Cryptographic Technologies

Chapter 5

Lecturer: Pei-yih Ting

Overview

- Goals of Cryptography
- Encryption and Decryption Algorithms
- Symmetric Algorithms: DES and AES
- Asymmetric Algorithm: RSA
- Pretty Good Privacy (PGP)
- Symmetric vs. Asymmetric Cryptosystems
- Digital Signatures
- Digital Certificates

Goals of Cryptography

- Four primary goals
  - Many applications provide multiple cryptographic benefits simultaneously
- Confidentiality is most commonly addressed goal
  - The meaning of a message is concealed in the ciphertext
  - The sender encrypts the message using a cryptographic encrypting algorithm with a suitable key
  - The recipient decrypts the message using a cryptographic decrytion algorithm with a matched key that may or may not be the same as the one used by the sender

Goals of Cryptography (cont'd)

- Integrity
  - Ensures that the message received is the same as the message that was sent
  - Uses hashing to create a unique message digest from the message that is sent along with the message
  - Recipient uses the same technique to create a second digest from the message to compare to the original one
  - This technique only protects against unintentional alteration of the message
  - A variation is used to create digital signatures to protect against malicious alteration

Goals of Cryptography (cont'd)

- Non-repudiation
  - The sender of a message cannot later claim he/she did not send it
  - Available only with asymmetric cryptosystems that can create digital signatures
- Authentication
  - A user or system can prove their identity to another who does not have personal knowledge of their identity
  - Accomplished using digital certificates in a asymmetric cryptosystem
  - Kerberos is a common cryptographic authentication system using symmetric cryptosystems

Cryptographic Algorithms

- Two types of cryptographic algorithms
  - Symmetric and asymmetric
- An encryption algorithm is used to conceal a message
  - transform from plaintext to ciphertext
- A decryption algorithm is used to uncover the message carried by ciphertext stream
  - transform from ciphertext back to plaintext
- Early algorithms embodied security through obscurity
- Modern algorithms are rigorously and openly examined
  - Less vulnerabilities and backdoors
  - Security depends solely on the length of the key

Cryptographic Algorithms (cont'd)

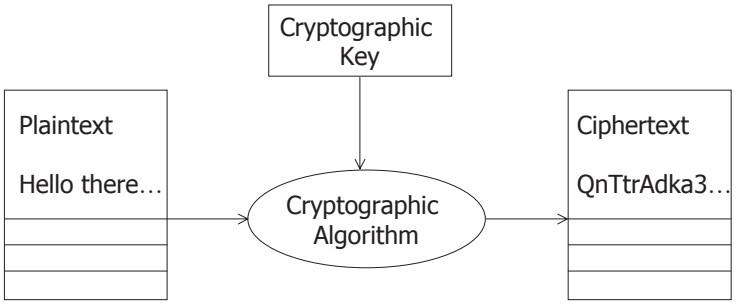


Figure 5.1 Basic encryption operation

Cryptographic Algorithms (cont'd)

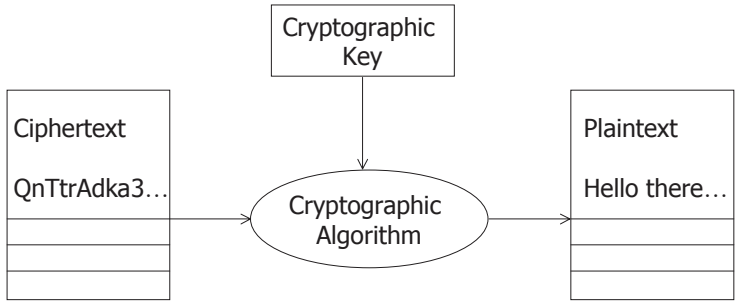


Figure 5.2 Basic decryption operation

Key Length

- Key length dominates the level of security
- The longer the key, the greater the degree of protection
- A common attack against cryptosystems is the brute force attack
  - All possible keys are tried
  - Longer keys create an enormous number of possible combinations, frustrating brute force attacks
  - The number of combinations is 2^n where n is the key length in bits

Key Length (cont'd)

Table 5.1 Possible Keys of a Given Length

Key Length	Approximate Number of Possible Keys
56 bits	72,057,594,037,927,936
128 bits	3.40×10^{38}
256 bits	1.16×10^{77}
512 bits	1.34×10^{154}
1,024 bits	1.80×10^{308}
2,048 bits	3.23×10^{616}

