

电子商务辅导：IDE数据的加密和解密电子商务师考试 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/645/2021\\_2022\\_\\_E7\\_94\\_B5\\_E5\\_AD\\_90\\_E5\\_95\\_86\\_E5\\_c40\\_645427.htm](https://www.100test.com/kao_ti2020/645/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_645427.htm) 数据的加密和解密 目前有许多种专门的数据加密的方法，它们在EDI系统中起了不小的作用。数据加密是指将通常使用的信息整理为某种只有靠译码还原才可辨认的特殊信息的处理过程。《数据加密标准》（DES）就是由ANSI支持发展出的加密码算法标准，它已广泛应用于EDI领域中。DES提出了10种可以使普通信息变为密码信息的密钥。只有使用相同的密钥的人，才可能将已加密数据破译。在系统中，关键是保持好对密钥的控制。它的保密强度也十分可靠。如果破译者采用密钥穷举的办法来求出密钥，那么长为100比特的密钥空间共有 $2^{100}$ 个密钥，即使用大型计算机，也要上千年才能完成。同时，这些安全服务还要与数字签名、访问控制、鉴别交换、流量填充、路由控制、回执、安全恢复等基本安全功能结合起来，才能有效地解决EDI在开放式网络中通信的保密问题。编码的功能是建立在加密方法基础上的。编码的目的不在保密，而在于保证数据的可靠传输，如银行帐户余额、订单数量等在发送存储过程中不发生变化。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](http://www.100test.com)