CHAPTER 16

PGP and S/MIME

(Solution to Odd-Numbered Problems)

Review Questions

1. Alice needs to include the identifiers of the algorithms in the packets sent to Bob. Each packet type has a field that defines the identity of the algorithm being used.

3. The secret key is encrypted with the public key and sent with the message.

5. PGP uses a web of trust; S-MIME uses certificates signed by CA's, but the user is responsible to keep a web of trust.

7.

- ❑ Encrypted message
- ❑ Signed message
- ❑ Certified message

9. In PGP, everyone in the community needs two rings (one public and one private); in S/MIME, the public keys are distributed through X.509 certificates.

Exercises

11. Alice can use two public-key algorithms and two public keys each sent separately in a public-key packet.

13.

a. For confidentiality, two packets need to be sent. A session key packet (type 1) and an encrypted data packet (type 9). However, the second packet contains either a compressed data packet (which contains a literal data packet) or simply a literal data packet.

b. For message integrity, two packets need to be sent. A signature packet (type 2) and a literal data packet (type 11).

c. The packets in part *b* also provide authentication.

d. Nonrepudiation needs a third party. Since e-mail communication is only between two parties, it is not possible to provide this security service.

e. To provide both confidentiality and message integrity, four packets are needed to be sent (type 1, type 9, type 2 and type 11).

f. Same as part *e*.

g. Same as part *e*.

h. This is impossible because there is no third party to provide nonrepudiation.

15. The following table shows the comparison:

Algorithms	***PGP***	***S/MIME***
No Encryption	✓	
IDEA	✓	
Triple DES	✓	✓
CAST-128	✓	
Blowfish	✓	
SAFER-SK 128	✓	
DES/SK	✓	
AES-128	✓	✓
AES-192	✓	
AES-256	✓	
RC2/40		✓

17. The following table shows the comparison:

Algorithms	***PGP***	***S/MIME***
MD2	✓	
MD5	✓	✓
SHA-1	✓	✓
double-width SHA	✓	
RIPEMED/160	✓	
TIGER/192	✓	
HAVAL	✓	

19.

a. Although the message can be sent without encoding, we show how to send it using Radix-64.The text to be sent in English is "This is a test". We add a null character at the end to make the English text multiple of 3 characters. We show

the space character with "_".

Text	ASCII code			R-64 code				Text
Thi	01000001	01101000	01101001	010000	010110	100001	101001	QWhp
s_i	01110011	00100000	01101001	011100	110010	000001	101001	cyBp
s_a	01110011	00100000	01100001	011100	110010	000001	100001	eyBh
_te	00100000	01111100	01100101	001000	000111	110001	100101	IHxl
st	01110011	01111100	00000000	011100	110111	110000	000000	c3wA

The text to be sent is "QWhpcyBpeyBhIHxlc3wA".

b. The message consists only of ASCII characters, so the English text and the quoted-printable text are the same. The text to be sent is "This is a test".