
	n	g	t	h	e	l	e
	t	t	e	r	o	r	d
	e	r					

在密钥 network 中，字母对应的数字从小到大排列是 eknortw，按照这个顺序读出上面矩阵的列即是密文:

EIEHGRGTRAPESEIEDPTHTAANTEUCIEYNEOTIDSRGLRRROREERTE MNHMBAHR

四、分析题

1. 看下图回答问题



（1） 该图是什么结构图

（2） 如果该图表示 MD5，说明 Y 和 CV 的长度

（3） 图中哪个是输出的摘要值。

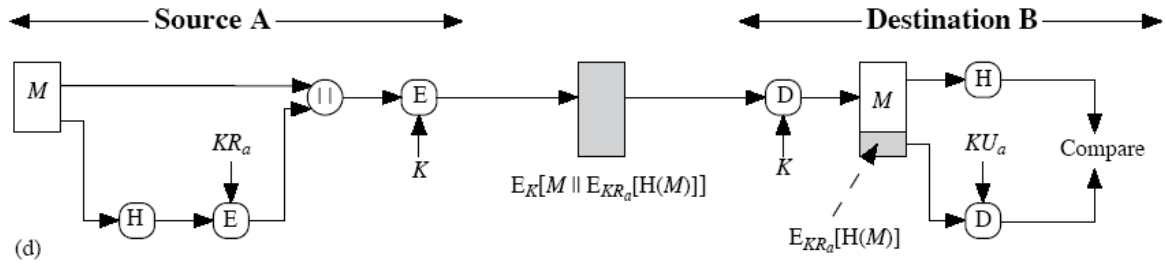
解:

（1）该图是迭代散列函数的一般结构图;

（2）Y 是 512 位，CV 是 128 位;

（3）CVL

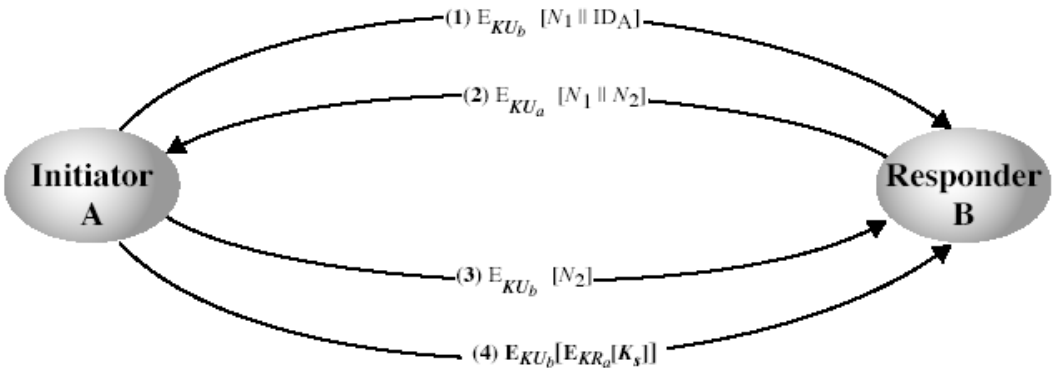
2. 如图是将 hash 码用于消息认证的一种方法，请回答下面的问题。



(1) 说出 KRa ， H(M) ， K 和 KUa 表示的意思。
(2) hash 码与 MAC 的区别是什么？
(3) 该方法具有什么功能？

解：(1)KR_a：A 的私钥　H(M)：散列值　K：共享密钥　KU_aA 的公钥
(2)Hash 函数不需要是用密钥，而 MAC 需要；
(3)提供安全服务的保密性与认证性；

