CompTIA Security+ Exam SY0-701

Lesson 3

Explaining Appropriate Cryptographic Solutions

Objectives

- Compare and contrast cryptographic algorithms
- Explain the importance of public key infrastructure and digital certificates
- Explain the importance of using appropriate cryptographic solutions for encryption and key exchange

Lesson 3

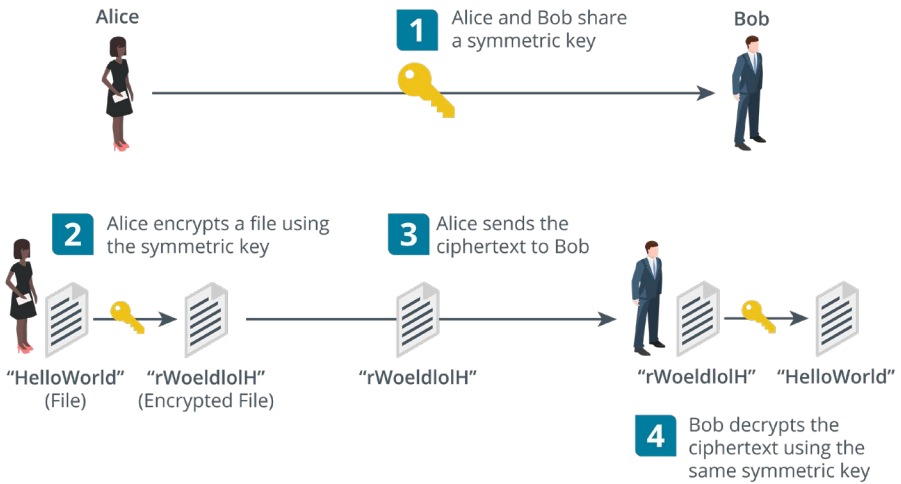
Topic 3A

Cryptographic Algorithms

Cryptographic Concepts

- Encryption and decryption—encoding and decoding
  - Plaintext is the unencoded message
  - Ciphertext is the coded message
  - Cipher is the means of change or algorithm
- Cryptanalysis is the art of cracking cryptographic systems
- Meet Alice and Bob (and observe Mallory, lurking)
- Hashing algorithms
- Encryption ciphers
  - Symmetric
  - Asymmetric

Symmetric Encryption



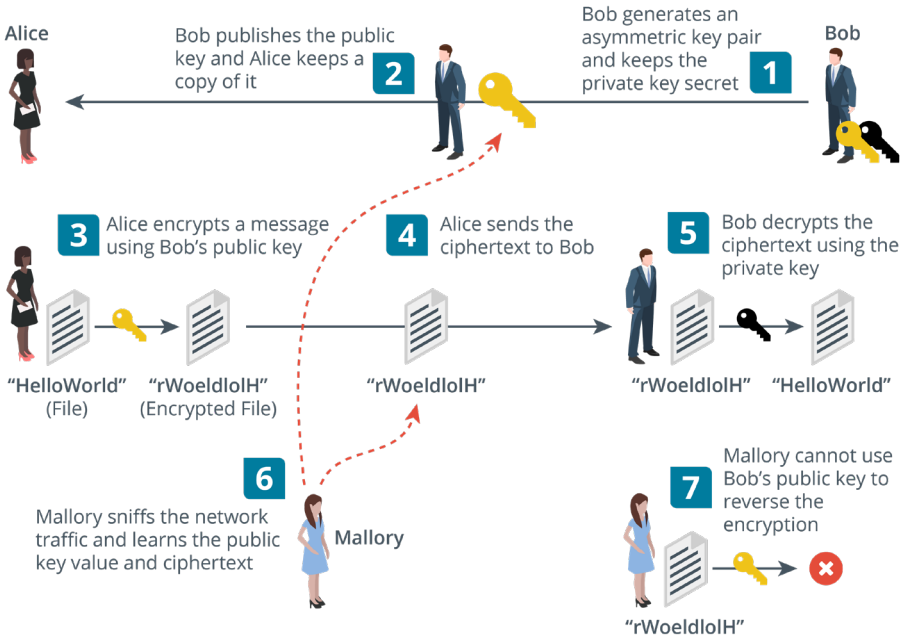
- Encryption uses a reversible process (algorithm) based on a key that is only known by authorized persons
- Substitution and transposition
  - Process should be too complex to unravel without the key
- Symmetric algorithms
  - Same secret key is used for encryption and decryption
  - Fast—suitable for bulk encryption of large amounts of data
  - Problem storing and distributing key securely
  - Confidentiality only— sender and recipient know the same key

