Elijah Andrushenko

09/19/2018

CPTS 427

Computer Security

Project 1

1.

A)

Log2(26^10) = 47

B)

67^8 = 48

C)

35 characters or 29 characters if upper case letters and non-alphabetic characters are used.

2.

Salts are helpful if a user wants to break many passwords since a random number is generated which makes it harder to track patterns in hashes.

3.

The 8 bit salt is easier to crack. Salts need to be unique thus a 32 bit salts is more likely to be unique compared to an 8 bit salt. An extreme example would be a 1 bit salt leaving you with either 1 or a 0 which is easy to guess and half the hashes would have the same salt. A 32 bit salt is much less likely to repeat if ever. Thus bigger salts are better.

4.

**DES** – block size is 40 and **AES** - block size is 48

5.

Openssl enc aes-128-ecb –d –message\_aes.enc –out test.txt

6.

No, because the cipher changes everytime the text in the file changes, therefore we can tell when changes to the file were made. Thus something was revealed in the cipher text.

7.

HMAC - 261fa267eea73ebac39e0b5ef989f36d1efd055d

HMAC (modified message.txt) – 2f81ff70758c8c783f803a456378219d1ddf6afb

HMAC (modified key) – 6f0e9d302ca0d0340404f9134e6169439fb80139

8.

ID: user1  
salt: LGOwUL7Q  
hash: mL/PgOcBwL94Jgg23tOBzX/zcaCMz4Px3qEYkcxHNVMOvIh9rMoprGyzzSmthsZ7bU4cXtdiTO5KVc5XqzcCy1  
ID: user2  
salt: CL5Fr2bN  
hash: IqeNKKpHYpih2mDgM6PVb4FpGnFHrnqu13bZVuDwv/108cjSH3VC613TkaQuTob8f6cZa2Qu8m7.VSdFIJD2z0  
ID: user3  
salt: Un/lqxkl  
hash: DErbxGi3vi9Q/iN36bvx7DEsx20xd1Zy0E2sSJ4/orFuNcL2FOKEgM/4xlYx3FZlXbg8nBoQgnQqcukhibH1J0  
ID: user4  
salt: Lx2zrG31

hash: pxnT3hv9w7EEp2Db0AaHPm6/C0DgD/GykGgjkYNUwCjZlZYE0Me69X/msH/br69lHJ4i71p4xU5/zNCizFWEJ.  
ID: user5  
salt: 6R1eYOtL  
hash: FqPV2vncS7I29cF2ZJL99Zl09uniaERmIzCEdgMeL/lWEQJA54M.fjAmRnocc.48WbcC9D3LR/7/rYXlFmMXW.

9.

See the code posted with this Word Document

10.

User1 – Bacon

User2 - Batman