



A **bTrade** White Paper

655 N. Central Ave.
Suite 1460
Glendale, CA 91203
(818) 334 4177

www.btrade.com

Fundamentals of Cryptography for Message Security

© 2011 bTrade LLC

All rights reserved.



Contents

Introduction	3
Chapter 1	3
Chapter 2	5
Chapter 3	6
Chapter 4	8
Chapter 5	11
Chapter 6	12
Chapter 7	14

Introduction

Cryptography, which can be defined as transforming or enciphering a text message into secret code called a cipher, has a long history dating back to ancient times. The main purpose of encryption is to protect information, and has been widely used by the military in times of war.

Chapter 1

A Short History of Cryptography

Chapter 2

Cryptographic Security Services

Chapter 3

Using Cryptography to Provide Privacy

Chapter 4

Digital Signatures

Chapter 5

Management of Public Keys

Chapter 6

Secure Messaging Using AS2

Chapter 7

bTrade Provides Cryptography for Message Security

Introduction

1. A Short History of Cryptography

Cryptography, which can be defined as transforming or enciphering a text message into secret code called a cipher, has a long history dating back to ancient times. The main purpose of encryption is to protect information, and has been widely used by the military in times of war. Ciphers have also been used by craftsmen trying to hide secret formulas and by participants in political intrigue. Mary Stuart, Queen of Scotland, was put to death for treason on the basis of cipher-encoded letters advocating the assassination of Queen Elizabeth I. Cipherying was also popular as amusement for the cultured classes. Edgar Allen Poe was noted for his deciphering skills and wrote a book that proved to be of use to British cryptanalysts in breaking German codes in World War I. The opposite of cryptography is called cryptanalysis, where methods are used to decipher encrypted information without knowledge of the encryption process used.

Early Cipher Systems

There has always been a competition between cryptographers, whose aim is to create more complex ciphers, and the cryptanalysts who try to break the cipher. Two early methods of encryption are **substitution** and **transposition** ciphers. In a substitution cipher, letters of the original message, called **plaintext**, are replaced with **ciphertext**, which may consist of one or more letters. A monoalphabetic cipher uses the same substitution scheme for the entire message, whereas a polyalphabetic cipher changes the substitution scheme at different points in the message. In a transposition cipher, the letters of the plaintext are left unchanged but are rearranged in a complex order. These cipher schemes were defeated by cryptanalysts using frequency analysis, which is based on the fact that languages use certain letters and combinations of letters with varying frequencies.

Electromechanical Cipher Machines

The first half of the twentieth century saw great advances in both cipher design and cryptanalysis. Electromechanical cipher machines were in wide use in the years leading to World War II, with the most famous being a rotor machine known as Enigma. The basic encryption element of the machine was a collection of rotors, or wheels, aligned in a row. Each wheel had the 26 letters of the alphabet inscribed on their outside edge, and transformed a letter typed on a keyboard through a series of electrical connections. For example, if three rotors were aligned to W, Y, and R, respectively, an A typed using the keyboard would be changed to W by the first rotor, Y by the second rotor, etc. The settings for each enigma machine were changed daily according to a codebook distributed previously, and often before each new message. Using several rotors vastly increased the number of possible combinations according to the formula 26^n , where n is the number of rotors.

Modern Cryptography

With the development of computers following World War II, cryptography and cryptanalysis became far more sophisticated, requiring backgrounds in theoretical mathematics. Many cryptosystems are based on solving difficult mathematical problems like the factoring of large integer numbers. In 1975, the first release of a cipher system by the federal government occurred in the form of the Data Encryption Standard (DES), developed by a research group at IBM, in an effort to develop secure electronic communication facilities for businesses. Although the DES cipher is no longer considered secure, the release of the DES specification stimulated an upsurge of public and academic interest in cryptography resulting in many new cipher systems that are in use today.

2. Cryptographic Security Services

The obvious use, or service, provided by cryptography is to protect the content of the message from everyone except the intended recipient. But there are other issues involved in confidential communications. How can the credentials of the parties involved in the communication be verified? How can assurance be provided that the content of the message was not altered during transmission? How can protection be provided against one party falsely denying that the message exchange took place? Security services that address these issues are described below.

