CRYPTOGRAPHY

SSCP®

Systems Security
Certified Practitioner

(ISC)²®

UNDERSTAND AND APPLY FUNDAMENTAL CONCEPTS OF CRYPTOGRAPHY

SSCP®

Systems Security
Certified Practitioner

(ISC)²®

High Work Factor

- **Work factor:**
  - The average amount of effort or work required to break an encryption system
- **If the work factor is sufficiently high:**
  - Encryption system is considered to be unbreakable, referred to as "economically infeasible" to break

Stream-Based Ciphers

Stream-based cipher:

- When a cryptosystem performs its encryption on a bit-by-bit basis
- Most commonly associated with streaming applications
- Mixes the plaintext with a keystream that is generated by the cryptosystem

Stream-Based Cipher Rules

Keystream should not be linearly related to the cryptovariable

Statistically unpredictable

Statistically unbiased

Long periods without repetition

Functional complexity

Block Ciphers

- Operate on blocks or chunks of text
- Strong
- Computationally intensive
- Initialization Vectors (IV)

Block Size

Produce a fixed length block of ciphertext

- padding

Evaluation of Algorithms

- **Symmetric key encryption:**
  - Only one key is used to encrypt and decrypt data
- **Asymmetric key encryption:**
  - Used to solve the problem of key distribution
  - Two keys are used; private and public keys