Key Length

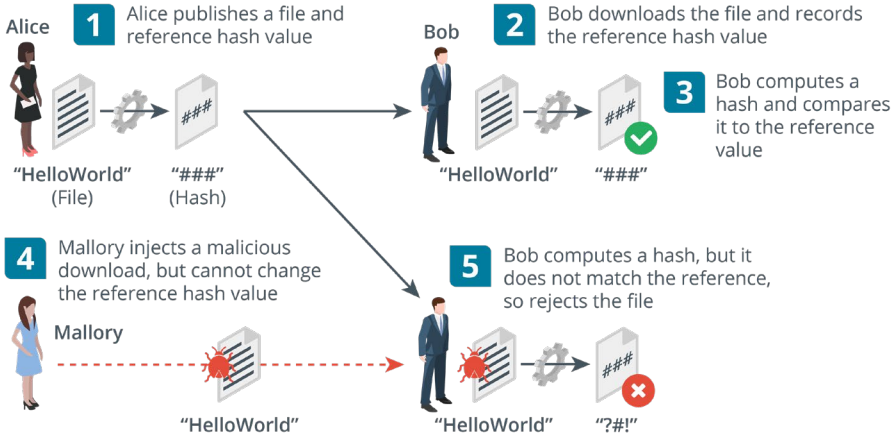
- Key ensures ciphertext remains protected even when the operation of the algorithm is known
- Range of key values is the keyspace
- Longer key bit length means a larger keyspace
  - Protects against brute force cryptanalysis
- Advanced Encryption Standard (AES/AES256)
  - 256-bit key is exponentially stronger than 128-bit key
  - Larger keys use more CPU/memory/power resources

Asymmetric Encryption

- Public/private key pair
  - If the public key encrypts, only the private key can decrypt
  - Private key cannot be derived from the public key
  - Private key must be kept secret
  - Public key is easy to distribute (anyone can have it)
- Used for small amounts of authentication data
- Different ciphers have different recommended key lengths
  - Rivest, Shamir, Adelman (RSA) cipher (2,048-bit or better)
  - Elliptic Curve Cryptography (ECC) cipher (256-bit or better)



