Chapter 8

Problems with Secret Key Exchange

Sharing and exchanging secret keys is fraught with problems, so much so that it's one of two reasons that public key cryptography was invented. The other, the need for digital signatures, is discussed in Chapter 12.

Let's reintroduce Alice and Bob and their offspring, Casey and Dawn, to help us look at conventional ways to distribute secret keys as well as typical problems with secret key distribution. Now Alice and Bob are retired and living in the upper Midwest. Their son, Casey, has taken over the California business. Their daughter, Dawn, is a well-connected bond trader in New York City.

In 1977, the year DES was released as a standard, Alice and Bob made their personal DES secret key. Bob uses DES to send Alice love notes and investment advice. They still keep their encrypted love notes.

Casey doesn't spend much time visiting his parents, but he does send them investment advice about secret deals. Because he doesn't trust the telephone (and especially electronic mail), he asks Bob for his secret key. Bob, an accommodating dad, immediately agrees, but then he remembers the encrypted romantic notes. So he makes another DES secret key to share with Casey. Figure 8-1 shows Casey sending Alice and Bob a confidential message.

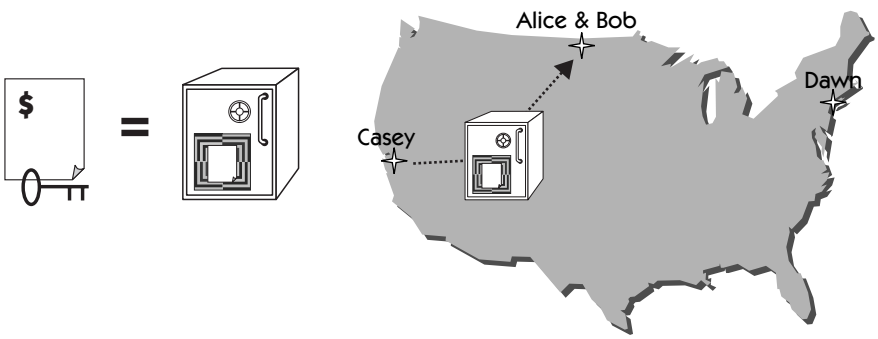


Figure 8-1 Casey wants to send Alice and Bob a confidential message.

The Problem and the Traditional Solution

How do Alice and Bob share the secret key with Casey? That is, how is it delivered to him? They can't send the secret key via mail (e-mail or postal mail or voice mail) because they can't be certain of the key's security in transit (see Figure 8-2).

Alice and Bob could personally deliver the secret key to Casey, or they could hire a trusted courier. This method, or something similar, was used for thousands of years and brings to mind a picture of a man carrying a briefcase handcuffed to his wrist. Let's assume that Casey somehow gets a secret key and that only Alice, Bob, and Casey know it.

Ancient Advice of Sun-Tzu

"A hundred ounces of silver spent for information may save ten thousand spent on war," wrote early fourth century B.C. Chinese general Sun-Tzu. Attuned to the value of intelligence gathering, he would have insisted upon the careful delivery and storage of secret keys. Because he believed "to subdue the enemy without fighting is the supreme excellence," he also would have endorsed clandestinely stealing your opponent's secret keys. His advice in *Ping-fa* (*The Art of War*), the earliest known text on war and espionage, is still studied by modern military strategists who take to heart that "nothing should be as confidential as the art of intelligence."

Soon after Alice and Bob begin exchanging secret messages with Casey, Dawn wants a secret key, too. For personal family reasons, she does not want to use the secret key her parents share with Casey and wants her parents to make a new secret key. So Alice (or Bob) must travel to New York City and deliver a secret key to Dawn.

Alice and Bob now have three secret keys[1]: one for their love notes, a second one they share with Casey, and a third one they share with Dawn.