Encryption Algorithm Characteristics

Type

Functions

Key size

Rounds

Complexity

Attack

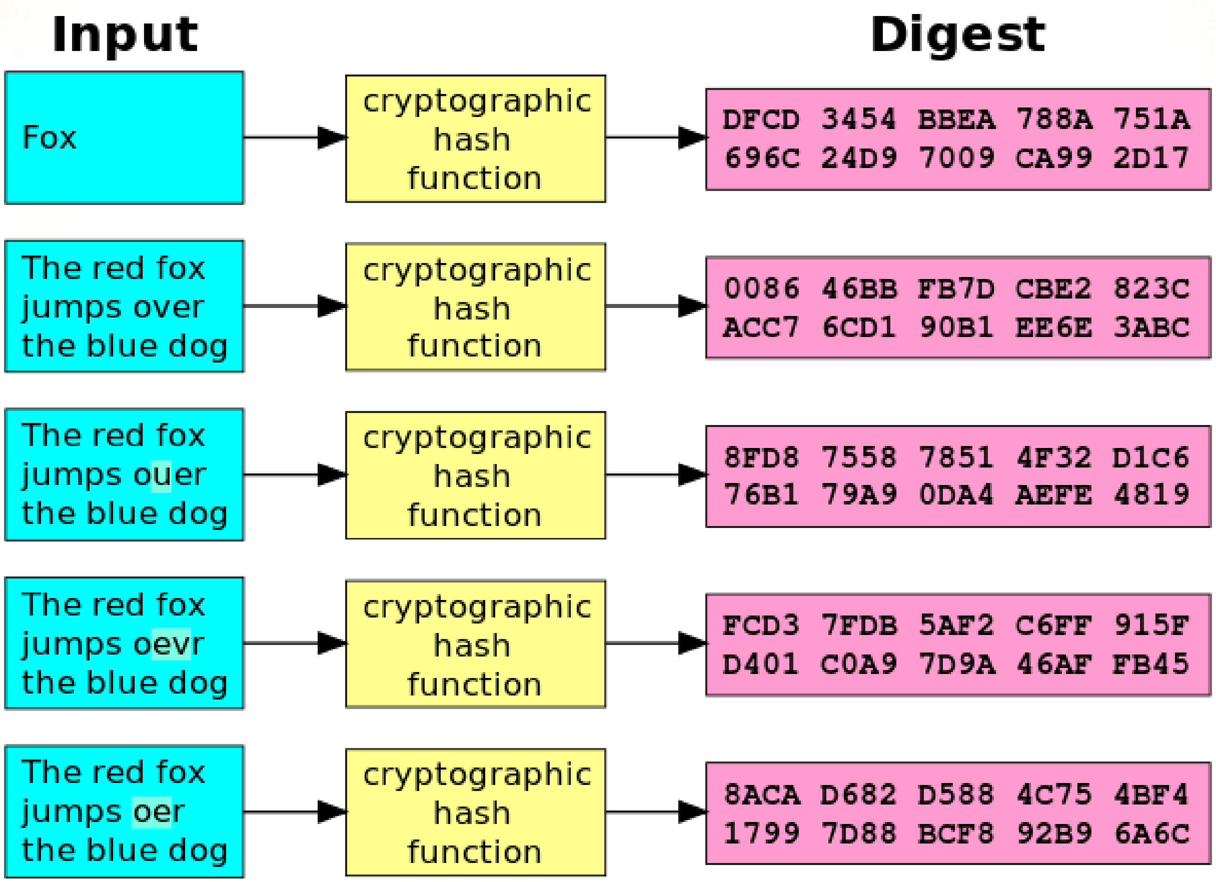
Strength

Hashing

Ideal cryptographic hash function is:

- Easy to compute the hash value for any given message
- Infeasible to generate a message that has a given hash
- Infeasible to modify a message without changing the hash
- Infeasible to find two different messages with the same hash

Cryptographic Hashing Function



Hashing Algorithms

Ideal cryptographic hash function is:

- Message Digest (MD) – 128 bit output
- Secure Hashing Algorithm (SHA-1) – 160 bit output
- HAVAL – variable output
- RIPEMD–160 – 160 bit output
  - No patent restrictions

Salting

- **Salt:**
  – Random data that is used as an additional input to a one-way function that hashes a password or passphrase

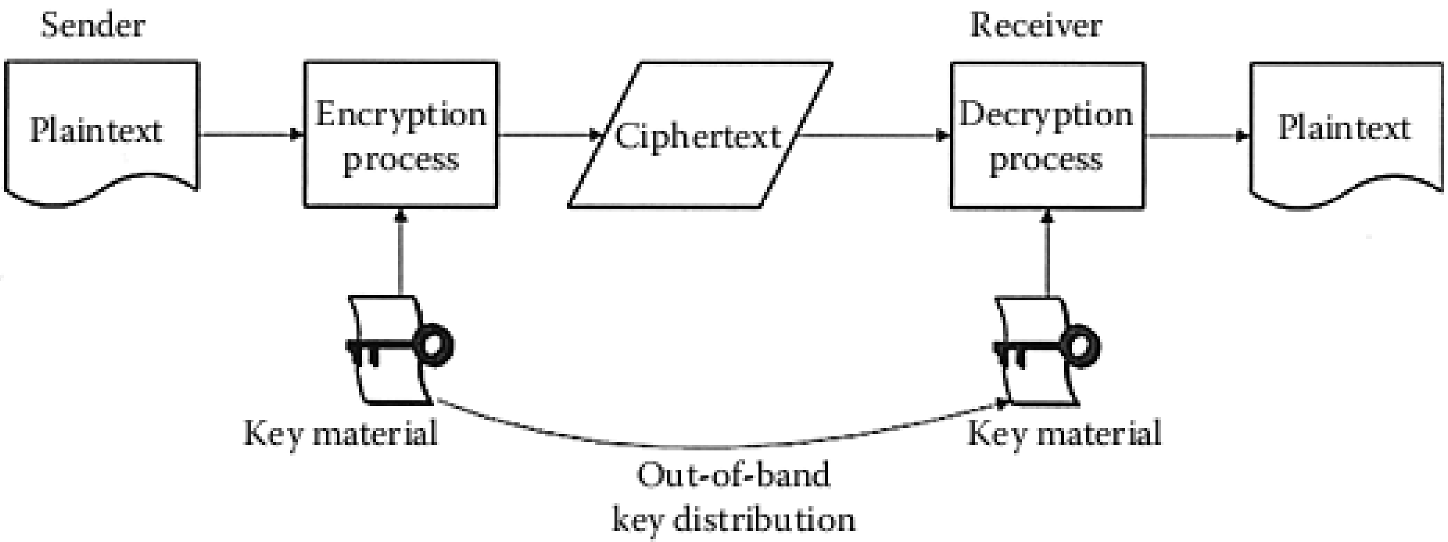
- **Primary function of salts:**
  – Defend against dictionary attacks and against pre-computed rainbow table attacks

Symmetric Cryptography

- Operate with a single cryptographic key that is used for both encryption and decryption of the message
- Fast, secure, cheap
- Main problem is $\boxed{\text{key management}}$