Hashing

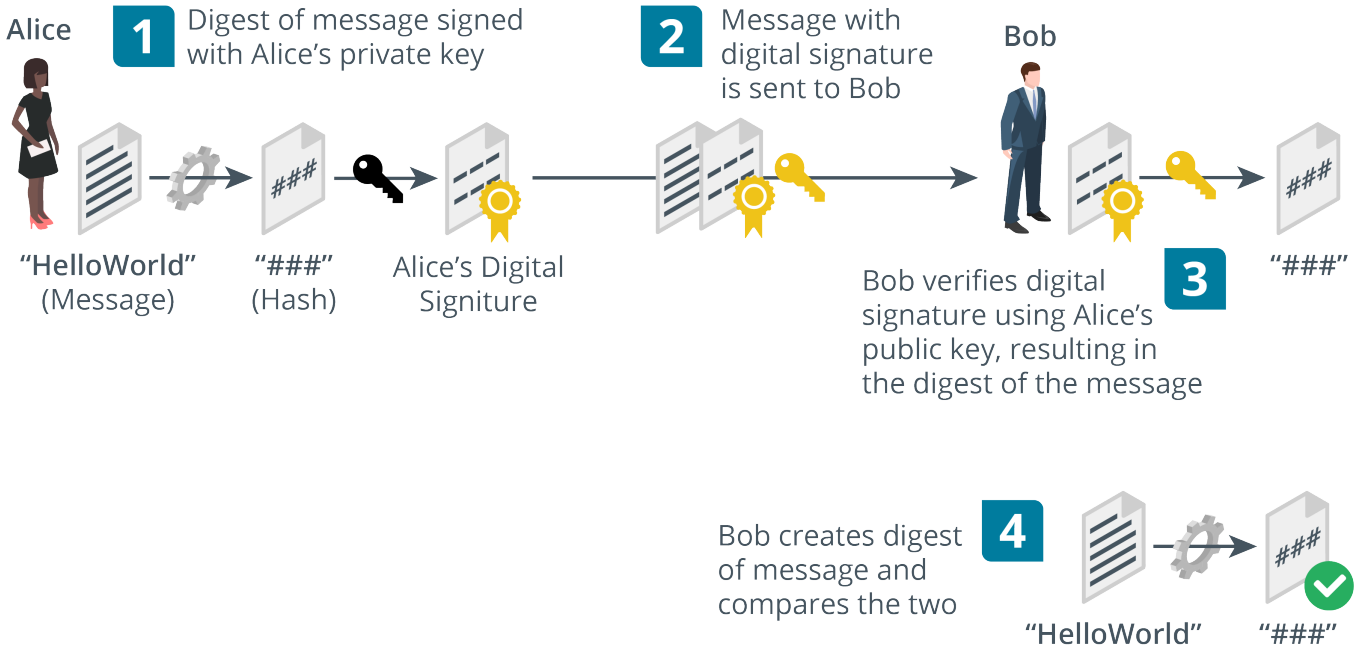


Images © 123rf.com.

- Fixed length digest from variable string with cryptographic properties
  - One-way (plaintext cannot be recovered from the digest)
  - Anti-collision (no two plaintexts are likely to produce the same digest)
- Used for password storage and checksums (integrity)
- Secure Hash Algorithm (SHA)
  - 256-bit or better
- Message Digest Algorithm (MD5)
  - 128-bit only

Digital Signatures

- Using public key cryptography with hashing
- Digital signatures provide integrity, authentication, non-repudiation



Review Activity: Cryptographic Algorithms

- Cryptographic concepts
- Symmetric encryption
  - Same secret key encrypts and decrypts
- Key length
- Asymmetric encryption
  - Public/private key pair
- Hashing
  - Non-reversible
- Digital signatures
  - Sign message hash with private key and validate with public key

