《计算机系统与网络安全技术》期末复习题-主观题（网安班）

（通用）简答题：5道*5分=25分

（网安班限选）应用题：3道*10分=30分

（图灵班和网安限选）综合题：2道*5分=10分

*简答题考察3-10章知识的基本概念，主要围绕作业

*应用题考察5-10的重点知识

*网安班考察一道Kerberos协议的应用或综合题

*网安班考察一道RSA加密算法的应用或综合题

三、 简答题（共5大题，共25分）

24 解释以下口令是否合适（5分）

(1) YZ675

(2) nait3

(3) Chengdu

(4) 13579

(5) hu2011

答案：参考如下进行回答

（1）个人所知道的信息：口令、个人标识码、以及对预先设置的问题的答案

（2）个人所持有的物品（令牌）：电子钥匙卡、智能卡和物理钥匙

（3）个人的生理特征（静态生物特征）：指纹认证、虹膜识别及人脸识别等

（4）个人的行为特征（动态生物特征）：语音模式和笔迹特征进行的识别，以及根据打字节奏进行的识别

25

（1）解释什么是自主访问控制（DAC）、强制访问控制（MAC）（2分）

（2）解释主体、客体和访问权的含义。（3分）

答案：（1）

自主访问控制（DAC）

基于请求者的身份和访问规则(授权）控制访问，规定请求者可以(或不可以)做什么。

强制访问控制（MAC）

通过比较具有安全许可的安全标记来控制访问。

（2）

主体：能够访问客体的实体，一般存在三类主体：

所有者

组

世界

客体：外界对其访问受到控制的资源。一个用来包含或接收信息的实体

访问权：描述了主体可以访问客体的方式

读/写

执行

创建/删除

搜索

26.

（1）解释下列术语:数据库、数据库管理系统和查询语言。（2分）

（2）数据库加密的缺点是什么?（3分）

答案:

（1）数据库：是存储一个或多个应用所用数据的结构化数据集合。
数据库还包含数据项之间以及数据项组之间的关系。
可能包含敏感并且需要保护的数据

数据库系统：它是创建、维护数据库的程序套件。
多个用户和应用提供特定的查询服务

查询语言：为用户和应用提供了访问数据库的统一接口

27．什么是路过式下载？（2分）它如何传播蠕虫？（3分）

答案：
利用应用程序中的缺陷（bug）来安装恶意软件。使得当用户浏览一个受攻击者控制的Web页面时，该页面包含的代码会攻击该浏览器的缺陷并在用户不知情或未允许的情况下向系统安装恶意软件。

在多数情况下，这类恶意软件不像蠕虫那样传播

等待那些无防备的用户浏览恶意的 Web页面来传播

28．哪些类型的资源被DoS攻击作为攻击目标？（2分）
洪泛攻击的目标是什么？（3分）

答：（1）
网络带宽
系统资源
应用资源
（2）
洪泛攻击的目标就是占据所有到目标组织的网络连接的容量。
流量可以被它们之间的路径上的高容量链路所处理，数据包随着链路容量降低而被逐渐丢弃
除非使用虚假地址作为数据包的源地址，否则任何一个攻击源都会被清晰的认识
网络性能受到显著的影响

四、 应用题(共3大题，共30分)

29. (网安班限选) (10分) 在RSA加密体制中，已知素数 p = 7，q = 11，公钥 e = 13，

(1) 简述公钥加密算法思想，及其优缺点 (3分)

(2) 试计算私钥 d 并给出对明文 m = 5 的加密，求其密文。(4分)

(3) 已知密文 c = 15，求其明文。请给出完整计算步骤。(4分)

答：(1)：

n=pq=77 (1分)

φ(n)=(p-1)(q-1)=60 (1分)

ed≡1 mod φ(n) (1分)

即13d mod 60 = 1

解得：d = 37 (1分)

(2)：

公钥 (n,e) =(77,13)

密文c = m^e mod n = 5^13 mod 77 = 26 (1分)

私钥 (n,d) =(77,37)

明文m = c^d mod n = 15^37 mod 77 = 71 (2分)

