CS 100 PreLecture 10 - Encryption

HW PRIOR TO LECTURE – All students read two sections in Blown to Bits, Historical Cryptography (starts pages 165-166) Breaking Substitution Ciphers (pages 166-169) and prepare answers for the below questions http://www.bitsbook.com/wp-content/uploads/2008/12/chapter5.pdf

1. How long has the art of cryptography been practiced?

2. Encrypt this message using the Caesar Cipher, as shown on p. 165:
   plaintext: `CS IS COOL`
   ciphertext:

3. A Caesar Cipher is an example of a large class of ciphers known as _____ ciphers.

4. The section called Breaking Substitution Ciphers (p. 166) describes a "random substitution cipher," in which each letter of the alphabet is randomly replaced with a different letter or character i.e. A→T, B→F… What makes a random substitution cipher more secure than a Caesar shift?

5. The reading shows a technique for cracking Chaucer's text, which was encrypted using a basic substitution cipher. That technique, which takes advantage of the fact that certain characters or groups of characters occur more often than others and can be used to crack any substitution cipher, is called: _____ _____.

6. Check the appropriate box: According the reading, a random substitution cipher…

	Is **actually easy** to crack	Is **actually hard** to crack
Looks easy to crack		
Looks hard to crack		

7. **Make a prediction** A Caesar shift cipher is supposedly easier to crack than random substitution. How long do you think it would take *you* to crack a message encrypted with a simple Caesar shift cipher? Note: there is no correct answer here; you're just making a prediction. **Circle one.**

   Less than 1 minute | About 1 minute | 5 - 10 minutes | 10 - 20 minutes | More than 20 minutes