Lab Activity

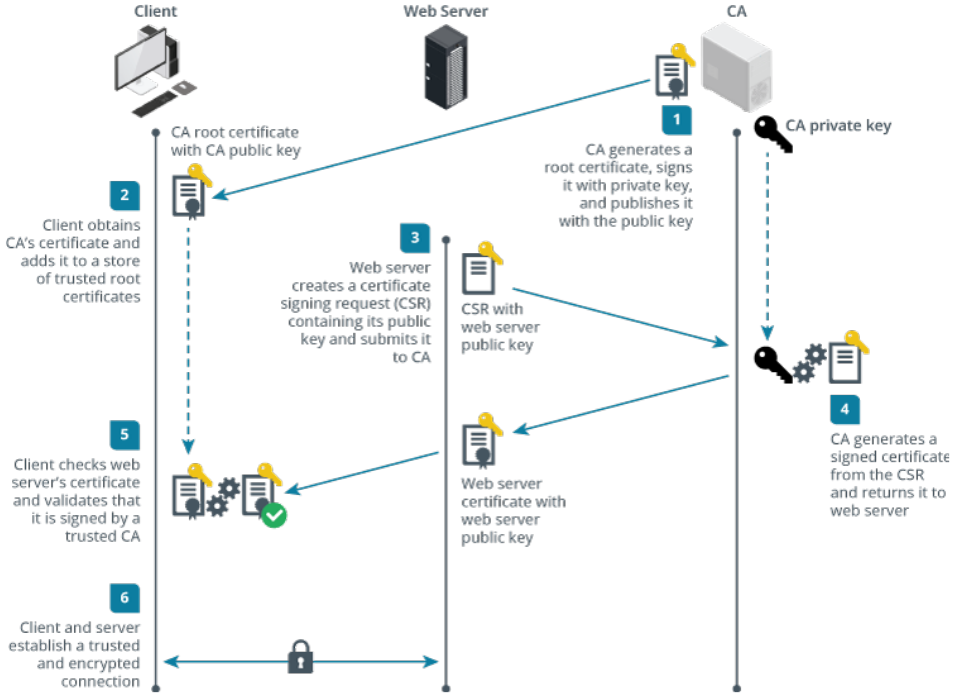
- Applied Lab: Using Storage Encryption

Lesson 3

Topic 3B

Public Key Infrastructure

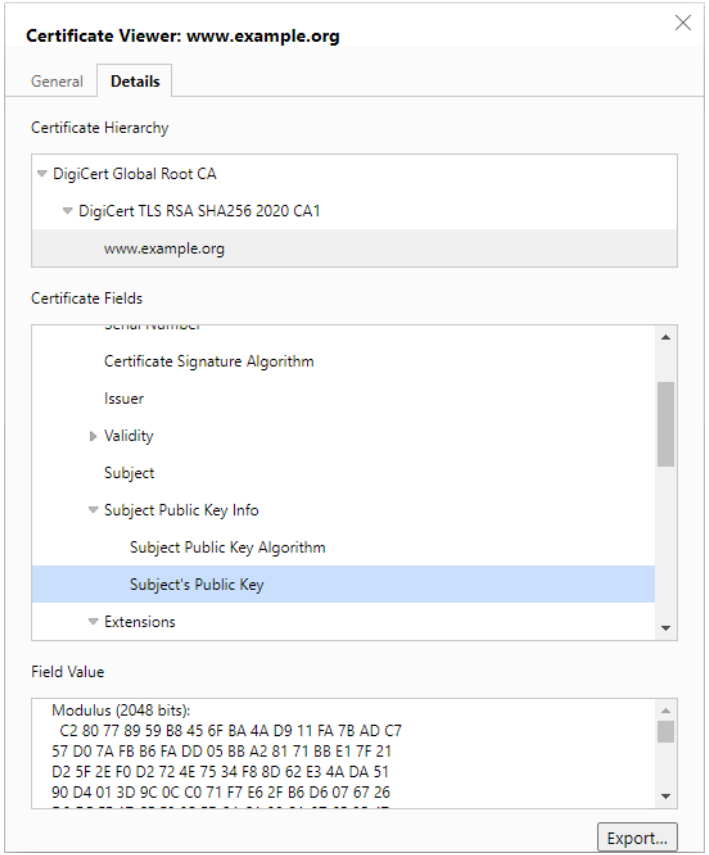
Certificate Authorities



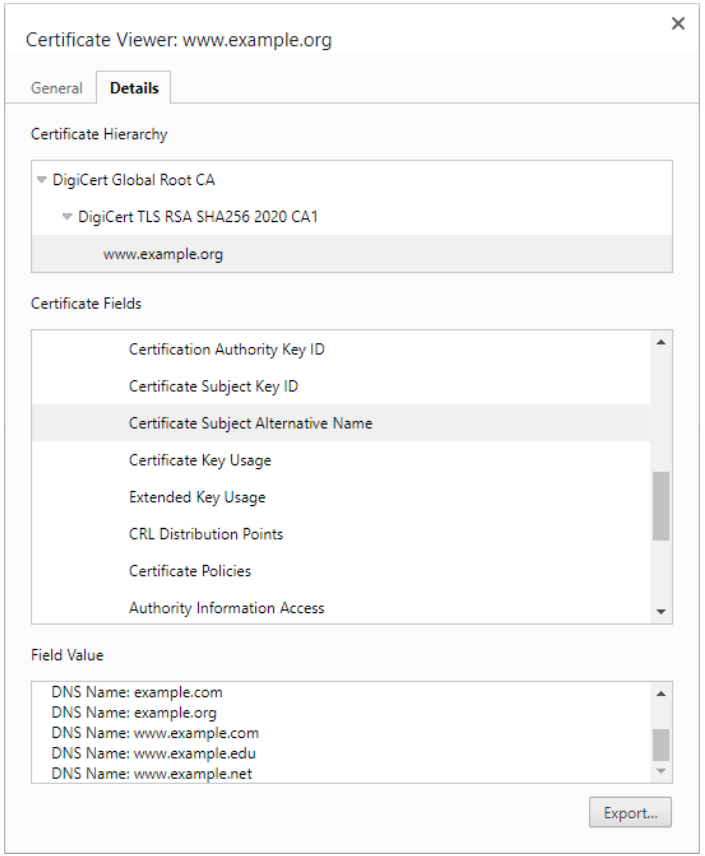
- Public key infrastructure (PKI)
  - Prove identity of a public key holder (subject user or computer)
- Certificate authority (CA)
  - Repository of certificates and public keys issued to verified subjects
- Third-party CA
  - Entity that has established widespread trust in its policies and procedures for issuing certificates