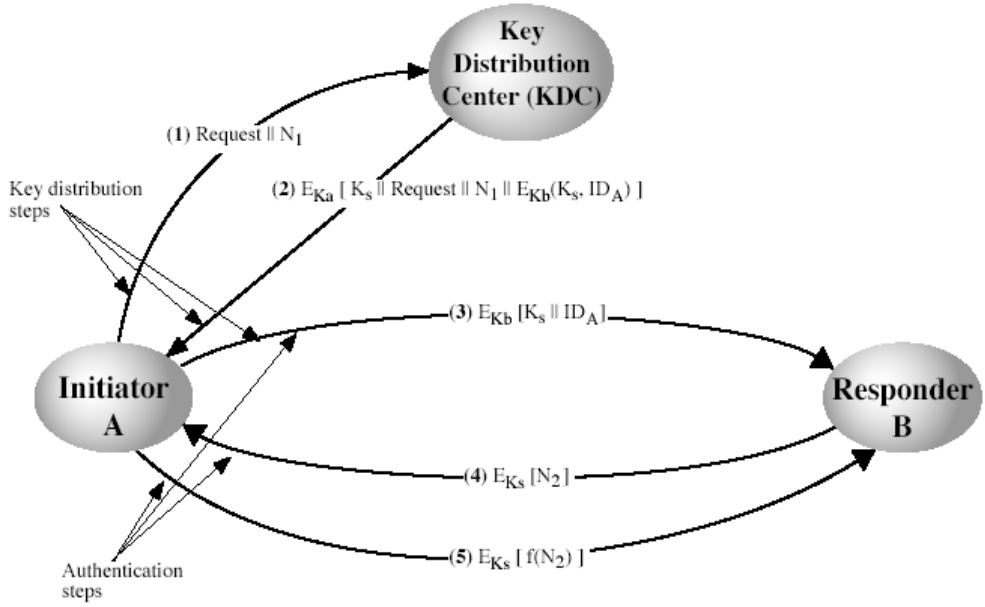
3 在下图中，A 和 B 互相知道对方的公钥，回答下面的问题：



(1) 该协议最终目的是想解决什么问题
(2) KUa, N，Ks 表示什么
(3) 协议的 1，2 步的目的是什么
(4) 协议的 2，3 步的目的是什么

解：
(1)使用公开加密算法分配对称密钥；
(2)KU_a：A 的公钥　N：临时交换号　K_s：会话密钥
(3)A 认证对方是否是 B；
(4)AB 双方相互认证身份；

下图是一个密钥分配协议



请回答下面问题：

(1) 说出 KDC，N， Ks ，Ka，Kb 的意思。

(2) Ks 由谁产生的？它的作用是什么？

(3) 步骤 4 和步骤 5 的主要目的是什么？

(4) 该协议存在潜在威胁，主要在哪个步骤？如何解决该问题？

解：

(1)KDC：密钥分配中心 N：临时交换号 K_s：临时会话密钥 K_a：A 拥有的与 KDC 共享的主密钥 K_b：B 拥有的与 KDC 共享的主密钥；

(2)K_s 是由密钥分配中心产生的；它的作用是对用户之间的通信进行保密，通信结束后 K_s 即刻被销毁；

(3)目的是使 B 相信第三步收到的消息不是一个重放，并且双方进行了认证，这是典型的挑战/应答认证方式；

(4)主要在步骤 5；解决该问题需要将 N_2 进行某种变换作为应答；

四、名词解释

1、防火墙

在计算机网络中，“防火墙”指一种将内部网和公众访问网分开的方法，实质是一门隔离技术。能增强内部网络的安全性。

2、拒绝服务

指一种常见的恶作剧的攻击方式，它使服务器忙于处理一些乱七八糟的任务，消耗大量的处理时间，以至于服务器无暇顾及用户的请求。

3、黑客

指利用通信软件，通过网络非法进入他人计算机系统，获取或篡改各种数据，危害信息安全的入侵者或入侵行为。

4、对称加密技术

在对称加密技术中加密和解密过程采用同一把密钥，通信时双方必须都具备这把密钥，并保证密钥不被泄露。

四、简答题：（每题 6 分共 24 分）

1、简述安全漏洞的类型：

答：（1）允许拒绝服务的漏洞。（2）允许有限权限的本地用户提高其权限的漏洞。（3）允许外来团体未经授权访问网络的漏洞。

2 简述代理防火墙和包过滤防火墙的优缺点？

答：包过滤防火墙工作在网络协议 IP 层，它只对 IP 包的源地址、目标地址及相应端口进行处理，因此速度比较快，能够处理的并发连接比较多，缺点是对应用层的攻击无能为力。

代理服务器防火墙将收到的 IP 包还原成高层协议的通讯数据，比如 http 连接信息，因此能够对基于高层协议的攻击进行拦截。缺点是处理速度比较慢，能够处理的并发数比较少。

