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）

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

表 1 初始置换表

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

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1：$n-1$之间的整数，通常n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 $p=13$， $q=17$， $e=7$

（1）计算 n，并求其欧拉函数 $\varphi(n)$。（2 分）

n=p*q=13*17=221

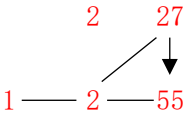
$\varphi(n)$ =(p-1)*(q-1)=12*16=192

（2）用辗转相除法验证 $\gcd(\varphi(n),e)=1$。（2 分）

192=7*27+1
7=3*2+1
3=1*3+0

可得 $\gcd(\varphi(n),e)=1$

（3）求解密钥 d 。（2 分）



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 $m=20$ 的加密过程。（2 分）

可能用到的模运算： $20^{137} \bmod 221=167$， $20^{55} \bmod 221=45$， $20^{29} \bmod 221=63$，

$20^{7} \bmod 221=45$

C= $20^{7} \bmod 221=45$

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：$167^{137} \bmod 221 = 20$， $45^{55} \bmod 221 = 20$， $45^{7} \bmod 221 = 20$

m= $45^{55} \bmod 221 = 20$

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）

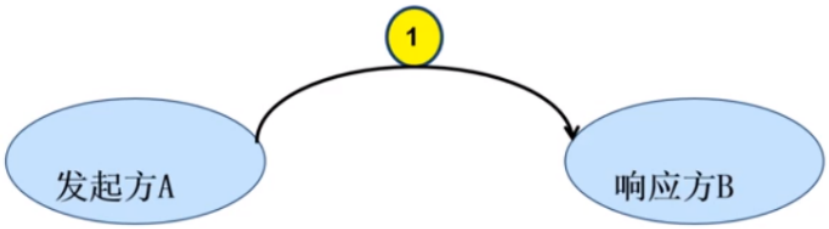
（3）在其密钥分配过程中，可以采取什么措施来防范重放攻击？为什么？（4 分）

（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。

（2）

基本的过程

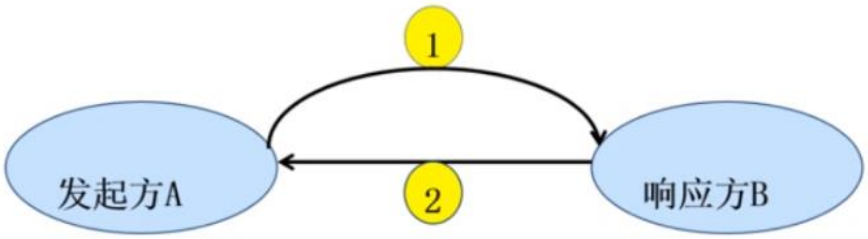
第一步，A 向 B 发出一个请求，请求的信息包括 A 的身份标识 IDA，和一个随机数 N1。请求的目的是希望与 B 进行通信，并请 B 产生一个会话密钥。



步骤1. A→B: IDA∥N1

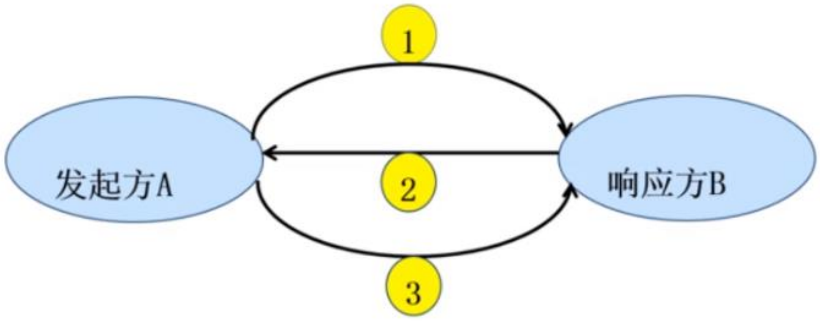
第二步，B 对 A 进行应答，应答的信息包括 B 产生的会话密钥 KS，A、B 的身份标识 IDA 和 IDB，还有经过一定规则变化的 N1 和 B 产生的随机数 N2。

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。



• **步骤2.** B→A：EMKm[Ks // IDA // IDB // f（N1） // N2]

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。



• **步骤3.** A→B：EKs[f（N2）]

使用B产生的会话密钥Ks对f（N2）进行加密，并发送给B。

（3）

加随机数。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，如发现报文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 metaID 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。

