卷1

三、计算题（每小题10分，共20分）

1. DES是第一个被公布出来的加密标准算法，它对固定位长的明文分组进行初始置换，分为左右两半部分，然后进行16轮的轮函数运算，最后再将左右两半合并起来，进行初始逆变换。

（1）在初始置换过程中，其置换表如表1所示，请填写表2，逆初始置换表中的空缺，并简要描述置换过程的原理。（4分）

表1 初始置换表 表2 逆置换表

置换过程的原理是：

第1位为58，则置换后第58位为1；第40位为1，则置换后第1位为40。

（2）下面是DES的一个S盒，如果输入为011001，求4位输出（6分）。

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

行号：1（01）

列号：12（1100）

对应的S盒中的值：1

输出值：0001

2. RSA算法的明文和密文是之间的整数，通常的大小为1024位的二进制数或309位的十进制数。假设选取两个素数，，

（1）计算，并求其欧拉函数。（2分）

n=p\*q=13\*17=221

=(p-1)\*(q-1)=12\*16=192

（2）用辗转相除法验证。（2分）

192=7\*27+1

7=3\*2+1

3=1\*3+0

可得

（3）求解密钥。（2分）

2 27

1 2 55

又商为偶数个

所以d=55

公钥（7，221），私钥（55，13，17）

（4）求解对明文的加密过程。（2分）

可能用到的模运算： ，，，

C=

所以密文C=45

（5）求解对密文的解密过程。（2分）

可能用到的模运算：，，

m=

解密完成

四、材料分析题（每小题10分，共30分）

1. Wi-Fi的方便之处在于不用拖着根线，只要在信号范围内，走到哪儿都能用——而无线电波给你带来的这种便利，攻击者也能享受到。为防止别人能这么方便地看到的你上网的数据，就需要对这些数据进行加密。WPA2是目前最常用的Wi-Fi加密协议。之前还有WPA，更早还有WEP。在WPA2/WPA的设计中，为保证安全性，一个密钥只能使用一次。但研究者发现，通过操纵重放加密握手消息（就是将你的手机和Wi-Fi路由器在通信过程中某些关键步骤的数据记录下来并重新发送出去），可以让已经使用过的密钥被再次使用。他们给这种攻击起了个名字叫“KRACK”，就是Key Reinstallation AttaCKs的意思。KRACK并不能破解出Wi-Fi密码。换句话说，并不能用来帮助“蹭网”。但攻击者可能用这种技术获得你的Wi-Fi通信内容，利用这些漏洞的影响包括解密、数据包重播、TCP连接劫持、HTTP内容注入等。

根据以上材料，分析回答以下问题：

（1）简述消息重放攻击原理。（3分）

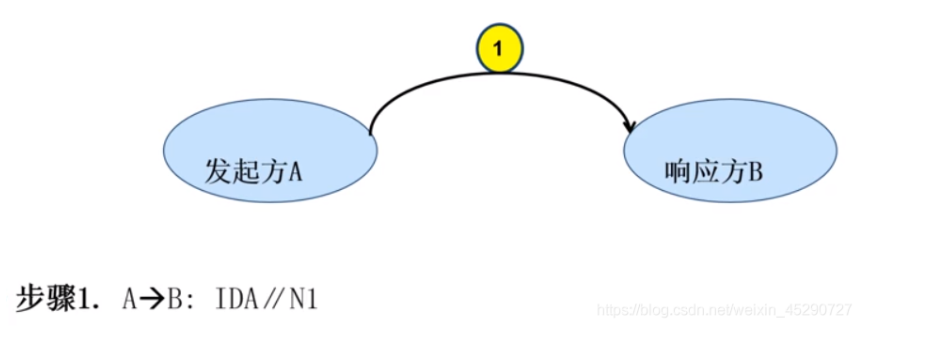
（2）若WPA2中涉及的密钥分配过程中无第三方的参与，其密钥分配过程可能是如何进行的？请简述该密钥分配过程。（3分）

