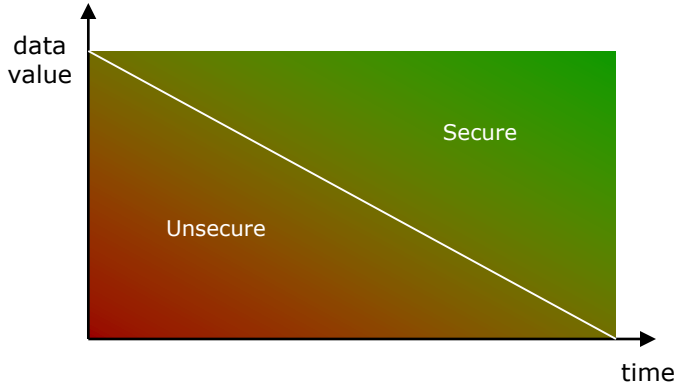
Introduction

- Definition
  - Techniques for mangling data
- Evaluation
  - Cost for breaking data > Value of encrypted data
  - Time for breaking data > Lifetime of encrypted data



Overview

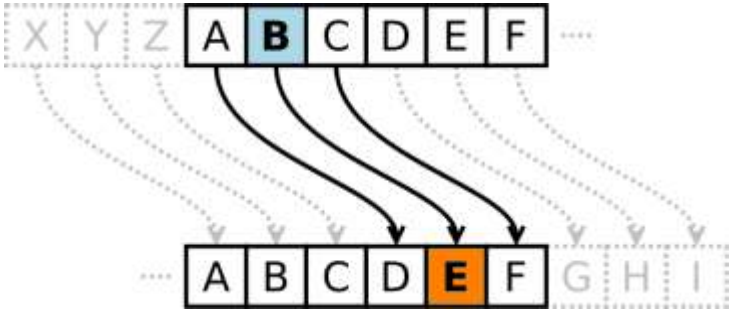
- Purposes
  - Encryption (confidentiality)
  - Integrity
  - Identity (authentication)
  - Non-repudation
- Cipher Types
  - No Key
  - One Key
  - Two Keys
  - Hybrid
  - Message Digest

No Key Encryption Systems

- Types
  - Substitution
    - Monoalphabetic
    - Polyalphabetic
  - Transposition

No Key System - Substitution Cipher

- Caesar Cipher
  - Letters substitution
  - The offset can be seen as the key



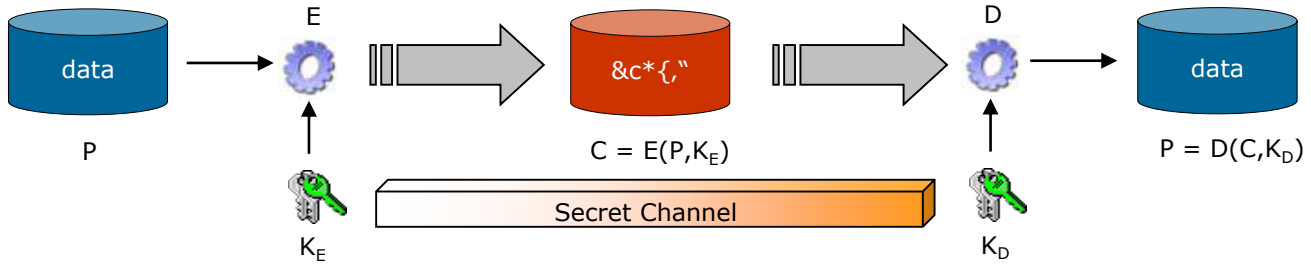
www.wikipedia.com

No Key System

- Issues
  - Encryption algorithm must be kept secret
  - Frequency of some letters in a language

Symmetric Key Algorithms

- Definition
  - Conventional, Private Key, Secret Key, One Key
  - The encryption algorithm is known and public
  - The source and destination share a common secret (key)
  - The key must be kept secret



- Issues
  - Key length must be as long a possible to make brute force attack difficult
  - Secret channel is required to propagate the key
  - The sender must trust the receiver to keep the key secret