代理服务器是防火墙技术的发展方向，众多厂商都在提高处理速度的同时基于代理开发防火墙的更高级防护功能。

3、如果你怀疑自己的计算机被黑客远程控制或被蠕虫感染，你计划采用哪些步骤检查自己的计算机？

答：断网、进程查看、网络端口查看、进程程序关联、自启动方式、查杀。

4、ARP 代表什么意思？有何用处？如何实施 ARP 欺骗？画出欺骗示意图，在图上标明欺骗步骤、各步骤的功能！

答：

(在每台装有 tcp/ip 协议的电脑里都有一个 ARP 缓存表，表里的 ip 地址与 mac 地址是一一对应的。 以主机 A（192.168.1.5）向主机 B（192.168.1.1）发送数据为例。当发送数据时，主机 A 会在自己的 ARP 缓存表中寻找是否有目标 IP 地址。如果找到了，也就知道了目标的 mac 地址，直接把目标的 mac 地址写入帧里面发送就可以了；如果在 ARP 缓存表里面没有目标的 IP 地址，主机 A 就会在网络上发送一个广播，目标 mac 地址是“ff-ff-ff-ff-ff-ff”，这表示向同一网段的所有主机发出这样的询问：“192.168.1.1 的 mac 地址是什么呀？”网络上的其他主机并不回应这一询问，只有主机 B 接受到这个帧时才向 A 作出回应：“192.168.1.1 的 mac 地址是 00-aa-0-62-c6-09。（如上表）”这样，主机 A 就知道了主机 B 的 mac 地址，就可以向主机 B 发送信息了。同时，它还更新了自己的 ARP 缓存表，下次再向 B 发送数据时，直接在 ARP 缓存表找就可以了。ARP 缓存表采用老化的机制，在一段时间里表中的某一行没有使用，就会被删除，这样可以大大减少 ARP 缓存表的长度，加快查询的速度。）

ARP 代表地址解析协议，用于完成 IP 地址和 MAC 地址的转换。

ARP 欺骗是黑客常用的攻击手段之一，ARP 欺骗分为二种，一种是对路由器 ARP 表的欺骗；另一种是对内网 PC 的网关欺骗。

第一种 ARP 欺骗的原理是——截获网关数据。它通知路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。第二种 ARP 欺骗的原理是——伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

（一般来说，ARP 欺骗攻击的后果非常严重，大多数情况下会造成大面积掉线。有些网管员对此不甚了解，出现故障时，认为 PC 没有问题，交换机没掉线的“本事”，电信也不承认宽带故障。而且如果第一种 ARP 欺骗发生时，只要重启路由器，网络就能全面恢复，那问题一定是在路由器了。为此，宽带路由器背了不少“黑锅”。）

5、为什么防火墙需要在进出两个方向上对数据包进行过滤？如果在某个方向上不进行过滤会有什么后果，举例说明！应用代理和分组过滤防火墙的各自优缺点是什么？

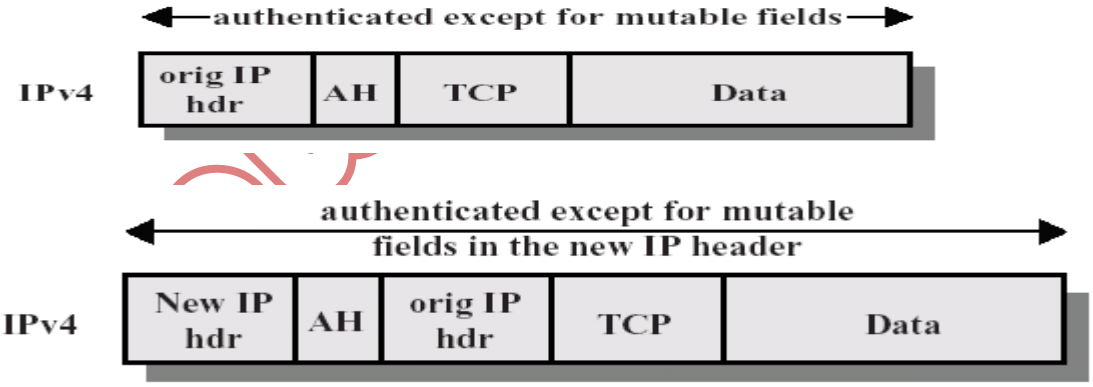
答：在进入方向过滤是为了防止被人攻击，而在出口方向过滤则是为了防止自己成为攻击的源头或者跳板。