Fast, secure, cheap

Out-of-Band Key Distribution



Basic Block Cipher Modes

Electronic Codebook Mode

Cipher Block Chaining Mode (CBC)

The Stream Modes of DES

Data Encryption Standard (Symmetric)

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Advantages and Disadvantages of DES

- **Advantages:**
  - Strong
  - Fast
- **Disadvantages:**
  - Not suitable for confidential information
  - Susceptible to brute-force attack

Advanced Encryption Standard (AES)

- **Rijndael algorithm**
- **Obliged to:**
  - Be flexible
  - Implementable on many types of platforms
  - Free of royalties

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

- Encryption protocol that forms part of the 802.11i standard for wireless local area networks
- Based on AES encryption using the CTR with CBC-MAC (CCM) mode of operation
  - 128 bit keys
  - 128 bit block size
  - 48 bit IV to minimize replay attack vulnerabilities

Additional Algorithms

- IDEA
- CAST
- SAFER
- BLOWFISH
- TWOFISH
- RC4 | RC5

Advantages and Disadvantages of Symmetric Algorithms

- **Advantages:**
  - Fast
  - Secure
  - Confidential
  - Can be implemented at no cost to the user

- **Disadvantages:**
  - Key management is difficult
  - Not able to provide non-repudiation

Asymmetric Cryptography

Provide an extensible and elastic framework in which to deploy cryptographic functions for:

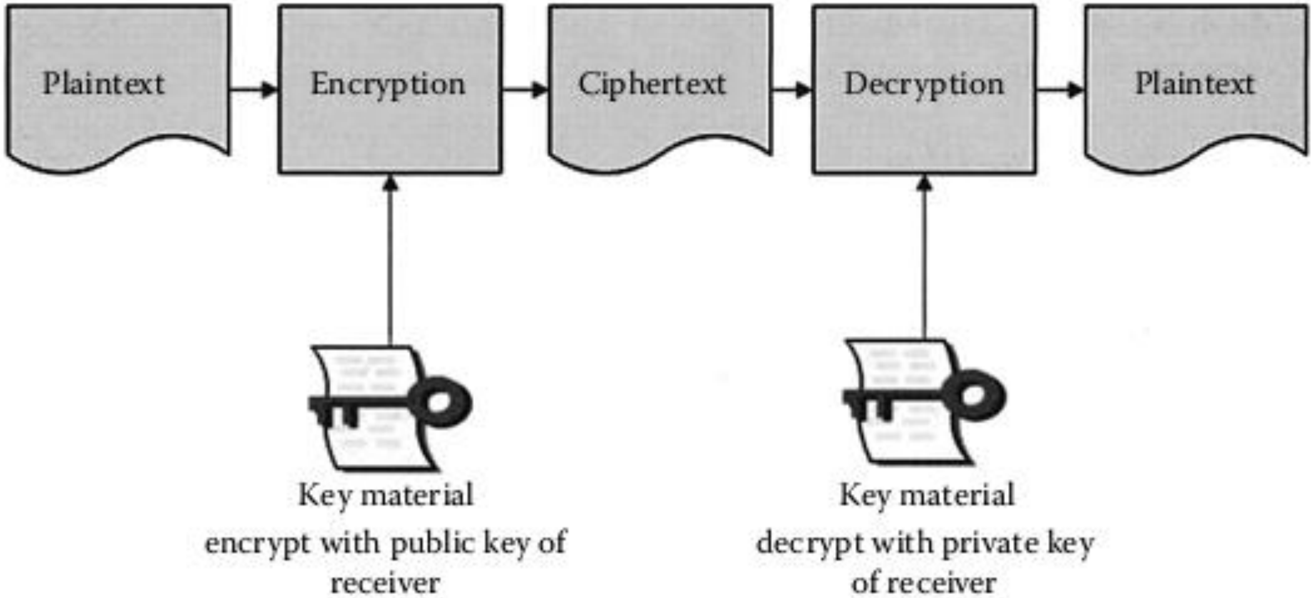
- Integrity
- Confidentiality
- Authentication
- Non-repudiation

Confidential Messages

Any message that is encrypted with a public key can only be decrypted with the corresponding other half of the key pair, the private key

