

choose one: Received Received help from:
(or more) no help Collaborated with: _____

Homework: /SI110/Models and Tools/Hashing & Digital Cryptography

1. Suppose I have a secret string *S*, and you have a scrambled Rubik's Cube that is the hash of *S*. So all you know is what the hashed cube looks like. Explain what you would have to do in order to find a string that hashes to the same value as *S*?

10/8/6/0

2. Why is it better to store usernames and hashes-of-passwords on a system, rather than usernames and passwords?

15/12/9/0

3. In the context of hashes and passwords (as opposed to spices), what is *salt*?

10/8/6/0

4. Read the notes and pay close attention to the Windows version of the **md5** command and how to use it. There are several examples. The md5 hash of the string *fragglерock* is:

10/8/6/0

5. From the in-class password activity: What things should any responsible website do to protect the passwords (and thus the identities) of its users?

15/12/9/0

6. Make up a strong password (something we believe you could actually remember!) and give an explanation for why you believe it's strong - i.e. what good properties does it have?

15/12/9/0

Password: _____	Explanation: _____
-----------------	--------------------

7. When we say "AES encryption with a 128-bit block size" what does *block* mean?

10/8/6/0

8. Read carefully in the notes the section that describes how to use the aes tool. I have encrypted a message for you using 128-bit AES encryption. Decrypt it!

The key is 2a0757a14360d2432f1f5e6ac0359a5d

The ciphertext is 0a2bfea6495bfdeaedacc7a1548735665a4612e7b4ef968f4722882333fbc632

15/12/9/0

The decrypted message (plaintext) is: