Jeff Kremer
11524078
CptS 427
Homework 3

General Questions (Part 1)

1. Password Entropy
   a) log2(26) * 10 = 4.7 * 10 = 47 bits of entropy
   b) log2(67) * 8 = 6 .1 * 8 = 48.8 ~ 49 bits of entropy
   c) log2(10) * 6 = 3.32 * 6 = 19.92 ~ 20 bits of entropy
   d) Human- Based entropy to == 49 bits of entropy
      I. first character = 4 bits; total entropy = 4 bits, total chars = 1
      II. next 7 characters = 2 per character; total entropy = 18 bits, total chars = 8
      III. chars 9 – 20 = 1.5 per character; total entropy = 34.5 bits, total chars = 20
      IV. chars 21+ = 1 bit per char; total entropy = 49.5 bits, total chars = 35
      V. assuming all lowercase chararcters: **35 characters to be equivalent to b)**
      VI. Assuming uppercase and special characters: (+6 entropy): **29 characters**

2. A salt is random data that is used in addition to a password when generating a password hash. Hashes do not need to be memorized, and thus dramatically increase the size of a hash table required to succesfully brute force a password, without placing additional burdens on the users.

3. System A will be much easier to crack, as 256 rainbow tables will be required to account for all salts. This is less than the Unix 12-bit salts. System B's 32-bit salt is not feasible to crack using rainbow tables due to requiring 2^32 full rainbow tables, the amount of storage to be required for this is extremely large.

4. V does not provide a random value to C to randomize the signed hash. An Eavesdropper or Man-in-the-middle could read/intercept the response, and in the future log into the system because the signed hash C sends to V never changes.

Code Questions (Part 2)

5. User Salts and Hashes:

User	Salt	Hash
user1	LGOwUL7Q	mL/PgOcBwL94Jgg23tOBzX/zcaCMz4Px3qEYkcxHNVMOvIh9rMoprGyzzSmthsZ7bU4cXtdiTO5KVc5XqzcCy1
user2	CL5Fr2bN	IqeNKKpHYpih2mDgM6PVb4FpGnFHrnqu13bZVuDwv/108cjSH3VC613TkaQuTob8f6cZa2Qu8m7.VSdFIJD2z0
user3	Un/lqxkl	DErbxGi3vi9Q/iN36bvx7DEsx20xd1Zy0E2sSJ4/orFuNcL2FOKEgM/4xlYx3FZlXbg8nBoQgnQqcukhibH1J0
user4	Lx2zrG31	pxnT3hv9w7EEp2Db0AaHPm6/C0DgD/GykGgjkYNUwCjZlZYE0Me69X/msH/br69lHJ4i71p4xU5/zNCizFWEJ.
user5	6R1eYOtL	FqPV2vncS7I29cF2ZJL99Zl09uniaERmIzCEdgMeL/lWEQJA54M.fjAmRnocc.48WbcC9D3LR/7/rYXlFmMXW.

6. Programming Portion

7. Results from Sample Files

User	Word
user1	Bacon
user2	Batman
user4	Washington
user5	Spokane