1、源 IP 为 100.1.1.1，目的 IP 为 100.1.1.255，这个报文属于什么攻击（子网掩码：255.255.255.0）

答：Smurf 攻击

【注：注意识别不同 DOS 攻击的特点和方式，例如 Smurf 攻击，由题意可以知道攻击的是广播地址，这个特点很显然是 Smurf 攻击。进一步要求考生知道 Smurf 攻击有两种攻击方式。一种是将源 IP 地址设置为被害主机，一种是将源 IP 地址设置为被害网络的广播地址。注意这两个攻击方式，同时也要注意可能考察其他 DOS 攻击的原理，例如 2018 年考察 Ping of death 的攻击原理，请注意复习。】

2、在这道题中，比较一下数字签名（DS）和消息认证码（MAC）两种安全服务。假设 Oscar 可以看到 Alice 发给 Bob 的所有消息已经 Bob 发挥给 Alice 的所有消息。除了数字签名的公钥，Oscar 不知道其他的公钥和密钥。请分别说明（i）数字签名（ii）消息认证码是否抵御任何攻击，如何抵御任何攻击。auth(x)分别有数字签名或消息认证码计算得到。

a.（消息完整性）Alice 将消息 x="Transfer $1000 to Mark"以明文的方式，加上 auth(x)一起发送给 Bob。Oscar 截获上述内容，并将“Mark”替换成“Oscar”，Bob 能否检测到？

b.（重放）Alice 将消息 x="Transfer $1000 to Mark"以明文的方式，加上 auth(x)一起发送给 Bob。Oscar 观测到上述内容，将其重复发送 100 遍给 Bob，Bob 能否检测到？

c.（发送者认证，同时第三方存在欺骗行为）Oscar 声称给 Bob 发送了消息 x，并附带有效的 auth(x)，但 Alice 声称她也发送了上述内容。Bob 能否区分究竟是哪种情况？

d.（认证中 Bob 存在欺骗行为）Bob 声称收到 Alice 发来消息 x（例如：x="Transfer $1000 to Bob"），并附带有效的 auth(x)，但 Alice 表并没有发送过上述内容。Alice 能否证实是哪种情况？

答：a、DS 和 MAC 都能检测出。

b、都无法检测出重放攻击，除非加上时间戳。

c、 DS：Bob 可以验证这个消息，Bob 使用双方公钥对 auth(x) 进行验证。

MAC：Bob 对双方发起挑战，应答成功则验证通过。（Alice 和 Bob 有 MAC 消息认证的密钥，而 Oscar 没有，

故 Bob 向 Alice、Oscar 两人发起不同挑战值的请求，只有 Alice 能发挥加密认证过后的 MAC 码，而 Bob 不行。即验证。）

d、 DS：Alice 要求 Bob 发送一份消息副本来证明 Bob 的要求。Alice 通过展示数字签名可以被 Bob 的公钥验证，证明 Bob 生成了该数字签名和消息。

MAC：无法验证。

【注：这道题目选自《网络安全基础：应用与标准》（William Stallings 著）第三章课后习题。通过这道题很好地说明了数字签名和消息认证码的应用，以及各种攻击形式的防御方法。这些方式在《信息安全导论》中并没有细致介绍，相当于是引申拓展，有一定难度。但这些知识可以对你理解后面的数字证书，安全协议，PKI 体系等等有帮助。望多加理解，才能真正掌握消息认证的知识。】

3、考虑公共素数 q=11 和本原根 α =2 的 Diffie-Hellman 方案（1）如果用户 A 有公钥 Y_A =9，请问 A 的私钥 X_A 是什么？（2）如果用户 B 有公钥 Y_B =3，请问共享密钥 K 是什么？

答： （1）公钥 Y_A =9， $Y_A = \alpha^{X_A} \mod q$， => 代入数据可得 $X_A = 6$

（2）B 的私钥为 $Y_B = \alpha^{X_B} \mod q$ ，代入数据可得： X_B =8 ， K = $Y_A^{X_B} \mod q$ ，代入数据的 K=3

【注：Diffie-Hellman 作为公钥密码体制的一种算法，应用非常广泛，也是可能会出计算题，例如 2018 年 837 就出过 DH 密钥计算，所以要作为重点掌握，同时还要掌握逆求 K，或私钥的算法。】

