分组密码和流密码的差别是什么？

分组密码和流密码都是对称加密算法的两种类型。它们的主要区别在于它们对待待加密数据的方式不同。分组密码将明文分成固定长度的块，而每个块单独加密。流密码则按位对待加密数据，逐位加密。因此，流密码适用于连续数据的加密，而分组密码适用于块数据的加密。

混淆与扩散的差别是什么？

混淆和扩散都是加密算法中常用的技术，以增加加密强度和难度。混淆是指在加密过程中使用一个或多个非线性的算法，将明文和密钥混合起来，以产生密文。而扩散是指改变明文中的每一个比特，以使密文的每一个比特都受到明文中的每一个比特的影响。混淆和扩散两者的目的都是使得密文和密钥之间的关系变得非常复杂，从而增加破解密文的难度。

解释什么是雪崩效应。

雪崩效应是指明文或密钥中的微小变化，可以导致加密结果的巨大变化。这种效应是加密算法中的一种重要特性，是衡量加密算法强度的重要因素之一。具有雪崩效应的加密算法，即使是对非常相似的明文或密钥进行加密，生成的密文也会有非常大的差异，从而防止攻击者通过分析密文推断出明文或密钥。

什么是三重加密？

三重加密是指使用三个不同的密钥对同一份明文进行加密的过程。三重加密可以提高加密强度，增加破解难度。常用的三重加密算法有3DES（Triple DES）和AES-TDEA（Triple Data Encryption Algorithm）等。

什么是中间相遇攻击？

中间相遇攻击是一种加密攻击技术，其基本思想是在加密过程中获取中间状态，然后通过对中间状态的分析，来猜测密钥或者加密结果。这种攻击技术对于分组密码尤其有效，因为分组密码在加密过程中涉及多个中间状态，攻击者可以尝试在这些中间状态上进行分析，从而获得密钥或者明文。

(1) 用4\*4的矩阵来描述状态的最初内容：

00 04 08 0c

01 05 09 0d

02 06 0a 0e

03 07 0b 0f

(2) 给出初始化轮密钥加后状态的值：

01 05 09 0d

05 09 0d 01

09 0d 01 05

0d 01 05 09

(3) 给出字节代替后状态的值：

63 cab3 30e6 0415

50 fbd8 4d12 2bc4

d2 7f f7f2 af0d

45 3b 3c6e a2cb

(4) 给出行移位后状态的值：

63 ca b3 30

fb d8 4d 12

f2 af 0d d2

a2 cb 45 3b

(5) 给出列混淆后状态的值：

ba 84 e8 1b

75 a4 8d 40

f4 8d 06 93

ec 87 ca 53