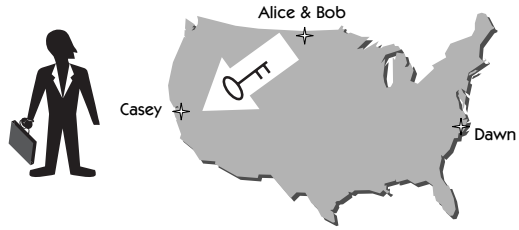


Figure 8-2 Delivering a secret key can be problematic. (Dawn now telecommutes from North Carolina.)

1. This assumes that they're using DES or the new AES standard, Rijndael. If they are using Triple DES, they have nine (or six) keys.

Alice and Bob use their shared secret key to ensure the confidentiality of their romantic letters. They use the secret keys they share with Casey and Dawn to ensure authentication, message integrity, and confidentiality with their children. Figure 8-3 shows the current arrangement. Although it includes only three people, it's already getting complicated.

The Ecstasy of the Agony

In the mid- to late 1800s, lovers used cryptography to communicate clandestinely in a very public place: the newspaper. But their amateur efforts were often the playground for budding cryptanalysts, who delighted in uncovering their lovelorn messages, which were printed in what was termed the "agony columns."

Charles Babbage, who expressed the principles behind today's computers back in the 1800s but could never make them work, was one who liked to cryptanalyze the agony columns. In school Babbage often suffered for his cleverness in decrypting others' notes. Cryptographic historian David Kahn quotes Babbage's remembrances: "The bigger boys made ciphers, but if I got hold of a few words, I usually found out the key. The consequence of this ingenuity was occasionally painful: The owners of the detected ciphers sometimes thrashed me, though the fault lay in their own stupidity."

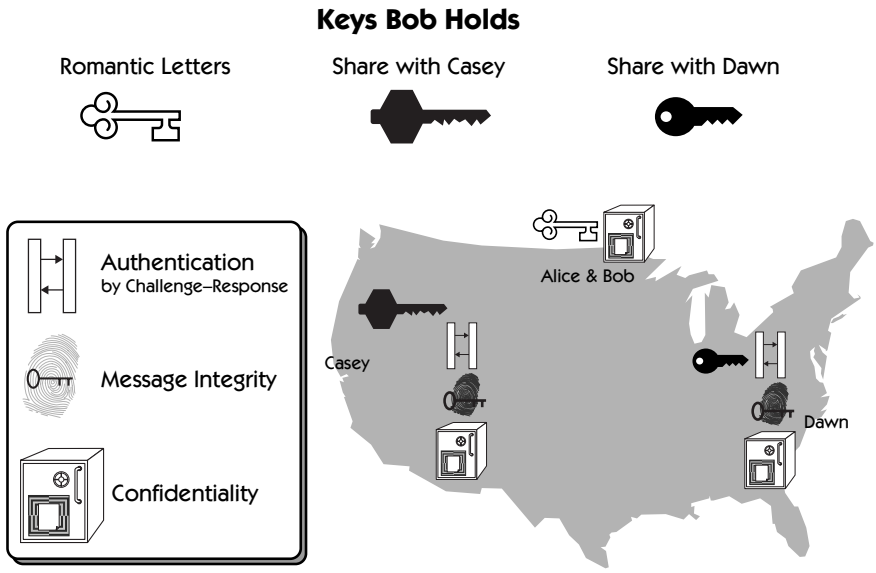


Figure 8-3 Secret keys and their uses.

Using a Trusted Third Party

The situation gets more complicated when Casey and Dawn decide to exchange secret messages through Bob. Figure 8-4 shows how it's done. First, Casey encrypts a message using the secret key he shares with Bob. Next, Bob decrypts the message and then encrypts it with the secret key he shares with Dawn. Then Dawn decrypts the message using the key she shares with Bob. Note that in Figure 8-4 the encrypted text Casey sends to Bob is different from the encrypted text Bob sends to Dawn. This is because there are two different encryption keys.

