

## Assignment 9

Computer Science 349

Spring 2004

Due: Start of class on Thursday May 6

**Reading:** Singh Chapter 6; Stinson §5.1, 5.2, 5.3

**Exercise 9.0.** True or False? Public cryptography makes it convenient to send the same message to several different users. Discuss your answer.

**Exercise 9.1.** Determine  $\gcd(24140, 16762)$ .

**Exercise 9.2.** Compute  $367^{-1}$  in  $Z_{1001}$  and  $1001^{-1}$  in  $Z_{367}$ .

**Exercise 9.3.** Perform encryption and decryption using the RSA algorithm for the following:

(a)  $p = 3, q = 11, a = 7, M = 5$ ;

(b)  $p = 5, q = 11, b = 3, M = 9$ ;

where  $K = (n, p, q, a, b)$  are as given in the definition of the RSA Cryptosystem 5.1 and  $M$  is the text to be encrypted.

**Exercise 9.4.** In a public-key system using RSA, you intercept the ciphertext  $C = 10$  sent to a user whose public key is  $b = 5, n = 35$ . What is the plaintext  $M$ ?

*Solution.* Here,  $n = 35 = 5 \cdot 7$ , so  $\phi(n) = 24$ , and  $a \equiv b^{-1} \equiv 5^{-1} \equiv 5 \pmod{24}$ , so  $M = C^d = 10^5 \equiv 5 \pmod{35}$ .

**Exercise 9.5.** In an RSA system, the public key of a given user is  $b = 31, n = 3599$ . What is the private key of this user? (*Hint:*  $3599 = 3600 - 1 = 60^2 - 1^2 = (60 - 1)(60 + 1) = 59 \cdot 61$  and each of these is prime.)

**Exercise 9.6.** As discussed in the Singh text, the first published public-key algorithm appeared in the seminal paper by Diffie and Hellman that defined public-key cryptography and is generally referred to as Diffie-Hellman key exchange. A number of commercial products employ this key exchange technique.

Consider a Diffie-Hellman scheme with a common prime  $q = 11$  and a primitive root  $\alpha = 2$ . That is, we calculate values to send across the insecure channel by using the one-way function  $2^x \pmod{11}$ . In the example given on page 265 of Singh, the common prime is also 11 and the primitive root is  $\alpha = 7$ .

(a) If user A has public key  $Y_A = 9$ , what is A's private key  $X_A$ ?

(b) If user B has public key  $Y_B = 3$ , what is the shared secret key  $K$ ?

**Exercise 9.7.** "But," said 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 message. I am sure this is completely within Moriarty's abilities. Now in this position he will ..."

Do what?

**Exercise 9.8.** Alice wants to give her bike to Bob. But their schedules make it impossible for them to meet. If both Alice and Bob have bicycle locks, can Alice let Bob have her bike without anyone stealing it?

**Exercise 9.9.** "This is a very interesting case, Watson," Holmes said. "The young man loves a girl and she loves him too. However, her father is a strange fellow who insists that his would-be-son-in-law must design a simple and secure protocol for an appropriate public-key cryptosystem he could use in his company's computer network. The young man came up with the following protocol for communication between two parties, for example, user A wishing to send message M to user B (messages exchanged are in the format [sender's name, text, receiver's name]):

1. A sends B (A,  $E_{K_{Ub}}[M, A]$ , B).
2. B acknowledges receipt by sending to A (B,  $E_{K_{Ua}}[M, B]$ , A).

(Here  $K_{Ub}$  is B's public key, and  $K_{Ua}$  is A's public key.)

"You can see that the protocol is really simple. But the girl's father claims that the young man has not satisfied his call for a simple protocol, because the proposal contains a certain redundancy and can be further simplified to the following:

1. A sends B (A,  $E_{K_{Ub}}[M]$ , B).
2. B acknowledges receipt by sending to A (B,  $E_{K_{Ua}}[M]$ , A).

"On the basis of that, the girl's father refuses to allow his daughter to marry the young man, thus making them both unhappy. The young man was just here to ask me to help."

"Hmm, I don't see how you can help him," Watson was visibly unhappy with the idea that the sympathetic young man has to lose his love.

"Well, I think I could help. You know, Watson, redundancy is sometimes good to ensure the security of protocol. Thus, the simplification the girl's father has proposed could make the new protocol vulnerable to an attack the original protocol was able to resist," mused Holmes. "Yes, it is so, Watson! Look, all an adversary needs is to be one of the users of the network and to be able to intercept messages exchanges between A and B. Being a user of the network, he has his own public encryption key and is able to send his own message to A or to B and to receive theirs. With the help of the simplified protocol, he could then obtain a message M user A has previously sent to B using the following procedure ..." What procedure?