Cryptography

Abdul Ahad
ISNM 2003 **Dated:** 3-12-2003

Abstract

Cryptography is the science of using mathematics to encrypt and decrypt data. It is the process of altering messages so as to hide their meaning from adversaries who might intercept them. Today it might be summed up as the study of techniques and applications that depend on the existence of difficult problems. *Cryptanalysis* is the study of how to compromise (defeat) cryptographic mechanisms, and *cryptology* (from the Greek *kryptós lógos*, meaning ``hidden word'') is the discipline of cryptography and cryptanalysis combined. Cryptography plays a crucial role in the transfer of confidential information across local networks and the Internet.

The Caesar Cipher

Julius Caesar is considered to be one of the first persons to have ever employed encryption for the sake of securing messages to communicate with his army. He decided that shifting each letter in the message would be his standard algorithm, and so he informed all of his generals of his decision. Using the Caesar Shift (3 to the right), the message,

"RETURN TO ROME"

would be encrypted as,

"UHWXUA WR URPH"

In this example, 'R' is shifted to 'U', 'E' is shifted to 'H', and so on. Now, even if the enemy did intercept the message, it would be useless, since only Caesar's generals could read it.

Key Terms

- *Plaintext* is a message readable by anyone.
- *Cipher text* is plaintext that has been modified to protect its secrecy.
- *Encryption* converts plaintext to cipher text.
- *Decryption* converts cipher text to plaintext.
- *Key* is actually a password string, used for encryption and decryption.

Cryptography Types

1. **Private-Key Cryptography**

In private-key cryptography, the sender and recipient agree beforehand on a secret *private key*. The plaintext is somehow combined with the key to create the cipher text. And then it is transferred to some insecure channel, it may be Internet or intranet and the receiver can decrypt this message with secret key. As no body else is supposed to know this key, sender and receive just manage to secure the message.

To break a message encrypted with private-key cryptography, an attacker must either exploit a weakness in the encryption algorithm itself, or else try an *exhaustive search* of all possible keys. If the key is large enough (*e.g.*, 128 bits), such a search would take a very long time, even with very powerful computers. The practical example of this type of cryptography might be the case of transferring the nuclear codes to the submarine or to nuclear silos sites by the US president.

But there was a major problem with this type of cryptography that sender and receiver both has to meet in advance in order to exchange the secret key. It could be a big problem when you have to communicate with the person that is too far to approach. And then if you think that you are smart enough to exchange the keys securely then why don't you exchange the information itself.

2. Public Key Cryptography

The idea of a public-key cryptosystem (using asymmetric algorithms) was proposed by Diffie and Hellman in their pioneering paper in 1976. Their revolutionary idea was to enable secure message exchange between sender and receiver without ever having to meet in advance to agree on a common secret key.

The setup of a public-key cryptosystem is of a network of users rather than a single pair of users. Each user in the network has a pair of keys associated with him, the public key, which is published under the users name in a *public directory* accessible for everyone to read, and the private-key, which is known only to the user. Running a key-generation algorithm generates the pair of keys. To send a secret message to a user everyone in the network uses the same exact method, which involves looking up the public key from the public directory, encrypting the message using the public key, and sending the resulting cipher text to the user. Upon receiving the cipher text, the receiver can decrypt by looking up his private key.

Comparisons

Private-key methods are efficient and difficult to break. However, one major drawback is that the key must be exchanged between the sender and recipient beforehand, raising the issue of how to protect the secrecy of the key.

While public key cryptosystems overcome a key limitation of conventional cryptosystem, this comes at a price. You need more processing power to encrypt and decrypt messages under a public key cryptosystem, in fact conventional encryption is reckoned to be 1000 times faster than public key encryption. Public keys need to be much

larger to ensure the same level of security that is possible with a much smaller conventional key. A conventional 80-bit key has the same strength as 1024-bit public key.

1. Public-key cryptography facilitates efficient signatures (particularly non-repudiation) and key management, and
2. Symmetric-key cryptography is efficient for encryption and some data integrity applications.

Conclusion

Often, cryptosystems use a combination of both conventional and public key cryptography. PGP for example, uses conventional cryptography to obtain the high security it provides with a smaller key size, and then use public key cryptography to encrypt just the conventional key that was used to encrypt the message.

If you surf the net, you have probably used cryptography sometimes even without knowing it, in fact each time you shop on the net or provide any personal information, there is a good chance that your browser is communicating securely with the other server using Secure Sockets Layer (SSL) which is based upon the RSA public key cryptography.