**2016/10/30**

**信管网考友答案分享：**

信管网重庆市考友：
问题一，认证是基某种收发双方共享的保密数据来鉴别对象的真实性数字签名中用于验证的数据是公开的。
认证只允许双方相互验证真实性，数字签名可允许第三方
数字签名双方不可抵赖具有公证人解决纠纷的能力，认证却不一定有
问题二，存在攻击者从口令表中获取用户口令，半途链接用户口令，用户和系统位置不均衡，只验证用户不验证系统，
利用单向函数加密口令，利用数字签名加密口令，口令的双向验证，一次性口令
问题三
属于报文内容认证
mac=c（m，k）
a→b m‖mac

信管网ningning：
1、（1）认证总是基于某种收发双方共享的保密数据来认证被鉴别对象的真实性，而数字签名中用于验证签名的是数据是公开的；
（2）认证允许收发双方互相验证其真实性，不准许第三者验证，而数字签名允许收发双方和第三者都能验证。
（3）数字签名具有发送方不能抵赖、接受方不能伪造和具有在公证人前解决纠纷的能力，而认证则不一定具备；
2、（1）攻击者可能从口令表中获取用户口令；攻击者可能在传输线路上截获用户口令；用户和系统的地位不平等；
（2）利用单向函数加密口令；利用数字签名方法验证口令；口令的双向认证；一次性口令；
3

**2016/10/31**

**信管网考友试题答案分享：**

信管网ningning：
1、（1）addrgroup1,（2）work\_time,（3）addr1,（4）lenove,（5）8080,（6）work\_time;
2、（7）192.168.20.1，（8）80，（9）192.168.20.2，（10）255、255、255、0，（11）192.168.20.1；
3、（1）打开浏览器，找到“internet选项（o）”·单击“internet选项（o）”弹出对话框，找到“连接”标签，单击“局域网设置（l）”，直接设置代理；（2）打开“本地连接 状态”对话框“属性（p）”按钮，单击“本地连接 属性”对话框“属性（r）”按钮，选择“使用下面的ip地址”-默认网关（d）；
4、在ie浏览器栏输入：http：//192.168.10.2，回车后，如果访问成功，即可出现正确的访问网页；

**2016/11/1**

**信管网考友试题答案分享：**

信管网ningning：
      1、（1）g，（2）i,（3）h,（4）j，（5）f,（6）b,（7）e，（8）d，（9）a，（10）c;
      2、错误的是：局限性，应该是：广泛性；
      3、（1）常使用自带的安全api，完全避免使用解释器或者提供参数化界面的api。
        （2）如果没法使用一个参数化的api，那么应该使用解释器具体的escape语法来避免特殊字符。
        （3）加强对用户输入的验证。
     4、（1）根据数据将要置于的html上下文对所有的不可信数据进行恰当的转义，或者是去掉（），没有html标签页面就是安全的；“白名单”的，具有恰当的规范化和解码功能的输入验证方法同样会有助于防止跨站脚本；用内容安全策略来抵御整个网站的跨站脚本攻击；用户学会控制自己的好奇心，尽量不去单击页面中不安全的链接；
        （2）最好的方法是将独有的令牌包含在一个隐藏字段中；该独有令牌同样可以包含在url中或作为一个url参数；要求用户重新认证或者判明他们是一个真实的用户也可以防护csrf攻击。

信管网ningning：
      1、（1）g，（2）i,（3）h,（4）j，（5）f,（6）b,（7）e，（8）d，（9）a，（10）c;
      2、错误的是：局限性，应该是：广泛性；
      3、（1）常使用自带的安全api，完全避免使用解释器或者提供参数化界面的api。
        （2）如果没法使用一个参数化的api，那么应该使用解释器具体的escape语法来避免特殊字符。
        （3）加强对用户输入的验证。
     4、（1）根据数据将要置于的html上下文对所有的不可信数据进行恰当的转义，或者是去掉（），没有html标签页面就是安全的；“白名单”的，具有恰当的规范化和解码功能的输入验证方法同样会有助于防止跨站脚本；用内容安全策略来抵御整个网站的跨站脚本攻击；用户学会控制自己的好奇心，尽量不去单击页面中不安全的链接；
        （2）最好的方法是将独有的令牌包含在一个隐藏字段中；该独有令牌同样可以包含在url中或作为一个url参数；要求用户重新认证或者判明他们是一个真实的用户也可以防护csrf攻击。

