Cryptography

- Data security
- Provides
  - Confidentiality
  - Integrity
  - Source authentication

Cryptography Uses

- Integrity and authentication
  - File hashing
  - E-mail digital signatures
  - VPN network traffic
  - Blockchain

Cryptography Uses

- Confidentiality
  - File, folder, and disk volume encryption
  - E-mail encryption
  - VPN network traffic
  - Mobile device encryption

Encryption

An encryption key is acquired

Key and data are fed into an encryption algorithm

The result is ciphertext

Hashing

- Provides file integrity
- Used to detect unauthorized modifications
- Can be used for digital evidence admissibility
- SHA-256 is commonly used

File Hashing Process

Raw data bits fed in

Results a unique value

Hash again

File Hashing

- Generate the hash in the future to detect changes from the original hash
- File hashing in Linux
  - md5sum <file>
- File hashing using Microsoft PowerShell
  - Get-FileHash <file> -Algorithm <algorithm>

Digital Signatures - Hashing

Uses a hashing algorithm to result in a hash value

Encrypted with the sender’s private key

Verifies the signature with the related public key

Digital Signatures

- Message authenticity
  - The message came from who it says it came from
  - The sender cannot refute having sent the message
    - "Non-repudiation"
    - Only the sender possesses the private key
    - The signature is verified the related public key

Symmetric Encryption

- Data confidentiality
- Protects sensitive data through encryption
- Original data is plain text
- Encrypted data is ciphertext

The Encryption Process

Plain text

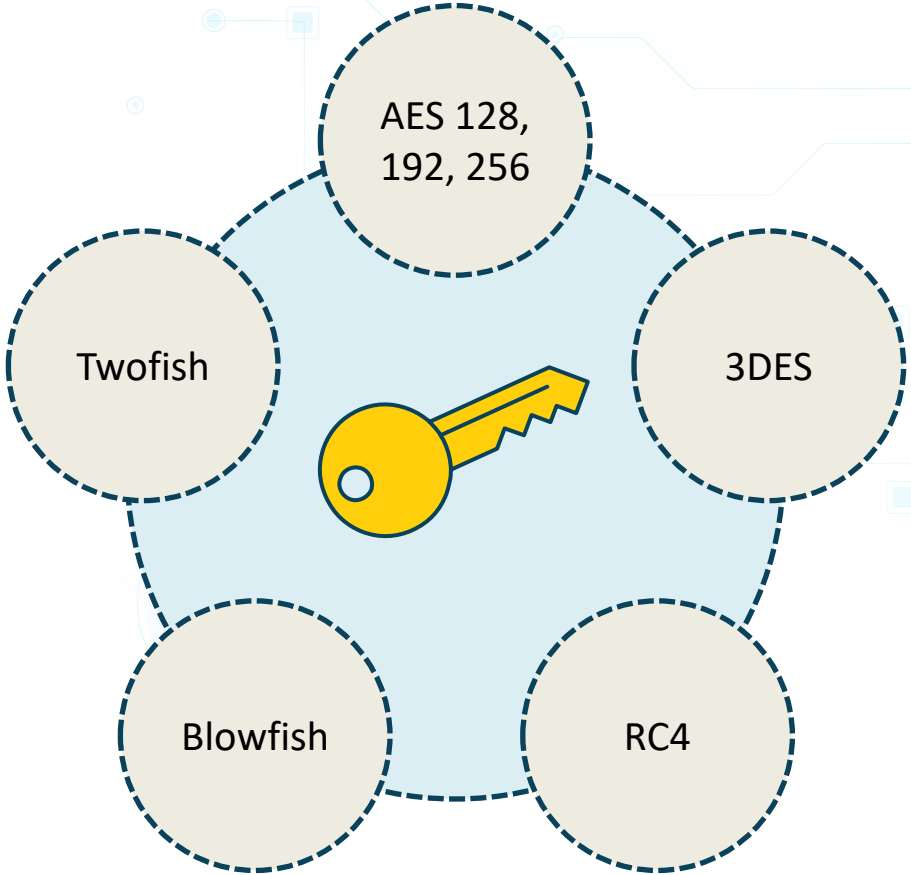
Plain text is fed into encryption algorithm with a key

Ciphertext

Symmetric Encryption

- Uses one unique key
  - Encryption
  - Decryption
- Also called a "secret key"
- The problem: securely distributing the key over a network

Common Symmetric Algorithms



Asymmetric Encryption

- Uses a public and private key pair
- The keys are mathematically related
- Also called "public key encryption"
- Requires a PKI certificate

