Assignment 1
Brute Force Attack Estimation

L. Towell, L.M.Towell@liverpool.ac.uk

November 5, 2019

1 Password List

Below is the password list that I have decided to use for this exercise.

N	Password
1	abc
2	P@ssW0rD
3	Th!$IsAV3ryL0n9pA$$w0rd

2 Salt and Iteration Count

For the purpose of this coursework I have hardcoded the salt used within this program, I have also decided to use an iteration count of 1024. The below table shows the time per run and the average time taken in milliseconds over 5 iterations to encrypt and decrypt the string "This is an example string" using the defined salt and iteration counts.

The below timings have been recorded running the program on a Macbook air with an Intel core i5 processor and 16GB of RAM. Timings on other machines are likely to differ.

Iteration time in milliseconds (ms)			
N	abc	P@ssW0rD	Th!$IsAV3ryL0n9pA$$w0rd
1	155.77	2.45	1.46
2	8.55	1.66	1.19
3	6.27	1.65	1.24
4	12.94	4.0	1.25
5	1.57	2.01	2.69
Average	7.33	2.35	1.57
The first iteration of abc has been omitted from the average			

3 Brute Force Attack Estimation

Given that it is specified that the attacker knows the salt, iteration count, encryption type, input string and cipher text used to encrypt the input string then the only piece of information the attacker would need to find is the password used to encrypt the string. In order to work out the password using a Brute force attach the attacker is going to have to iterate through each possible character that could be used in each different combination.

If we presume that passwords are made of uppercase, lowercase numbers and special characters and they are limited to traditional ASCII encoded characters then this gives the attacker a possible 95 characters for each character in the password. The equation for working out a password via brute force attack is therefore 95^n where n is the number of characters within the password. The table below shows the amount of possible combinations for N character lengths.

Number of characters	Possible password combinations
1	95
2	9025
3	857375
4	81450625
5	7737809375
6	735091890625
7	69833729609375
8	6634204312890620
9	630249409724609000
10	59873693923837900000
15	463291230159753000000000000000
20	35848592240854200000000000000000000000
23	3073568677250240000000000000000000000000000000
25	277389573121834000000000000000000000000000000000

In order to estimate the time taken to brute force an attack we need to look at the time taken to iterate through every combination possible considering that in the worse case the last combination will be the password we are attempting to discover. the calculation for estimating time taken to discover a password is therefore the time taken to try one password (one iteration) mutliplied by the number of possible combinations. For example if we say the time taken for 1 iteration is 1ms then we can assume that it would take in the worst case to crack a 3 character password (abc) which would be 95^3 (857375 combinations) * the taken to complete one iteration e.g. 1ms per attempt would take 857375ms or 857.375 seconds or 14.3 minutes.

The image 1 is a table of times taken to

4 How Does Iteration Count Affect Brute Force Timing?

What does iteration count mean?

What is the maximum value of iteration count?

5 Brute Force Attack Estimation Without Known Iteration Count

Essentially if a hacker does not know the iteration count of an application then they have to try the same brute force attack multiple times for multiple iteration counts which essentially means that the time taken grows exponentially. E.g. If the iteration count was 300 and the hacker started their hack attempt with an iteration count of 1 they would have to work out the characters in the password $95^n * i$ where i is the number of iterations needed to reach the one initially used when hashing the password.

6 Comparison with Online Services

Password	My Estimation	Online Estimation
abc	400 ns	1
P@ssW0rD	?	9 hrs
Th!$IsAV3ryL0n9pA$$w0rd	1	19 Septillion Years