**2016/11/25**

**信管网考友试题答案分享：**

信管网hjcenry2016：
【问题1】
对称加密算法：des，3des，
非对称加密算法：rsa，hmac，
【问题2】
发送方用pb加密签名，接收方用sb解密和验签

**2016/12/2**

**信管网考友试题答案分享：**

信管网testjing：
问题1 （1）认证总是基于某种收发双发共享的保密数据来认证被鉴别对象的真实性，而数字签名用户验证签名的数据是公开的。 （2）认证允许收发双发互相验证其真实性，不允许第三者验证；而数字签名允许收发双发和第三方都可以验证； （3）数字签名具有发送方不能抵赖，接收方不能伪造和具有在公证人前解决纠纷的能力；而认证不一定具备 问题2 存在问题： 攻击者可能从口令表中获取用户口令；攻击者可能在传输线路上截获用户口令。用户和系统的地位不平等，这里只有强制验证用户的身份，并没有用户验证系统的身份。 改进机制： 利用单向函数加密口令；利用数字签名验证口令；口令的双向验证；一次性口令 问题3： 报文内容认证 若发送方a向接收方b发送报文m，则a计算mac=e（m,.k）并将报文m和mac一起发给接收方， a->b：m||mac。 若接收方收到报文后用相同的密钥k进行相同的计算得出新的mac，并将其与收到的mac进行比较，若二者相等，则（1）接收方可以相信报文未被修改，（2）接收方可以相信报文来自意定的发送方。

信管网重庆市考友：
问题一，认证是基某种收发双方共享的保密数据来鉴别对象的真实性数字签名中用于验证的数据是公开的。
认证只允许双方相互验证真实性，数字签名可允许第三方
数字签名双方不可抵赖具有公证人解决纠纷的能力，认证却不一定有
问题二，存在攻击者从口令表中获取用户口令，半途链接用户口令，用户和系统位置不均衡，只验证用户不验证系统，
利用单向函数加密口令，利用数字签名加密口令，口令的双向验证，一次性口令
问题三
属于报文内容认证
mac=c（m，k）
a→b m‖mac

**2016/12/5**

1. 保密性：网络安全解决措施，信息不泄露给非授权用户、实体或过程，或供其利用的特性； 完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性； 可用性：可被授权实体访问并按需求使用的特性。即当需要时能否存取所需的信息。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击； 2.保密性；完整性；可用性； 3.（1）对称密钥管理；（2）公开密钥管理/数字证书； 4.rsa算法；缺点：（1）产生密钥麻烦；（2）速度太慢

**2016/12/14**

**信管网考友试题答案分享：**

1. 信管网testjing：
1、远程镜像技术，快照技术，基于ip的san互连技术 2、数据容灾，指建立一个异地的数据系统，改系统是本地关键应用数据的一个可用复制 应用容灾，指在一定建立一套完整的与本地产生系统相当的备份应用系统 3、在局域网内部署三台备用服务器，分别是his,pacs以及其他业务系统的容灾服务器。针对不同的业务对rto.rpo的要求，his和pacs数据库服务器部署镜像软件，ris,lis,cis等其他四台数据库服务器上分别部署连续数据保护cdp软件

**2016/12/23**

问题1：abc
问题2：cab
问题3：发现频繁项目集，生成关联规则
问题4：（1）表示用户a通常登陆在每天上午登陆，登陆主机为192.168.1.119，登陆ip192.168.1.201 表示用户经常执行vi程序，执行命令时使用的参数通常是以.c为后缀的问题。括号内的分别是置信度和支持度
（2）关联规则和序列模式
（3）可以判断出用户a是个c程序员，工作时间每天上午，通常使用192.168.1.201登陆，使用gcc编译和gdb来调试程序

**2016/12/24**

1\双重宿主主机体系 以一台双重宿主主机做为防火墙的主体，隔离内外网 、被屏闭的主机体系 以一台路由器和一台内网堡垒主机做为防火墙体系主体，通过包过滤方式实现 隔离外网，保防内网 、被屏闭的内网体系 由dmz,外部路由器，内部路由器，堡垒主机构成的防火墙体系，外部路由器保护dmz和内网，内部路由器保护内网，隔离dmz 2\（1）被屏闭的内网体系 （2）外部过滤器作用，隔离外部互联网，保护dmz和内网 内部过滤器作用，隔离dmz，保护内网 3、（1）＊（2）10.20.100.8（3）10.20.100.8（4）＊（5）udp（6）10.20.100.1（7）udp（8）10.20.100.2