Asymmetric Encryption

Secure key distribution

Not an issue

Public key can be made public

Private key must **not** be shared

Asymmetric Encryption

Encryption

- The sender requires the *recipient's* public key
- Decryption occurs with the *recipient's* related private key

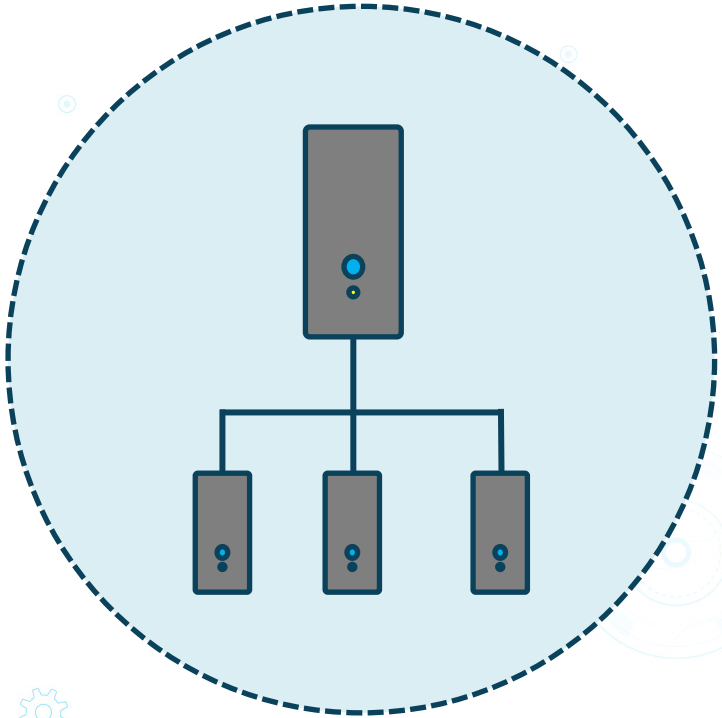
Digital signature

- Created with a private key
- Verified with the related public key

Common Asymmetric Algorithms

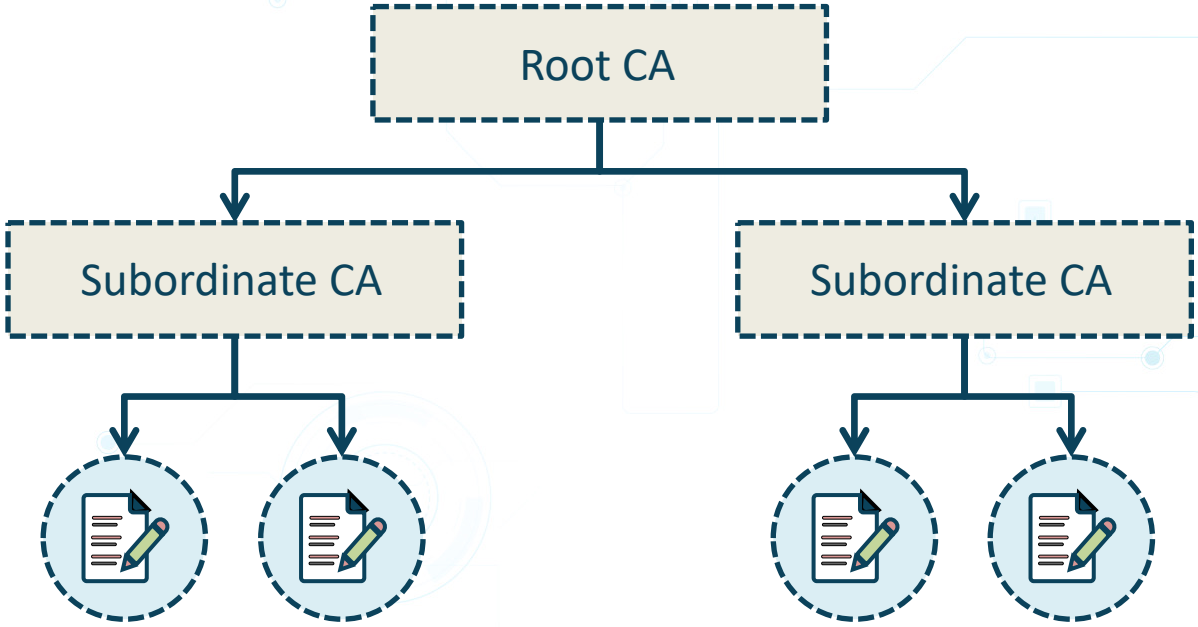
- RSA
- ElGamal
- ECC

PKI Hierarchy

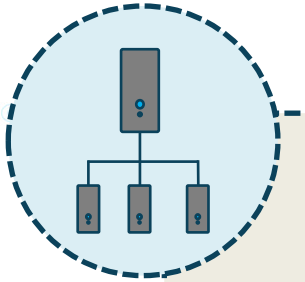


- A hierarchy of digital security certificates
- Certificates are issued and managed by Certificate Authorities (CAs)
  - Private CAs
  - Public CAs

