import java.nio.charset.StandardCharsets;

import java.security.MessageDigest;

import java.security.NoSuchAlgorithmException;

import java.security.SecureRandom;

/\*\*

\*

\* @author Shubham Khedaskar

\*/

public class salting {

public static SecureRandom random = new SecureRandom();

public static void main(String[] args) {

String password1 = "shubham";

String password2 = "secret1234";

MessageDigest md, md1;

try{

// Select the message digest for the hash computation -> SHA-256

md = MessageDigest.getInstance("SHA-256");

// Generate the random salt

byte[] salt1 = new byte[16];

salt1 = getSalt();

System.out.println("salt: "+salt1);

// Passing the salt to the digest for the computation

md.update(salt1);

// Generate the salted hash

byte[] hashedPassword1 = md.digest(password1.getBytes(StandardCharsets.UTF\_8));

//converting to string from bytes

StringBuilder sb = new StringBuilder();

for (byte b : hashedPassword1)

sb.append(String.format("%02x", b));

System.out.println("\nsalted hash: "+sb);

md1 = MessageDigest.getInstance("SHA-256");

byte[] salt2 = new byte[16];

salt2 = getSalt();

System.out.println("\nsalt2: "+salt2);

md1.update(salt2);

byte[] hashedPassword2 = md.digest(password2.getBytes(StandardCharsets.UTF\_8));

StringBuilder sb1 = new StringBuilder();

for (byte b2 : hashedPassword2)

sb1.append(String.format("%02x", b2));

System.out.println("\n hash: "+sb1);

}catch(NoSuchAlgorithmException e){

e.printStackTrace();

}

}

private static byte[] getSalt() {

byte[] salt = new byte[16];

random.nextBytes(salt);

return salt;

}

}