Email Encryption with Public Key Cryptography

Kayla Gursahaney
ENGL 220c
Assignment 4: Definition and Description
March 24, 2016

Introduction

Public key cryptography is a form of data encryption that is typically used to protect information transmitted over the Internet. Also known as asymmetric encryption or public key encryption (PKE), this method ensures that information sent through email or other electronic communication forms can only be accessed by the person or people the sender wants to see it. Without some form of encryption, information sent over the Internet can easily be intercepted and read or altered by third-party eavesdroppers. Public key cryptography can also be used to verify the identity of the sender, depending on the encryption method.

What is Cryptography?

In the simplest terms, **cryptography** is the study of encoding information and making readable messages unreadable. For as long as written communication has existed, cryptographic formulas, called **algorithms**, has been used to ensure that sensitive information can only be accessed by those who are meant to see it. Today cryptography is primarily used in cybersecurity to protect electronic information stored in computers and transmitted across the Internet.

When information is encrypted, the original message, or **plaintext**, in converted into an unintelligible code, or **ciphertext**. When information is decrypted, the process is reversed and the ciphertext is reverted back to the original plaintext, which can now be read and understood. Ideally, only the intended recipient of the information should be able to decrypt the ciphertext and access the original message.

Symmetric vs Asymmetric Encryption

Encryption algorithms are usually categorized based on the number of keys they require. A **key** is a piece of data that determines the output of an algorithm. When different keys are used with the same algorithm and plaintext, different ciphertexts are created.

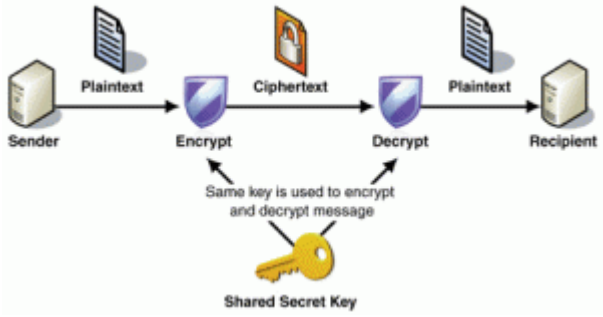
Symmetric

In symmetric encryption, the same key is used to both encode and decode the plaintext message (Figure 1). This key is known to both the sender and the recipient, but must be kept secret from potential eavesdroppers. By knowing the key used to encrypt the message, and individual would also be able to decrypt it.

Asymmetric

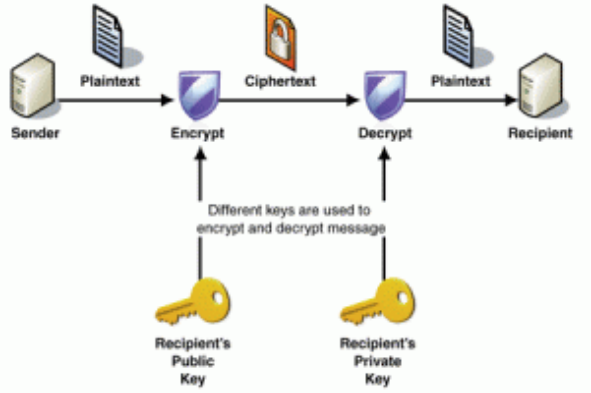
In asymmetric encryption, the algorithm requires two complementary keys. The sender uses the first key to encrypt the information, while the recipient uses the second key to decrypt the ciphertext (Figure 2). Unlike symmetric key encryption, an individual would not be able to decode the message if they know the key that was to encrypt it, making this method more secure. Public-key cryptography is an example of asymmetric encryption.

Figure 1: Symmetric Encryption



Source: Sachi Mani Software Blogs

Figure 2: Asymmetric Encryption



Source: Sachi Mani Software Blogs

Public and Private Keys

All asymmetric encryption methods require two complementary keys. These are known as the public key and the private key.

Public Key

As the name suggests, a person's public key can be accessed by anyone. When the sender encrypts their message using the recipient's public key, they ensure that only the recipient will be able to decrypt it with their corresponding private key.

Private Key

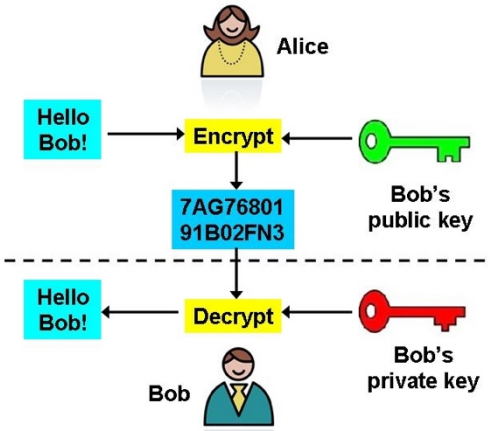
A person's private key is known only to that specific individual, and is used to decrypt messages encoded with their public key. Senders can also encrypt messages with their own private keys as a means of verifying the sender's identity.

How Public Key Cryptography Works

Consider the following scenario: Alice wants to send her friend Bob an email, but is afraid that the contents of her message will be intercepted while the email is travelling across the Internet. Fortunately, both her and Bob's computers use public key cryptography to protect the information in the message from eavesdroppers (Figure 3).

1. Alice uses Bob's public key to encrypt the message. This ensures that only Bob will be able to decrypt the message.
2. Alice sends the encrypted message to Bob over the Internet. If the message is intercepted, its contents cannot be accessed by third-party eavesdroppers.
3. Bob receives the encrypted message and uses his private key to decrypt it. He is now able to read the plaintext message.

Figure 3: Public Key Cryptography



Source: Wellesley College, CS110: Computer Science & the Internet

Enveloped Public Key Encryption

Enveloped Public Key Encryption (EPKE) is a more secure form of public key cryptography, in which the sender encrypts their message using both the recipient's public key and the sender's private key. In addition to protecting the information within the message, this verifies the sender's identity by creating a digital envelope.

1. Alice uses Bob's public key to encrypt the message. This ensures that only Bob will be able to decrypt the message.
2. Alice uses her private key to encrypt the message again. This creates a digital envelope and verifies the sender's identity.
3. Alice sends the encrypted message to Bob over the Internet. If the message is intercepted, its contents cannot be accessed by third-party eavesdroppers.
4. Bob receives the encrypted message and uses Alice's public key to decrypt the digital envelope.
5. Bob uses his key to decrypt the second level of encryption. He is now able to read the plaintext message.

Conclusion

In today's digital age, nearly all important information is communicated across open networks like the Internet, where data can easily be intercepted. Encryption methods such as public key cryptography are one way of ensuring that electronic communication is more secure.