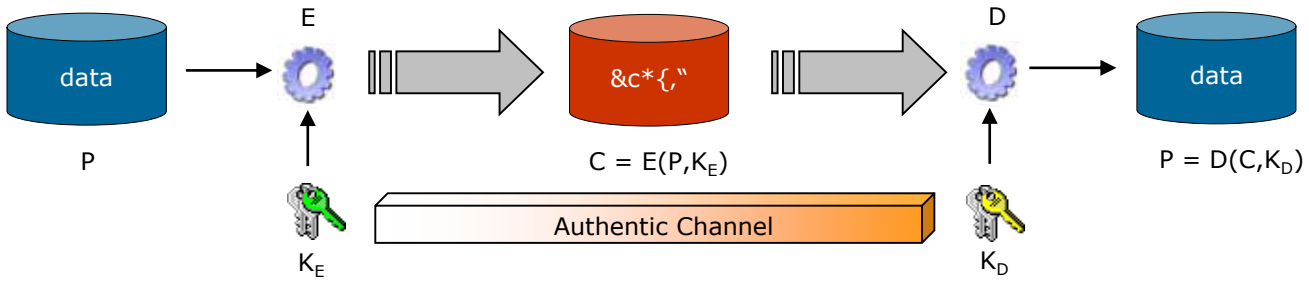
Symmetric Key Algorithms

- Characteristics
  - Extremely fast
  - Used for bulk encryption
- Implementations

Algorithm	Name	Key length
DES	Data Encryption Standard	56 bits
DESX	Data Encryption Standard Expanded	56 bits
3DES	Triple Data Encryption Standard	168 bits
AES	Advanced Encryption Standard. (RIJNDAEL)	256 bits

Asymmetric Key Algorithms

- Definition
  - Public Key
  - The encryption algorithm is known and public
  - The source and destination use different keys that are mathematically related
  - The public key can be shared to...anyone!



- Characteristics
  - Very slow
  - Infeasible to derive the private key from the public key
  - Secret channel is not required to propagate the key
  - The sender must not trust the receiver to keep a key secret

Asymmetric Key Algorithms

- Implementations

Algorithm	Name	Key length
DSA	Digital Signature Algorithm	512 bits
RSA	Rivest Shamir and Adleman	512 to 4.096 bits

- Usages
  - Encryption:
    - The sender encrypts the data with the public key of the receiver
    - The receiver reads the data with his private key
  - Non-repudation:
    - The sender encrypts the data with his private key
    - The receiver reads the with the public key of the sender

Asymmetric Key Algorithms

- Challenge
  - Public key must be authenticated
- Usages

Message Digest Algorithms

- Definition
  - Map a variable-length plaintext into a fixed-length ciphertext
  - Digital fingerprint
  - Mathematical summary
- Characteristics
  - No key is used
  - infeasible to determine the input based on its digest
  - impossible to find an arbitrary input that has a particular, desired digest
  - infeasible to find two different inputs that have the same digest

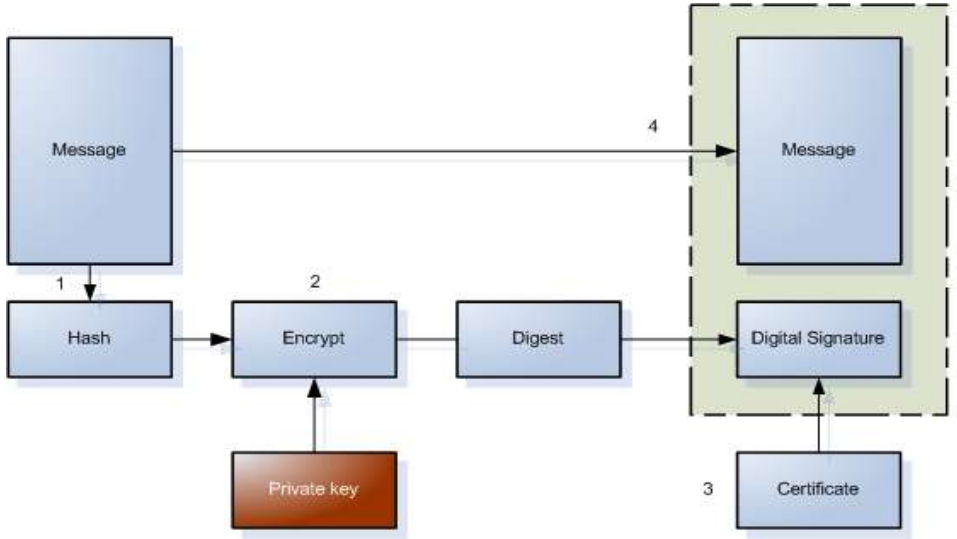
Message Digest Algorithms

- Usages
  - Implementation of messages integrity
- Implementations

Algorithm	Description	Digest Length (bits)
MD5	Message Digest	128
SHA-1	Secure Hash Algorithm	160

