

电子商务：数字签名 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/493/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c67_493090.htm 数字签名是公开密钥加密技术的另一类应用。它的主要方式是：报文的发送方从报文文本中生成一个128位的散列值（或报文摘要）。发送方用自己的专用密钥对这个散列值进行加密来形成发送方的数字签名。然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方。报文的接收方首先从接收到的原始报文中计算出128位的散列值（或报文摘要），接着再用发送方的公开密钥来对报文附加的数字签名进行解密。如果两个散列值相同，那么接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别和不可抵赖性。

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