Confidentiality

Cryptography converts plaintext messages from an originator into ciphertext, which then must be unscrambled by the recipient of the message. Confidentiality (privacy, secrecy) is a service ensuring that information contained in a message is not revealed to unauthorized persons.

Authentication

Authentication is the process of verifying parties in a communication. Basic authentication in a computer-linked network is commonly done through the use of logon passwords. Since passwords can be stolen or forgotten, other techniques such as digital signatures have been developed to provide authentication.

Integrity

Integrity means ensuring that the data has not been tampered with during transmission. The goal is to detect alteration or destruction of data during transmission. Digital signatures, as explained later, allow verification of data consistency by comparing message digests generated before and after message transmission.

Non-Repudiation

Repudiation occurs when either the message originator or recipient falsely denies that the exchange took place, and is an important issue for trading partners

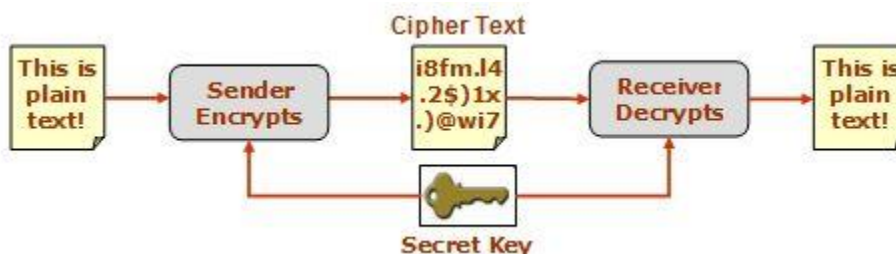
transacting business. Non-repudiation of origin and non-repudiation of delivery are services that protect against threats from legitimate parties rather than from outside attackers.

3. Using Cryptography to Provide Privacy

A cryptosystem, or encryption algorithm, is the mathematical function used to encrypt and decrypt data. These algorithms rely on a **secret key**, a randomly-generated data value (string of bits) used for encryption and decryption. Because encryption algorithms are generally well known, the needed secrecy is provided by protecting the key from discovery instead of the encryption method. The length of the key in number of bits (or key strength) determines how difficult it will be for an attacker with massive computing capabilities to decrypt the text without knowing the key. The following string of ASCII characters represents a key of 128 bits (16 bytes): 42385F213EJ47359. There are two types of key-based cryptosystems, secret-key and public-key systems.

Secret-Key Systems

Secret-key algorithms, also called symmetric algorithms, form the foundation of the cryptographic process. A single key, which both sending and receiving parties must have, is used to encrypt and decrypt a message. Secret-key systems may be depicted by the following diagram:



There are two vulnerabilities of the secret-key approach. The first is related to key-strength. DES was based on a 56-bit key, meaning that there are 2^{56} possible key

values (called keyspace). Computing technology had advanced by the late 1990s to the point that it was possible by brute force to try every combination to find the one that successfully decrypts. This led to the development of other encryption algorithms such as *Advanced Encryption Standard (AES)*, which uses key sizes of 128, 192, and 256 bits, *Triple Data Encryption Standard (3-DES)*, which uses a multiple encryption approach, and *Proprietary ciphers* such as those from RSA Security (RC2, RC4, etc.), IDEA, Blowfish, and CAST.

The second weakness of the secret-key approach is how to keep the key secret, so that only the intended message recipients have the key. The difficulty in providing secure key management (the generation, transmission and storage of keys) and the need to change the value of the secret-key periodically, ideally whenever a new message is sent, led to the development of public-key cryptography.

