DH Key Generation:

```
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.PrivateKey;
import java.security.PublicKey;

public class KeyPairGen{
  public static void main(String args[]) throws Exception{
    KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("DH");

    keyPairGen.initialize(2048);

    KeyPair pair = keyPairGen.generateKeyPair();

    PrivateKey privKey = pair.getPrivate();

    PublicKey publicKey = pair.getPublic();
    System.out.println("Keys generated");
    System.out.println(publicKey);
  }
}
```

```
shankar@shankar-ThinkPad-L450:~/Documents/AU/sem6/security/lab/week10$ java KeyPairGen.java
Keys generated
SunJCE Diffie-Hellman Public Key:
y:
    d6954e2c 0b342d74 4c5c31cf bef3618d 3d219580 f76b87b3 fd6a7690 cb618917
    6b10ff26 b9036c70 3a1fd08d 2be94093 28167ced 89a60753 a608cef3 9dfe2ee2
    3245a1ca b0147872 1fcc1287 378de133 c3c4508d 695b330c 0060143d 4e96c658
    a70023c6 b1f637a4 c7f6876c c7c1b71e fab7b1c5 f05f7900 87a0e4cf 4ff368d2
    f932f720 a83f2f2f 4582b7b5 c117fc26 26e15807 362114de 21960157 fcaed143
    21e5a30e bf355ff4 89016f32 661d5bcb a282f3e5 10edb2ea 4979c29a c8c95f82
    1b333694 a897f646 fcf616b5 5e41ccd0 70f62b9e 52404516 2876b4ac 71b16349
    abfbb7f4 fdc31544 6e4b86da 0948f189 fbc453b0 06744c01 4368b43d 2c79b32b
p:
    ffffffff ffffffff c90fdaa2 2168c234 c4c6628b 80dc1cd1 29024e08 8a67cc74
    020bbea6 3b139b22 514a0879 8e3404dd ef9519b3 cd3a431b 302b0a6d f25f1437
    4fe1356d 6d51c245 e485b576 625e7ec6 f44c42e9 a637ed6b 0bff5cb6 f406b7ed
    ee386bfb 5a899fa5 ae9f2411 7c4b1fe6 49286651 ece45b3d c2007cb8 a163bf05
    98da4836 1c55d39a 69163fa8 fd24cf5f 83655d23 dca3ad96 1c62f356 208552bb
    9ed52907 7096966d 670c354e 4abc9804 f1746c08 ca18217c 32905e46 2e36ce3b
    e39e772c 180e8603 9b2783a2 ec07a28f b5c55df0 6f4c52c9 de2bcbf6 95581718
    3995497c ea956ae5 15d22618 98fa0510 15728e5a 8aacaa68 ffffffff ffffffff
g:
    02
l:
    1024
```

DSA KEY GENERATION:

```
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.PrivateKey;
import java.security.PublicKey;

public class KeyPairGen{
   public static void main(String args[]) throws Exception{
      KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("DSA");

      keyPairGen.initialize(2048);

      KeyPair pair = keyPairGen.generateKeyPair();

      PrivateKey privKey = pair.getPrivate();

      PublicKey publicKey = pair.getPublic();
      System.out.println("Keys generated");
      System.out.println(publicKey);
   }
}
```

```
shankar@shankar-ThinkPad-L450:~/Documents/AU/sem6/security/lab/week10$ java KeyPairGen.java
Keys generated
Sun DSA Public Key
    Parameters:
    p:
    8f7935d9 b9aae9bf abed887a cf4951b6 f32ec59e 3baf3718 e8eac496 1f3efd36
    06e74351 a9c41833 39b809e7 c2ae1c53 9ba7475b 85d011ad b8b47987 75498469
    5cac0e8f 14b33608 28a22ffa 27110a3d 62a99345 3409a0fe 696c4658 f84bdd20
    819c3709 a01057b1 95adcd00 233dba54 84b6291f 9d648ef8 83448677 979cec04