（3）在其密钥分配过程中，可以采取什么措施来防范重放攻击？为什么？（4分）

1. 将手机和Wi-Fi路由器在通信过程中某些关键步骤的数据记录下来并重新发送出去，可以让已经使用过的密钥被再次使用。

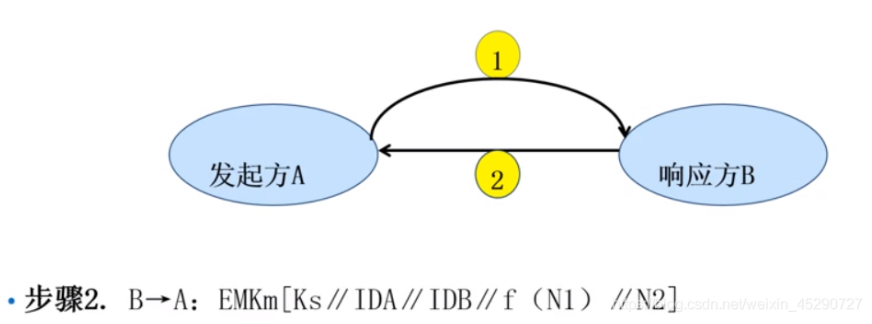
基本的过程

第一步，A向B发出一个请求，请求的信息包括A的身份标识IDA，和一个随机数N1。请求的目的是希望与B进行通信，并请B产生一个会话密钥。

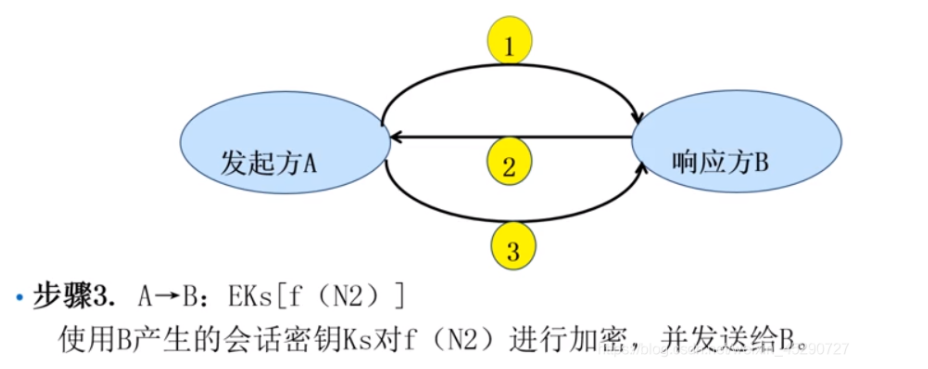


第二步，B对A进行应答，应答的信息包括B产生的会话密钥KS，A、B的身份标识IDA和IDB，还有经过一定规则变化的N1和B产生的随机数N2。

注意，B发送的这条应答消息，是用B与A之间共享的的主密钥加密过的。主密钥的作用就是作为生成临时会话密钥的种子，主密钥的分发则一般使用离线安全物理通道完成。



第三步，A使用KS加密过的对N2的变换结果再发送给B，让B知道A已经正确收到了KS。



（3）

加[随机数](https://baike.baidu.com/item/%E9%9A%8F%E6%9C%BA%E6%95%B0/2454368" \t "_blank)。该方法优点是认证双方不需要时间同步，双方记住使用过的[随机数](https://baike.baidu.com/item/%E9%9A%8F%E6%9C%BA%E6%95%B0)，如发现[报文](https://baike.baidu.com/item/%E6%8A%A5%E6%96%87)中有以前使用过的随机数，就认为是重放攻击。（例如上面提到的发送随机数N1与N2）

https://blog.csdn.net/weixin\_45290727/article/details/106056981?utm\_medium=distribute.pc\_relevant.none-task-blog-2%7Edefault%7EBlogCommendFromBaidu%7Edefault-16.control&depth\_1-utm\_source=distribute.pc\_relevant.none-task-blog-2%7Edefault%7EBlogCommendFromBaidu%7Edefault-16.control