30. （网安班限选）（10分）

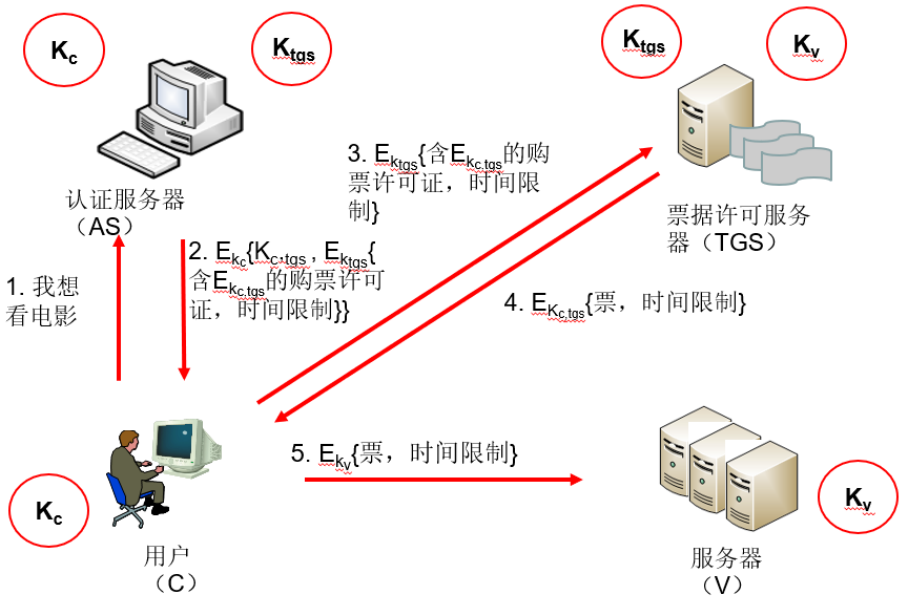
如图所示，假设用户C和认证服务器AS共享对称密钥K_c，认证服务器AS和票据许可服务器TGS共享对称密钥K_{tgs}，票据许可服务器和服务器V共享对称密钥K_v，试回答如下问题：

（1）试分析消息2中的$K_{c,tgs}$是由哪个实体负责颁发的？（2分）

（2）接上一个问题，为什么需要该实体来颁发$K_{c,tgs}$？（2分）

（3）$K_{c,tgs}$的作用是什么？换言之，为什么需要颁发$K_{c,tgs}$？（3分）

（4）用户和服务器之间是否实现了双向认证？如果没有，有何措施来实现？（3分）



•答案：（1）$K_{c,tgs}$是由认证服务器为用户和票据许可服务器颁发的。（2分）

•（2）由于用户和票据许可服务器之间没有任何共享信息。因此很显然他们之间没办法去实现会话密码的交换。然而，由于认证服务器和用户之间共享了密钥K_c，而认证服务器和票据许可服务器之间共享了密钥K_{tgs}，因此可由认证服务器为用户和票据许可服务器颁发$K_{c,tgs}$。（2分）

•（3）用于解决用户和票据许可服务器之间的安全通信的问题。（2分）

•（4）只是一个单向认证，也就是解决了服务器认证用户的问题，而没有解决用户认证服务器的问题。只需要在后面两条消息当中进行简单的变换，就可以解决他们的身份证证的双向认证问题了。在第四条消息，当票据许可服务器向用户返回这样一个票据的时候，他可以返回一个用户和服务器之间将要使用的临时的会话密钥 $K_{c,v}$。（2分）相应的，需要借助之前的方法，由票据许可服务器为用户和服务器颁发一个临时会话密钥$K_{c,v}$。此外，使用来加密票据许可服务器发送的使用K_v加密的含$K_{c,v}$的票和时间限制，即 E_{kv}{含$K_{c,v}$的票，时间限制}。相应的，服务器对其使用$K_{c,v}$解密以后，就可以票使用$K_{c,v}$加密后返回给用户（即$E_{kc,v}${时间限制}），而用户可以通过解密来验证服务器的身份。（2分）

