**密码学原理与实践**

**实验-2-密码执行(3)**

**学院名称 智能与计算学部**

**专 业 网络空间安全**

**学生姓名 石子跃**

**学 号 3020244294**

**年 班 级 2020级1班**

**2022年 10 月 29 日**

## 实验问题-6-研究Shamir窍门和扩展Shamir窍门的效率优势

## 1.1实验原理





## 1.2 实验要求

**研究Shamir窍门和扩展Shamir窍门的效率优势**

要求：计算多模幂，并统计用Shamir窍门和扩展Shamir窍门时需要的乘法次数。

输入：g, h, a, b, p<=232

输出：gahb(mod p)；Shamir窍门需要的乘法次数m，扩展Shamir窍门需要的乘法次数n (统计初始计算的乘法)

## 1.3关键技术的程序实现方法与代码

#### 算法1 Shamir窍门

1. ul\_64 Shamir(ul\_64 g,ul\_64 h,ul\_64 a,ul\_64 b,ul\_64 p,int & m){
2. m = 0;
3. ul\_64 gh = g\*h;
4. m++;
5. ul\_64 A = 1;
6. ul\_64 ai,bi;
7. int t = get\_L(a)>get\_L(b)?get\_L(a):get\_L(b);
8. for(int i = t;i>=0;i--){
9. if(i!= t){
10. *// A = A\*A;*
11. A = mod2(A,A,p);
12. m++;
13. }
14. ai = (a>>i)&1;
15. bi = (b>>i)&1;
16. if(ai!=0||bi!=0){
17. if(ai!=0 && bi==0)
18. { *//A = A\*g;*
19. A = mod2(A,g,p);
20. m++;}
21. else if(bi!=0 && ai==0){
22. *//A = A\*h;*
23. A = mod2(A,h,p);
24. m++;}
25. else {
26. *//A = A\*g\*h;*
27. A = mod2(A,gh,p);
28. m++;}
29. }
30. }
31. return A;
32. }

#### 扩展Shamir窍门

1. ul\_64 exp\_Shamir(ul\_64 g,ul\_64 h,ul\_64 a,ul\_64 b,ul\_64 p,int & n){
2. n = 0;
3. int d[64] = {0};
4. int f[64] = {0};
5. int t = NAF(a,d);
6. int t\_b = NAF(b,f);
7. t = t>t\_b?t:t\_b;
8. *// cout<<"wNAF如下:"<<endl;*
9. *// for(int j = t;j>=0;j--){*
10. *//     cout<<d[j]<<" ";*
11. *// }cout<<endl;*
12. *// cout<<"wNAF如下:"<<endl;*
13. *// for(int j = t;j>=0;j--){*
14. *//     cout<<f[j]<<" ";*
15. *// }cout<<endl;*
16. float g\_1 = 1/g, h\_1 = 1/h, g\_1h = h/g, gh\_1 = g/h, g\_1h\_1 = 1/(g\*h), gh = g\*h;
17. n = n+4;
18. ul\_64 A = 1;
19. for(int i = t;i>=0;i--){
20. *// cout<<A<<endl;*
21. if(i!=t){ A = mod2(A,A,p);n++;}
22. if(d[i]!=0||f[i]!=0){
23. *// cout<<"12"<<endl;*
24. if(d[i]==0&&f[i]==1){A = A\*h;n++;}
25. else if(d[i]==0&&f[i]==-1){A = A\*h\_1;n++;}
26. else if(d[i]==1&&f[i]==1){A = A\*gh;n++;}
27. else if(d[i]==1&&f[i]==0){A = A\*g;n++;}
28. else if(d[i]==1&&f[i]==-1){A = A\*g/h;n++;}
29. else if(d[i]==-1&&f[i]==-1){A = A/g/h;n++;}
30. else if(d[i]==-1&&f[i]==0){A = A/g;n++;}
31. else if(d[i]==-1&&f[i]==1){A = A\*g/h;n++;}
32. }
33. }
34. return A;
35. }

## 1.4数据测试结果