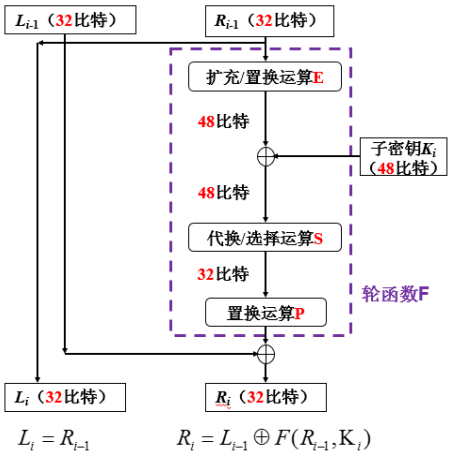
4. 请简述云计算的虚拟化特点，安全架构和常用安全措施。(5 分)

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）



$$\begin{vmatrix} (\ ) & 1 & 2 & 3 & 4 & (\ ) \\ (\ ) & 5 & 6 & 7 & 8 & (\ ) \\ (\ ) & 9 & 10 & 11 & 12 & (\ ) \\ (\ ) & 13 & 14 & 15 & 16 & (\ ) \\ (\ ) & 17 & 18 & 19 & 20 & (\ ) \\ (\ ) & 21 & 22 & 23 & 24 & (\ ) \\ (\ ) & 25 & 26 & 27 & 28 & (\ ) \\ (\ ) & 29 & 30 & 31 & 32 & (\ ) \end{vmatrix}$$

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

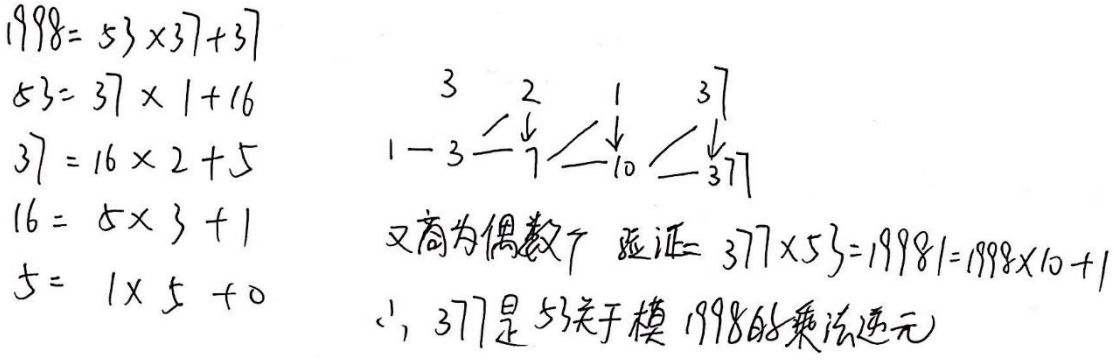
输出值：0111

2. 计算 18 的欧拉函数 $\varphi(18)$。（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 $\varphi(18)$=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 $k=5$ 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：

$C_i = E(P_i) = P_i + 5$

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$X_A = g^x \ mod \ n$，发给 B

3. B 选一个大的随机数 y，计算$Y_B = g^y \ mod \ n$，发给 A

4. A 计算$K = (Y_B)^x = g^{xy} \ mod \ n$

5. B 计算$K = (X_A)^y = g^{xy} \ mod \ n$

A、B 交换了秘钥 K

（2）

攻击者 Eve 修改X_A为X_E发给 B，修改Y_B为Y_E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

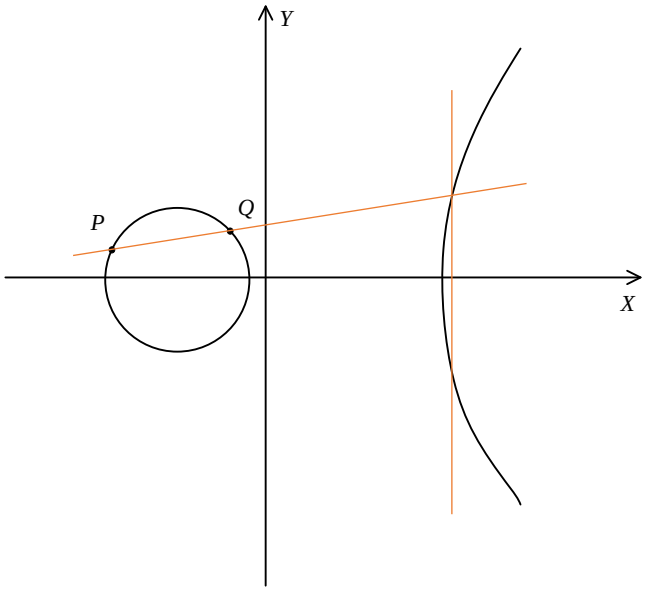
非对称加密算法缺点：

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$P+Q$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R',过R'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kP，很难求出私钥，即基点P，其中，k为正整数。请根据图 2 中的基点P的位置，作出$2P$和$3P$的位置，并简述其过程。（2 分，其中作图 1 分，过程描述 1 分）