2. 5G网络，即第五代移动通信网络，正所谓“4G改变生活，5G改变社会”。5G的存在，不仅仅是网络的升级，而是真正实现万物互联的基础，改变此前1-4G以“人与人互联”的理念，转而将物联网、工业、生活、医疗、交通等多个行业进行深度融合，做到真正的改变生活。5G消灭了基于手机用户识别码（IMSI）的用户非法定位威胁，保障了用户数据的完整性，降低了漫游区欺骗风险，增强了运营商之间链接的安全性，提升了物联网抵御DoS攻击的能力……可以说是带来了很多正面的、积极的影响，对于提升网络安全可能有划时代的意义。但5G面临的安全挑战，也是前所未有的，例如，伪基站问题、用户大数据保护、用户位置隐私保护等。旧的问题尚未解决，新的技术又来挑战，5G在促进万物互联的同时，也许还会成为黑客世界的一场狂欢。

（1）请简述出现伪基站问题的原因，以及解决方法。（3分）

（2）请简述DoS攻击的原理，以及其常见的形式。（3分）

（3）你认为5G应采用哪些安全措施来提高安全性能？请至少列出2项。（4分）

（1）

原因：伪基站利用了GSM手机系统的单向验证体制。手机连接基站时会受到身份鉴定，但是基站要连接手机却不用进行任何验证。

解决方法：留意手机信号突然消失、安装拦截软件等。

（2）

原理：以极大的通信量或大量的连接请求冲击网络或者计算机，使得网络或者计算机的资源消耗殆尽，从而造成网络崩溃等。

常见形式：带宽攻击、连通性攻击

（3）

1.隐私保护：用户标识动态加密

2.威胁识别：回溯分析、原地址检测

3.请分析RFID的主要安全技术，以及Hash-Lock协议和David数字图书馆协议的特点和区别。(5分)

主要安全技术：标签封杀法、阻塞标签法、裁剪标签法、法拉第罩法、主动干扰法等。

Hash-Lock协议特点：双向认证、但没有ID动态刷新机制，容易受到假冒攻击和重传攻击。

David数字图书馆协议特点：必须在标签电路中实现随机数生成器和安全伪随机函数两大模块，不适用于低版本的RFID系统。

区别：Hash-Lock协议使用metalID来代替真实标签ID，而David数字图书馆协议是基于预共享秘密的伪随机函数来认证。

4.请简述云计算的虚拟化特点，安全架构和常用安全措施。(5分)

虚拟化特点：保真性、高性能、安全性。

安全架构：物理层、计算单元，存储、可信计算、网络层、管理层、信息层、应用层。

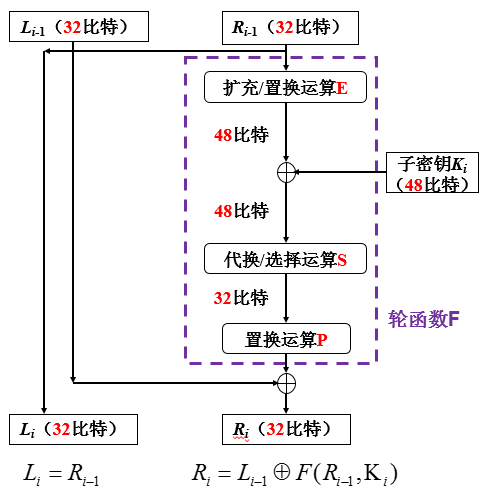
常用安全措施：基于属性的加密和代理重加密、同态加密HE等。

卷2

三、计算题（共20分）

1. DES是第一个被公布出来的加密标准算法，它对固定位长的明文分组进行初始置换，分为左右两半部分，然后进行16轮的轮函数运算，最后再将左右两半合并起来，进行初始逆变换。

（1）如下图所示，在轮函数的运算过程中，E盒运算是将输入的32位数据，转换成48位的输出，请简要描述转换过程，并填写下面的矩阵。（4分，其中过程2分，矩阵填写2分）