Digital Certificates

- Contains subject's public key
- Information identifying the subject plus usage and validity
- Digital certificate standards
  - X.509 Public Key Infrastructure (PKIX)
  - PKCS (Public Key Cryptography Standards)



Root of Trust

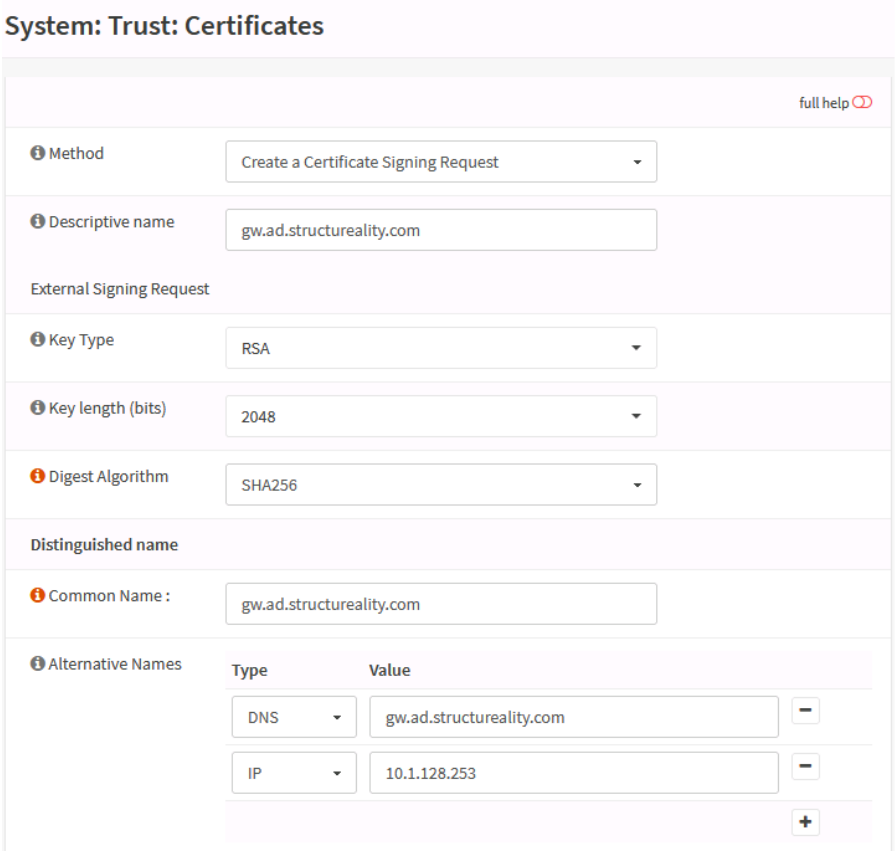


Screenshot used with permission from Microsoft.

