CHAPTER 29

Cryptography and Network Security

Exercises

1.

a. This is ***snooping*** (the attack to confidentiality service). Although the contents of the test is not confidential on the day of the test, it is confidential before the test day.

b. This is ***modification*** (the attack to integrity service). The value of the check is changed (from $10 to $100).

c. This is ***denial of service*** (the attack to availability service). Sending so many e-mails may crash the server and the service may be interrupted.

3. Double encryption here does not help. Encryption with k_1 followed by encryption with k_2 is the same as encryption with $k = (k_1 + k_2) \bmod 26$. The following shows the proof. P is the plaintext and C is the ciphertext.

$$C = [(P + k1) \bmod 26) + k2] \bmod 26$$
$$C = (P \bmod 26 + k_1 \bmod 26 + k_2) \bmod 26$$
$$C = (P \bmod 26) \bmod 26 + (k_1 \bmod 26) \bmod 26 + k_2 \bmod 26$$
$$C = P \bmod 26 + k_1 \bmod 26 + k_2 \bmod 26 = (P + k_1 + k_2) \bmod 26$$
$$\mathbf{C = (P + k) \bmod 26}, \text{ where } k = (k_1 + k_2) \bmod 26$$

5.

a. A 3-bit circular left shift of (**100**11011) is (11011**100**)

b. A 3-bit circular right shift of (11011**100**) is (**100**11011)

c. The original word in Part *a* and the result of Part *b* are the same, which shows that circular left shift and circular right shift operations are inverses of each other.

7.

a. (01001101) ⊕ (01001101) = (**00000000**), which means that if the two input words are the same, all the bits in the output word becomes 0's. This property is used in ciphers.

b. (01001101) ⊕ (10110010) = (**11111111**), which means that if the two input words are complement of each other, all the bits in the output word becomes 1's. This property is also used in ciphers.

9.

a. Using 26 for space, the plaintext is: **19070818260818261914200607**

b. For encryption, we create 4-digit blocks:

$P_1 = 1907$	$\rightarrow$	$C_1 = 1907^{13} \bmod 12091$	$= 10614$
$P_2 = 0818$	$\rightarrow$	$C_2 = 0818^{13} \bmod 12091$	$= 7787$
$P_3 = 2608$	$\rightarrow$	$C_3 = 2608^{13} \bmod 12091$	$= 1618$
$P_4 = 1826$	$\rightarrow$	$C_4 = 1826^{13} \bmod 12091$	$= 10717$
$P_5 = 1914$	$\rightarrow$	$C_5 = 1914^{13} \bmod 12091$	$= 4084$
$P_6 = 2006$	$\rightarrow$	$C_6 = 2006^{13} \bmod 12091$	$= 6558$
$P_7 = 07$	$\rightarrow$	$C_7 = 07^{13} \bmod 12091$	$= 6651$

c. We can use the private key, $d = 3653$ to decrypt the message.

$C_1 = 10614$	$\rightarrow$	$P_1 = 10614^{3653} \bmod 12091$	$= 1907$
$C_2 = 7787$	$\rightarrow$	$P_2 = 7787^{3653} \bmod 12091$	$= 0818$
$C_3 = 1618$	$\rightarrow$	$P_3 = 1618^{3653} \bmod 12091$	$= 2608$
$C_4 = 10717$	$\rightarrow$	$P_4 = 10717^{3653} \bmod 12091$	$= 1826$
$C_5 = 4084$	$\rightarrow$	$P_5 = 4084^{3653} \bmod 12091$	$= 1914$
$C_6 = 6558$	$\rightarrow$	$P_6 = 6558^{3653} \bmod 12091$	$= 2006$
$C_7 = 6651$	$\rightarrow$	$P_7 = 6651^{3653} \bmod 12091$	$= 07$

The plaintext is:19070818260818261914200607 or "THIS IS TOUGH".

