

Review Questions

- 10.1 What are two different uses of public-key cryptography related to key distribution?
- 10.2 List four general categories of schemes for the distribution of public keys.
- 10.3 What are the essential ingredients of a public-key directory?
- 10.4 What is a public-key certificate?
- 10.5 What are the requirements for the use of a public-key certificate scheme?
- 10.6 Briefly explain Diffie-Hellman key exchange.
- 10.7 What is an elliptic curve?
- 10.8 What is the zero point of an elliptic curve?
- 10.9 What is the sum of three points on an elliptic curve that lie on a straight line?

Problems

- 10.1 Users A and B use the Diffie-Hellman key exchange technique a common prime $q = 71$ and a primitive root $\alpha = 7$.
 - a. If user A has private key $X_A = 5$, what is A's public key Y_A ?
 - b. If user B has private key $X_B = 12$, what is B's public key Y_B ?
 - c. What is the shared secret key?
- 10.2 Consider a Diffie-Hellman scheme with a common prime $q = 11$ and a primitive root $\alpha = 2$.
 - a. Show that 2 is a primitive root of 11.
 - b. If user A has public key $Y_A = 9$, what is A's private key X_A ?
 - c. If user B has public key $Y_B = 3$, what is the shared secret key K ?
- 10.3 "But," said Dr. Watson, "your clients use Diffie-Hellman key exchange protocol in their network. It is based on discrete logarithm, and this is known to be a hard problem, isn't it?"

"Yes, Watson," nodded Holmes, "for appropriate choice of parameters the discrete logarithm problem is really hard. My clients know that and that's why they opted for this method of key distribution. Unfortunately their security consultants didn't realize that an active adversary might often be more successful than the passive one. An adversary also knows that he can't solve a discrete logarithm problem in a reasonable time, thus he has to try something else. And because I am sure Moriarty himself is interested in my clients' communications, I must suppose some kind of active attack on their network. Moriarty would never stay passive, Watson."

"Do you think, Holmes," Dr. Watson added, surprised, "that Moriarty could find a way to break the Diffie-Hellman key exchange scheme?"

"Oh, it is not so hard, Watson," smiled Holmes. "All that Moriarty needs is to place himself somewhere in the communication path to be able not only to intercept but also to change all the messages. I am sure this is completely within Moriarty's abilities. Now in this position he will . . ."

- 10.4 In 1985, T. ElGamal announced a public-key scheme based on discrete logarithms, closely related to the Diffie-Hellman technique. As with Diffie-Hellman, the global elements of the ElGamal scheme are a prime number q and α , a primitive root of q . A user A selects a private key X_A and calculates a public key Y_A as in Diffie-Hellman. User A encrypts a plaintext $M < q$ intended for user B as follows:
 1. Choose a random integer k such that $1 \leq k \leq q - 1$.
 2. Compute $K = (Y_B)^k \pmod{q}$.
 3. Encrypt M as the pair of integers (C_1, C_2) where

$$C_1 = \alpha^k \pmod{q} \quad C_2 = KM \pmod{q}$$
 User B recovers the plaintext as follows:
 1. Compute $K = (C_1)^{X_B} \pmod{q}$.
 2. Compute $M = (C_2 K^{-1}) \pmod{q}$.

een, a considerably
furthermore, for equal
RSA is comparable
C with a shorter key

9]; the emphasis is on
contain some rather stiff
more concise descrip-
survey treatments are

Cryptography. Can-
ryptography. Norwell,
Journal, December 1999.
ography." Dr. Dobb's
ography. New York:
Computer Applications.
Greenwich, CT: Man-
. FL: CRC Press, 2002.

urve cryptography and

PROBLEMS

ve root
key certificate
key directory
oint