Chapter 10

Confidentiality Using Public Keys

Electronic commerce introduces new twists on old security issues. But the move from hard copy to electronic communications means that we need a new way to ensure the security of the communications we send and receive.

Public key cryptography can provide all the digital assurances we need, but for simplicity this chapter shows only how public and private mechanics offer Internet users confidential communications and easier key delivery. To explain in more detail how confidentiality is ensured, Chapter 11 examines one of the math tricks used to create pairs of public and private keys. Chapter 12 discusses how cryptography offers users the additional assurances of authentication, integrity, and nonrepudiation.

To illustrate confidentiality, let's pay another visit to Alice, who is now working as an Internet stockbroker. The transactions between Alice and her customers also show how public key cryptography provides a manageable solution to the problem of key distribution.

New Twists on Old Security Issues

Figure 10-1 shows Alice's interactions as an Internet stockbroker with her customers. Both broker and customer know that their communications pass through many computers and want assurances that their messages are confidential.

Let's examine only how Bob (the customer) delivers confidential messages (e.g., BUY 100 shares WigitCo. @ 14) to Alice. For the moment, we're not concerned about how Alice communicates confidential messages to the customer or how both parties get other assurances. The one-way arrow in Figure 10-1 symbolizes confidential messages being delivered to Alice. In Chapters 19, 20, and 21 you'll learn how real-world systems offer confidential messages to Bob as well as Alice.

Confidentiality before the digital age

Figure 10-2 is a simple illustration of confidentiality before the electronic age. The envelope represents confidentiality. Each of Alice's customers personally delivers the envelope to Alice or uses a trusted courier service such as the

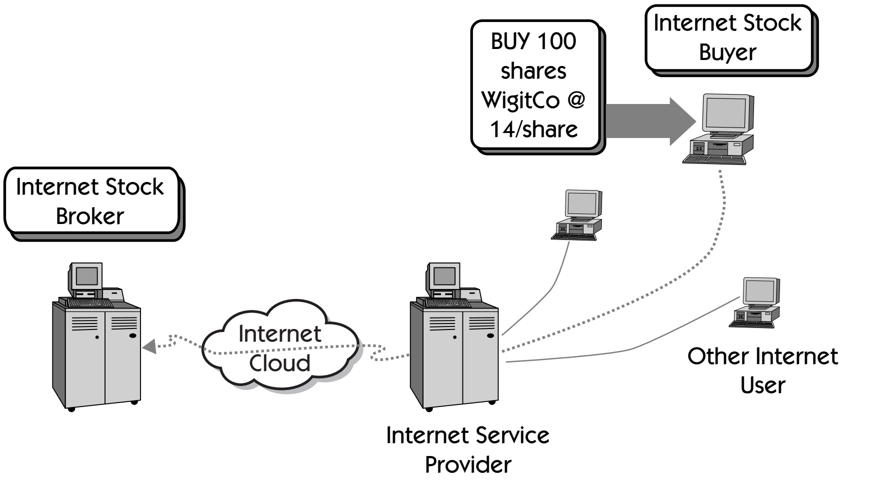


Figure 10-1 Internet business: A customer sends a buy order to a stockbroker.

U.S. Postal Service. Because Alice's customers trust that no one opens the envelope before it is put into Alice's mail slot, they trust the confidentiality of their messages.

Figure 10-2 provides an analogy that helps explain what happens with public key cryptography. Anyone who puts a message in Alice's secure mailbox is assured that only Alice can read the contents. The picture doesn't imply that Alice can securely deliver a message to a particular customer that no one else can read. Figure 10-3 shows something Alice would never do. Alice would never put an envelope addressed to one of her customers on the other side of the brick wall; she can't be sure that someone else won't open and read, destroy, or even alter the contents of the letter.

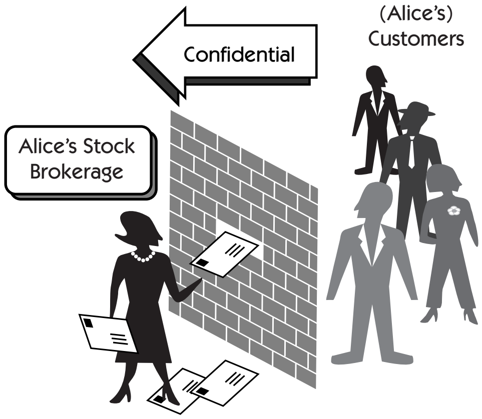


Figure 10-2 Alice receives confidential orders from Bob and others.

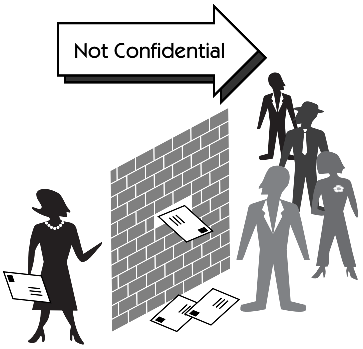


Figure 10-3 Alice can't send confidential messages to her customers in the same way they send them to her.

