《密码学》课程设计实验报告

实验序号：06　　实验项目名称：Hash 函数

学　　号		姓　　名		专业、班	18 信安 3-4 班
实验地点	网安基地新珈楼 B308	指导教师	王张宜	时间	2020.12.01

一、　实验目的及要求

教学目的：

(1) 掌握 Hash 函数的基本概念和安全性要求；

(2) 掌握 SHA 系列 Hash 函数和 SMS3 的算法结构；

(3) 掌握 HMAC 的算法结构与应用；

(4) 了解 Hash 函数的安全性。

实验要求：

(1) 掌握 Hash 函数的安全性；

(2) 掌握 SHA 系列 Hash 函数的实现；

(3) 了解 Hash 函数实现中的相关优化算法；

(4) 了解 Hash 函数分析的相关算法。

二、实验设备（环境）及要求

Windows 操作系统，高级语言开发环境

三、实验内容与步骤

3.1 编程实现 SM3 算法

其中涉及到的基本运算包括：

$f_t(B,C,D)$　= 第t步使用的基本逻辑函数

<<<s　= 32位的变量循环左移s位

+　= 模2^{32}加法

3.1.1 基本逻辑函数的编程实现

建议：采用“宏”实现

FF1(x,y,z)=x⊕y⊕z

```
#define FF1 (x,y,z) (x^y^z)
```

FF2(x,y,z)=(x∧y)∨(x∧z)∨(y∧z)

```
#define FF2 (x,y,z) ((x&y)|(z&(x|y)))
```

GG1(x,y,z)=x⊕y⊕z，　（同FF1）

```
#define GG1(x,y,z) (x^y^z)
```

GG2(x,y,z)=(x∧y)∨(¬ x∧z)

```
#define GG2(x,y,z) (z^(x&(y^z)))
```

复习与思考：

（A）C语言中“宏”与“函数”的区别：

1.宏会在编译器在对源代码进行编译的时候进行简单替换，不会进行任何逻辑检测，即简单代码复制而已。

2.宏进行定义时不会考虑参数的类型。

3.参数宏的使用会使具有同一作用的代码块在目标文件中存在多个副本，即会增长目标文件的大小。

4.参数宏的运行速度会比函数快，因为不需要参数压栈/出栈操作。

5.参数宏在定义时要多加小心，多加括号。

6.函数只在目标文件中存在一处，比较节省程序空间。

7.函数的调用会牵扯到参数的传递，压栈/出栈操作，速度相对较慢。

8.函数的参数存在传值和传地址（指针）的问题，参数宏不存在。

（B）思考：

1、证明上述“宏”定义的正确性，即证明（必做题）

(z^(x&(y^z)))= (x∧y)∨(¬x∧z)

((x&y)|(z&(x|y)))= (x∧y)∨(x∧z) ∨(y∧z)

提示： 方法1：真值表穷举

方法2：参考《离散数学》

2、分别统计上述两类的计算效率，即需要执行CPU基本指令的次数。

3.1.2 32 位的变量循环左移 s 位的编程实现

对于循环移位ROTL或ROTR，定义“宏”：

#define rotlFixed _lrotl

#define rotrFixed _lrotr

对于VC提供的_lrotl及_lrotr函数，实现过程是通过两次算术移位及一次加法（异或、或）运算实现。因此一次循环移位需要调用3次基本指令实现。

对于w位的循环移位，即：

算术左移位 $SHL^n(x)=x<<n$（移位后，低位补0）

算术右移位 $SHR^n(x)=x>>n$（移位后，高位补0）

循环右移位 $ROTR^n(x)=(x>>n) \vee (x<<w-n)$

循环左移位 $ROTL^n(x)=(x<<n) \vee (x>>w-n)$

3.1.3 模 2^{32} 加法

直接将变量类型声明为unsigned int，其中+运算即“模2^{32}加法”。

注：对于x86处理器，如Intel或AMD的主流CPU，基本的比特逻辑与、或、非、异或以及32位字加法（模2^{32}加法）、64位字加法（模2^{64}加法，需要64位CPU及OS支持）、算术移位SHR或SHL，需要1条指令实现；相应的C语言提供了基本运算符。

综上所述， SM3算法使用的全部是简单运算，执行效率高。

思考：试统计单步SM3算法的各个运算次数和总基本指令数。

3.2 生日碰撞实验（必做题）

收集你熟悉的亲朋好友的生日并比较，尝试找出生日相同的人。记录找到第一对生日相同时尝试的人数n。将具体实验数据与下表中理论估计值进行对比。

	单向性	抗弱碰撞	抗强碰撞
攻击类型	原像攻击	第二原像攻击	碰撞攻击
q次尝试后的成功概率	$\varepsilon = 1-(1-\frac{1}{N})^q$	$\varepsilon = 1-(1-\frac{1}{N})^q$	$\varepsilon = 1-\prod_{i=1}^{q-1}(\frac{N-i}{N})$
计算复杂度	$O(2^n)$	$O(2^n)$	$O(2^{n/2})$

n	生日不重复的概率	n	生日不重复的概率	n	生日不重复的概率	n	生日不重复的概率	n	生日不重复的概率
1	1.000000	11	0.858859	21	0.556312	31	0.269545	41	0.096848
2	0.997260	12	0.832975	22	0.524305	32	0.246652	42	0.085970
3	0.991796	13	0.805590	23	0.492703	33	0.225028	43	0.076077
4	0.983644	14	0.776897	24	0.461656	34	0.204683	44	0.067115
5	0.972864	15	0.747099	25	0.431300	35	0.185617	45	0.059024
6	0.959538	16	0.716396	26	0.401759	36	0.167818	46	0.051747
7	0.943764	17	0.684992	27	0.373141	37	0.151266	47	0.045226
8	0.925665	18	0.653089	28	0.345539	38	0.135932	48	0.039402
9	0.905376	19	0.620881	29	0.319031	39	0.121780	49	0.034220
10	0.883052	20	0.588562	30	0.293684	40	0.108768	50	0.029626

四、实验结果与数据处理

<table>
<tr><td colspan="2">五、分析与讨论</td></tr>
<tr><td>六、教师评语

签名：
日期：</td><td>成绩</td></tr>
</table>