How Encryption Works

Encryption, or the process of obscuring or concealing data to keep it private, is one of the most common security methods used on the Internet. Encrypted data appears as a string of gibberish. To read encrypted data, you must be able to decrypt it. In most cases, only a person with the correct key, which is a type of mathematical password, can decode the information.

To encrypt data, a cipher or encryption algorithm (mathematically based instructions) is used to obscure the meaning of the original data. The original message is called plaintext, and the final form (the encrypted version) is called ciphertext. An encryption key changes the way plaintext is encrypted into ciphertext to make it harder to decode. The recipient of the data or message must have a copy of the key to decrypt the ciphertext back into readable plaintext.

Two types of encryption keys exist: symmetric (secret) key and asymmetric (public) key. In symmetric-key cryptography, the same key is used to encrypt and decrypt a message. This means both the sender and the recipient must know the key. The primary weakness of this method is that the sender must find a secure method for transmitting the key. And because both machines must use the key during a transmission, the encrypted message and key are vulnerable to interception and decryption.

In asymmetric-key cryptography, a widely known public key is used to encrypt a message; the private key, known only to the recipient, is used to decrypt the message. Private keys are mathematically related to public keys. Its primary weakness is the long time it takes to encrypt and decrypt files.

Bob's Computer

Bob encrypts his message to Mary using the secret key.

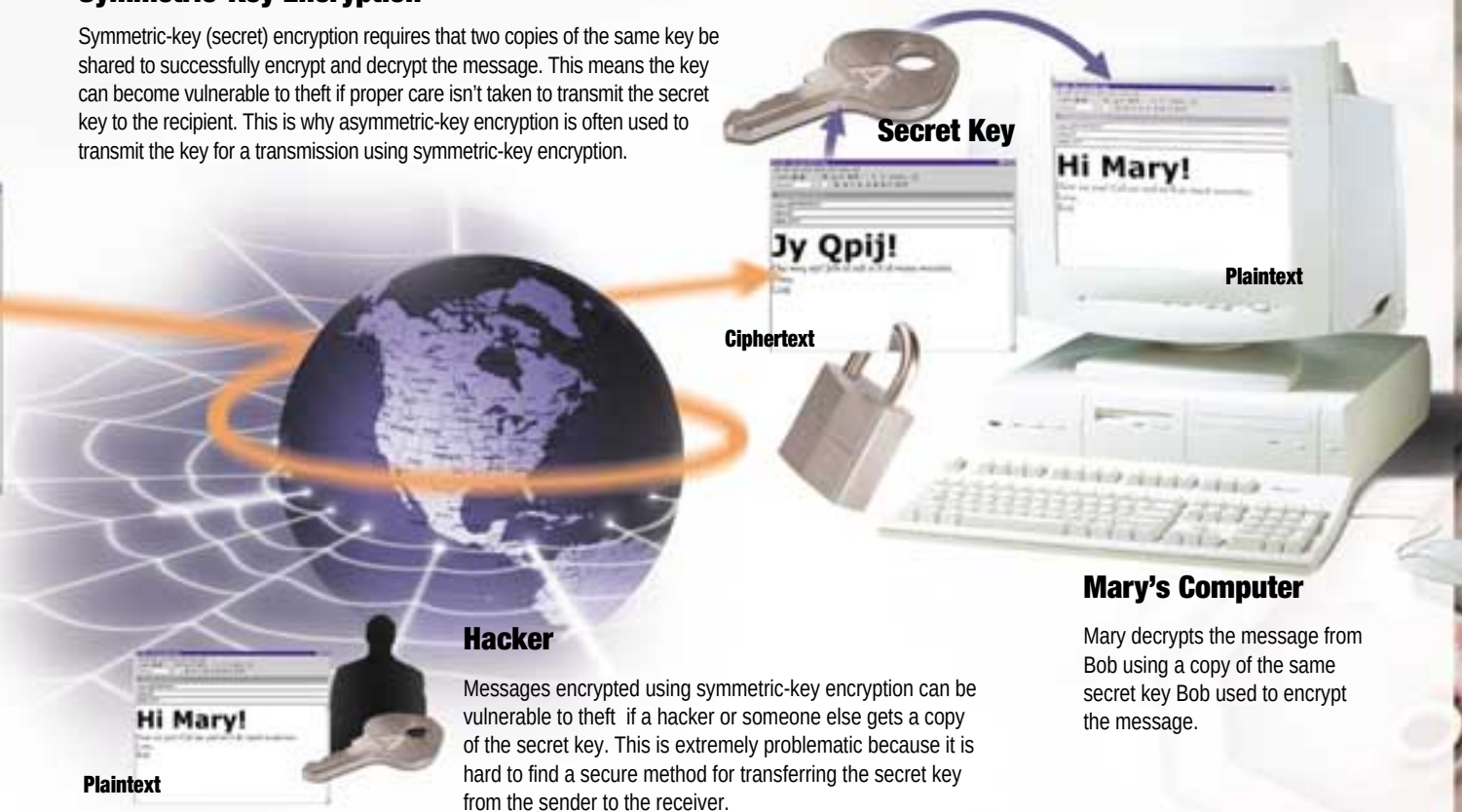
Bob's Computer

Bob encrypts a message for Mary with the public key that she sent him.

