口令加密算法 - Java加密与安全 - 飞扬学院

Java加密与安全

口令加密算法

PBE算法

PBE：Password Based Encryption

由用户输入口令，采用随机数杂凑计算出密钥再进行加密

Key通过口令和随机salt计算得出，提高了安全性

PBE算法内部使用的仍然是标准对称加密算法（例如AES）