10 points for each of the following questions

1. Random J. Programmer discovers a much faster method of generating a 64-bit signature for a message using secret key technology. The idea is to simply encrypt the first 64 bits of the message, and use that as the signature. What's wrong with this idea?
2. Vigenere Cipher uses a set of mono-alphabetic substitution rules to encrypt message. For example, with key = (3 1 5), an encoder substitutes first letter in plaintext by letter+3, second letter by letter+1, third letter by letter+5. Please describe a known plaintext attacks against Vigenere Cipher.
3. What's wrong of designing a hash function that adds up the words of a message and uses the result as the hash output?
4. Random J. Protocol-Designer has been told to design a scheme to prevent messages from being modified by an intruder. Random J. decides to append to each message a hash of that message. Why doesn't this solve the problem? (We know of a protocol that uses this technique in an attempt to gain security.)
5. Given a random key K of length m bits. K is used as a one time-pad to encrypt plaintext message P1 (of length m bits) to obtain ciphertext C1. K is then also used to encrypt plaintext P2 (of length m bits) to obtain ciphertext C2 (i.e., the key is reused!). If the adversary is able to obtain C1, C2, and P2 (known plaintext attack), explain how he can compute P1.
6. How many pairs of cipher text and plaintext should be available to break Hill's Cipher? Please explain your reason and describe a way to achieve this attack.
7. Alice needs to send a private letter to Bob through an insecure communication channel. Describe an economic way against eavesdropper to protect the confidentiality of the letter. Assume that Alice and Bob do not have any pre-shared secret.
8. Alice and Bob want to establish a secure communication channel between them. They do not care about the confidentiality of the messages being transmitted, but they do want to ensure the integrity and authenticity of the messages. Assume A and B share a common key K. Answering the following questions.

   a. (3 points) How can they achieve their goal only with secret key cryptography?
   b. (3 points) How can they achieve their goal with hash function *h* and the key?
   c. (4 points) Can they get non-repudiation? If yes, how? If no, why?