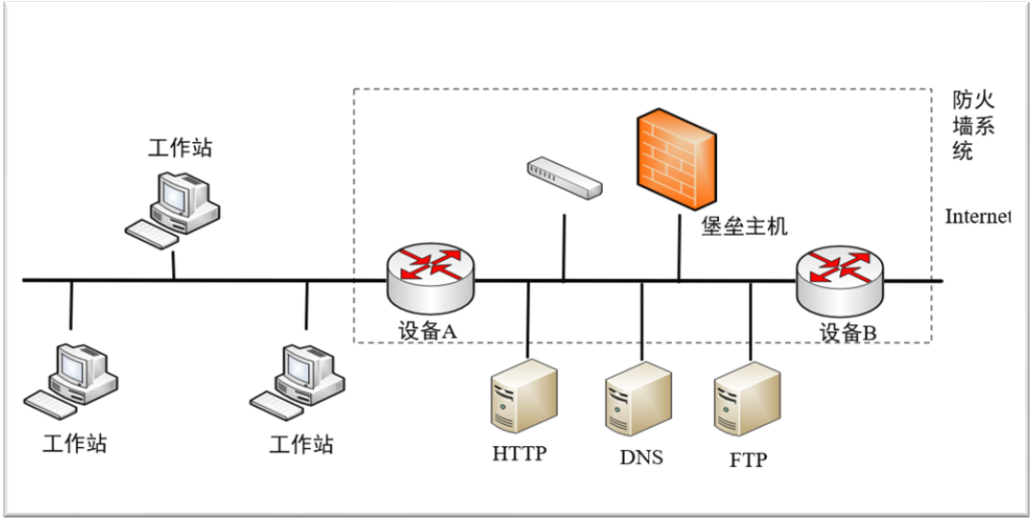
31. （10分）（网安班限选）堡垒主机是一种被强化的可以防御网络攻击的计算机。如图所示，试回答如下问题：

（1）图示的拓扑结构对应哪一种防火墙结构？（2分）

（2）简述该防火墙系统的工作原理。（2分）

（3）设备A和设备B分别代表什么？它们的作用是什么？（2分）

（4）该防火墙结构有什么优缺点？（4分）



答案：（1）屏蔽子网结构防火墙系统（2分）

（2）屏蔽子网结构的防火墙需要连接外部网络的外部路由器和连接内部网络的内部路由器之间的协同工作，才能完成防火墙的功能。即外部路由器、内部路由器和堡垒主机协调工作来提供安全保护功能。（2分）

（3）设备A：内部路由器（或内部包过滤路由器）它用于屏蔽内部网络，过滤内部数据，转发内部数据到堡垒主机（1分）；设备B：外部路由器（或外部包过滤路由器），它用于执行包过滤功能，将数据包转发到堡垒主机。（1分）

（4）优点：安全性高、灵活性好、隐蔽性好（2分）；缺点：成本高，配置复杂。（2分）

五、 综合题(共1大题，共10分)

32. （5分）（图灵班和网安班限选）

基于可证明数据持有权（PDP）（如图所示）的远程数据完整性检测（RDC）协议是一类特殊的网络安全密码协议，它常用于检测远程存储在云服务器端（如云盘服务器）的大文件数据完整性。它的原理简要如下：云用户可以将大规模数据集外包存储在云服务器上，在确认过服务器存储完成之后删除掉本地文件数据，并且在这之后可以定期访问云服务器，以此检测之前存储的数据是否完整。这里，客户不需要取回整个数据集（否则，外包存储变得没有意义），只需要通过取回并检测其中极少的一部分（如0.001 %的数据），即可以极大的概率验证数据的完整性（如99.999%以上的完整性概率）。试回答以下问题：

（1）试分析该协议用到的一种核心密码原语（如：哈希、签名或加密），并对其原理进行简要解释（如哈希的性质、加密是公钥还是私钥、签名的原理）。（1分）

（2）根据小问1进一步分析，该原语具体放在RDC协议里的哪一步？根据图作简单分析。（2分）

（3）为了帮助用户实现远程数据检测（RDC），用户在将云文件进行上传的时候，需要根据文件计算一些元数据，并将元文件和数据一起上传至云端，试分析为什么？（提示：围绕元数据的作用来回答）（2分）

