SI110 Introduction to Cyber Security AY12S
Technical Foundations

Name: _____

Alpha: _____

Hand in a stapled, printed copy with your answers.

Homework: /SI110/Models and Tools/Cryptographic Hashes & /SI110/Models and Tools/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.

a. Explain why it is impossible to recover S with certainty that what you have is indeed the original secret string S?

b. Explain what you would have to do in order to find a string that hashes to the same value as S?

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

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

4. The *MD5* hash of a string is not a Rubik's Cube, or course, it is a:

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

6. I have encrypted a message for you using 128-bit AES encryption with a key that is the MD5 hash of my secret passphrase. The encrypted message (ciphertext) is: **ba66c97876953863d508777b2f725783**
... and the secret passphrase is: **The Goat is old and gnarly**
What is the plaintext message (i.e. decrypt the ciphertext)?