    b434a6ac 2e75e998 5de23db0 292fc111 8c9ffa9d 8181e733 8db792b7 30d7b9e3
    49592f68 09987215 3915ea3d 6b8b4653 c633458f 803b32a4 c2e0f272 90256e4e
    3f8a3b08 38a1c450 e4e18c1a 29a37ddf 5ea143de 4b66ff04 903ed5cf 1623e158
    d487c608 e97f211c d81dca23 cb6e3807 65f822e3 42be484c 05763939 601cd667
    q:
    baf696a6 8578f7df dee7fa67 c977c785 ef32b233 bae580c0 bcd5695d
    g:
    16a65c58 20485070 4e7502a3 9757040d 34da3a34 78c154d4 e4a5c02d 242ee04f
    96e61e4b d0904abd ac8f37ee b1e09f31 82d23c90 43cb642f 88004160 edf9ca09
    b32076a7 9c32a627 f2473e91 879ba2c4 e744bd20 81544cb5 5b802c36 8d1fa83e
    d489e94e 0fa0688e 32428a5c 78c478c6 8d0527b7 1c9a3abb 0b0be12c 44689639
    e7d3ce74 db101a65 aa2b87f6 4c6826db 3ec72f4b 5599834b b4edb02f 7c90e9a4
    96d3a55d 535bebfc 45d4f619 f63f3ded bb873925 c2f224e0 7731296d a887ec1e
    4748f87e fb5fdeb7 5484316b 2232dee5 53ddaf02 112b0d1f 02da3097 3224fe27
    aeda8b9d 4b2922d9 ba8be39e d9e103a6 3c52810b c688b7e2 ed4316e1 ef17dbde

  y:
    84f10a2a 8ce0ee94 3506409d 0f069b62 de7a8356 ef2961e5 cc0c708b 93e25d3f
    1fe75e1e 9bf04453 89211aae a7596a2d bcf8db85 49586109 f37570bd 09bef546
    0b459b72 75a066c5 ba2800c5 c1061be8 713df405 250542d5 0d491710 0b88a2f2
    fa5587aa 608b475f 1940a621 b84787bb b75453bc 3069b1d7 7e361bf4 77552698
    d4ce73cc b9b8092d 954b80c7 39cdf099 f3361c77 4a9d624d 5076b56e ef3f8da8
    c57380cc e4e14aa0 db4be155 b733f491 553c5bea 3ffe9e7e 09569f11 5a56ec53
    b1ca6c5e 2df2eb99 e52538f8 4a545541 e44e10f7 85242e44 145c950c 22e620dc
    13eebfce 8fcc14cf c73b915f 9a36071e 7718a3a3 6666a194 603644dc 8bc82f95
```

RSA Key Generation:

```
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.PrivateKey;
import java.security.PublicKey;

public class KeyPairGen{
  public static void main(String args[]) throws Exception{
    KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("RSA");

    keyPairGen.initialize(2048);

    KeyPair pair = keyPairGen.generateKeyPair();

    PrivateKey privKey = pair.getPrivate();

    PublicKey publicKey = pair.getPublic();
```

```
        System.out.println("Keys generated");
        System.out.println(publicKey);
    }
}
```

```
shankar@shankar-ThinkPad-L450:~/Documents/AU/sem6/security/lab/week10$ java KeyPairGen.java
Keys generated
Sun RSA public key, 2048 bits
  params: null
  modulus: 27368523523606147834003769551774698108936564021676689590283504550921532850320751354762677999989964648289042349935468682309204714066964538616803860322326603050553366506170699120486708742946938178817876077413097322768895428551647452161777828987718806007645239503267035226372542071502384874447117184890985018049610028282841579160799128191489386490833850296219740599869013565409818110177569515224477846325804906082385357154715462401722331041977147331189673534073626392064569209448422907693954044680181903258280457901557476698593556375667081790821740097792366372054403937953661632260804404936582374351829842184077408635181
  public exponent: 65537
```