应用代理工作在应用层，可以对分组内容进行安全检查和过滤。

分组过滤防火墙工作在网络层，只能对网络层协议头或者链路层协议头进行过滤，功能稍微弱一点，但是速度快，且对用户透明。

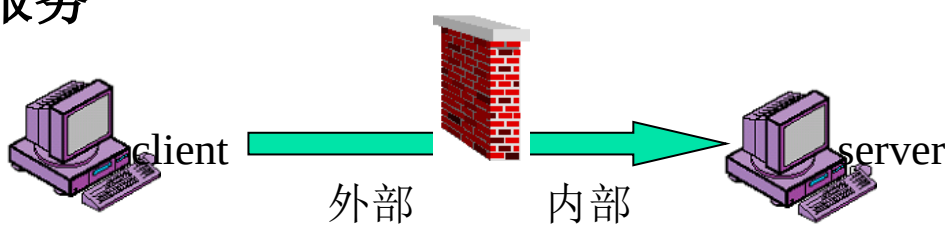
6、IPSec 包括几个子协议，各个子协议的用途？AH 的两种工作模式是什么？及其封包格式？

答：IPSec 包括 AH（认证头）、ESP（封装有效载荷）和 IKE(密钥交换)三个子协议。AH 可实现包括 IP 头中不变字段和 IP 包数据部分完整性认证，ESP 可实现加密和完整性认证。



7、分析填写包过滤防火墙路由表，过滤条件是双向允许 ftp 服务；

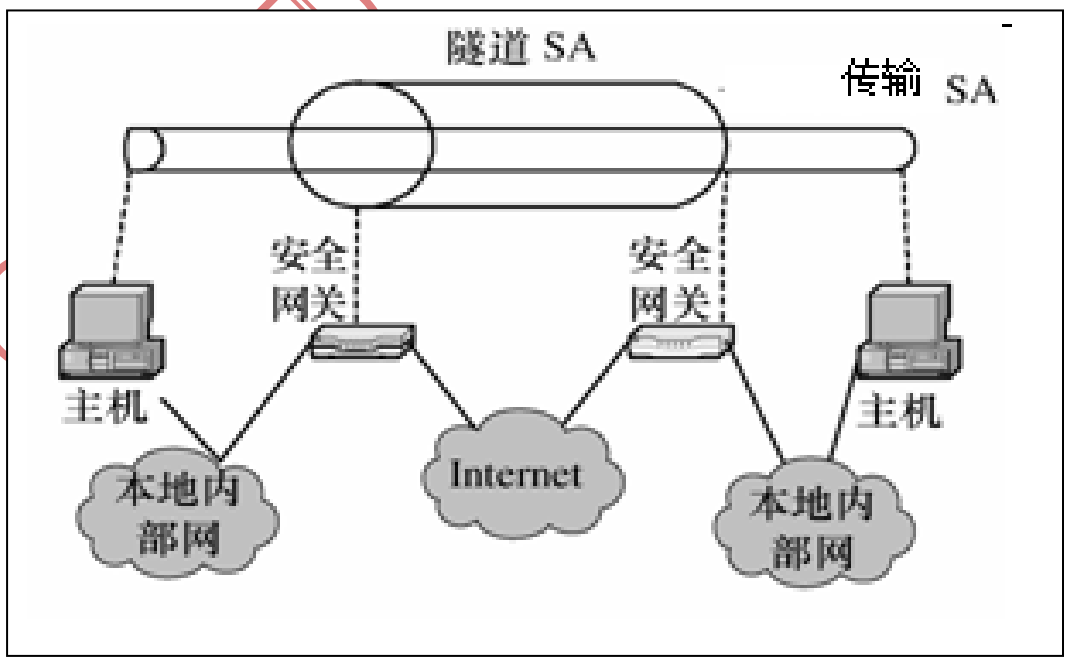
ftp服务



- 往内包的特性(用户操作信息)
  - IP源是外部地址
  - 目标地址为本地server
  - TCP协议，目标端口23
  - 源端口>1023
  - 连接的第一个包ACK=0，其他包ACK=1
- 往外包的特性(显示信息)
  - IP 源是本地 server
  - 目标地址为外部地址
  - TCP 协议，源端口 23
  - 目标端口>1023
  - 所有往内的包都是 ACK=1

服务方向	包的方向	源地址	目的地址	协议	源端口	目的端口	ACK
出	出	内部	外部	TP	>1023	23	any
出	入	外部	内部	TCP	23	>1023	1
入	入	外部	内部	TCP	>1023	23	any
入	出	内部	外部	TCP	23	>1023	1

8、写出如下图所示两个安全网关之间数据包应用安全服务后，数据包的封包格式（两主机之间采用传输模式，两网关之间采用隧道模式）



解：

新 IP 报头	**AH**	**原 IP 报头**	**AH 报头**	**TCP/UD 报头**	**应用程序数据**