Compiled by Bill Hayes
Graphics & Design by Lori Garris

Symmetric-Key Encryption

Symmetric-key (secret) encryption requires that two copies of the same key be shared to successfully encrypt and decrypt the message. This means the key can become vulnerable to theft if proper care isn't taken to transmit the secret key to the recipient. This is why asymmetric-key encryption is often used to transmit the key for a transmission using symmetric-key encryption.



Mary's Computer

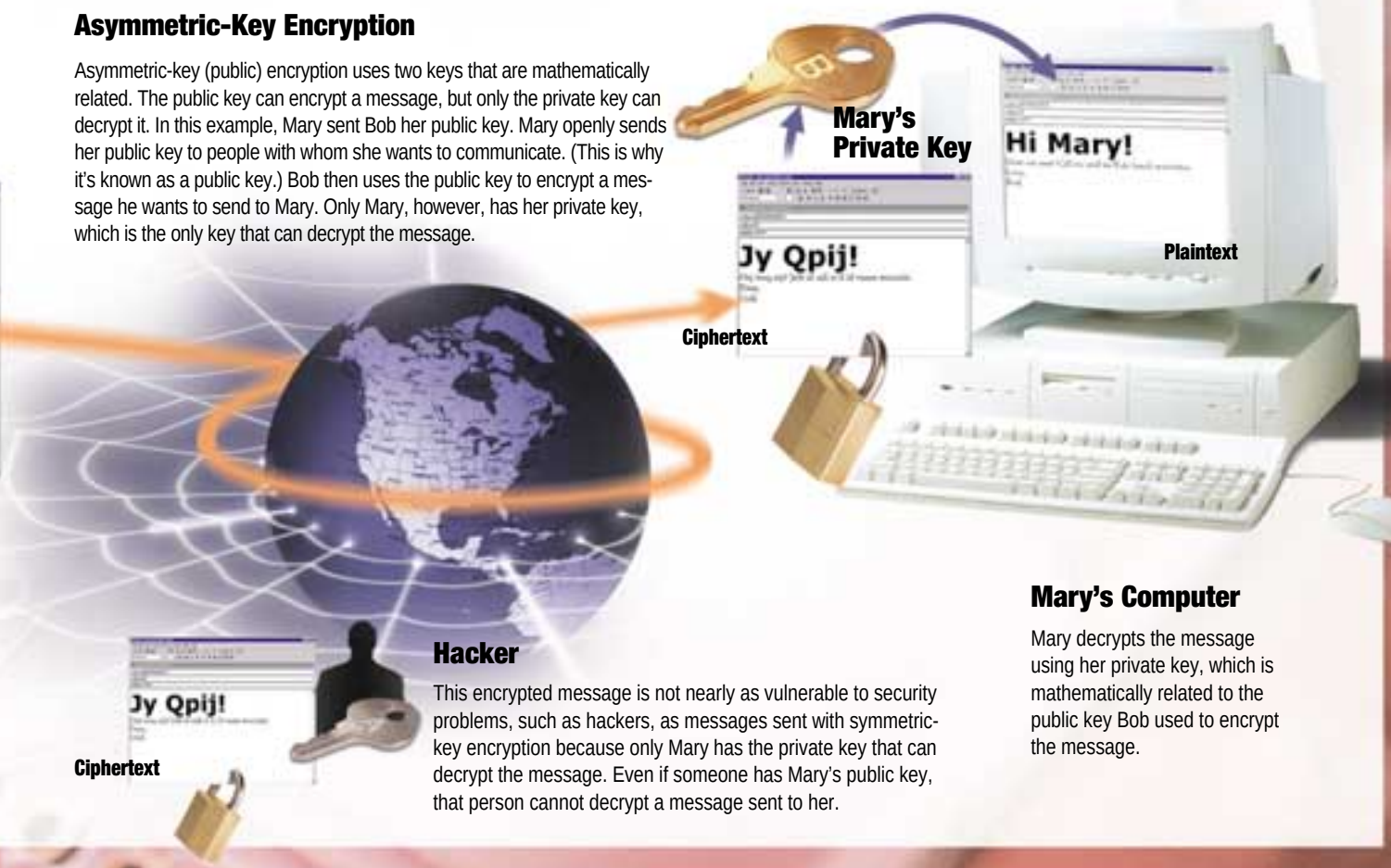
Mary decrypts the message from Bob using a copy of the same secret key Bob used to encrypt the message.

Hacker

Messages encrypted using symmetric-key encryption can be vulnerable to theft if a hacker or someone else gets a copy of the secret key. This is extremely problematic because it is hard to find a secure method for transferring the secret key from the sender to the receiver.

Asymmetric-Key Encryption

Asymmetric-key (public) encryption uses two keys that are mathematically related. The public key can encrypt a message, but only the private key can decrypt it. In this example, Mary sent Bob her public key. Mary openly sends her public key to people with whom she wants to communicate. (This is why it's known as a public key.) Bob then uses the public key to encrypt a message he wants to send to Mary. Only Mary, however, has her private key, which is the only key that can decrypt the message.



Mary's Computer

Mary decrypts the message using her private key, which is mathematically related to the public key Bob used to encrypt the message.

Hacker

This encrypted message is not nearly as vulnerable to security problems, such as hackers, as messages sent with symmetric-key encryption because only Mary has the private key that can decrypt the message. Even if someone has Mary's public key, that person cannot decrypt a message sent to her.