**Key Exchange**

1. **Diffie:**

**Program:**

import java.util.\*;

import java.lang.\*;

import java.math.\*;

public class diffie

{

public static BigInteger power(BigInteger a,int b,BigInteger p)

{

if(b==1)

return a;

else

return (a.pow(b)).mod(p);

}

public static void keygen()

{

Scanner sc=new Scanner(System.in);

int b,i,a;

BigInteger x,y,ka,kb,g,p;

System.out.println("Enter p");

p=sc.nextBigInteger();

System.out.println("Enter g");

g=sc.nextBigInteger();

System.out.println("Enter a");

a=sc.nextInt();

x=power(g,a,p);

System.out.println("Enter b");

b=sc.nextInt();

y=power(g,b,p);

ka=power(y,a,p);

System.out.println("Alice:");

System.out.println("Private Key : "+a);

System.out.println("Computed public key : "+x);

System.out.println("Shared Secret : "+ka);

kb=power(x,b,p);

System.out.println("Bob:");

System.out.println("Private Key : "+b);

System.out.println("Computed public key : "+y);

System.out.println("Shared Secret : "+kb);

}

public static void main(String[] args)

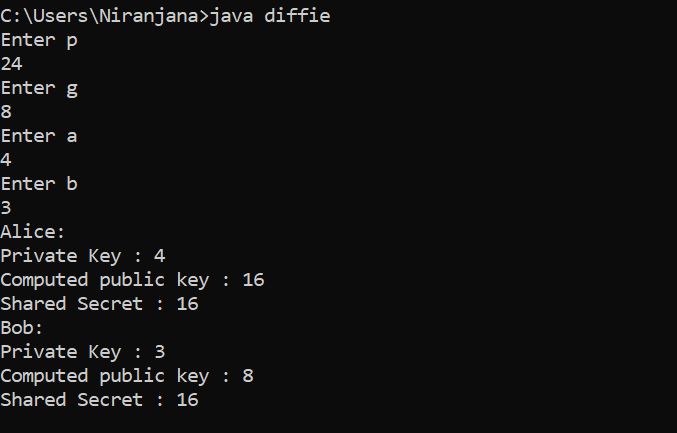
{

keygen();

}

}

**ScreenShot:**



1. **Elgamal:**

**Program:**

import java.util.\*;

import java.lang.\*;

import java.math.\*;

public class elgamal

{

public static BigInteger power(BigInteger a,int b,BigInteger p)

{

if(b==1)

return a;

else

return (a.pow(b)).mod(p);

}

public static void keygen()

{

Scanner sc=new Scanner(System.in);

int b,i,xa;

BigInteger x,y,ka,kb,q,a;

System.out.println("Enter q");

q=sc.nextBigInteger();

System.out.println("Enter a");

a=sc.nextBigInteger();

System.out.println("Enter xa");

xa=sc.nextInt();

x=power(a,xa,q);

System.out.println("Enter k");

b=sc.nextInt();

y=power(x,b,q);

BigInteger c1,c2,m;

c1=power(a,b,q);

System.out.println("Enter M");

m=sc.nextBigInteger();

c2=(m.multiply(y)).mod(q);

System.out.println("Alice:");

System.out.println("K : "+y);

System.out.println("C1 : "+c1);

System.out.println("C2 : "+c2);

ka=power(c1,xa,q);

kb=ka.modInverse(q);

BigInteger m2;

m2=(c2.multiply(kb)).mod(q);

System.out.println("Bob:");

System.out.println("K : "+ka);

System.out.println("K inv : "+kb);

System.out.println("M : "+m2);

}

public static void main(String[] args)

{

keygen();

}

}

**ScreenShot:**

