Homework Assignment #2

1. (10 points) Decrypt the following encrypted quotation. Explain the process.

oczmz vmzor jocdi bnojv dhvod igdaz

admno ojbzo rcvot jprvi oviyv aozmo

cvooj ziejt dojig toczr dnzno jahvi

fdiyv xcdzq zoczn zxjiy

1. (20 points) Suppose Alice and Bob have RSA public keys in a file on a server. They communicate regularly using authenticated, confidential messages. Eve wants to read the messages but is unable to crack the RSA private keys of Alice and Bob. However, she is able to break into the server and alter the file containing Alice’s and Bob’s public keys.
   1. How should Eve alter that file so that she can read confidential messages sent between Alice and Bob, and forge messages from either?
   2. How might Alice and/or Bob detect Eve’s subversion of the public keys?
2. (10 points) Explain why hash collisions occur. That is, why must there always be two different plaintexts that have the same hash value?
3. (10 points) What property of a hash function means that collisions are not a security problem? That is, why can an attacker not capitalize on collisions and change the underlying plaintext to another form whose value collides with the hash value of the original plaintext?
4. (10 points) Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root a = 2.

If user A has public key Ya = 9, what is A’s private key Xa?

If user B has public key Yb = 3, what is the shared secret key K?

1. (20 points) In this problem we will compare the security services that are provided by digital signatures (DS) and message authentication codes (MAC). We assume that Oscar is able to observe all messages sent from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how (i) DS and (ii) MAC protect against each attack. The value auth(x) is computed with a DA or a MAC algorithm, respectively.
2. (Message integrity) Alice sends a message x = “Transfer $1000 to Mark” in the clear and also sends auth(x) to Bob. Oscar intercepts the message and replaces “Mark” with “Oscar”. Will Bob detect this in either case (i) DS and (ii) MAC?
3. (Replay) Alice sends a message x = “Transfer $1000 to Oscar” in the clear and also sends auth(x) to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect his in either case (i) DS and (ii) MAC?
4. (Sender authentication with cheating third party) Oscar claims that he sent some message x with a valid auth(x) to Bob but Alice claims the same. Can Bob clear the question in either case (i) DS and (ii) MAC?
5. (Authentication with Bob cheating) Bob claims that he received a message x with a valid signature auth(x) from Alice (e.g., “Transfer $1000 from Alice to Bob”) but Alice claims she has never sent it. Can Alice clear this question in either case (i) DS and (ii) MAC?
6. (10 points) Explain why hash collisions occur. That is, why must there always be two different plaintexts that have the same hash value? What property of a hash function means that collisions are not a security problem. That is, why can an attacker not capitalize on collisions and change the underlying plaintext to another form whose value collides with the hash value of the original plaintext?
7. (10 points) Does a PKI (Public Key Infrastructure) perform encryption? Explain your answer. Does a PKI use symmetric or asymmetric encryption? Explain your answer. Why does a PKI need a means to cancel or invalidate certificates? Why is it not sufficient for the PKI to stop distributing a certificate after it becomes invalid?