Public-Key Cryptography

To solve the key management problem, Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography in 1976. In their system, each party has a pair of related keys: a **public key** which is published to all partners, and a **private key** which always is kept secret. With this approach, the sender and receiver no longer need to share a secret key. In a public-key encryption algorithm, the private key is always mathematically related to the public key. The most widely used public-key cryptosystem is RSA Security's RSA algorithm, which supports key lengths up to 3,072 bits. Using the RSA algorithm, an attacker trying to derive the private key from the public key would have to factor the product of two extremely large prime numbers. The RSA algorithm is used for two purposes:

1. To ensure confidentiality of the secret-key used for message encryption; in this manner, the secret-key can be changed with each message
2. To verify, or authenticate, the sending party by attaching a digital signature to the message (discussed in the next chapter)

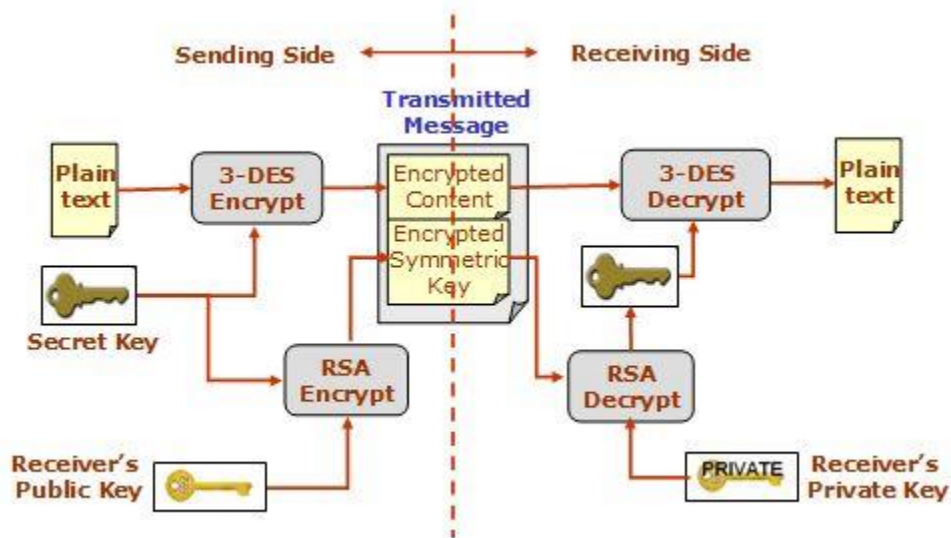
Example

Please refer to the following diagram for an illustration of public-key cryptography. On the *sending* side the following steps occur:

1. Using a secret-key generated for this message only, the plaintext is encrypted using a secret-key encryption algorithm such as 3-DES
2. Using the receiver's public-key, the symmetric key in Step 1 is encrypted using the RSA algorithm
3. The cipher text from Steps 1 and 2 are assembled to form the transmitted message.

On the *receiving* side the steps are reversed:

1. Using the receiver's private-key, the encrypted symmetric key is decrypted using the RSA algorithm,
2. Using the decrypted secret key, the message cipher text is decrypted with the symmetric key.

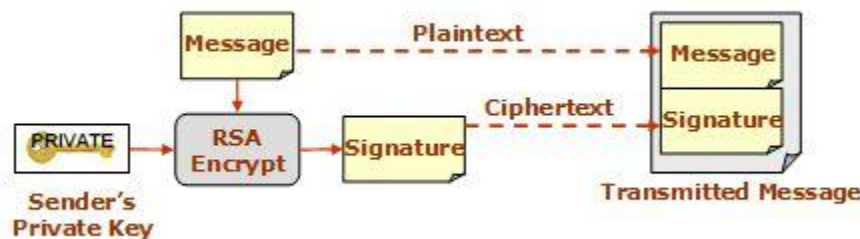


4. Digital Signatures

So far we have only considered how cryptography is used to provide confidentiality. A digital signature is a string of encrypted data that can be appended to a message to provide the other security services discussed in Section 2.

Authentication

A digital signature can be added to any message, whether encrypted or not, to provide authentication of sender using a public-key cryptosystem such as RSA. This process is illustrated by the following diagram:



In this case, the digital signature is made by encrypting the message using the sender's private key. At the receiving end, the signature can be verified (authenticated) using the sender's previously distributed public-key.