4、有三种典型的方式使用随机数作为挑战。假设 Na 是 A 生成的，A 与 B 共享密钥 K，f()是一个函数，三个应用是：

应用 1	应用 2	应用 3
(1) A->B: Na	(1) A->B: E(K,Na)	(1) A->B: E(K,Na)
(2) B->A:E(K,Na)	(2) B->A:Na	(2) B->A:E(K,f(Na))

描述每种应用适用于何种条件。

答：区别在于漏洞，应用 1：可以通过重放攻击的形式进行仿冒用户 B。应用 2：攻击者视图预测合理的响应，如果存在 nonce 值则不会成功。应用 3：两方消息都加密，且 f()保证两次 Na 不同，从而更安全。

【注：应该 837 考试不会这么考察协议让人分析，该题目选自《网络安全基础：应用与标准》第四章课后习题第 4.2 题，仅做参考了解。】

5、考虑基于非对称加密技术的单向认证：A->B:IDa;B->A:R1;A->B:E(PRa,R1)。请解释协议，分析该协议易受到什么类型的攻击。

答：此为挑战-应答协议，R1 为挑战值，用 A 的私钥签名 R1，用 A 的公钥进行解密认证。攻击者可以利用这个协议让 A 签名消息，并将此签名和消息发送给 D，声称该消息是 A 发送的。

6、考虑基于非对称加密技术的单向认证：A->B:IDa;B->A:E(PUa,R2);A->B:R2。请解释协议，分析该协议易受到什么类型的攻击。

答：此协议也是挑战应答方式用于 AB 间认证，只有 A 可以解密 R2。攻击者可以利用这种机制，使 A 解密从网络窃听到的消息（他人使用 A 公钥加密的消息）。即将该消息作为 R2 使用。

【注：上面两道题目同样选自《网络安全基础：应用与标准》不过相对较简单，注意公钥与私钥的应用模型特点，从这两个应用模型特点考虑攻击形式，很容易就得到答案。此处仅作为提高篇题目，目的是为了加深对非对称密钥的理解。个人认为不太可能在 837 考试中见到类似题目，如果实在想不出攻击方式，可作为拓展阅读。】

7、考虑下列协议，它让 A、B 决定一个新鲜共享的对话密钥 K'_{AB}，假设他们已经有了一个长期密钥 K_{AB}：

（1）A->B：A，N_A　（2）B->A：$E(K_{AB},[N_A,K'_{AB}])$　（3）A->B：$E(K'_{AB},N_A)$

a.我们首先要理解协议设计者的理由：为什么 A 与 B 认为他们可以通过这个协议和对方共享 K'_{AB}？为什么他们相信共享的密钥是新鲜的。

b.假设 A 开始和 B 使用这个协议，然而通信被 C 截获。说明 C 如何利用反射开始新的协议，使得 A 认为他已经同意了 B 使用新鲜的密钥（尽管实际上她只是和 C 进行了通信），从而使得 a 中的理由错误。

c.提出一个改进的协议使其可以避免这种攻击。

答：（a）A 确认 K'_{AB} 因为他的 N_A 从第二步被老密钥进行加密，B 认为 K'_{AB} 是共享的，是因为第三步，N_A 被新密钥 K'_{AB} 加密，只有 A、B 知道新密钥。A 认为密钥是新鲜的是因为，第二步中，N_A、K'_{AB} 一同包括在消息 2 中。因此，第二步肯定发生在第 1 个消息被接收之后。

（b）C 利用一下方式重放：

① A->C(B)：A, N_A　② C(B)->A：B，N_A ③ A->C（B）：$E(K_{AB},[N_A,K'_{AB}])$ ④：C(B)->A:$E(K_{AB},[N_A,K'_{AB}])$

⑤：$E(K'_{AB},N_A)$　解释：C 无法加密 N_A，所以要开启一个新的交换，冒充 B 得到 A 加密的 N_A，在捕获到这个加密后的 $E(K_{AB},[N_A,K'_{AB}])$ 反射给 A，使 A 确信与 B 通信（实际上为 C）

（c）增加发送方和接受方信息，如：$E(K_{AB},[A,B,N_A,K'_{AB}])$

【注：太难了，不会这么考的，就当拓展知识面了。】