As long as the key holder keeps her private key secure, there exists a method of transmitting a message confidentially

Using Public Key Cryptography to Send a Confidential Message



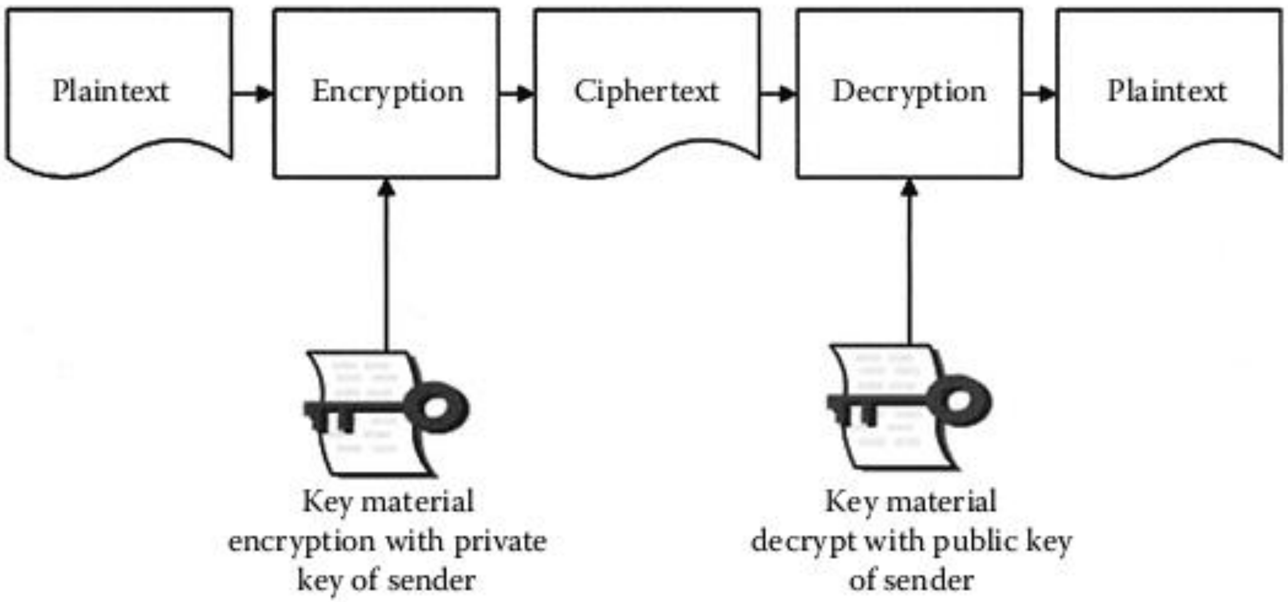
Open Message

Messages encrypted with the private key of a sender, can be opened or read by anyone with the corresponding public key

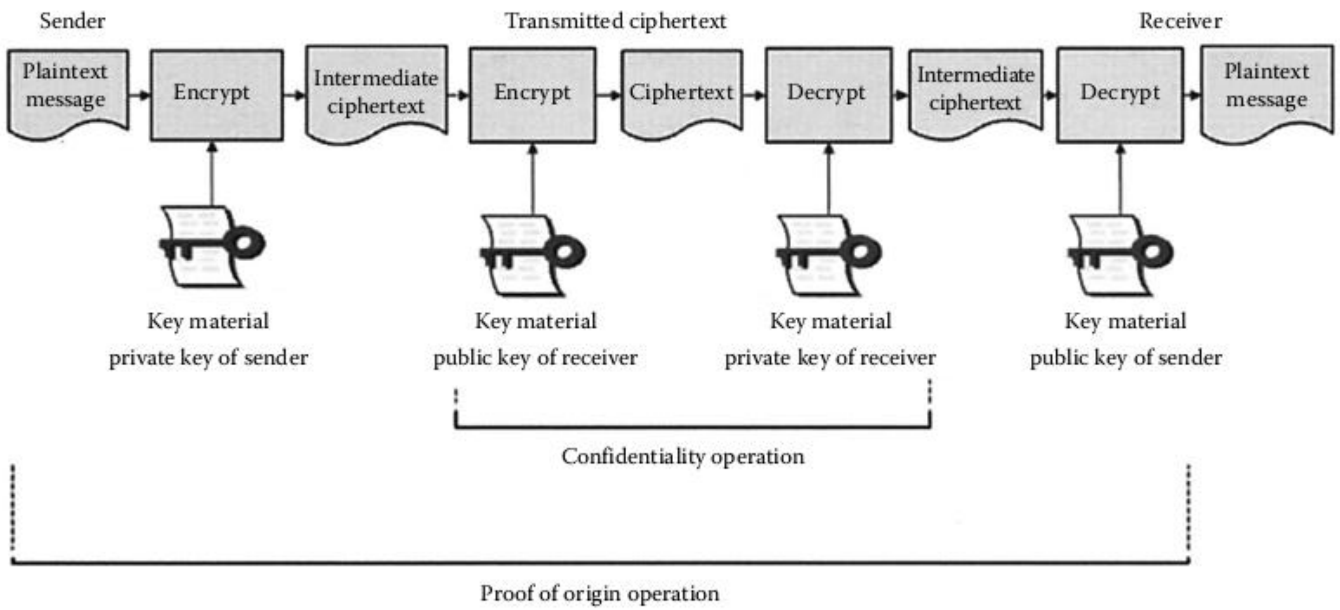
To send a message and provide proof of origin, encrypt it with your own private key