- Root certificate
  - Self-signed, so users must trust in the CA's security procedures
- Single CA
  - CA issues certificates directly to subjects
- Hierarchical/chain of trust
  - Root CA
  - Intermediate CAs
  - Leaf certificates
- Self-signed certificates
  - Use certificate security without PKI, but provide no root of trust

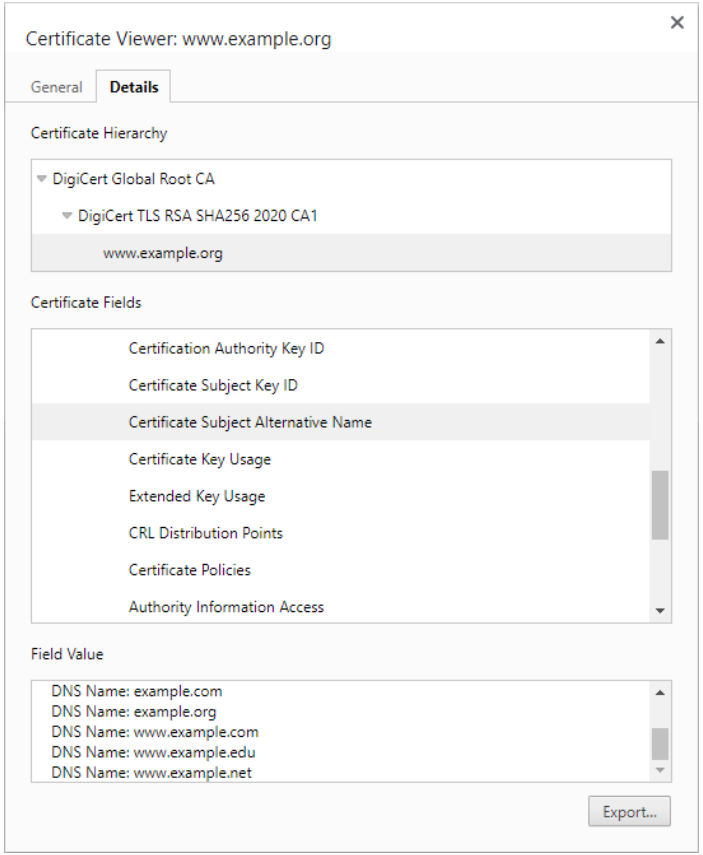
Certificate Signing Requests

- Registration identification and authentication procedures
- Certificate Signing Request (CSR)
  - Subject generates key pair and sends public key to CA with CSR
  - Subject does NOT send private key: this must be kept known to the subject
  - CA performs subject identity checks
  - CA signs and issues certificate



