CS 4476(5413) FINAL EXAMINATION

April 14th, 2005

Duration: Three hours

Name:

Student Number:

Note. Each student is asked to solve 10 problems. All the students should solve 3 problems in Set A. For students of CS 4476, choose 4 problems in Set B, 3 problems in Set C. For students of CS 5413, choose 3 problem from Set B, 4 problems from Set C. If you have chosen more than 10 problems, please indicate which of the problems you want to be marked. This examination set has total 14 pages. Check the pages before you start to solve problems.

Set A

Problem 1.

Suppose x and y satisfy the following equations:

$$\begin{aligned} 2x &\equiv 7 \pmod{17}, \\ 3y &\equiv 1 \pmod{17}. \end{aligned}$$

Compute $6xy + 10x \pmod{17}$.

Problem 2.

Answer the following questions.

1. Why a hash function should have the property that it is difficult to find $x \neq x'$ such that they have the same hash value?

2. Why a certificate is used in PGP?

3. What is the main difference between using a Diffie-Hellman key exchange and using an RSA to establish a session key?

4. List two methods of using a hash function to authenticate a message (assume that a secret key and public keys are established) .

Problem 3.

The packet filtering rules for a firewall are as in the following diagram.

rule	action	src	port	dest	port	flag
1	block	hecker.com	*	*	*	
2	allow	{ our hosts}	*	*	*	
3	allow	*	*	*	*	ACK
4	allow	*	*	*	25	
5	allow	*	*	*	> 1024	
6	block	*	*	*	*	

Answer the following questions.

1. What is the default of the filtering?

2. Suppose the port of SSH server is 22. What will happen when our hosts try to use SSH to connect some outside host, or some outside host try to use SSH to connect our host? Why?

3. If the rule 1 and rule 3 are exchanged, then what kinds of traffic control will be changed?

Set B

Problem 4.

A dual signature DS is defined as follows.

$$DS = Sig_K(h(h(\texttt{PI})||h(\texttt{OI}))),$$

where h is a hash function, Sig_K is customer's signature, `PI` is customer's payment information, `OI` is customer's order information. What kind message should the financial institute have together with the DS, so that the institute is able to check and do the payment?

Problem 5.

In a one time password system, the user chooses a secret pass-phrase. This pass-phrase is then passed though a secure hash function N times. The resulting value is stored in the server. Next time, when the user wants to login, what should he do and what should the server do?

Problem 6.

Why the PGP defined methods for public key certification while the message is encrypted by a block cipher?

Problem 7.

In SSH, a client initializes the connection. Then both sides send out a KEXINIT packet including the list of algorithms (encryption, compression, key exchange, etc.) supported by the machine. Then how do they decide the algorithms they will use?

Problem 8.

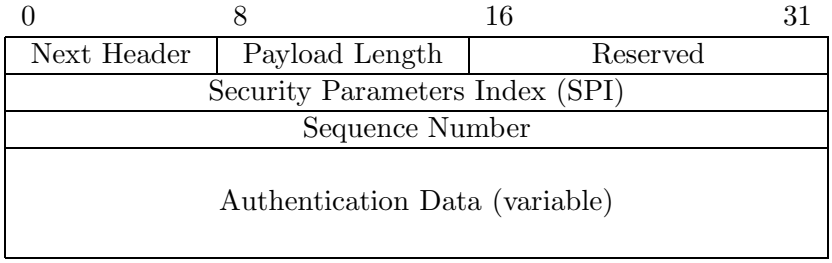
In PGP, when a pair of keys is generated, the system asks the owner to provide a passphrase `paph` for the private key K_p. Then the system computes $k = SHA(\texttt{paph})$ and $y = e_k(K_p)$, where $e_k()$ is the DES encryption function. The value of y is recorded in file `private-key`. Write an algorithm for the user to retrieve the private key.

Problem 9.

In SET (Secure Electronic Transaction), a merchant need to provide certificates to other parties and check other parties' certificates. Describe all of those certificates (the owner of the certificate and the purpose of the certificate).

Problem 10.

An IPSec AH is as follows:



Indicate the purpose of the fields of Payload Length and Sequence Number in this header. Why these fields are necessary?

Set C

Problem 11.

Suppose Alice wants to send Bob message M. Indicate which one of the followings are the best way for Alice to send M. Explain why.

- $Sig_A(h(M)), e_K(M)$
- $Sig_A(M), h(M)$
- $e_K(h(M)), e_K(M)$
- $h(M), e_K(h(M)||M)$

Here $e_K()$ is a block cipher (K is shared by Alice and Bob), h is a secure hash function, $Sig_A()$ is Alice's signature.

Problem 12.

The Diffie-Hellman key exchange between two parties are as follows:

1. A chooses $x_A \in \mathbb{Z}_p^*$ and sends B $y_A = \alpha^{x_A} \pmod{p}$.
2. B chooses $x_B \in \mathbb{Z}_p^*$ and sends A $y_B = \alpha^{x_B} \pmod{p}$.
3. The common key of A and B is $\alpha^{x_A x_B} \pmod{p}$.

What is a man-in-the-middle attack? Modify the above protocol to prevent the man-in-the-middle attack.

Problem 13.

Suppose A and B want to establish a session key. They plan to use the following method:

- $A \longrightarrow B : E_{PubB}(R_a), e_{R_a}(\alpha^x), h(R_a)$
- $A \longleftarrow B : E_{PubA}(R_b), e_{R_b}(\alpha^y), h(R_a)$

The session key is α^{xy}. Here E is a public key encryption function, $PubB$ and $PubA$ are public keys of B and A respectively, e is a block cipher, R_a and R_b are random numbers, h is a secure hash function, α is a primitive element of $\mathbb{Z}_q$. Does this method work? Give necessary conditions and improvements so that the method can work securely.

Problem 14.

Now some computer login systems use a hash function. In that case, a long pass-phrase can be used. The pass-phrase first goes through the hash function. The hash value then serves as the regular password. Are there any security problems for that method? How to improve the method?

Problem 15.

List two network security protocols, one is at application level and other is at IP level. Discuss the advantages and disadvantages by comparing these two protocols.