个人答案，不一定正确，只聊有主观成分的题目，而且包含非常多应试中的小心思，只供大家参考，详细版题目见一楼，其中出现的一些严重信息缺漏我会指出。

一、填空

1. 缩写，3A 是比较偏的，而且一般叫 3A，不叫 AAA；SSL 平时一般直接叫 SSL，考试的时候我把英文写出来了；其他两个简单。
2. 没记错的话是 PPT 第一章原文，考察安全攻击与安全特性的关系。
3. 双方的随机数，考察主密钥的计算方法，不可能考公式的，考前经常看到有同学在背臭公式。
4. 略
5. 略
6. 考察 AH 的源端外出处理策略，另外还有目的端进入处理策略，以及 ESP 对应的两个策略，PPT 第三章中非常详细地介绍了。
7. base64 把 3 个 8 比特变成 4 个 6 比特，扩展 33%，信安实践经常出，实现兼容性功能，PPT 第八章 PGP 部分提到过。
8. 双重数字签名，出自 PPT 第八章 SET 部分，是薛老师的两个心头好之一。

二、选择（后面选择题是不定项选择，多选一个选项或者少选一个都可以拿到一分，所以笔者总是利用规则使得分期望最大。）

1. 不会，考试中我选择 C，因为觉得比较符合常识，服务端去写一些信息，客户端读，这样实现信息的传递。
2. 这道题说的是数字信封场景下，回忆版写的有一点问题，数字信封是薛老师的心头好之二，数字信封发送者用接受者的公钥加密对称的会话密钥，所以接受者用自己的私钥解密，选 D。
3. 不会，蒙 C。
4. C。
5. 这题应该是选 C，回忆版写的有些问题，C 应该是屏蔽子网型防火墙。
6. 根据最基本的内容，我只选 ABC，但是有可能是 ABCDE，所以我选 ABCE 去保证至少得一分。
7. 注意要选错误的，我选择 BE，这题回忆版又有一些问题，原题是说 PKI 提供了哪些安全机制，MAC 不被提供，所以选择 B，DE 中选择错误的 E，C 也可能错误，我最后选择 BE，保证至少拿一分。
8. 同样求稳选择 BD，E 是 RA 的作用，由于这个系统中有 RA，我倾向于不选 E，C 有可能正确，但是不正确的可能性更大。
9. 记不得，但是可以排除 ABC，最后选择 DE。
10. DNSSec 这部分我没看，所以完全不会，倾向于认为 DE 是 DNS 的功能。

三、简答

1. 第一问图解，记忆力好的直接默写，不记得的也可以直接倒推，很简单。
   第二问错误扩散，作业原题改数字 1 + 64/16 = 5。
   第三问 IV 的作用，个人认为有两点，一是防止字典攻击（相同明文加密出相同的密文），二是这个加密模式下，加密第一步是对 IV 先进行加密的，然后再异或明文，所以没有 IV 的话这个加密模式都不能正常进行。
2. 这是作业原题，在 SSL 协议中。
3. 注意这个方案基于数字签名，一定要主要基于数字签名，而不是公钥加密，我考试时写错了，还好最后及时改正。
   本题只需要完成 A 对 B 的验证，A 给 B 发自己的身份，随机数，时间戳，加上自己的签名摘要，B 回复 A 的随机数，新时间戳，自己的身份，以及自己的签名摘要。
   双方都可以用对方的公钥验证签名，同时消息也不可篡改，基于随机数挑战应答完成认证，基于时间戳实现抗重放。
4. 答了两点，一是数字签名效率很低，二是 SSL 和 IPSec 都通过协商对称密钥完成了会话密钥交换，在这个前提下还用数字签名是没必要的，第二点纯属个人理解，这是小测原题，老师上课讲过，但是我没听。
5. 这题很有意思，信道不安全怎么实现通信，我认为题设有点不严谨，我先假设不安全信道中没有主动攻击，否则直接把 AB 间所有的通信截断，他们连话都说不上，肯定不能通信了，所以信道不可靠指的是只有被动攻击，威胁消息的机密性，但是消息还是会忠实地传递到对方，那这个问题就非常简单了，AB 使用非对称密码即可，公钥通过明文传输，双方用对方的公钥加密信息后传输，不公开私钥的情况下机密性绝对有保证。
6. 第一问，PPT 上这个部分很抽象，我无法理解并用自己的话描述，当时直接全文默写。
   第二问，使用 KeyID 进行对应，然后介绍一下 KeyID 是什么。
   第三问，加密存储在私钥环中。
7. 第一问，设置好相应的 NAT 规则即可。
   第二问，其实问的是 DNAT 由于 PREROUTING 实现，答理由的时候考虑时序即可，这一步转换必须在路由之前做好（你猜为什么叫 PREROUTING）。
   第三问，不仅有请求，还有响应，A，C 上都很简单，保持不变即可，在 B 上把 IP 转好，A 向 C 发请求的时候在 B 上做好 DNAT，C 响应 A 的时候在 B 上做好 SNAT。