The recipient then has some guarantee that the message did, in fact, originate with the sender

Using Public Key Cryptography to Send a Message with Proof of Origin



Confidential Messages with Proof of Origin



Diffie–Hellmann Algorithm

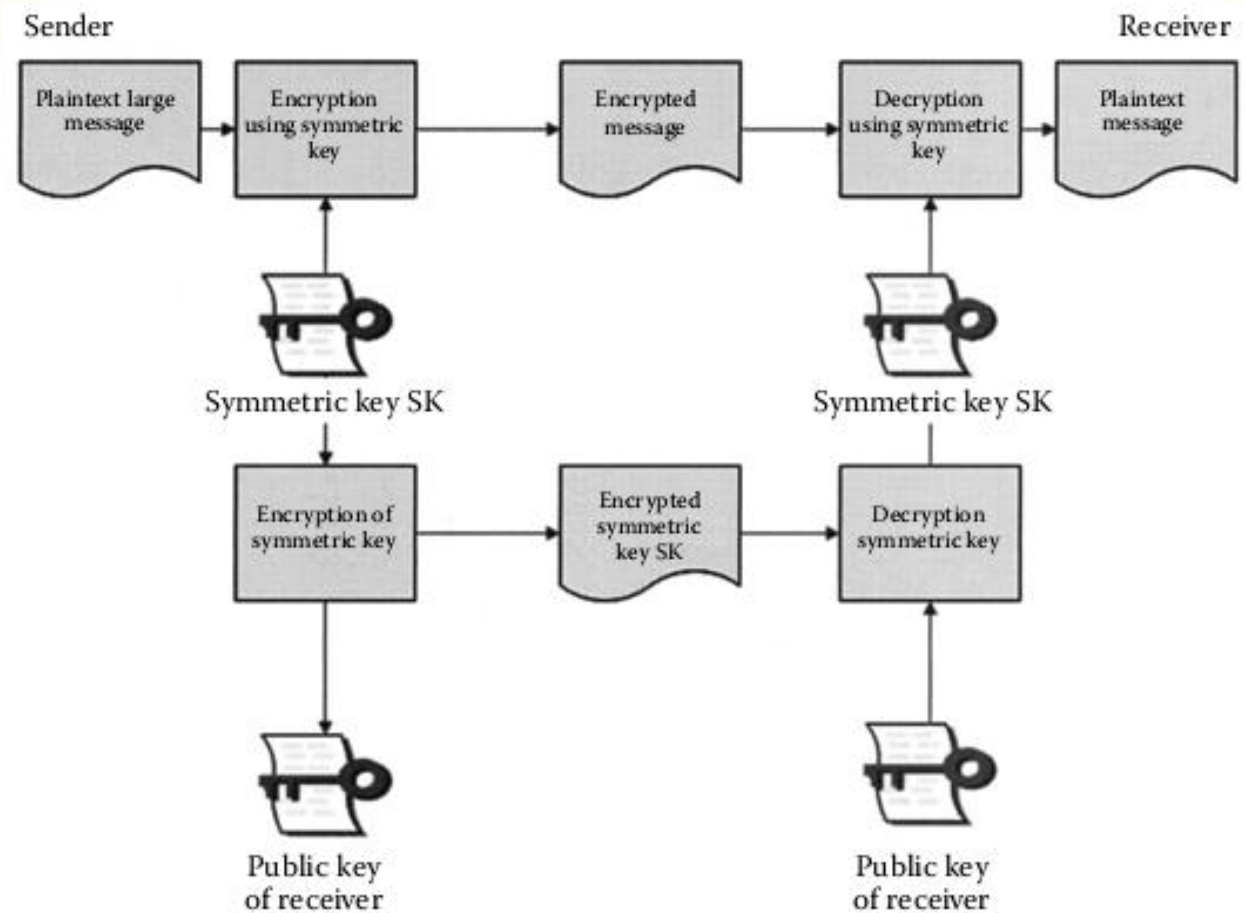
- Key exchange algorithm
- Enables two users to exchange or negotiate a secret symmetric key that will be used for message encryption

