Part3

Part3a

```
import java.io.Console;
import javax.xml.bind.DatatypeConverter;
import java.security.*;
import java.io.*;
import java.util.*;

public class Part3{

    public static void main(String []args){


     try {

            Console c = System.console();

            SecureRandom salt = new SecureRandom();
            byte[] salt_bytes = new byte[16];
            salt.nextBytes(salt_bytes);

            MessageDigest md = MessageDigest.getInstance("MD5");
            md.update(salt_bytes);

            String sl = DatatypeConverter.printHexBinary(salt_bytes);
            c.printf(sl);

       }
```

```
    catch(NoSuchAlgorithmException ex){
          // if any error occurs
      ex.printStackTrace();
    }
    catch(Exception ex) {
      // if any error occurs
      ex.printStackTrace();
    }
   }
}
```

Part3b

```
import java.io.Console;
import java.io.IOException;
import java.security.*;
import java.io.ByteArrayOutputStream;
import javax.xml.bind.DatatypeConverter;

import java.util.*;

public class Lab4Class {
   public static void main(String[] args) {

          Console console = System.console();

          if( console == null ) {
              System.out.print("Console unavailable");
             return;
          }
```

```
String password = console.readLine("Enter password:");

try {
        SecureRandom salt = new SecureRandom();
        int salt_len = 16;
        byte salt_bytes[] = new byte[salt_len];
        salt.nextBytes(salt_bytes);

        ByteArrayOutputStream data_to_hash = new ByteArrayOutputStream();
        data_to_hash.write(salt_bytes,0,salt_len);
        data_to_hash.write(password.getBytes());

        MessageDigest md = MessageDigest.getInstance("MD5");

        md.update(data_to_hash.toByteArray());

        byte[] digest = md.digest();
        String hash_pwd = DatatypeConverter.printHexBinary(digest).toUpperCase();

        String salt_str = DatatypeConverter.printHexBinary(salt_bytes).toUpperCase();

        console.printf("Storing into db hash:" + hash_pwd);
        console.printf("\n");
        console.printf("Storing into db salt:" + salt_str);
        console.printf("\n");

} catch (NoSuchAlgorithmException e) {
        System.out.print("MD5 not supported for some reason");
```

```
                return;
            } catch (IOException e) {
              System.out.print("Could not prepare data for hashing");
              return;

            }

    }

}
```