转换过程：把8个4位的块，分别向左右各扩充一位，每一行的最后两位为下一行的开头两位，最后一行的最后两位为第一行的开头两位。

（2）下面是DES的一个S盒，如果输入为111011，求4位输出（4分）。

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

行号：3（11）

列号：13（1101）

对应的S盒中的值：7

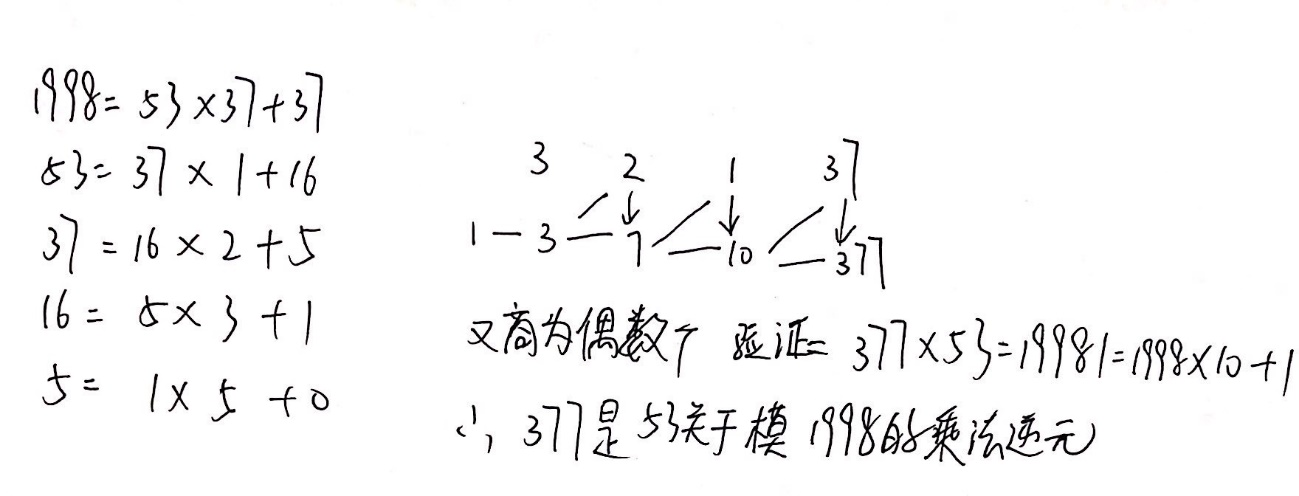
输出值：0111

2. 计算18的欧拉函数。（3分，其中结果1分，过程2分）

小于等于18且与18互素的有1，5，7，11，13，17

所以=6

3. 用辗转相除法求53关于模1998的乘法逆元，并验证。（6分，其中结果1分，过程5分）



4. 凯撒密码属于加法密码，当密钥时，列出加密公式，并填写下面表格中的密文，再对“Cryptography”进行加密。（3分）

加密公式为：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | … | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | … | 24 | 25 |
| F | G | H | I | J | K | L | … | D | E |

Cryptography对应的加密结果为：

Hwduytlwfumd

四、材料分析题（每小题10分，共30分）

1. 无线通信(Wireless communication)是利用电磁波信号可以在自由空间中传播的特性进行信息交换的一种通信方式，其方便之处在于不用拖着根线，只要在信号范围内，走到哪儿都能用。而无线电波给你带来的这种便利，攻击者也能享受到。“蹭网”，指的是未经主人允许，侵占并盗用他人上网资源的一种行为。随着“蹭网”一族的出现，许多公共场所以及个人的网络都在被他人“蹭用。由于蹭网者身份不明以及被蹭网来源不明，无论是蹭他人网还是被蹭网，都可能会导致信息数据泄露等安全隐患。为防止别人能这么方便地看到的你上网数据，就需要对这些数据进行加密。为保证安全性，一个密钥只能使用一次。但攻击者通过操纵重放攻击，可以让已经使用过的密钥被再次使用。Diffie-Hellman算法常用于得到一个共享的会话密钥，来保障用户的通信安全。在每一次通信之前，用户都可以共享一个新的会话密钥，从而防止密钥被攻击者破解。

