数字签名和加密的基本原理及其区别 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/289/2021_2022__E6_95_B0_E5_AD_97_E7_AD_BE_E5_c101_289641.htm 数字签名主要经过以下几个过程： 信息发送者使用一单向散列函数（HASH函数）对信息生成信息摘要；信息发送者使用自己的私钥签名信息摘要；信息发送者把信息本身和已签名的信息摘要一起发送出去；信息接收者通过使用与信息发送者使用的同一个单向散列函数（HASH函数）对接收的信息本身生成新的信息摘要，再使用信息发送者的公钥对信息摘要进行验证，以确认信息发送者的身 份和信息是否被修改过。 数字加密主要经过以下几个过程： 当信息发送者需要发送信息时，首先生成一个对称密钥，用该对称密钥加密要发送的报文；信息发送者用信息接收者的公钥加密上述对称密钥；信息发送者将第一步和第二步的结果结合在一起传给信息接收者，称为数字信封；信息接收者使用自己的私钥解密被加密的对称密钥，再用此对称密钥解密被发送方加密的密文，得到真正的原文。 数字签名和数字加密的过程虽然都使用公开密钥体系，但实现的过程正好相反，使用的密钥对也不同。数字签名使用的是发送方的密钥对，发送方用自己的私有密钥进行加密，接收方用发送方的公开密钥进行解密，这是一个一对多的关系，任何拥有发送方公开密钥的人都可以验证数字签名的正确性。数字加密则使用的是接收方的密钥对，这是多对一的关系，任何知道接收方公开密钥的人都可以向接收方发送加密信息，只有唯一拥有接收方私有密钥的人才能对信息解密。另外，数字签名只采用了非对称密钥加密算法，它能保

证发送信息的完整性、身份认证和不可否认性，而数字加密采用了对称密钥加密算法和非对称密钥加密算法相结合的方法，它能保证发送信息保密性。google_ad_client = "pub-4504000360271476".google_alternate_color = "FFFFFF".google_ad_width = 468.google_ad_height = 15.google_ad_format = "468x15_0ads_al".//2007-08-31: cisco.chinaitlab.comgoogle_ad_channel = "6111910507".google_color_border = "cccccc".google_color_bg = "FFFFFF".google_color_link = "000033".google_color_text = "000000".google_color_url = "008000".// 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com