Appendices

A Password Encryption & Decryption Program

```
import javax.crypto.Cipher;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.PBEKeySpec;
import javax.crypto.spec.PBEParameterSpec;

import java.math.BigDecimal;
import java.math.RoundingMode;
import java.security.Key;

/**
 * Example of using Password-based encryption
 */

public class PasswordBasedEncryption {
    public static void main(String[] args) throws Exception {
        // setup iteration count
        int iterationCount = 5;

        // Setup passwords used to encrypt values

        String[] passwords = new String[] { "abc", "P@ssW0rD", "Th!$IsAV3ryL0n9pA$$w0rd" };
        System.out.println("Password based encryption timings");

        for (int i = 0; i < passwords.length; i++) {
            System.out.println("------------------------------");
            // initialise time array
            double[] time = new double[6];
            System.out.println("Password used: " + passwords[i]);

            for (int j = 0; j < iterationCount; j++) {
                PBEKeySpec pbeKeySpec;
                PBEParameterSpec pbeParamSpec;
                SecretKeyFactory keyFac;
                // start timing
                long startTime = System.nanoTime();
                // Salt
                byte[] salt = { (byte) 0xc7, (byte) 0x73, (byte) 0x21, (byte) 0x8c, (byte) 0x7e,
                    (byte) 0xc8,
                        (byte) 0xee, (byte) 0x99 };

                // Iteration count
                int count = 1024;

                // Create PBE parameter set
                pbeParamSpec = new PBEParameterSpec(salt, count);

                // Initialization of the password
                char[] password = passwords[i].toCharArray();

                // Create parameter for key generation
                pbeKeySpec = new PBEKeySpec(password);

                // Create instance of SecretKeyFactory for password-based encryption
                // using DES and MD5
                keyFac = SecretKeyFactory.getInstance("PBEWithMD5AndDES");

                // Generate a key
                Key pbeKey = keyFac.generateSecret(pbeKeySpec);
```

```
            // Create PBE Cipher
            Cipher pbeCipher = Cipher.getInstance("PBEWithMD5AndDES");

            // Initialize PBE Cipher with key and parameters
            pbeCipher.init(Cipher.ENCRYPT_MODE, pbeKey, pbeParamSpec);

            // Our plaintext
            byte[] cleartext = "This is an example string".getBytes();

            // Encrypt the plaintext
            byte[] ciphertext = pbeCipher.doFinal(cleartext);
            System.out.println("Cipher text: " + Utils.toHex(ciphertext));

            pbeCipher.init(Cipher.DECRYPT_MODE, pbeKey, pbeParamSpec);

            // Decrypt the plaintext
            byte[] ciphertext2 = pbeCipher.doFinal(ciphertext);
            String plainText = new String(ciphertext2);

            // end time
            long endTime = System.nanoTime();

            // calculate total time and add to the time array
            long totalTime = endTime - startTime;

            double totalTimeMs = totalTime / 1000000.0;
            BigDecimal totalTimeMsRounded = new BigDecimal(totalTimeMs).setScale(2,
                RoundingMode.HALF_EVEN);
            double roundedTotalTime = totalTimeMsRounded.doubleValue();
            time[j] = roundedTotalTime;

            // output of all times and key components of the encryption algorithm
            System.out.println("Decrypted text: " + plainText);
            System.out.println("loop " + (j + 1) + ": " + roundedTotalTime + "ms");
        }
        // summed time calculation to output average over the iteration counts.
        double summedTime = 0;
        for (var k = 0; k < time.length; k++) {
            summedTime += time[k];
        }

        // Work out and print the average time for each password

        System.out.println("Total time:" + new BigDecimal(summedTime).setScale(2,
            RoundingMode.HALF_EVEN));
        double avgTime = summedTime / iterationCount;
        System.out.println("average time:" + new BigDecimal(avgTime).setScale(2,
            RoundingMode.HALF_EVEN));

    }
  }
}
```

B Output of Appendix A when ran in terminal

```
Password based encryption timings
-----------------------------
Password used: abc
Cipher text: c4d03d30be1dfdd3c5ace92ebe5bacb959c80a9e9213a21dd5615cf275e8688f
Decrypted text: This is an example string
loop 1: 117.31ms
Cipher text: c4d03d30be1dfdd3c5ace92ebe5bacb959c80a9e9213a21dd5615cf275e8688f
Decrypted text: This is an example string
loop 2: 1.56ms
Cipher text: c4d03d30be1dfdd3c5ace92ebe5bacb959c80a9e9213a21dd5615cf275e8688f
Decrypted text: This is an example string
loop 3: 2.09ms
Cipher text: c4d03d30be1dfdd3c5ace92ebe5bacb959c80a9e9213a21dd5615cf275e8688f
Decrypted text: This is an example string
loop 4: 1.96ms
Cipher text: c4d03d30be1dfdd3c5ace92ebe5bacb959c80a9e9213a21dd5615cf275e8688f
Decrypted text: This is an example string
loop 5: 2.32ms
Total time:125.24
average time:25.05
-----------------------------
Password used: P@ssW0rD
Cipher text: b639839be3610610478c09998f8ede508799d641f60110840dd59b2e0790b125
Decrypted text: This is an example string
loop 1: 2.11ms
Cipher text: b639839be3610610478c09998f8ede508799d641f60110840dd59b2e0790b125
Decrypted text: This is an example string
loop 2: 2.14ms
Cipher text: b639839be3610610478c09998f8ede508799d641f60110840dd59b2e0790b125
Decrypted text: This is an example string
loop 3: 1.74ms
Cipher text: b639839be3610610478c09998f8ede508799d641f60110840dd59b2e0790b125
Decrypted text: This is an example string
loop 4: 1.67ms
Cipher text: b639839be3610610478c09998f8ede508799d641f60110840dd59b2e0790b125
Decrypted text: This is an example string
loop 5: 1.7ms
Total time:9.36
average time:1.87
-----------------------------
Password used: Th!$IsAV3ryL0n9pA$$w0rd
Cipher text: fffecd4d43d0e33255d4c82f86a71f235257be392215d5f1aa9a33a14b884e51
Decrypted text: This is an example string
loop 1: 1.7ms
Cipher text: fffecd4d43d0e33255d4c82f86a71f235257be392215d5f1aa9a33a14b884e51
Decrypted text: This is an example string
loop 2: 1.67ms
Cipher text: fffecd4d43d0e33255d4c82f86a71f235257be392215d5f1aa9a33a14b884e51
Decrypted text: This is an example string
loop 3: 1.64ms
Cipher text: fffecd4d43d0e33255d4c82f86a71f235257be392215d5f1aa9a33a14b884e51
Decrypted text: This is an example string
loop 4: 1.62ms
Cipher text: fffecd4d43d0e33255d4c82f86a71f235257be392215d5f1aa9a33a14b884e51
Decrypted text: This is an example string
loop 5: 1.6ms
Total time:8.23
average time:1.65
```