Use of Hash Functions

Applying signature encryption to the entire message, as illustrated in the above diagram, doubles the transmitted message size, causing processing and communications overheads. To improve the encrypting scheme, a **hash function** is used to transform what might be a large message to a shorter fixed-length value, called a **digest**, which represents the original message. The basic requirements for a cryptographic hash function $H(x)$ are as follows:

1. The input x can be of any length,
2. The output (digest) must have a fixed length,
3. $H(x)$ is relatively easy to compute for any x ,
4. $H(x)$ is one-way (Can't determine x from the digest),
5. $H(x)$ is collision-free (Each x should produce a unique digest).

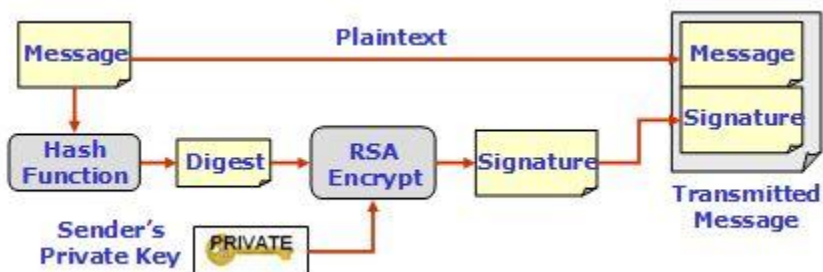
Two commonly used hash functions are SHA-1 (from the U.S. government), which generates a 160-bit digest, and MD-5 (from RSA Data Security) which generates a 128-bit digest.

Data Integrity

When signature encryption is applied to hashed data, as illustrated by the following figures, not only is authentication provided with less overhead, but the ability to check on data integrity is provided also.

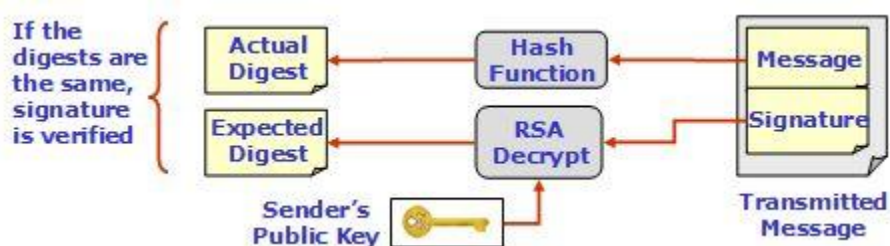
On the *sending* end, the following occurs:

1. A hash function is used to produce a digest of the original message,
2. The digest is encrypted with the sender's private-key to produce a signature,
3. The message and the signature are assembled to form the transmitted message.



On the *receiving* end, the following occurs:

1. The transmitted message is hashed a second time to produce the *actual* digest,
2. The signature is decrypted to produce the *expected* digest,
3. If the expected and actual digests are identical, not only is the signature verified, but the data integrity as well.



Non-Repudiation

Non-Repudiation is a service which protects against one party to the communication denying that it occurred, and consists of two basic types. Non-repudiation of *origin* protects the message recipient by preventing disagreements as to

whether a message was sent and/or the time it occurred. Non-repudiation of origin is provided when the sender digitally signs the message.

Non-repudiation of *delivery* protects the message originator by providing proof that the message was received by the recipient, the time it was received, and that the message sent was the same one as received. Non-repudiation of delivery is provided to the originator when the recipient sends a digitally signed acknowledgment of the transmission, as discussed further in Section 6.

5. Management of Public Keys

Our examples have shown that it is not important to keep public keys confidential. However, public key cryptography is totally compromised if intruders can substitute non-authentic public keys. Public key users must be assured that the key is the correct public key for the other party. Digital certificates, also called digital IDs, provide the authentication necessary for public keys.

Certificates are issued by a certification authority (CA) and typically conform to standard X.509 from the International Telecommunication Union in Geneva. A certificate contains your name, a serial number, expiration date, a copy of the certificate holder's public key and the digital signature of the certificate-issuing authority. Digital certificates are kept in registries so that users can obtain other users' public keys. Certificates can also be exchanged between trading partners by email.

Digital certificates can be obtained over the web from several certification authorities. The process of obtaining a certificate at a CA website involves generating the public-private key pair locally by the client machine. The private-key remains on the local machine for confidentiality. The public-key is uploaded to the CA and is included in the digital certificate.

