CHAPTER 14

Entity Authentication

(Solution to Odd-Numbered Problems)

Review Questions

1. There are two differences between message authentication and entity authentication. First, message authentication might not happen in real time; entity authentication does. Second, message authentication simply authenticates one message; the process needs to be repeated for each new message. Entity authentication authenticates the claimant for the entire duration of a session.

3. A fixed password is a password that is used over and over again for every access. A one-time password is a password that is used only once.

5. In challenge-response authentication, the claimant proves that she knows a secret without sending it to the verifier.

7. In a dictionary attack, Eve is interested in finding one password, regardless of the user ID. Eve can create a list of numbers. She then applies the hash function to every number until she finds a match with a hashed password.

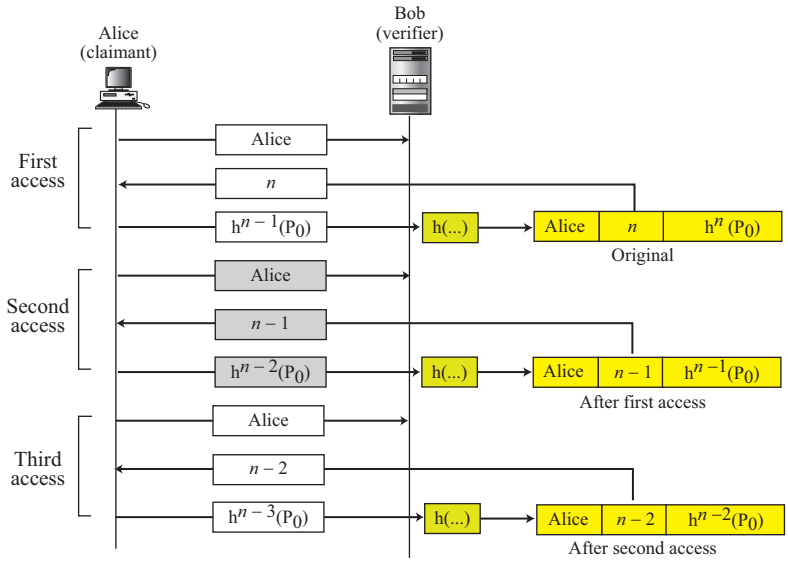
9. Biometrics is the measurement of physiological or behavioral features that identify a person (authentication by something inherent). Biometrics measures features that cannot be guessed, stolen, or shared. These techniques can be divided into two broad categories: *physiological* and *behavioral*.

Exercises

11. A system may require that users frequently change their passwords. In this case, a validity period is defined for each password. Near the end of the period, the system warns the user to create a new password and use the password-changing process to change the password.

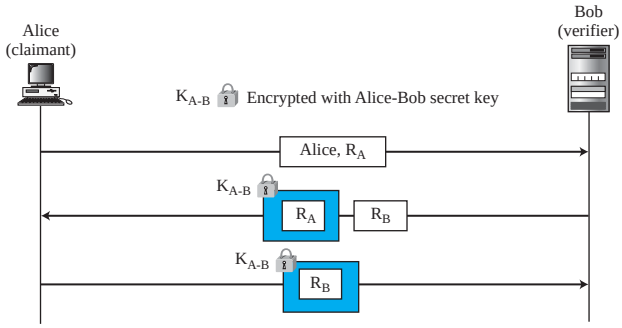
13. See Figure S14.13.

Figure S14.13 *Solution to Exercise 13*



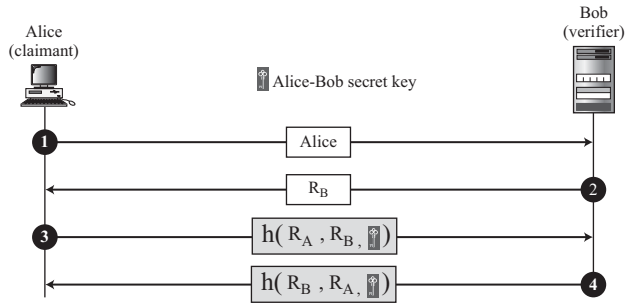
15. It can be done. However, it is very inefficient. It can be done using three exchange as shown in Figure S14.15. But this efficient protocol is subject to an attack called reflection attack (See solution to Exercise 30).

Figure S14.15 *Solutions to Exercise 15*



17. See Figure S14.17.

Figure S14.17 *Solution to Exercise 17*



19. The following table shows the comparison.

Authentication	*Feature*	*Protocol in Figure 14.7*	*Protocol in Figure 14.10*
Authentication of Bob	Challenge	Bob's nonce is sent in plaintext (second exchange).	Alice challenges Bob by sending her nonce encrypted with Bob's public key (first exchange)
	Response	Alice should show that she have the secret by encrypting Bob's nonce and send the encrypted nonce (third exchange).	Bob shows that he possesses his private key by decrypting Alice's nonce and resending it in the second exchange.
Authentication of Alice	Challenge	Alice's nonce is sent in encrypted form (third exchange).	Bob challenges Alice by sending his nonce encrypted with Alice's public key (second exchange)
	Response	Bob should show that he have the secret by encrypting Alice's nonce and send the encrypted nonce (fourth exchange).	Alice shows that she possesses her private key by decrypting Bob's nonce resending it in the third exchange

21. All three protocols use witness, challenge, and response. However, the value of these three items are different in different protocols as shown in the following table.

	Witness	*Challenge*	*response*
Figure 14.13	$x = r^2 \bmod n$	c: (0 or 1)	$y = rs^c \bmod n$
Figure 14.15	$x = r^2 \bmod n$	$(c_1, c_2, \ldots c_k)$	$y = rs_1^{c1} s_2^{c2} \ldots s_k^{ck} \bmod n$
Figure 14.16	$x = r^e \bmod n$	c: *(1 to e)*	$y = rs^c \bmod n$

23. $p \leftarrow 569 \quad q \leftarrow 683 \quad n \leftarrow 388{,}267 \; s \leftarrow 157 \; v \leftarrow 24{,}649$

r	$x \leftarrow r^2 \bmod n$	c	$y \leftarrow rs^c \bmod n$	$y^2 \bmod n$	$xv^c \bmod n$
203,122	130663	0	203122	**130,663**	**130,663**
153,271	292,873	1	379,260	**366,513**	**366,513**
377,245	345,180	1	210,881	**247,049**	**247,049**

The values of the last two columns should be the same if Alice is honest or has preguessed the value of c.

25. $p \leftarrow 683 \quad q \leftarrow 811 \quad n \leftarrow 553{,}913 \; \phi(n) \leftarrow 552{,}402 \quad s \leftarrow 157 \; e \leftarrow 7 \quad v \leftarrow 444751$

r	$x \leftarrow r^e \bmod n$	c	$y \leftarrow rs^c \bmod n$	$y^e v^c \bmod n$	x
15,024	519,635	1	153,116	**519,635**	**519,635**
7,235	135,522	3	35,444	**135,522**	**135,522**
423	200,972	4	18,109	**200,972**	**200,972**

The values of the last two columns should be the same if Alice is honest or has preguessed the value of c correctly.

27. In the Fiat-Shamir protocol, a dishonest claimant can correctly responds to a change with the probability of 1/2. The probability that a dishonest claimant responds correctly 15 times is then $P = (1/2)^{15} = 1/32768 \approx 0.0000305$, which is very small.

29. In the Guillou-Quiquater protocol, a dishonest claimant can correctly responds to a change with the probability of $1/(e - 1)$ because the challenge value is between 1 and e. The probability that a dishonest claimant responds correctly 15 times is then $P = [1/(e - 1)]^{15}$, which is extremely small when e is large.