电子商务概论知识辅导：DES算法 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/170/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_170730.htm

第三节 DES算法 数据加密标准DES(data encryption standard)算法是由美国IBM公司研制的一种分组密码算法，是一个迭代分组密码。DES是一个使用最为广泛的加密算法，虽然从DES出现后又产生了许多常规加密算法，但DES仍是此类算法中最重要中的一个。在正式讨论DES算法之前，为了更好的理解算法的实际工作过程，我们先来看一个简化的DES算法，以此加深对DES算法的理解。

图6.9 简单DES的加密过程 一、简单DES简单DES的加密算法是以8bit的明文分组和10bit密钥作为输入，产生8bit密文分组作为输出。1、加密过程简单DES的加密过程如图6.9所示。

2、加密算法构成：简单DES的加密算法包括4个基本函数：一个初始置换函数IP；一个fk函数；一个用来交换数据的SW置换函数；一个逆置换函数IP⁻¹。（1）初始置换函数IP数据原先所在位置IP置换2 6 3 1 4 8 5 7 初始置换IP是将明文M中数据的排列顺序按一定的规则重新排列，而生成新的数据序列的过程。如图6.10所示：图6.10 简单DES的初始置换

设8bit数据K各位分别为K1、K2、K3、K4、K5、K6、K7、K8，则经过IP置换后，各位分别为K2、K6、K3、K1、K4、K8、K5、K7。例：设8bit数据为11110011，则初始置换的结果为：经IP置换 1111001110111101 （2）fk函数fk函数是多个置换函数和替代函数的组合函数。fk函数将输入它的8bit数据进行分组，分成左4位和右4位，然后进行如下运算。
$$fk(L,R) = (LF(R, SK), R)$$
L 输入的左边4位分组R 输入的右边4位

分组 逐位异或 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