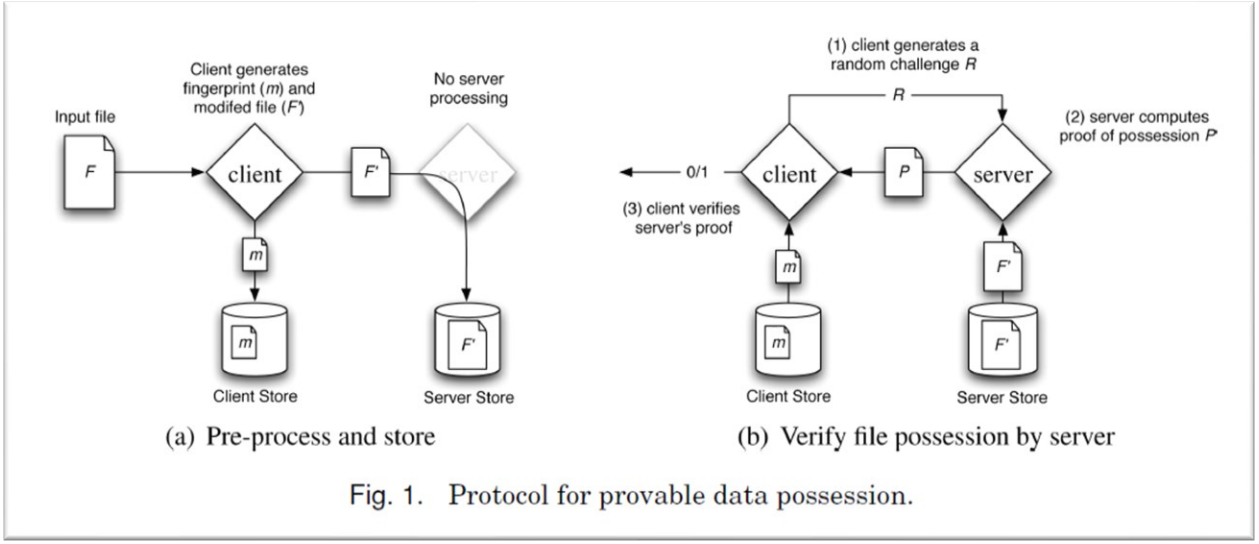


Fig. 1. Protocol for provable data possession.

33. （5分）（图灵班和网安班限选）

数据库已经成为黑客的主要攻击目标，因为它们存储着大量有价值和敏感的信息。这些信息包括金融、知识产权以及企业数据等各方面的内容。网络罪犯开始从入侵在线业务服务器和破坏数据库中大量获利，因此，确保数据库的安全成为越来越重要的命题。网络的高速发展为企业和个人都带来了无限机遇，想要建立一个在线业务，最重要的就是建立一个全面的数据库，与此同时，保护你共享在网络中的数据安全也是至关重要的。

（1）考虑一个简化的大学数据库，其中包括关于课程(名字、编号、日期、时间、房间号、最大注册人数)、讲课的教师和听课的学生的信息。给出一个有效管理这些信息的关系数据库。（3分）

（2）SQL注入攻击对Web应用程序构成了严重的安全威胁：它们允许攻击者不受限制地访问应用程序底层的数据库以及这些数据库包含的潜在敏感信息。试分析简述SQL注入攻击的原理和防范措施。（2分）

答案：

SQL 注入攻击(SQLi)

是一类针对数据库的最普遍和最危险的基于网络的安全威胁。

一般而言，SQLi攻击利用的是Web应用程序页面的性质。

通过发送恶意的SQL命令到数据库服务器就可以发起SQLi攻击。

最常见的攻击目标是从数据库中批量提取数据。

根据环境的不同，还可以利用SQL注入来:

- 修改或删除数据
- 执行任意操作系统命令
- 启动拒绝服务(DoS)攻击

Course Name	Course Number	Day	Time	Room Number	Max Enrollment

Faculty Name	Course 1	Course 2	Course 3

Student Name	Course 1	Course 2	Course 3