11. The key which is concatenated with the message in a MAC should be a secret between Alice and Bob; no one else should know this secret. When Alice sends a MAC to Bob, the key cannot be the public key of Bob or the private key of Alice. If the key is the public key of Bob, every one (including Eve) knows this key and can use it to create a MAC to pretend that she is Alice. If the key is the private key of Alice, no one (including Bob) knows the key. So Bob cannot verify that a MAC has truly created by Alice.

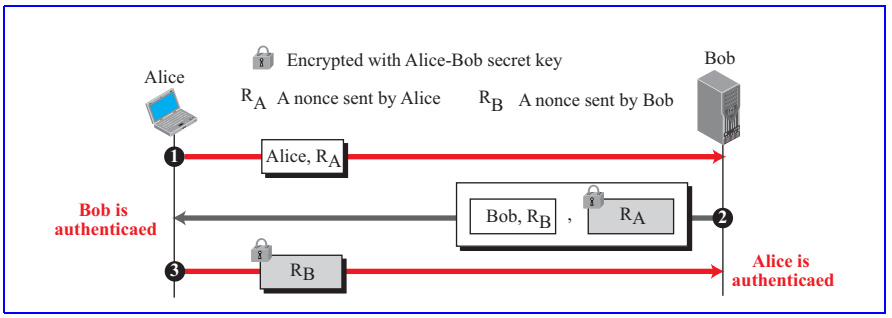
12. Figure 29.E13 shows one simple, but not very secure solution. It shows the idea, but it is vulnerable to some attacks. There are some better, but more complicated solutions.

a. In the first message, Alice sends her identification and her nonce.

b. In the second message, Bob sends his identification, his nonce, and encrypted Alice's nonce. Alice's nonce is encrypted with the shared secret key. When Alice receives this message and decrypts her nonce, Bob is authenticated for her because only Bob can encrypt Alice's nonce with the shared secret key.

c. In the third message, Alice sends encrypted Bob's nonce. When Bob receives this message and decrypts his nonce, Alice is authenticated for Bob because only Alice can encrypt Bob's nonce with the shared secret key.

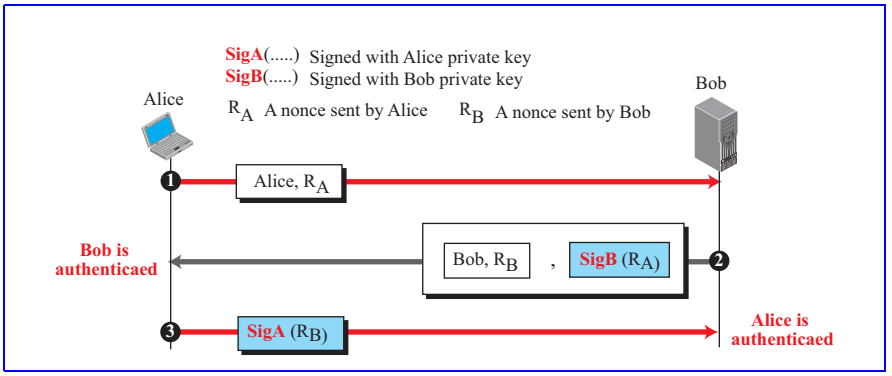
Figure 29.E13 *Solution to Exercise 13*



d.

15. Figure 29.E15 shows one simple, but not very secure solution. It shows the idea, but it is vulnerable to some attacks. There are some better, but more complicated solutions.

Figure 29.E15 *Solution to Exercise 15*



a. In the first message, Alice sends her identification and her nonce.

b. In the second message, Bob sends his identification, his nonce, and signed Alice's. Bob uses his private key to sign the message carrying Alice's nonce. When Alice receives this message and verifies the signature, Bob is authenti-

cated for her because only Bob could have signed Alice's nonce using his private key.

c. In the third message, Alice sends Bob a signed message that include the Bob's nonce. Alice signs this message with her private key. When Bob receives this message, Alice is authenticated for Bob because only Alice can sign a message with her private key.