Assignment 1

1) A ciphertext has been generated with an affine cipher. The most frequent letter of the ciphertext is 'B', and the second most frequent letter of the ciphertext is 'U'. Break this code. **(10 pts)**

2) Suppose someone suggests the following way to confirm that the two of you are both in possession of the same secret key. You create a random bit string the length of the key, XOR it with the key, and send the result over the channel. Your partner XORs the incoming block with the key (which should be the same as your key) and sends it back. You check, and if what you receive is your original random string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key. Is there a flaw in this scheme? **(15 pts)**

3) Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof, and explain a bit why you think so. **(20 pts)**

a) Carol changes the amount of Angelo's check from $100 to $1,000.

b) Gina forges Roger's signature on a letter and sends the letter to Rachel.

c) Rhonda registers the domain name “AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.

d) Jonah and Peter were original acquaintance, Jonah even told Peter his credit card number and information. However, Peter made a mischief, and inform the credit card company to cancel the card.

e) Henry sends a doc containing a Trojan horse to Marry, and Marry opened the file, and sends her PIN to Henry. Henry now can have access to Marry's computer.

4) A well designed hash function normally has multiple properties, including collision resistance, which means it is very hard for one to find a pair of inputs x≠y, such that h(x) = h(y). Could we just use a collision resistant function to do encryption? i.e., Enc(k,m)=f(k,m), where f is a collision resistant function. **(15 pts)**

5) Why Diffie-Helman key exchange algorithm alone is not secure against man in the middle attacks, please show step by step. How can we improve security and make sure that the algorithm is secure against MITM attacks? (Draw a schema for both problems and explain the steps) **(20 pts)**

6) We know that a digital signature is for the purpose of ensuring data integrity and authenticity. **(20 points)**

a) Checksum adds all the bits of the message (or blocks), is checksum a good way to construct a digital signature scheme? How about a hash function, i.e, Sign(M)= h(M)?

b) If we use a hash to generate a signature in a more complicated way as follows Sign(k,m) = σ = h(k) XOR m XOR h(m), and m, σ will be sent along. Would this be a secure signature? Briefly explain.