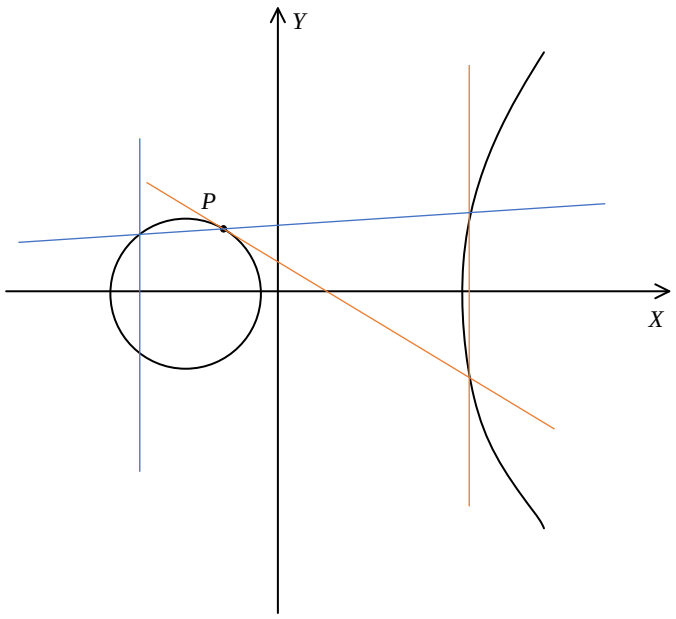


图 2

描述：过 P 作切线交椭圆曲线于$2P'$，过$2P'$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$3P'$，过$3P'$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构成 Abel 加法群上椭圆离散对数的计算困难性。

进行身份认证管理

原理：节点加入网络前先要对其身份ID进行认证，是合法节点才进行通信和数据传输，汇聚节点或基站处有合法节点的列表，当有节点被俘获时需要从合法节点列表中删除这些节点。

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$q=11$，本原根$\alpha=2$。

（1）如果 Alice 的私钥 $x=3$，则其公钥 X_A 的计算公式和结果？（3 分）

$$X_A = \alpha^x \ mod \ g$$
$$X_A = 2^3 \ mod \ 11 = 8$$

（2）如果 Bob 的私钥 $y=2$，则其公钥 Y_B 的计算公式和结果？（3 分）

$$Y_B = \alpha^y \ mod \ g$$
$$Y_B = 2^2 \ mod \ 11 = 4$$

（3） Alice 计算得出的密钥 K 的计算公式及结果？（2 分）

$$k = Y_B^x \ mod \ g$$
$$k = 4^3 \ \text{mod } 11 = 9$$

（4）Bob 计算得出密钥 K 的计算公式及结果？（2 分）

$$k = X_A^y \ mod \ g$$
$$k = 8^2 \ \text{mod } 11 = 9$$

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 $\varphi(n)=(p-1)(q-1)$；

③ 选择随机数 e，使得 $1<e<\varphi(n)$并且 $gcd(e,\varphi(n))=1$，(____n_____,e)是公钥；（1 分）

④ 计算 e 模 $\varphi(n)$的逆元，即 $de \equiv 1 mod(\varphi(n))$，即计算私钥；

⑤ 加密变换 $E_k(x)$ =_____ $x^e \ mod \ n$_____（设明文为 x，形如 $x^? \ mod \ ?$）（1 分）

⑥ 解密变换 $D_k(y)$ =_____ $y^d \ mod \ n$_____（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 $p=11$，$q=13$：

（1 分）计算 n =____11_____×_____13____=_____143____

（1 分）计算 $\varphi(n)$ =_____10____×____12_____=____120_____

（3 分）选取的 $e=7$，请用辗转相除法求私钥 d：

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：$D_k(123)$ = ____123^{103} mod 143_____=_____85____

[所有可能的复杂运算：
$7\times103\equiv1 \bmod 120$　　$7\times41\equiv1 \bmod 143$　　$7\times2\equiv1 \bmod 13$
$7\times8\equiv1 \bmod 11$　　$123^{103} \bmod 143=85$　　$123^{143} \bmod 103=45$
$103^{123} \bmod 143=64$　　$143^{103} \bmod 123=5$　　$143^{123} \bmod 103=3$　]

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 SPINS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