Advantages and Disadvantages of Asymmetric Key Algorithms

- **Advantages:**
  - Allows you securely to send a message across an untrusted medium
  - Low overhead

- **Disadvantages:**
  - Extremely slow
  - Impractical for everyday use
  - Ciphertext output may be much larger than the plaintext

Hybrid Cryptography



Message Digests

Small representation of a larger message

Used to ensure the authentication and integrity of information not the confidentiality

Message Authentication Code (MAC)

A small block of data that is generated using a secret key and then appended to the message

Much smaller than the message generating it

Given a MAC, it is impractical to compute the message that generated it

Given a MAC and the message that generated it, it is impractical to find another message generating the same MAC

Chosen Plain-Text

To execute the chosen attacks, the attacker knows the algorithm used for the encrypting

Social Engineering for Key Discovery

Through coercion, bribery, or befriending people in positions of responsibility, spies or competitors are able to gain access to systems without having any technical expertise

Brute Force

Brute force is trying all possible keys until one is found that decrypts the ciphertext. This is why key length is such an important factor in determining the strength of a cryptosystem

Differential Cryptanalysis

- Measures the exact execution times and power required by the crypto device to perform the encryption or decryption
- By measuring this, it is possible to determine the value of the key and the algorithm used

Linear Cryptanalysis

- Uses a linear approximation to describe the behavior of the block cipher
- Given sufficient pairs of plaintext and corresponding ciphertext:
  - Bits of information about the key can be obtained
  - Increased amounts of data will usually give a higher probability of success

Rainbow Table

Map plaintext into a hash

One-way process

A rainbow table is a look-up table of sorted hash outputs

Ciphertext-Only Attack

- One of the most difficult because the attacker has so little information with which to start
- The attacker starts with is some unintelligible data that may be an important encrypted message
- Becomes simpler when the attacker is able to gather several pieces of ciphertext and look for trends

Known Plaintext

- The attacker has access to ciphertext and the plaintext versions of the same message
- The goal is to find the link — the cryptographic key that was used to encrypt the message

Chosen Ciphertext

- **Chosen Ciphertext**
  - Attacker has access to the decryption device and attempts to defeat the cryptographic protection by decrypting chosen pieces of ciphertext to discover the key

- **Adaptive chosen ciphertext**
  - The attacker can modify the ciphertext prior to putting it through the algorithm

Dictionary Attack

- Used most commonly against password files
- Exploits the poor habits of users who choose simple passwords based on natural words

Replay Attack

Meant to disrupt and damage processing by sending repeated files to the host

If there are no checks or sequence verification codes in the receiving software, the system might process duplicate files

Factoring Attack

This attack:

- Is aimed at the RSA algorithm
- Attempts to find the keys through solving the factoring of these numbers

UNDERSTAND REQUIREMENTS FOR CRYPTOGRAPHY

SSCP®

Systems Security
Certified Practitioner

(ISC)²®

Legislative and Regulatory Compliance

Safe harbor provisions:

– A set of good faith conditions to be followed in order to protect the organization from penalties under a law

European Data Protection Directive

When processing is necessary for compliance with a legal action

When processing is required to protect the life of the subject

When the subject of the personal data has provided consent

When the processing is performed within the law and scope of "public interest"