PKI Hierarchy



PKI Hierarchy



- The issuing CA digitally signs issued certificates
- Root CAs should be brought offline when possible
- A compromised root CA
  - All certificates are compromised
- A compromised subordinate CA
  - Certificates issued under that CA are compromised

PKI Certificates

- Issued by a CA
- Issued to
  - User
  - Device
  - Software
- Issued for the purposes of
  - Encryption
  - Integrity
  - Authentication
- Stored in files and smartcards

PKI Certificate Contents

X.509 version number	CA signature	CA signature algorithm used
Certificate serial number	Issued date	Expiry date
Certificate intended use	Subject name	Public/private keys

Public and Private Keys

Public

- Can be shared publicly with any user or device
- Recipient public key is used when encrypting message
- Used to verify digital signatures

Private

- Must be available only to the key owner
- Can be embedded in cards
- Encrypted messages are decrypted using this key
- Used to create digital signatures

PKI Usage

Need	Solution
E-mail confidentiality	Encrypt message with recipient public key

PKI Usage

Need	Solution
E-mail confidentiality	Encrypt message with recipient public key
E-mail authenticity and integrity	Generate message hash and encrypt with sender private key

PKI Usage

Need	Solution
E-mail confidentiality	Encrypt message with recipient public key
E-mail authenticity and integrity	Generate message hash and encrypt with sender private key
Secure network communication to web server	Use a PKI certificate with TLS v1.1 or higher to enable HTTPS

PKI Usage

Need	Solution
E-mail confidentiality	Encrypt message with recipient public key
E-mail authenticity and integrity	Generate message hash and encrypt with sender private key
Secure network communication to web server	Use a PKI certificate with TLS v1.1 or higher to enable HTTPS
Multifactor authentication to a VPN	Smartcards with embedded private key

PKI Usage

Need	Solution
E-mail confidentiality	Encrypt message with recipient public key
E-mail authenticity and integrity	Generate message hash and encrypt with sender private key
Secure network communication to web server	Use a PKI certificate with TLS v1.1 or higher to enable HTTPS
Multifactor authentication to a VPN	Smartcards with embedded private key
Single card for facility and computer access	Common access card (CAC) with embedded private key

PKI Certificate Lifecycle

- Certificate issuance controls
- Key management controls
- Certificate retirement controls

PKI Lifecycle

Certificate issuance

Certificate usage

Certificate renewal, expiry, and revocation

PKI Certificate Lifecycle Management

- Assign PKI administrative roles
- Enable auditing
- Monitor certificate expiry dates
- Mobile device remote wipe
  - Lost or stolen device containing certificates

Securing Network Traffic

- Secure Sockets Layer (SSL)
  - Deprecated due to many known vulnerabilities
  - Uses a PKI certificate
  - Disable in client app and server-side

Transport Layer Security (TLS)

Supersedes SSL

TLS v 1.0 (deprecated), 1.1, 1.2, 1.3 (August 2018)

Uses a PKI certificate

Configured client and server-side

Securing Network Traffic

- The use of TLS v1.1 or higher is sometimes mandated by laws, regulations, and to attain security accreditations such as PCI DSS
- Secure Multipurpose Internet Mail Exchange (S/MIME)
  - Uses a PKI certificate
  - Used to encrypt and digitally sign e-mail messages

Securing Network Traffic with IPSec

- Used to secure any type of network traffic
- Does *not* imply using a VPN
- Encapsulating Security Payload (ESP)
- Authentication Header (AH)

In this exercise, you will

- Distinguish the difference between symmetric and asymmetric encryption
- Describe the digital signing process
- Define the relationship between HTTPS and PKI certificates
- Use Microsoft PowerShell to generate a file hash

Symmetric and Asymmetric Encryption

- Symmetric
  - One key encrypts and decrypts
- Asymmetric
  - Public key of recipient encrypts
  - Private key of recipient decrypts

Digital Signing - Hashing

- The message content uses a hashing algorithm to result in a hash value
- The hash value is encrypted with the sender’s private key
- The recipient verifies the signature with the related public key

HTTPS and PKI

- HTTPS
  - Configured on a web server
  - Standard port is TCP 443
  - Requires a PKI certificate to encrypt communications