## 产品防伪 1.0

## 例2 产品防伪

Step1 酒厂选择一个MAC算法以及密钥;

Step2 酒厂对生产的每一瓶酒进行编号,并建立数据库。

Step3 酒厂计算每瓶酒编号 $t_i$ 的杂凑值得到MAC $(t_i)$ ,将防伪码  $t_i \parallel$  MAC $(t_i)$  印到瓶盖上,并且将防伪码存入数据库。

## 检验方法:

用户输入防伪码后,酒厂数据库计算编号的 MAC值,并通过其编号查出数据库中的杂凑值, 将二者比较。二者不一致时判定防伪码假;一致 时再检查数据库中是否有该码已检验过的记录。 若无,则判定防伪码真,并记录检验时间;若有 记录,告知用户该酒的检验时间。

防伪码 检测客户端	:编号m  MAC(m	服务端
真假: 检验时间: (如果已经检验过) 防伪码:	防伪码 真假信息 检验时间	服务端利用自己的密钥将编号m取 MAC'(m),与已经存储的MAC(m)进行比较,如果不相同,则为假,如果相同查看以前是否检测过,如果检测过返回每次的检测时间,如果没有检测过则记录该次检测时间并传到客户端。

## 所需工作:

- 1、 选取一个 MAC 算法和一个密钥。
- 2、 使用我们上学期使用的 LocalDB 数据库进行数据的存储,只需要创建两张表格,一张产品检测表,属性有编号、MAC(编号); 第二张表时间记录表,属性有编号、检验时间。