OPERATE AND IMPLEMENT CRYPTOGRAPHIC SYSTEMS

SSCP®

Systems Security
Certified Practitioner

Public Key Infrastructure (PKI)

Publish public keys/certificates

Certify that a key is tied to an individual or entity

Provide verification of the validity of a public key

Functions of a CA

- CA "signs" an entity's digital certificate to certify the certificate content accurately represents the certificate owner
- The functions of a CA may be distributed among several specialized servers in a PKI

X.509 Certification Issued by VeriSign

Field	Description of Contents
Algorithm Used for the Signature	Algorithm used to sign the certificate
Issuer Name	X.500 name of CA
Period of Validity	Start Date/End Date
Subject's Public Key (algorithm, parameters, key)	Owner of the public key
Issuer Unique Identifier	Public key and algorithm used to create it
Subject's Unique Identifier	Optional field in case the public key owner has more than one X.500 name
Extensions	
Digital Signature of CA	Hash of the certificate encrypted with the private key of the CA

Advances in Key Management

Extensible Markup Language (XML)

XML Key Management Specification 2.0 (XKMS)

Key Length

Key length is the size of a key which a cryptographic algorithm used in ciphering or deciphering protected information

Keys control how an algorithm operates so only the correct key can decipher the information

Key Distribution

Keys can be distributed in a number of ways:

- “Out-of-band” key exchange

The use of a Key Distribution Center (KDC) for key management requires the creation of two types of keys:

- Master keys
- Session key

Key Storage and Destruction

Trusted, tamperproof hardware security modules

Passphrase-protected smart cards

Key wrapping the session keys

Splitting cipher keys and storing

Protecting keys using strong passwords/passphrases

Key expiry

Key Storage and Destruction

All centrally stored data that is related to user keys should be signed

Backup copies should be made of central/root keys

Provide key recovery capabilities

Archive user keys for a sufficiently long crypto period

Factors Affecting Risk Exposure

The strength of the cryptographic mechanisms

The embodiment of the mechanisms

The operating environment

The volume of information flow

The security life of the data

The security function

The re-keying method

Factors Affecting Risk Exposure

The key update or key derivation process

The number of nodes in a network that share a common key

The number of copies of a key and distribution of those copies

The threat to the information

Web of Trust

- Used in PGP, GnuPG, and other OpenPGP-compatible systems
- Establishes authenticity of the binding between a public key and its owner
- Decentralized trust model

Secure Protocols

IP Security (IPSec) is a suite of protocols for communicating securely with IP by providing mechanisms for authenticating and encryption

Authentication Header (AH)

The authentication header is used to prove the identity of the sender and ensure that the transmitted data has not been tampered with

Encapsulating Security Payload (ESP)

The encapsulating security payload encrypts IP packets and ensures their integrity

Internet Key Exchange (IKE)

Internet key exchange allows communicating partners to prove their identity to each other and establish a secure communication channel

Secure/Multipurpose Internet Mail Extensions (S/MIME)

- Widely accepted method for sending digitally signed and encrypted messages
- Allows you to encrypt e-mails and digitally sign them
- S/MIME provides two security services:
  - Digital signatures
  - Message encryption

Process for Digitally Signing an E-Mail

1. Message is captured
2. Information uniquely identifying the sender is retrieved
3. Signing operation is performed on the message
4. Digital signature is appended to the message
5. Message is sent

Process for Verifying a Digital Signature of an E-Mail Message

1. Message is received
2. Digital signature is retrieved from the message
3. Message is retrieved
4. Information identifying the sender is retrieved
5. Signing operation is performed on the message
6. Digital signature included with the message is compared to digital signature produced on receipt
7. If the digital signatures match, the message is valid

Process for Encryption of an E-Mail Message

1. Message is captured
2. Information uniquely identifying the recipient is retrieved
3. Encryption operation is performed on the message using the recipient's information to produce an encrypted message
4. Encrypted message replaces the text in the message
5. Message is sent

Process for Decrypting an E-Mail Message

1. Message is received
2. Encrypted message is retrieved
3. Information uniquely identifying the recipient is retrieved
4. Decryption operation is performed on the encrypted message using the recipient's unique information to produce an unencrypted message
5. Unencrypted message is returned to the recipient