Definition: trusted third party

In effect, the children want their parents to be a conduit for messages. Bob (or Alice) is the conduit, or *trusted third party* (TTP). That may sound like a nice title, but remember that the TTP must decrypt and encrypt each message, resulting in twice the work of either Casey or Dawn. Some cryptographic

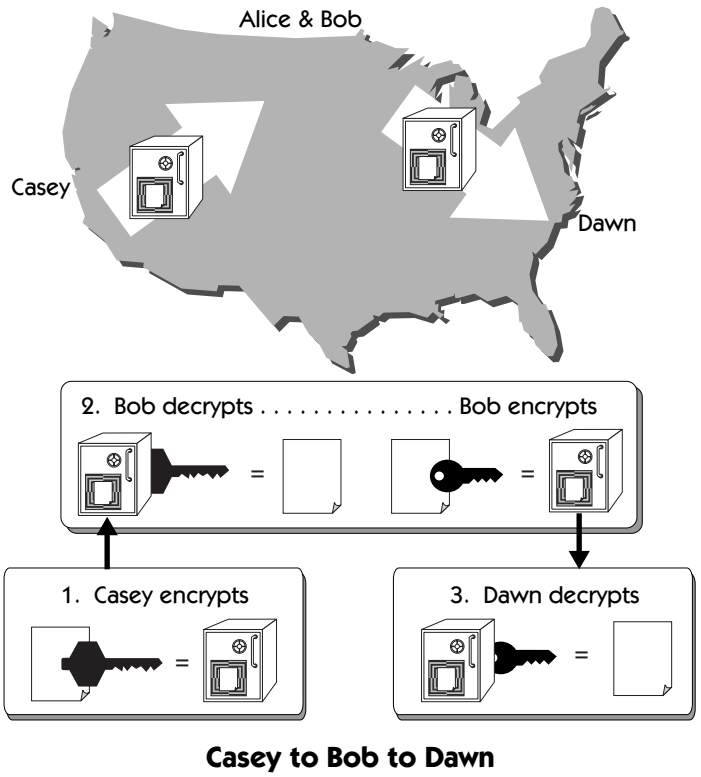


Figure 8-4 Bob becomes a trusted third party for Casey and Dawn.

literature calls this the military model because the troops, Casey and Dawn, must communicate through a superior ranking solider, Bob or Alice.

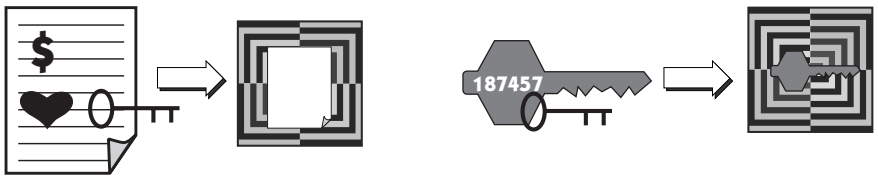
After Bob spends a few hours decrypting and encrypting messages, he realizes that it would be better if Casey and Dawn were able to communicate directly. Bob makes another secret key. But Alice, Bob, Casey, and Dawn don't want to travel to deliver or pick up the key. They don't trust couriers because keys can be lost, stolen, or even sold (or copied) by an untrustworthy courier.

Cryptographers often use secret keys to encrypt other secret keys.

But because Alice and Bob are a TTP, no one has to travel. That's because secret keys can encrypt secret keys in the same way that secret keys encrypt love notes or financial text. A cryptographic key is just like a text message except that it contains only a long, random number. In fact, cryptographic keys are often used to encrypt secret keys, as shown in Figure 8-5. Cryptographers often refer to encrypting a secret key as *wrapping* it.[2] One more, perhaps obvious, point: the cipher and key wrapping (encrypting) another key should be at least as strong as the key being wrapped. It's silly to wrap (encrypt) a 168-bit Triple DES key or a Rijndael key with a weaker 56-bit DES key.

Trusted Third Parties Aren't Always So Trustworthy

Marie Antoinette and Louis XVI trusted a good-looking Swede, Count Axel Fersen, to help them escape their fate in the French Revolution. Fersen handled enciphering and deciphering the heavy traffic of cryptographic correspondence to and from the co-conspirators during the two months before the planned escape. It wasn't Fersen's fault that the king and queen were caught in their disguise as servants. After all, he'd had extensive experience encrypting and decrypting his own love notes to and from Marie before this assignment. If King Louis had known, he might not have considered this trusted third party so trustworthy!



