Assignment

Sub: Computer Security

Q 1. The Shift Cipher is not secure, because there are only 26 possible keys. Mary uses a key space of Z_{10}^{1024}. For a key $K \in Z_{10}^{1024}$, he uses the following encryption function:

$$E_K(x) = x + K \pmod{26}.$$

Do you think it is more secure than Shift Cipher?

Q2. We can define a Shift Cipher on Z_2^{128} for binary files as follows:

- Divide the plaintext into blocks of size 128 bits.
- Select a random key K which is a 128 bits binary string.
- For each block B, define eK(B) = B xor K.

Do you think that method is secure? How to attack that encryption method?

Q 3. Do you think the Permutation Cipher is more secure than the Substitution Cipher? Why?

Q4. Suppose in a Vigen´ere Cipher, a key of size is 8. The ciphertext is: ABCDEFGH. Find a key such that the plaintext is iloveyou. Find another key such that the plaintext is ihateyou. Explain in this case why the cipher cannot be broken under cipher text only attack.

Q 5. The Autokey Cipher is not secure because its key space is very small. However, it can be easily generalized to have a very large key space in an obvious way (for example, use a method similar to problem 3), so that the brute force attack is not feasible. Do you think in that case the Autokey Cipher is secure? Why?

Q6. In DES, all the permutations, operations, functions and S-boxes are published. Why these public knowledge will not effect the security of the encryption?

Q 7. Can you see the relationships between some DES modes and some kinds of stream ciphers?

Q 8. Suppose Alice has a signature function SigA using public key system, Bob has a public key B. Alice wants to send message x to Bob. Alice sends (SigA(EB(x)),EB(x)) to Bob. If the signature and encryption function are safe and all the public keys are certificated. Do you think Alice's message is safe? Why?

Q 9. Why S-boxes in AES have inverses, but S-boxes in DES do not?

Q 10. Suppose Oscar knows that Alice and Bob use a 64-bit DES with secret key K to communicate. Oscar also knows a plaintext x and the according ciphertext y. But Oscar does not know they are using ECB mode or CBC mode of DES. Find some way to help Oscar to determine the mode Alice and Bob used.

Q 11. When Oscar does not know the key of a block cipher, he cannot decrypt the message. But he might delete some blocks or rearrange the blocks so that Bob will get wrong information. For example, if the message is:

please do not pay the one million dollars to Oscar

If some blocks are deleted, then Bob might receive the following message:

pay the one million dollars to Oscar

Suggest some methods to prevent such kind attacks.

Q 12. If two people use RSA cryptosystems with the same value of n, but different values of a and b (Keys are different). Do you think that is fine? Why?

Q 13. Why should a secret key have a lifetime, even the encryption system is very secure?

Q 14. The Data Authentication Algorithm is based on CBC mode of DES. Could we create a MAC function based on OFB mode of DES? Why?

Q 15. Suppose Bob uses an RSA system with n = 187, b = 7 as public key. Alice uses a DSS with parameters p = 71, q = 7, α= 30, β= 20, a =3. Now Alice wants to send a number x = 2 to Bob which is both encrypted and authenticated. Calculate and explain what values Alice should send to Bob.

Q 16. If an authentication server uses following method to establish a session key for U and V .

(a) U sends IDU, TS1 to AS.

(b) AS sends eK_U (K||ID_V ||T||L) to U.

(c) AS sends $e_K V$ (K||ID_U||T||L) to V.

(d) U sends eK(T + 1) to V .

The notations used above are the same as used in Kerberos. Is this method not as good as the method used in Kerberos? Why?

Q 17. If three users in a net want to share a common secret key. Design a scheme similar to Kerberos to establish the key.

Q 18. In One-time password defined in RFC 2289, what kind information the user must remember for next login using one-time password?

Q 19. In one-time password protocol, a passphrase is used. What is the difference between a password and a passphrase? Can we use a password instead of a passphrase in that protocol?

Q 20. One way to solve the key distribution problem is to use a line from a book that both the sender and the receiver possess. Typically, at least in spy novels, the first sentence of a book serves as the key. Consider the following message:

SIDKHKDM A: HCRKIABIE SHIMC KD LFEAILA

This ciphertext was produced using the first sentence of a book. Sentence is:
"The snow lay thick on the steps and the snowflakes driven by the wind looked black in the headlights of the cars. A simple substitution cipher was used."

a. What is plaintext if encryption algorithm uses only mono alphabetic substitution?
b. How secure is it?