Problems for CS 4476

2010

Chapter 2

1. Alice uses the shift cipher to send one letter to Bob. Do you think it is safe for plaintext only attack? Why?

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

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

   Do you think it is more secure than Shift Cipher?

3. We can define a Shift Cipher on $\mathbb{Z}_{2^{128}}$ 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 $e_K(B) = B \oplus K$.

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

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

5. Suppose in a Vigenére 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.

6. 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?

Chapter 3

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

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

3. What is an idempotent cryptosystem? The S-box used in AES can be considered as a simple encryption function S. Is S idempotent? Why do you think so?

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

5. 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.

6. Suppose E is a 64-bit DES encryption function and F is a 128-bit AES encryption function. Which combination of the following functions is better? Do you think the security of these two methods is significantly different?

   - $E_{K_1}(F_{K_2}())$
   - $F_{K_2}(F_{K_3}())$

7. 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.

Chapter 4

1. 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?

2. Compare RSA and ElGamal encryption systems: what are the advantages and disadvantages.

3. Can we perform a probabilistic analysis for the RSA encryption system if we use RSA to encrypt English text? How about the ElGamal system?

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

Chapter 5

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

2. Suppose Alice has a signature function Sig_A using public key system, Bob has a public key B. Alice wants to send message x to Bob. Alice sends $(Sig_A(E_B(x)), E_B(x))$ 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?

3. Suppose Bob uses an RSA system with $n = 187$, $b = 7$ as public key. Alice uses a DSS with parameters $p = 71, q = 7, \alpha = 30, \beta = 20, a = 3$. 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.

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

   (a) U sends ID_U, TS_1 to AS.

   (b) AS sends $e_{K_U}(K||ID_V||T||L)$ to U.

   (c) AS sends $e_{K_V}(K||ID_U||T||L)$ to V.

   (d) U sends $e_K(T+1)$ 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?

5. If 3 users in a net want to share a common secret key. Design a scheme similar to Kerberos to establish the key.

6. Explain why there is a CA in PKI certification while there is no CA in PGP certification.

7. Suppose Alice has RSA key pair a_A (private) and b_A (public), and Bob has RSA key pair a_B (private) and b_B (public). They also have AES and MD5 algorithms. Find an efficient and security way for them to communicate over the internet.

Chapter 6

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

2. 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?

Chapter 7

1. Answer the following questions about PGP.

   (1). In PGP, Bob has a public key encryption system. If Alice uses the public key to encrypt the message, will it cause problems?

   (2). Explain the purpose of using a passphrase in PGP for the security consideration.

2. What are the benefits to use Radix-64 in PGP?

Chapter 8

1. Indicate the differences of authentication methods between SSL and SSH. Explain the reason of these differences.

2. Explain why SET uses dual signature.

Chapter 9

1. The following is an IPv4 packet applying an AH which uses HMAC-SHA-1 to produce ICV.

New IP-H	AH	orig. IP-H	TCP-H	Data

   Indicate what part of the above packet is used as input of the ICV.

2. Efficiency is very important for an encryption system. What features in AES reflect the consideration of efficiency?

3. Explain why the input of MAC values are different for transport mode and tunnel mode in IPSec.

4. Explain why nonce are used in ISAKMP message exchange and cookies are not used.

5. In AH, a sequence number is used to prevent replay attack. Can we use a nonce instead of the sequence number?

6. Design filtering rules for a router in a screened host firewall, single-homed bastion configuration. (You may specify some services the local network providing).