Public key cryptography is asymmetric. The public key encrypts (disguises). The private key decrypts (removes the disguise).

The public key cryptographic system we're about to describe works in the same way. Alice's customers can deliver confidential messages to her, but this doesn't mean that she can deliver confidential messages to any of her customers. Recall that secret key cryptography is a symmetric relationship: The sender and the receiver use the same key to encrypt and decrypt. Public key cryptography, on the other hand, is an asymmetric relationship: Public key methods create two different but mathematically related keys. What is encrypted with one key can be decrypted only with the other key. Alice's customers use the public (encryption) key, and Alice uses the private (decryption) key. This means that a message encrypted with Alice's public key is a confidential transmission between the customer and Alice. Figure 10-4 shows how we illustrate the three different kinds of keys in this book.

Another analogy can help clarify this confidentiality scenario: Public key cryptography is like a postal mailbox. Anyone can drop a letter into a mailbox, but only the person with the key (the postal employee) can open the mailbox and retrieve the mail. Similarly, anyone can use Alice's public key to encrypt a message, but only Alice (or another person who has her private key) can decrypt the message.

A message encrypted with a public key cannot be decrypted with the public key; similarly, a letter put in the top of a mailbox cannot be retrieved through the top.

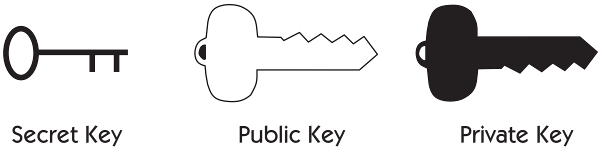


Figure 10-4 Secret keys, public keys, and private keys as represented in this book.

Confidentiality Assurances

Figure 10-5 shows Bob using Alice's public key to encrypt a message to Alice. Even though BlackHat intercepts and copies the message, he cannot decrypt the message without Alice's private key. If BlackHat tries to decrypt the message using Alice's public key, he gets gibberish. Public key cryptography gives BlackHat a tough problem while providing a trapdoor to an easy problem for Alice.

Even Bob can't decrypt a message he encrypts with Alice's public key. This means that if Bob needs to keep a readable record, he should save a plaintext copy of each message he encrypts with Alice's (or anyone's) public key.

Knowing Alice's public key doesn't give BlackHat any practical help figuring out her private key. Strong public key methods ensure that figuring out the private key is as close to impossible as cryptographers can make it. Chapter 11 shows a simple example of the principles used, and Appendix A delves deeper into some of the mathematical intricacies.

Distribution of Public Keys

It doesn't matter if anyone knows your public key.

Public key cryptography is designed so that it doesn't matter who knows or has Alice's public (encryption) key. As a result, it's easier to deliver public keys than secret keys.

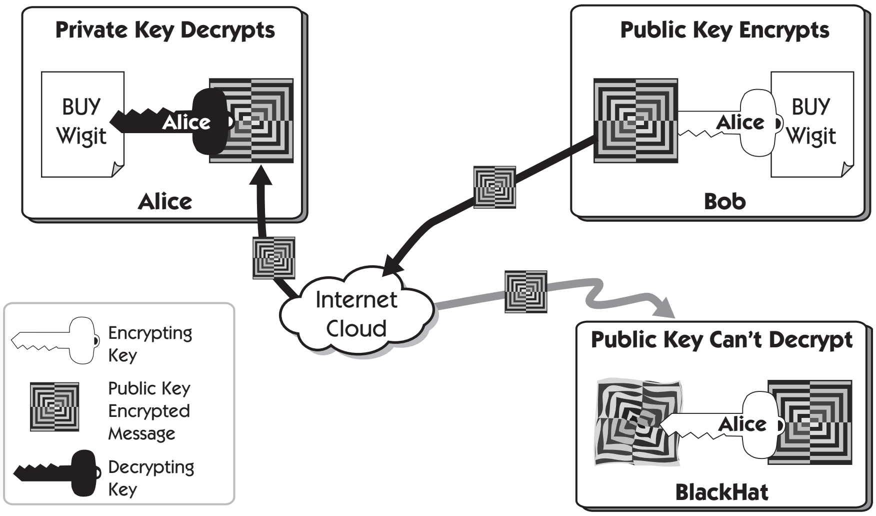


Figure 10-5 Bob sends a public key encrypted message to Alice. BlackHat copies the message but can't decrypt what the public key has encrypted.

Alice shares her public key.

In our brick wall and envelope analogy, all of Alice's customers use the same mail slot—that is, Alice's public key—to encrypt messages. This means that Alice need create only a single public key and share the identical public key with all her customers. This arrangement is much easier than sharing a different secret key with each customer.

All of Alice's customers use the same public key.