Symmetric Algorithms

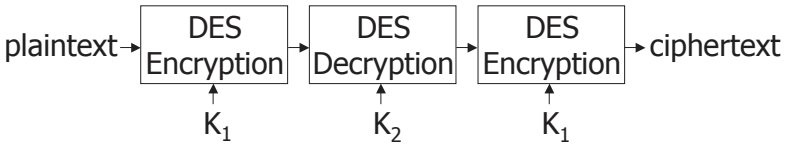
- The sender and receiver using the same key (in some cases, there are two keys but can be easily derived from one another)
- Key is called ***shared secret key*** or ***secret key***
- Symmetric cryptosystems are sometimes called ***secret key cryptosystems***

Data Encryption Standard (DES)

- One of the most common symmetric cryptosystems since 1977, FIPS 46-6
- Uses a 56-bit key with four modes of operation
  - Electronic codebook (ECB), ciphertext block chaining (CBC), output feedback (OFB), ciphertext feedback (CFB)
- A fatal problem
  - A 56-bit key is no longer considered strong enough to survive brute force attacks nowadays
- Current applications of DES use three separate iterations of DES encryption on each message
  - Triple DES (3DES)

DES (cont'd)

- 3DES provides an acceptably strong level of protection, equivalent to a 112-bit key algorithm
- Variations of 3DES use either 2 or 3 keys
  - 3DES-EEE (encrypt-encrypt-encrypt) uses 3 keys
  - 3DES-EDE (encrypt-decrypt-encrypt) can use from 1 to 3 keys with different levels of protection



Advanced Encryption Standard (AES)

- Solicited in a competition sponsored by the National Institute of Standards and Technology (NIST), 1997
- Candidate algorithms published their inner workings
- Winner was the Rijndael algorithm, 2001
- AES allows the user to select from 3 different key lengths
  - 128, 192, or 256 bits
  - The longer the key, the greater the security
- AES is gaining momentum, but the volume of applications that use DES makes conversion slow

Asymmetric Algorithms

- Differ from symmetric algorithms because sender and receiver use different keys that cannot be derived from each other
- Each user has a pair of keys
  - Public key and private key
  - Keys are mathematically related – Messages encrypted with public key can only be decrypted with private key
  - Public keys are freely distributed so that anyone can use them to encrypt a message
- Asymmetric cryptosystems are referred to as ***public key cryptosystems***

Asymmetric Algorithms Example

- Renee and Michael wish to communicate sensitive information
  - Renee and Michael share their public keys
  - When Renee sends a message to Michael, she encrypts it with Michael's public key
  - Only Michael can decrypt the message because decryption requires his private key, which he does not share with anyone

Asymmetric Algorithms (cont'd)

- Rivest, Shamir, Adelman algorithm (RSA)
  - One of the most well-known public key cryptosystem
  - Published in 1976
  - Relies on the fact that it is extremely difficult to factor large composite numbers
  - Supports digital signature

Pretty Good Privacy (PGP)

- A cross-platform solution for email and file encryption
- An implementation of several cryptographic algorithms (including RSA)
- Supports management of a decentralized public key infrastructure
- PGP is a proprietary product.
- An alternative, GnuPG, has been released under the Free Software Foundation's Open License http://www.gnupg.org

The Web of Trust Model

- Key exchange is a difficult problem
  - Before PGP, it was necessary to exchange keys offline
- PGP introduced the "web of trust" model
  - Allows users to rely on the judgment of others that a public key is authentic
- Four levels of trust
  - Implicit trust: for keys that you own
  - Full trust: trust this user to provide other keys to you
  - Marginal trust: requires at least one other user that you marginally trust to vouch for any new public key
  - Untrusted: do not trust a user to introduce you a new key

Symmetric vs. Asymmetric Cryptosystems

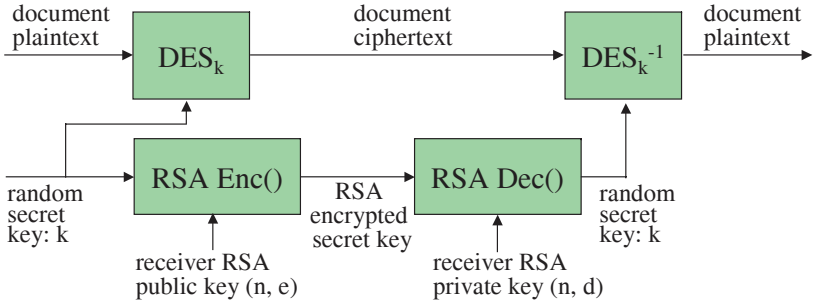
- Choice between symmetric and asymmetric cryptosystems:
  - Symmetric cryptosystems don't scale well
  - Key exchange for symmetric cryptosystem is difficult
  - Symmetric cryptosystems are efficient. Asymmetric cryptosystems are slower than symmetric ones
  - Symmetric cryptosystems are excellent for securing the ends of a communication circuit such as a Virtual Private Network
  - Asymmetric cryptosystems are more practical when there are a large number of users