(a) Encrypting Messages (b) Encrypting a Secret Key

Figure 8-5 Secret keys are used to encrypt (a) messages and (b) other secret keys.

2. For a real-world example, see Part IV.

Key Distribution Center and Key Recovery

Kerberos, a cryptographic authentication system, acts as a KDC.

At the top of Figure 8-6, Bob sends Casey and Dawn the new secret key encrypted with the respective secret keys they share with Bob. Bob and Alice are now a key distribution center (KDC)[3] (Figure 8-7). Other names for this setup include key exchange authority and key exchange center.

At the bottom of Figure 8-6, Casey and Dawn use the new secret key and exchange encrypted messages. The messages need not be passed through Bob. Casey and Dawn trust that Bob will not intercept messages and decrypt their message using the secret key he made. In fact, Bob can (and arguably should) destroy his original copy of Casey and Dawn's secret key.

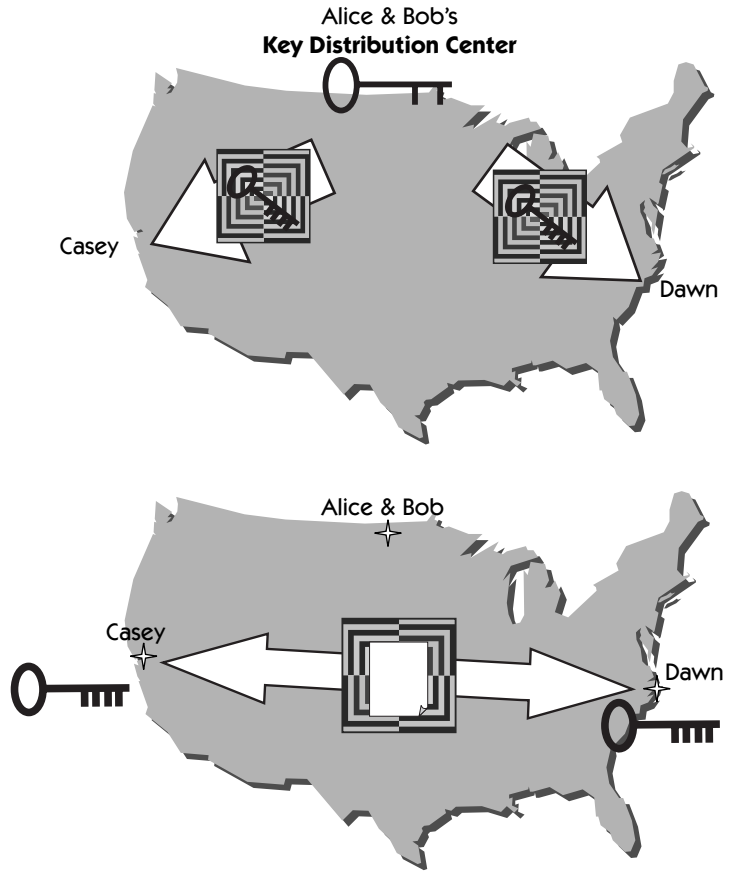


Figure 8-6 Alice and Bob assume the role of a key distribution center.

3. Kerberos, used extensively in Microsoft Windows 2000, is modeled on a KDC.

Key escrow

But Casey and Dawn may ask Bob to keep a copy in case one of them loses the secret key. Bob is now a key *recovery* (or key *escrow)* agent. Bob should hold Casey and Dawn's key in an encrypted form so that it cannot be used even if lost or stolen. In the larger world, there is heated debate about who should have access to secret keys and how they should be recoverable.