Figure 10-6 shows customers encrypting their messages using Alice's public key. Although the customers' encrypted messages pass through many computers before reaching Alice, the customers are confident that their messages are confidential because only Alice has the matching private decryption key.

Alice can send Bob the encrypting (public) key over an insecure (public) communication line, such as unencrypted e-mail, telephone conversation, and so on. Many people even put their public keys on their business card. Alice can advertise her public key in *The New York Times* or on her Internet Web site (see Figure 10-7). In fact, as we'll see in Chapters 16 and 17, some companies want as many people as possible to know and trust their public key. See authors' public keys in Epilogue.

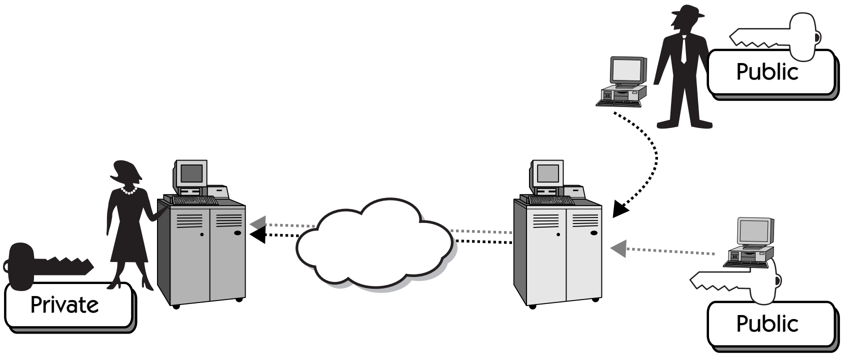


Figure 10-6 A public/private key pair. The senders have the encryption key, and the receiver has the decryption key.

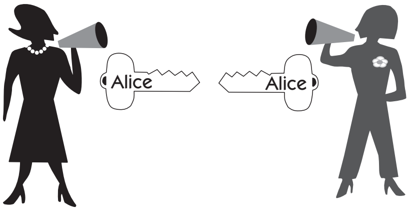


Figure 10-7 Alice announces her public key and even pays a third party to advertise it.

Attacking public keys

If BlackHat intercepts Alice's public key distribution to her customers and substitutes his own public key for Alice's, he can masquerade on the Internet as Alice. This subterfuge is known as a *man-in-the-middle* attack (see Chapter 22). Alice uses digital certificates (discussed in Chapter 16) to prevent man-in-the-middle and other attacks.

Two-Way Confidentiality

Alice can't use her private key to send confidential messages to her customers. As you have seen, she can't be sure that someone else won't pick up and read the message (see Figure 10-8).

If Alice wants to send confidential messages to a customer, she must have that customer's public key or must exchange a secret key with that customer. Two cryptographic security systems—Secure Socket Layer (Chapter 20) and IPsec (Chapter 21)—offer Alice and her customers two-way confidentiality and even more.

Alice can and does use her RSA private key to authenticate herself and her messages to her customers, and you'll see how that happens in Chapter 12. But before we jump into our public key cryptographic sportscar and drive it full speed ahead, let's look under the hood at some simple math tricks.

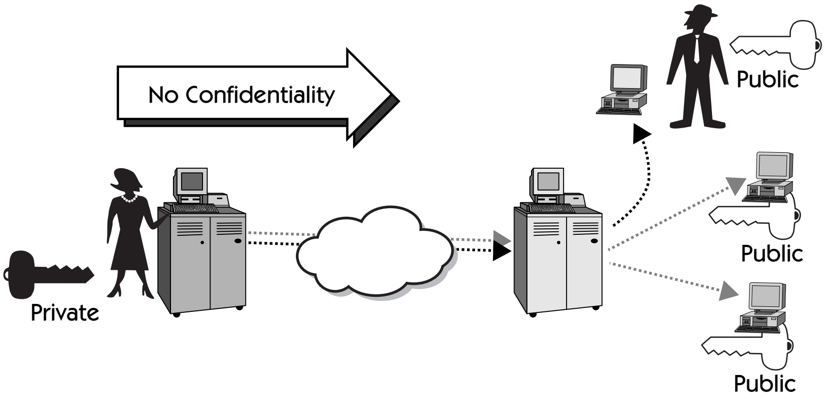
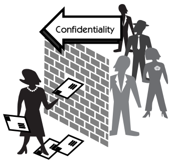
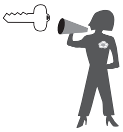


Figure 10-8 Alice can't send her customers confidential messages using only her private key.

Review





A public key is used to encrypt a message that can be decrypted only by the matching private key. Knowledge of the public key doesn't help BlackHat to quickly decipher a public key encrypted message or figure out the private key. Because the public key doesn't need to be concealed and is widely distributed, key distribution is much easier than in secret key cryptography.

Anyone can use Alice's public key to encrypt messages. Only Alice, the holder of the matching private key, can quickly decrypt messages encrypted with her public key. If Alice wants to send confidential messages to her customers, she needs a separate public key for each of them.