**Homework #2**

Bailey Metz

**Question 1:** Security Objectives: Classify each of the following actions as a violation of Confidentiality, Integrity, Availability, Authenticity, or their combination.

1.      John copies Mary’s homework. **This is a violation of confidentiality.**

2.      Paul crashes Linda’s system. **This is a violation of availability and integrity.**

3.       Carol changes the amount of Pete’s check from $100 to $1,000. **This is a violation of integrity.**

4.       Eve obtains Steve’s credit card and has the credit card company cancel the card and replace it with a new one. **This is a violation of integrity, confidentiality, and availability.**

5.      Harry guesses Julia’s password and gains access to her account. **This is a violation of authenticity.**

**Question 2**: What does it mean to have layered security protection?  
  
**Typically when we talk about layered security protection, we are talking about software that has multiple security protocols in place to protect sensitive data. Without valid authentication at all points, complete access is denied.   
  
For example, two-factor authentication is an example of layered security protection because in order to gain access to certain data, a user usually needs a valid username+password as well as an additional code sent via text or an answered phone call to the phone number on file with the user’s account.**

**Question 3**: How does symmetric key encryption support

Confidentiality: **Symmetric key encryption supports confidentiality in the sense that if any person knows/sees the ciphertext or encrypted plaintext, it is no better than NOT knowing/seeing the ciphertext. The plaintext is still protected! It is only decipherable using the symmetric key which should only be known to authorized users.**

Integrity: **A message cannot be accurately modified without knowing the symmetric key to decrypt the ciphertext and then encrypt it again once changes have been made.**

Availability: **Strong symmetric key ciphers are rather inexpensive to produce and “simple” to distribute since only one key is needed to encrypt and decrypt messages/data. This makes them affordable, effective, and more easily available to give to those who need it.**

Authentication: **Symmetric key encryption supports authentication because information that is encrypted with one symmetric key cannot be decrypted with any other key besides the key it was encrypted with. Therefore, if the symmetric key remains safe and is only known by authorized parties, symmetric key encryption supports authentication.**

Non-repudiation: **If a message is sent using symmetric key encryption (one unique key for encryption/decryption) then it cannot be disputed that the message was encrypted with any other symmetric key. The sender (with the key) cannot deny sending/encrypting the message.**

**Question 4**: Give a detailed description of the Meet-in-the-middle attack against double-DES. What is the effective key size and why?

**In order to effectively intercept and decrypt a double-DES encrypted message, at least one ciphertext and plaintext pair must be known by the attacker. Most DES attacks typically use a method of brute force using these known pairs. So if we have several plaintext/ciphertext pairs, we can use a brute force method to attempt to break the double-DES.**

**Using one of those pairs, we first encrypt a known plaintext using all possible keys and store the results. This stores every encryption combination possible. Next, we decrypt the encrypted ciphertexts using all 256 possible keys (because double-DES has 256 possible key encryption methods).**

**Once we decrypt with every possible key, we need to look for a match between the stored outputs of the possible encryptions. When a match is found, we have possibly found a correct pair of keys. More than one pair is possible, but the number of pairs will likely be quite small. If this happens, however, we could try each possible pair of keys and if more than one plaintext/ciphertext pair is known (for the key pair), then the other pairs could be used to verify which key is correct.**

**Therefore, it takes twice as long to break double-DES using brute force. DES has 56-bit encryption key (256) and double-DES has two 56-bit key encryption (2x256 =** **257).**

**\*\*A side note would be to complete this entire method, we would need at least 257 bits of storage space which is approximately 18,014.40 Terabytes or 18.01 Petabytes. So storage space could be an “added” security measure to double-DES (though to be clear, this does not increase its security STRENGTH).**

**In conclusion, however, double-DES only doubles the strength of a single DES encryption key which is not incredibly greater security. However, two-key triple DES (which also uses two 56-bit keys) gives the strength equivalent to approximately 80-bit key encryption. This is almost 16,000,000 times stronger than 56-bit double-DES encrypti*on.***