Storing secret keys

For extremely important keys, Bob may choose to split up Casey and Dawn's key into two or more parts, keeping the parts separate. In this way, all the parts must be lost or stolen before the key is compromised. Key splitting and key recovery are interesting topics, but they are beyond the scope of this book.

Problems with Using a Trusted Third Party

Although it's convenient to have a trusted third party to create a common secret key, this approach has a number of problems. Let's take a look.

Growth in the Number of Secret Keys

Secret key sharing and distribution is a big, big problem.

Although secret key delivery isn't difficult if you have only a few users, it's almost impossible to deliver secret keys to a large network of users. For example, if Casey has offices in all three West Coast states, each office wants a secret key with every other office. Bob must make and send three new secret key pairs, as shown in Figure 8-7.

Opening an office in each of the 50 states greatly expands the number of different keys. Each state office must have 50 different secret keys (one key for each of the states and one key for Bob). This means that there are more than 1,200 secret keys.

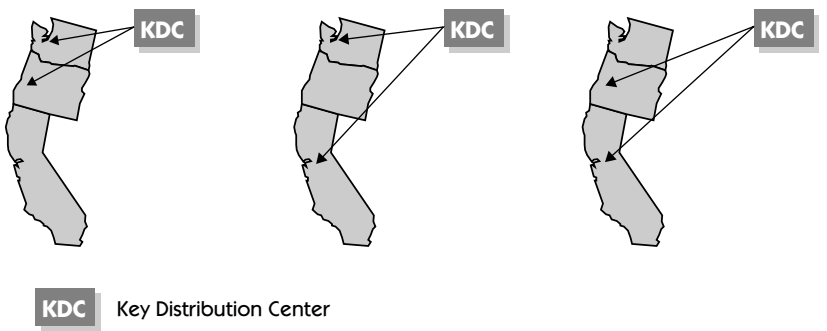


Figure 8-7 As the business grows, so does the number of shared secret keys.

In general, a key distribution center supporting X sites, where each site needs a secret key with every other site, must make almost (X * X)/2 keys.[4] This means that a KDC supporting 1,000 sites must make almost (1,000 * 1,000) /2 = 500,000 keys, an unmanageable number of keys.

Trust and Lifetime

Of course, Casey and Dawn totally trust their parents, but they must also implicitly trust everyone who has access to Bob's computer. If Bob's computer holds many secret keys, it is a worthwhile target. Once Casey and Dawn's shared secret key is compromised, any encrypted message they ever sent that was previously intercepted and saved can also be decrypted. Old encrypted messages may still have value to an adversary.

The best encryption algorithm is useless if you don't protect your secret key.

Secret keys are not secure forever. They can be stolen, lost, forgotten, destroyed, stored in insecure ways, or copied without authorization. A secret key that has been used many times probably hides more secrets than a secret key that has been used only once. An adversary is more likely to go after the secret key that has been used many times. In Part IV, "Real-World Systems," we'll see how new secret keys are easily shared.

A better way to handle key management is available through public key cryptography. In Chapter 9 we examine a clever technique for exchanging secret keys over public channels that sets the framework for methods being used today.

Review

Secret communications with secret keys implies that *only* trusted parties should have copies of the secret key. Although secret keys can assure us of confidentiality, authentication of users, and message integrity, in a global world we must be able to securely distribute keys at a distance in a timely manner. If security is to be maintained, key distribution must be as solid as the cryptographic method and must be able to ensure that only trusted parties have copies of the keys. Obviously, key distribution is a significant problem.

Traditional methods of key distribution use trusted couriers to place the initial secret key. If the key is shared with a trusted third party (TTP), additional keys can be shared because secret keys can encrypt secret keys for distribution in the same way that secret keys encrypt love notes and financial statements. When the TTP encrypts any additional keys with the shared secret key, the TTP is often referred to as a key distribution center (KDC).

4. Exactly: X * (X-1) / 2.

The KDC is often burdened with extensive key management and can become a bottleneck. Additionally, if the KDC also acts as a key escrow agent, the KDC itself is an attractive target.

Public key encryption makes (secret) key distribution much easier.