根据以上材料，分析回答以下问题：

（1）请简述Diffie-Hellman算法的过程。（5分）

（2）在Diffie-Hellman密钥分配过程中，容易受到中间人攻击，请简述中间人攻击的原理。（4分）

（3）怎样防范中间人攻击？（1分）

（1）

1.A与B协商一个大素数n和g，g是n的本原根。

2.A选一个大的随机数x，计算，发给B

3.B选一个大的随机数y，计算，发给A

4.A计算

5.B计算

A、B交换了秘钥K

（2）

攻击者Eve修改为发给B，修改为发给A，此时A、B也会按照上述流程算出结果，但双方均不知道这个结果是被攻击者Eve修改过的。

（3）

在每一次通信之前，用户都可以共享一个新的会话密钥，从而防止密钥被攻击者破解。

2. RFID技术是支持物联网获取物体信息的典型技术，其RFID标签通常价格低廉设备简单，容易受到攻击；又由于其计算资源和存储资源非常有限，无法支持复杂的密码学算法。因此，在很多RFID低成本无源电子标签中，如RFID门票中，所进行的加密算法只支持轻量级加密算法，即只是为了换取一个时间代价，令标签在一定时间内安全即可。流密码中的RC4算法和分组密码中的PRESENT算法都属于对称加密算法，能较容易地做到算法的轻量化。而椭圆曲线加密算法是非对称加密算法。利用ATmaga-32单片机硬件平台对这三种算法的运行效率和密码破译时间进行分析比较，得出在硬件资源同样极端受限的环境下，椭圆曲线加密算法的运行效率要高于另外两种，所生成的密码最难被破译，证明了非对称加密算法同样可以做到轻量化。

根据以上材料，结合所学知识分析回答以下问题：

（1）简述对称加密算法和非对称加密算法的优缺点，并列出2种对称加密算法和2种非对称加密算法的名称。（6分）

对称加密算法优点：

计算量小，加密速度快

对称加密算法缺点：

秘钥容易泄露，初始分配不便

对称加密算法举例（2种）：

DES、AES

非对称加密算法优点：

安全性高、秘钥易于保管

非对称加密算法缺点：

计算量大，加解密速度慢

非对称加密算法举例（2种）：

RSA、Diffie-Hellman

（2）请在下图的椭圆曲线上作出的位置，并简述其过程。（2分，其中作图1分，过程描述1分）



描述；经过P、Q做一条直线交于椭圆曲线的另一点,过做Y轴的平行线交椭圆曲线R，则有P+Q=R

（3）椭圆曲线加密算法的所基于的数学难题是根据公钥，很难求出私钥，即基点，其中，为正整数。请根据图2中的基点的位置，作出和的位置，并简述其过程。（2分，其中作图1分，过程描述1分）



图2

描述：过P作切线交椭圆曲线于，过做直线平行于Y轴交椭圆曲线另一点于2P；连接2P与P交椭圆曲线于另一点，过做直线平行于Y轴交椭圆曲线另一点于3P.

3.无线传感器网络WSN（Wireless Sensor Network）是一种自组织网络，通过大量低成本、资源受限的传感节点设备协同工作实现某一特定任务。传感器网络为在复杂的环境中部署大规模的网络，进行实时数据采集与处理带来了希望。但同时WSN通常部署在无人维护、不可控制的环境中，除了具有一般无线网络所面临的信息泄露、信息篡改、重放攻击、拒绝服务等多种威胁外，WSN还面临传感节点轻易被攻击者物理操纵，并获取存储在传感节点中的所有信息，从而控制部分网络的威胁。用户不可能接受并部署一个没有解决好安全和隐私问题的传感网络，因此在进行WSN协议和软件设计时，必须充分考虑WSN可能面临的安全问题，并把安全机制集成到系统设计中去。只有这样，才能促进传感网络的广泛应用，否则，传感网络只能部署在有限、受控的环境中，这和传感网络的最终目标——实现普遍性计算并成为人们生活中的一种重要方式——是相违反的。