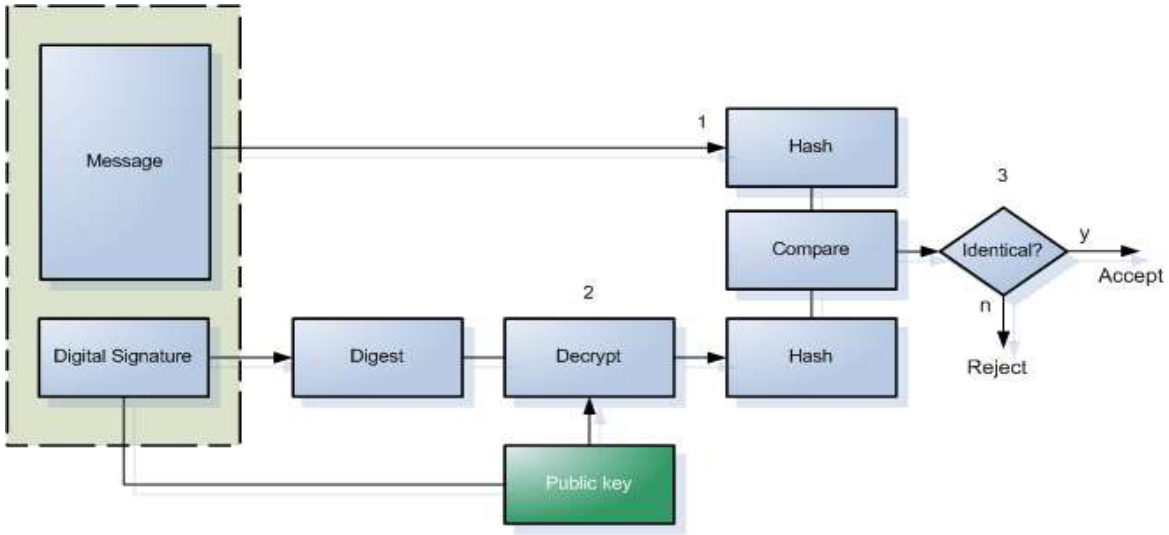
Digital Signatures - Construction

- Vouches for the origin (identity) of data (sender)
  - Non-repudiation
  - Integrity (tampering)
- Applying a signature does not encrypt the message
  - Digital signature includes the encrypted digest and information about the signer´s digital certificate



Digital Signatures - Verification

- Compute the hash from the message
- Decrypt the digest from the digital signature
- Compare the hashes and interprete
  - Sender has been identified
  - Content has not been changed

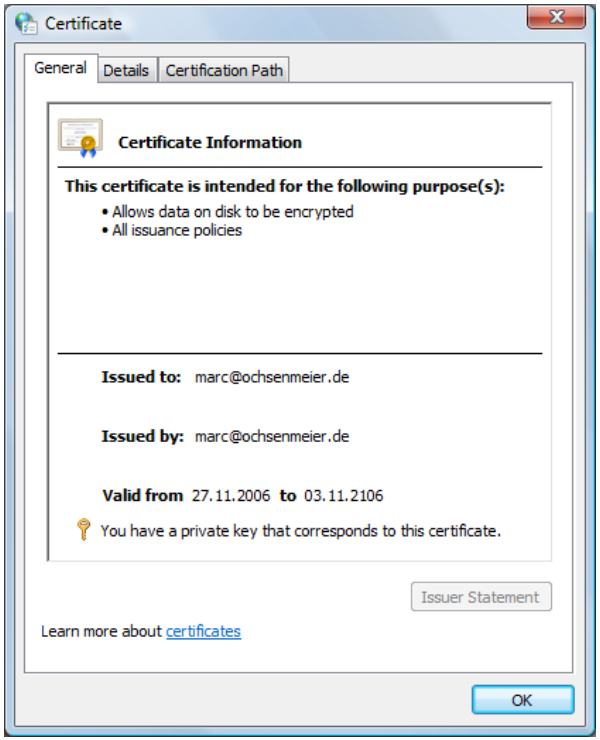


Digital Certificates

- Definition
  - A Digital Certificate is a set of two files
  - Contain private and public keys
- Purposes
  - Document the identity of a person/business via a Certificate Authority
  - Document the binding of a public key to a subject
  - Validate the public key of a subject
- Usages
  - Identify system users
  - Control access to computers, networks, and documents
  - Establish secure connections and transactions
  - Encrypt emails and data

Digital Certificates

- Creation
  - Issued by a trusted Certificate Authority (CA)
  - The purposes and limitations of a Digital Certificate are put in the Certificate
- Issue
  - Authenticity of a Certificate



PKI Applications

- EFS
- S/MIME
- IPSEC
- SMART CARD
- SSL
- Code Signing
- VPN

Links

- Windows Internals (Microsoft Press, M.Russinovich)
- Network Security Essentials (Prentice Hall, William Stallings)
- Step-by-Step Guide to Encrypting File System (EFS), www.microsoft.com
- How to manage the encrypted file system in Windows Enterprise Server
- Cryptography, a very short introduction, Fred Piper