Project 3: implement length extension attack for SM3, SHA256, etc

长度扩展攻击

已知消息M的哈希值及M的长度 进行消息的填充以实现长度扩展攻击

具体做法如下：

1.将消息M的哈希值作为初始IV输入 任意消息x作为明文 求此种情况下的哈希值

2.不改变初始IV输入 将M||len（M）||X作为明文 求此种情况下的哈希值

3.由于上述两种情况最终填充的结果不同，故二者最终的结果不同，但可将中间过程展开发现有一部分是相同的

SM3的长度扩展攻击

实验过程

M： Wang Lei 202000141016 长度为 168 bits

M‘: length_extension_attack 长度为 184 bits

将M||padding||len（M）||M’作为函数的输入，得到输出哈希值

由于此时的M长度较少，实际做哈希时只走了一轮，故填充只需将sm3_calc函数中的长度扩展部分重现即可，之后将M‘拼接到M||len(M)后一并输入sm3函数，实现代码如下：

```
    unsigned char input[256] = "Wang Lei 202000141016";
    unsigned int bitLen=21*8;
    if (IsLittleEndian())
        ReverseMessage(&bitLen);
    input[21] = 0x80;
    memset(input + 21 + 1, 0, 64 - 21 - 1 - 8 + 4);
    memcpy(input + 64 - 4, &bitLen, 4);
    //cout << input << endl;
    unsigned char attack[256] = "length_extension_attack";
    //int ilen = 23;
    memcpy(input + 64, attack, 23);
    int ilen = 87;
```

得到哈希值：

CDB5FE10 DBC3685A F5D83A7A B19146C1 2ADB3DDB C0F6DFD8 45013C6F 05CF1FB5

```
Wang Lei 202000141016€
69626535  1813167948  605421470  1800692868  3952684674  4028095018  2849635751  2099691493
length_extension_attack€
3451256336  3687016538  4124588666  2979088065  719011291  3237404632  1157708911  97460149
Hash:
CDB5FE10 DBC3685A F5D83A7A B19146C1 2ADB3DDB C0F6DFD8 45013C6F 05CF1FB5
```

得到消息M的哈希值为message:

04266AA7 6C12BF4C 2415FF9E 6B546484 EB992E82 F017DA2A A9D9FDA7 7D26BFE5

此哈希值与上一张图片中的第二行数字的十六进制表示一致，故上文结果无误；

```
message:
Wang Lei 202000141016

Hash:
04266AA7 6C12BF4C 2415FF9E 6B546484 EB992E82 F017DA2A A9D9FDA7 7D26BFE5
```

将此哈希值作为初始IV进行长度扩展攻击(需要在SM3_basic.cpp文件中改变SM3Init()函数)

得到如下结果：

```
message:
length_extension_attack€

压缩消息前
 4266AA7 6C12BF4C 2415FF9E 6B546484 EB992E82 F017DA2A A9D9FDA7 7D26BFE5
压缩消息后:
 CDB5FE10 DBC3685A F5D83A7A B19146C1 2ADB3DDB C0F6DFD8 45013C6F 5CF1FB5
€
压缩消息前
 CDB5FE10 DBC3685A F5D83A7A B19146C1 2ADB3DDB C0F6DFD8 45013C6F 5CF1FB5
压缩消息后:
 68CBB189 5A74DB0B 3957CCE4 F6BD383B 4728C991 282D7090 4E81416B 2FAFD964
Hash:
68CBB189 5A74DB0B 3957CCE4 F6BD383B 4728C991 282D7090 4E81416B 2FAFD964
```

分析如下

第一种情况下，M是21个字节，求M的哈希后M||padding共64个字节，将23个字节M'拼接到其后，消息总共87个字节，故最终填充后的字节长度为87；

第二种情况下，得到了M的哈希值作为初始IV，但M'的消息只有23个字节，故最终填充的字节长度与第一种情况不同，二者最终的哈希值不应相同，但若将M'进行填充输出M的哈希值作为初始IV的SM3函数，其中间结果与第一种情况的哈希值相同。