结合你的专业知识，回答以下问题：

（1）在WSN的节点能量、计算能力、存储能力、通信范围等方面分析其相对于传统计算机网络，面临哪些更严重的挑战。(5分)

（2）传感节点被物理操纵是传感器网络不可回避的安全问题，结合你所学的信息安全知识，简述可以采用何种安全机制提高节点本身的安全性能并其简述原理。(5分)

（1）

节点能量：计算机可以随时充电，但WSN数目庞大范围广，环境复杂，有些甚至人无法到达，更换电池非常麻烦，需要考虑节能因素。

计算能力：WSN体积较小，功耗小，所以导致处理器能力较弱，需要利用好有限的计算资源，而计算机网络会好很多，与PC机本身有关。

存储能力：WSN存储能力有限，需要在程序和硬件上多做考虑。

通信范围：WSN是通过“多跳”来解决数据的传输，通信范围一般只有几十米，而计算机网络可以通过网线和WLAN等实现更远的传输。

（2）

可以利用轻量级密码算法ECC，提高了安全性，也节省了能耗和存储空间。原理是是利用椭圆曲线上的[有理点](https://baike.baidu.com/item/%E6%9C%89%E7%90%86%E7%82%B9/11033217)构成Abel加法群上椭圆[离散对数](https://baike.baidu.com/item/%E7%A6%BB%E6%95%A3%E5%AF%B9%E6%95%B0/4538780)的计算困难性。

