一种哈希密文再加密及再加密后的解密方法

所属领域：加密技术

成果简介

1. 成果的基本情况

现有的用户名加密的技术有 MD5、SHA 等加密手段。MD5 加密的主要方式是将用户的明文进行哈希加密形成密文，然后将密文存储在数据库里面，以后用户登录时，将其输入的密码转换成 MD5 码后与数据库存储的密文进行比对，判断是否一致。虽然密码在经过 MD5 加密后的 128bit 的大整数是无法通过数学方式解密的。但是，这样的加密方式并不意味着百分之百的安全。虽然，MD5 码加密不存在逆过程，对于较为复杂的用户密码，MD5 码加密之后很难通过枚举的手段进行破译。但是，数量众多的用户密码并不都是复杂的密码，这就为用户的信息安全带来了大量的问题。本发明所要解决的技术问题在于针对上述现有技术中的不足，提供一种高效、快速、能够进一步加强原始哈希密文的安全性、加密开销小、实用性强的哈希密文再加密方法。

2. 主要技术指标

加密过程：（1）设定一个固定的第一噪声插入位置 N1，从所述第一噪声插入位置 N1 处将原始哈希密文分成前半哈希密文和第一后半哈希密文。（2）随机生成一个噪声字符串，所述噪声字符串的长度 L1 的取值范围为 0<L1<10，L1 为自然数；在所述第一后半哈希密文中随机找一个插入所述噪声字符串的第二噪声插入位置 N2，并在所述第二噪声插入位置 N2 处插入所述噪声字符串，形成带噪声后半哈希密文。（3）将所述前半哈希密文、第二噪声插入位置 N2、噪声字符串的长度 L1 和带噪声后半哈希密文依次合并，生成再加密好的噪声密文。

解密过程：（1）取得第一噪声插入位置 N1 的值。（2）根据所述第一噪声插入位置 N1，从所述再加密好的噪声密文中，取得所述第二噪声插入位置 N2 的值和噪声字符串的长度 L1 的值, 从所述第一噪声插入位置 N1 处将所述再加密好的噪声密文分成前半哈希密文和第二后半哈希密文，并在所述第二后半哈希密文中去掉前两位，形成了带噪声后半哈希密文。（3）在所述带噪声后半哈希密文中，根据所述第二噪声插入位置 N2 和所述噪声字符串的长度 L1，去掉所述噪声字符串，形成了第一后半哈希密文。（4）将所述前半哈希密文和第一后半哈希密文依次合并，生成解密后的哈希密文。

本发明与现有技术相比具有以下优点：

1）本发明的加密与解密方法简单，实现方便。

2）本发明的加密方法能够对哈希密文进行高效、快速的再加密，破解难度更高。

3）本发明加密解密操作的开销在微秒级别，所带来的加密解密开销非常小。

4）本发明的实用性强，便于推广使用。

3. 应用范围

数据加密与信息安全。

4. 市场需求及经济效益分析

本发明的方法简单，实现方便，能够高效、快速的对哈希密文进行再加密和再加密后的解密，能够进一步加强原始哈希密文的安全性，加密解密开销小，实用性强，便于推广使用。

5. 合作方式：专利权转让　专利权许可　技术转让　技术入股　合作开发　技术服务　双方协商

6. 联系方式

负责人姓名：龚星宇　　电　话：18629488083　　E-mail：108615030@qq.com