A private-key used for decrypting secret-keys needs to be backed-up in order to prevent the loss of encrypted information should the private-key be lost. However, in order to support non-repudiation, a private-key for creating digital signatures should be created, used, and destroyed on the same machine, with no back-up. Therefore, it is

common practice to use different key-pairs for digital signatures and encrypting. In order to distinguish between a signing certificate and an encrypting certificate, different e-mail addresses or common names can be used.

6. Secure Messaging Using AS2

Applicability Statement 2 (AS2) is a document published by the Internet Engineering Task Force (IETF) that describes how to exchange structured business data securely using either the HTTP or HTTPs transfer protocol. There are two essential parts of AS2 as they relate to security services, S/MIME and MDNs.

S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions), given in IETF Standard RFC 2633, specifies how to package a plaintext business document for transmission over the internet by optionally adding encryption and digital signatures in addition to the required header information and the message itself. Any combination is allowed: plaintext, encrypted but not signed, signed but not encrypted, or encrypted and signed.

If the S/MIME message is digitally signed, non-repudiation of origin is provided to the recipient, that is, the sender cannot falsely claim that he did not send the message. It is important to note that encryption and signing in AS2 is done before transmission occurs, as contrasted with Transport Layer Security (TLS). It is possible to use both types of services by sending an S/MIME package over HTTPs.

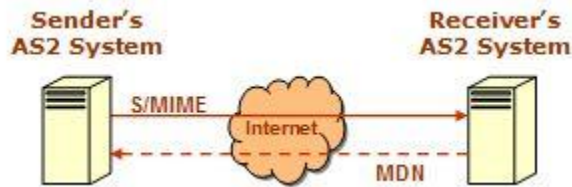
MDNs

IETF Standard RFC 2298 specifies a special message format called a Message Disposition Notification (MDN). If the sender requests an MDN, the receiver is expected to return an MDN to the sender with a status showing whether the original message was received okay or not and the time it was received. MDNs can be digitally signed or unsigned. If the MDN is signed by the recipient of the business message, non-repudiation of delivery is provided to the originator. That is, the recipient cannot falsely claim he did not receive the S/MIME package, or that it was received at some time other than stated in the MDN. MDNs can be transmitted synchronously, that is, in the same

HTTP session where the S/MIME message was sent, or asynchronously in a separate session via HTTP or email.

Security Services Provided by AS2

The following diagram illustrates the process of AS2 communication between two trading partners.



Both the sender and receiver must have a product that implements the AS2 standard. The encryption, signing, and MDN options are generally agreed to in advance between the two trading partners. The diagram above assumes that an MDN has been requested.

The degree of security services provided depends on which options are selected. Note that using AS2 can provide all of the possible security services if the S/MIME is encrypted and signed by the sender with a request for a signed MDN from the recipient. The following table summarizes the relationship between the AS2 options and the security services provided.

Cells that are marked with an 'X' indicate that the security service listed in the first column is provided.

Security Service Provided	AS2 S/MIME Options			MDN Option
	Encrypt	Sign	Encrypt & Sign	Sign
Message Confidentiality	X		X	
Authenticate Sender		X	X	
Message Integrity		X	X	
Non-repudiation of Origin		X	X	
Non-repudiation of Delivery				X

7. bTrade Provides Cryptography for Message Security

bTrade develops Enterprise Data Encryption technology solutions for enterprises that share sensitive data across applications and organizations, and face complex security and compliance mandates. bTrade has deep expertise and a proven track record serving a number of industries, including Financial Services, Automotive, Manufacturing, Consumer Packaged Goods, Retail, Healthcare, Life Sciences, Technology, Transportation & Logistics, Government & Public Sector, and more. Our products and solutions can be deployed and managed through a variety of delivery channels, including software, on-premise appliances, SaaS, Hosted, and VMWare. Thousands of customers depend on bTrade solutions to gain control and oversight of the movement of critical corporate data to facilitate data growth, reduce security risk, and improve IT and business efficiency.

bTrade was founded in 1990 and is led by eBusiness visionaries who have delivered industry-leading business integration solutions to thousands of enterprise customers worldwide. bTrade is privately held and profitable with its global headquarters located in Glendale, CA USA.