卷3

三、计算题（每小题10分，共20分）

1. Diffie-Hellman算法是一种公开密钥算法，其唯一目的是使得两个用户能够安全地交换密钥，得到一个共享的会话密钥，算法本身不能用于加密和解密。假定Alice和Bob之间需要交换密钥，选择公开模数，本原根。

（1）如果Alice的私钥，则其公钥的计算公式和结果？（3分）

8

（2）如果Bob的私钥，则其公钥的计算公式和结果？（3分）

4

1. Alice计算得出的密钥K的计算公式及结果？（2分）

mod 11= 9

（4）Bob计算得出密钥K的计算公式及结果？（2分）

mod 11= 9

2. 根据提示，完成RSA算法描述和RSA加解密实例。

（1）完成RSA算法描述：

① 选择两个大素数*p*和*q*；

② 计算乘积*n=pq*，计算欧拉函数*φ(n)=(p-1)(q-1)*；

③ 选择随机数*e*，使得*1<e<φ(n)*并且*gcd(e,φ(n))=1*，(*\_\_\_\_n\_\_\_\_\_ ,e*)是公钥；（1分）

④ 计算*e*模*φ(n)*的逆元，即*de≡1mod(φ(n))*，即计算私钥；

⑤ 加密变换*Ek(x) =\_\_\_\_\_\_\_\_ xe mod n\_\_\_\_\_\_\_*（设明文为*x*，形如*x? mod ?*）（1分）

⑥ 解密变换*Dk(y) =\_\_\_\_\_\_\_\_yd mod n\_\_\_\_\_\_*（设密文为*y*，形如*y? mod ?*）（1分）

（2）依提示步骤完成RSA解密：

已知两个素，：

（1分）计算*=*\_\_\_\_11\_\_\_\_\_\_\_\_\_\_13\_\_\_\_=\_\_\_\_\_143\_\_\_\_

（1分）计算*=*\_\_\_\_\_10\_\_\_\_\_\_\_\_12\_\_\_\_\_=\_\_\_\_120\_\_\_\_\_

（3分）选取的，请用辗转相除法求私钥：

120=7\*17+1

7=1\*7+0

又商为奇数个

所以逆元为120-17=103

d=103

（1分）公钥：（\_\_\_\_\_7\_\_\_\_，\_\_\_\_143\_\_\_\_\_），私钥：（\_\_\_\_103\_\_\_\_\_）。

（1分）试对密文123，恢复明文数字：\_\_\_\_ mod 143\_\_\_\_\_=\_\_\_\_\_85\_\_\_\_

[ 所有可能的复杂运算：

*7×103≡1 mod 120 7×41≡1 mod 143 7×2≡1 mod 13  
7×8≡1 mod 11 123103mod 143=85 123143mod 103=45  
103123mod 143=64 143103mod 123=5 143123mod103=3* ]

四、材料分析题（每小题10分，共30分）

1. 随着车辆通信的广泛应用，也带来了一系列的安全隐患，有可能使驾驶者的个人隐私泄露。为了保障车辆用户的通信安全与隐私保护，需要完善车辆安全隐患存在的环节和加强现阶段车辆通信网络安全架构。车联网属于无线通信的一部分，车辆的网络通信过程中将要遇到的安全威胁也主要是由于无线网络的条件限制。如果安全威胁不能得到防御，车辆通信的过程将收到很大的阻碍。WTLSP和802.1x等标准正逐步在安全方面得到完善。在标准的制定过程中，关注通信过程中的安全隐患存在的环节尤其重要。2014年Visual Threat在SyScan360安全会议上，成功展示了第一款对汽车信息攻击的Android应用程序。无需额外定制硬件电路，只需在网上购买现有的汽车OBD硬件接口设备，利用OBD的安全漏洞就可以对汽车进行攻击。

根据以上材料，分析回答以下问题：

（1）请举出3种在无线通信过程中可能遭遇的安全攻击，并解释其攻击原理。（6分）

（2）请举出3种可以防御以上3种攻击的技术，并简述其原理。（6分）

（3）请设计一个简单的安全系统，包含以上三种安全防御技术，说明这三种技术在系统中的先后顺序，是否可以结合使用，怎样结合？（3分）

（1）

阻塞攻击：干扰无线电波频率，布置N个攻击节点，使全网瘫痪。

洪泛攻击：攻击者不断与邻居节点建立新连接，从而使资源耗尽。

黑洞攻击：攻击者声称自己有一条高质量的路由到基站的路径，使得大量节点向攻击者发送数据，则攻击者的邻居节点电源耗尽，形成黑洞，接下来的数据无法传递。

（2）

扩频通信：防范阻塞攻击。扩频之后干扰信号的能力减弱。

客户端谜题：防范洪泛攻击。客户想跟服务器建立连接，则必须证明自己已经为了连接分配了一定资源，服务器才为客户连接，这样做会增大攻击者发起攻击的代价。

基于地理位置的路由协议：防范黑洞攻击。通信通过接收节点的实际位置自然寻址，所以在别的位置成为黑洞会变得很困难。

（3）

先是客户端谜题，随后是基于地理位置的路由协议，扩频通信与这两种防范方式结合使用。因为先要建立连接，再进行发送，而扩频通信与是贯穿整个通信过程的，与建立连接与传输不冲突。

2. XX云Web应用防火墙（Web Application Firewall，WAF）帮助XX云内及云外用户应对Web攻击、入侵、漏洞利用、挂马、篡改、后门、爬虫、域名劫持等网站及Web业务安全防护问题。企业组织通过部署XX云网站管家服务，将Web攻击威胁压力转移到XX云网站管家防护集群节点，分钟级获取XX Web业务防护能力，为组织网站及Web业务安全运营保驾护航。XX云Web应用防火墙是独家基于AI引擎的WAF，融合XX亿级威胁情报，打造更聪明的威胁识别大脑，精准有效拦截Web威胁；它采用高级Bot行为管理、CC防护人机识别、DNS劫持检测，满足业务安全运营防护需求，更有价值；独家30线独享BGP IP链路接入防护，服务延迟业界最低，保障受护业务访问速度；具有一键无缝接入百G抗DoS能力，应对敏感大流量DoS攻击时，无惧突发风险。

