蓝晨钰
软件工程 计应2班
学号：10389092
Oct. 15.

MD5与密码保护

MD5即Message-Digest Algorithm 5（信息摘要算法5），常用与确保信息传输完整一致，是一种广泛应用的散列（Hash）算法之一。MD5一度被称为"数字指纹"而广泛应用于文件签名，还由于其不可逆性，很多系统都采用MD5作为加密算法来进行密码保存。但由于MD5的弱点被不断发现以及计算机能力的不断提升，已经可以人为的制造出MD5碰撞，使MD5不再具有唯一性，也因此也逐渐变得不适合应用于安全环境。

> 什么是MD5碰撞？简单的来说，就是存在并能找到两个或两个以上的不同数据进行MD5运算后有相同结果。

山东大学数学系教授，中国密码学家，王小云女士在2004年的国际密码讨论年会上，与其研究同事展示了MD5及其相关的碰撞范例，并提供了能快速计算出MD5碰撞的算法，引起了轩然大波。

尽管如此，由于MD5已经被主流语言所广泛支持，在安全要求并不是十分高的情况下，MD5算法依然有广泛的作用。在密码保护方面来说，总体来看还是安全的，相比明文传输和明文保存（CSDN？），在传输或者保存的时候进行一次MD5加密，就能很大程度的提高密码的安全性。

事实上，目前破解MD5的主要方法，并不是上面提出的计算MD5碰撞，即使是简单的碰撞也是需要消耗相当的时间进行计算的，因此破解的方法主要还是依靠密码词典。即常用的密码并进行MD5处理后建库，通过和现有的MD5数值（一般可以通过抓包或者拖库获得）进行比对，从未破解出密码。一般来说，如果是一些弱密码，比如有意义的字符或者数字，通过这种手段是很容易破解出来的。

针对这样的破解方法，一般的网站开发者只需要一些简单的技巧就能提高密码的安全程度：在用户注册的时候，对密码进行判断，要求用户必须是足够位数，比如8位以上，包含字母数字，大小写，甚至是特俗字符。这样用户使用的密码就不是那么轻易就能被破解的了。

更有效的方法，是对录入的密码加上足够复杂度的干扰字串。比如在用户的密码后面，附上以用户信息为种子特定算法计算出的字符串，再一起进行MD5加密，这样就能保证密码的复杂度，使得上述的破解方法更加难以进行。破解者已经无法从MD5本身，或者数据库看到MD5的具体处理过程，必须看到处理的源代码，才能进行相关破解。

另外，再研究了MD5算法的具体实现后，我们还能通过改动来定制出属于自己的MD5算法。我们知道MD5算法有4个Magic Number，最简单的定制方法，即是使用自己的Magic Number，这样，如果别人不知道Magic Number的话，是没法通过对比字典来进行破解的。

最后要说明的是，尽管我们有这样那样的防范措施，但是不可否认的是MD5的确已经越来越不适用于当今的安全环境。当我们需要更安全的算法时，就应当抛弃MD5，转而使用如SHA-256这样的安全散列算法，该算法是美国国家安全局（NSA）设计，美国国家标准与技术研究院（NIST）发布的，目前还没有出现有效的SHA-256的碰撞算法。另外该算法已经开源，是MD5的一个不错的替代。