TABLE 5.2 Comparison of Symmetric and Asymmetric Cryptosystems

Symmetric Cryptosystems	Asymmetric Cryptosystems
Provide confidentiality among all participants who share the same secret key	Provide confidentiality between individual users of a cryptosystem
Provide integrity against modification by individuals who do not possess the secret key	Provide integrity against modification by anyone other than the sender of the message
Provide for authentication between two individuals when they are the only ones who possess the secret key	Provide for authentication of any individual user of the cryptosystem
Do not provide for nonrepudiation	Provide for nonrepudiation
Require shorter keys than asymmetric algorithms to achieve the same level of security	Require longer keys than symmetric algorithms to achieve the same level of security
Operate faster than asymmetric algorithms	Operate slower than symmetric algorithms
Are not easily scalable	Scale well to environments with large numbers of users
Do not facilitate the use of digital certificates	Lend themselves well to digital certificate hierarchies
Make the exchange of cryptographic keys difficult (often requiring offline exchange)	Allow for the exchange of public keys over otherwise insecure transmission media

Digital Envelop

- Hybrid system (public key and secret key)
  - Efficiency: computation of RSA is about 1000 times slower than DES
  - Key exchange and scalability: RSA requires trusted third party as certificate authority, each user has only one public key



Digital Signatures

- Add integrity and non-repudiation functionalities to cryptosystems
- Non-repudiation can only be enforced with asymmetric algorithms
- Signature creation
  - A unique message digest is created by applying a hash function to the message
  - Variations of the Secure Hash (SHA-1, SAH-256, SHA-384, SHA-512) and MD (MD2, MD4, MD5, RIPEMD160) Algorithms are commonly used
  - Sender encrypts the message digest with his/her private key

Digital Signatures (cont'd)

- Signature verification
  - Recipient decrypts the message and extracts the plaintext message and digital signature
  - Recipient applies the same hash function to the message as that used by the sender to create a new message digest
  - Recipient decrypts the digital signature using the sender's public key to extract the sender's message digest
  - The recipient compares the two message digests
  - If the message digests match, signature is authentic
  - Non-matching signatures can be malicious but also can be due to transmission errors, etc.

Digital Certificates

- Digital certificates allow a third party to vouch for a public key and therefore digital signature
- The third party does the work to verify the identity of the sender
- Certification Authorities
  - The third parties that verify and certify the identity of a sender
  - Two of the most common CAs are VeriSign and Thawte

Digital Certificates (cont'd)

- Certificate generation
  - Sender selects and pays a CA
  - Sender submits required information for CA to verify their identity (typically involves credit checks, business records checks, and may require that the requestor appear in person before a notary or other official)
  - CA issues a digital certificate following the X.509 standard
  - CA signs the digital certificate
- Certificate verification
  - A digital certificate can be used to securely transmit the sender's public key to any entity that trusts the CA and accepts the certificate

Summary

- Goals of cryptography are confidentiality, integrity, non-repudiation, and authentication
- General steps in cryptography are to
  - Create a plaintext message
  - Use a cryptographic key and encryption algorithm to produce a ciphertext message
  - Apply the same or a related key and decryption algorithm to the ciphertext message
  - Recreate the original plaintext message
- There are two types of cryptographic algorithms
  - Symmetric (uses a shared secret key)
  - Asymmetric (uses a public and private key pair)

Summary (cont'd)

- Digital signatures are used to add integrity and non-repudiation functionality to cryptosystems
- Digital signatures are created using hash functions applied to the message to create a message digest that is then encrypted
- Digital certificates allow a third party Certificate Authority to verify the identity of a sender who may not be well known to the recipient
- A digital certificate is a copy of a user's public key that has been digitally signed by a Certificate Authority.

Assignments

- Reading: Chapter 5
- Practice 5.7 Challenge Questions

- Turn in Challenge Exercise 5.1, 5.2, 5.3, 5.4 two weeks from now