根据以上材料，结合所学知识分析回答以下问题：

（1）简述防火墙的基本功能。（5分）

（2）简述DoS攻击的原理。（5分）

（3）XX云Web应用防火墙可能采用的体系结构有几种？这几种体系结构的名称是什么？（5分）

（1）

1.集中安全管理

2.重新部署NAT

3.安全警报

4.审计与记录网络的访问与使用情况

5.向外发布信息

（2）

原理：以极大的通信量或大量的连接请求冲击网络或者计算机，使得网络或者计算机的资源消耗殆尽，从而造成网络崩溃等。

（3）

3种

包过滤防火墙、应用代理防火墙、双穴主机防火墙

3.美国当地时间2016年10月21日，为美国众多公司提供域名解析网络服务的Dyn公司遭大规模网络攻击。Dyn公司在当天早上确认，其位于美国东海岸的DNS基础设施所遭受DDoS攻击来自全球范围，严重影响其DNS服务客户业务，甚至导致客户网站无法访问。该攻击事件一直持续到当地时间13点45分左右。这是美国遭遇的史上最大规模的网络攻击，大半个美国互联网一度处于瘫痪状态。遭到攻击影响到的厂商服务包括：Twitter、Github、Soundcloud、Spotify、Heroku，据称PayPal、BBC、华尔街日报、Xbox官网、CNN、星巴克、纽约时报、金融时报等的网站访问也遭到了影响。Dyn公司称此次DDoS攻击事件涉及IP数量达到千万量级，其中很大部分来自物联网和智能设备，并认为攻击来自名为“Mirai”的恶意代码。

目前，依托IoT设备的僵尸网络的规模不断增长，典型的IoTDDoS僵尸网络家族包括2013年出现的CCTV系列、肉鸡MM系列(ChiekenMM)、BillGates、Mayday、PNScan、gafgyt等众多基于Linux的跨平台DDoS僵尸网络家族。

其中在本次事件中被广泛关注的Mirai的主要感染对象是物联网设备，包括：路由器、网络摄像头、DVR设备。从事DDoS网络犯罪组织早在2013年开始就将抓取僵尸主机的目标由Windows转向Linux，并从x86架构的Linux服务器设备扩展到以嵌入式Linux操作系统为主的IoT设备。这些设备主要是MIPS、ARM等架构，因存在默认密码、弱密码、严重漏洞未及时修复等因素，导致被攻击者植入木马。由于物联网设备的大规模批量生产、批量部署，在很多应用场景中，集成商、运维人员能力不足，导致设备中有很大比例使用默认密码、漏洞得不到及时修复。

根据以上材料，分析回答以下问题：

（1）根据材料分析，为什么大半个美国互联网会断网？不安全的IoT设备是如何导致Twitter、PayPal等网站无法访问的？ (3分)

（2）根据上述材料和所学知识简述，加固物联网安全，主要在哪些环节或层次分别采取什么安全措施？ (3分)

（3）相对于传统计算机网络安全，物联网安全面临哪些特殊的挑战？(4分)

（1）

因为DNS基础设施遭到大量DDoS攻击，而DNS又是域名系统，所以网站无法打开。

不安全的IoT设备因存在默认密码、弱密码、严重漏洞未及时修复等因素，导致被攻击者植入木马。这些木马会将数量达到千万级的IP账号用于DDoS攻击中，使得Twitter、PayPal等网站无法访问。

（2）

感知层安全：保证信息采集的安全，可以使用SPIN等安全框架来保证安全。

网络层安全：保证网络与系统的安全，可以使用IPSec等网络层的安全协议来保障安全。

应用层：保证信息处理与利用的安全，可以使用EPCglobal等架构来保障安全。

（3）

1.感知节点的本地安全问题 2.感知网络的传输与信息安全问题 3.核心网络的传输与信息安全问题 4.物联网业务的安全问题