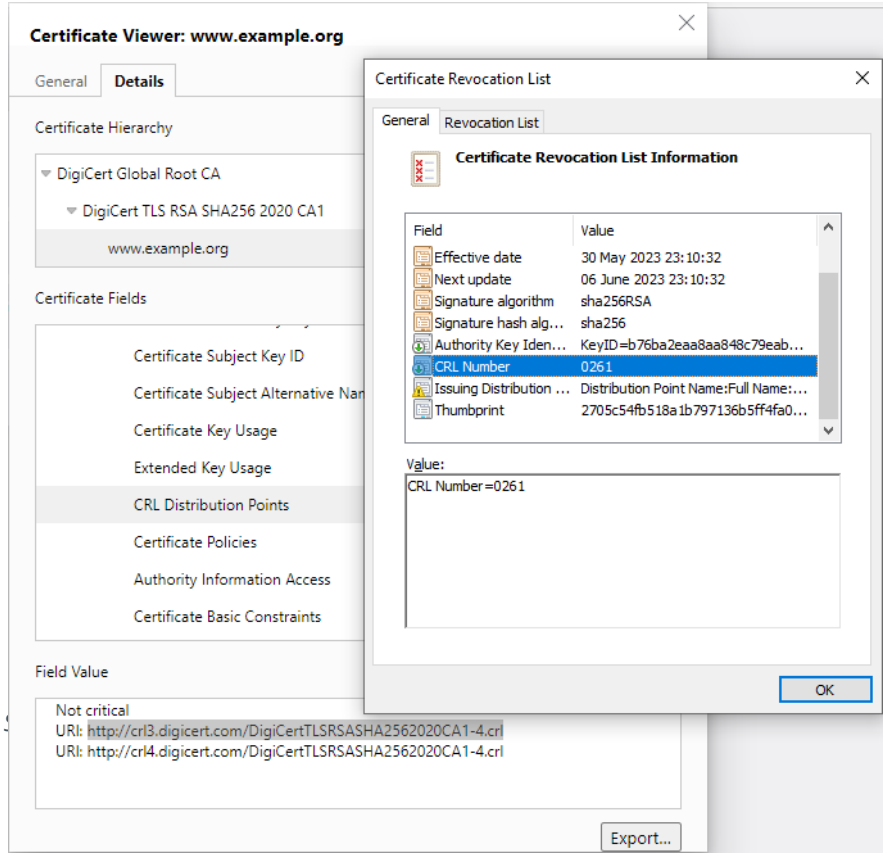
Subject Name Attributes

- Common Name (CN)
  - Legacy method of recording fully qualified domain name (FQDN)
  - Deprecated by standards
  - BUT still used in many implementations
- Subject Alternative Name (SAN)
  - Structured identifiers: name and/or IP address
  - List multiple host/subdomains
  - Use wildcard subdomain



Screenshot used with permission from Microsoft.

Certificate Revocation



- Revocation versus suspension
- Reason codes
- Certificate Revocation List (CRL)
  - List of revoked and suspended certificates
  - Browser CRL checking
- Online Certificate Status Protocol (OCSP)
  - Client queries single certificate per transaction
  - Provide real-time status information (though some rely on CRLs)

Key Management

- Key lifecycle
  - Key generation
  - Storage
  - Revocation
  - Expiration and renewal
- Decentralized key management
  - Each host or user account stores its own private key
- Key management system
  - Keys are generated and stored on a centralized server
  - Key Management Interoperability Protocol (KMIP)

Cryptoprocessors and Secure Enclaves

- Key generation challenges
  - Entropy and random number generation
  - Tamper-evident storage
- Trusted Platform Module (TPM)
  - Cryptoprocessor implemented on CPU (or motherboard)
- Hardware Security Module (HSM)
  - Cryptoprocessor in removable or dedicated hardware form factor (or virtual appliance)
  - Reduced attack surface and tamper-evident
- Secure enclave
  - Protect keys loaded in system memory

```
GnuPG needs to construct a user ID to identify your key.

Real name: James Pengelly
Email address: jpengelly@comptia.org
Comment:
You selected this USER-ID:
    "James Pengelly <jpengelly@comptia.org>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/kali/.gnupg/trustdb.gpg: trustdb created
gpg: directory '/home/kali/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/kali/.gnupg/openpgp-revocs.d/C3E
1D43D17CBCC7C80A3D4889564BC94BD4E1D99.rev'
public and secret key created and signed.

pub   rsa2048 2023-05-31 [SC] [expires: 2025-05-30]
      C3E1D43D17CBCC7C80A3D4889564BC94BD4E1D99
uid                      James Pengelly <jpengelly@comptia.org>
sub   rsa2048 2023-05-31 [E] [expires: 2025-05-30]
```

Key Escrow

- Keys can be backed up to protect against data loss
- Anyone with access to backup keys could impersonate the true key holder
- Escrow backup
  - Placing archived keys with a trusted third party
- M-of-N control
  - Key recovery processes can be protected by M of N control
  - Split key into multiple parts held by different key recovery agents

Review Activity: Public Key Infrastructure

- Certificate authorities
- Digital certificates
- Root of trust
- Certificate signing requests
- Subject name attributes
- Certificate revocation
- Key management
- Cryptoprocessors and secure enclaves
- Key escrow

Lesson 3

Topic 3C

Cryptographic Solutions

Encryption Supporting Confidentiality

- Data states
  - Data at rest, data in transit, data in use
- Bulk encryption
  - Using a private asymmetric key is inefficient for large amounts of data
  - Private key (key encryption key) is used to encrypt a symmetric key (media/data encryption key)

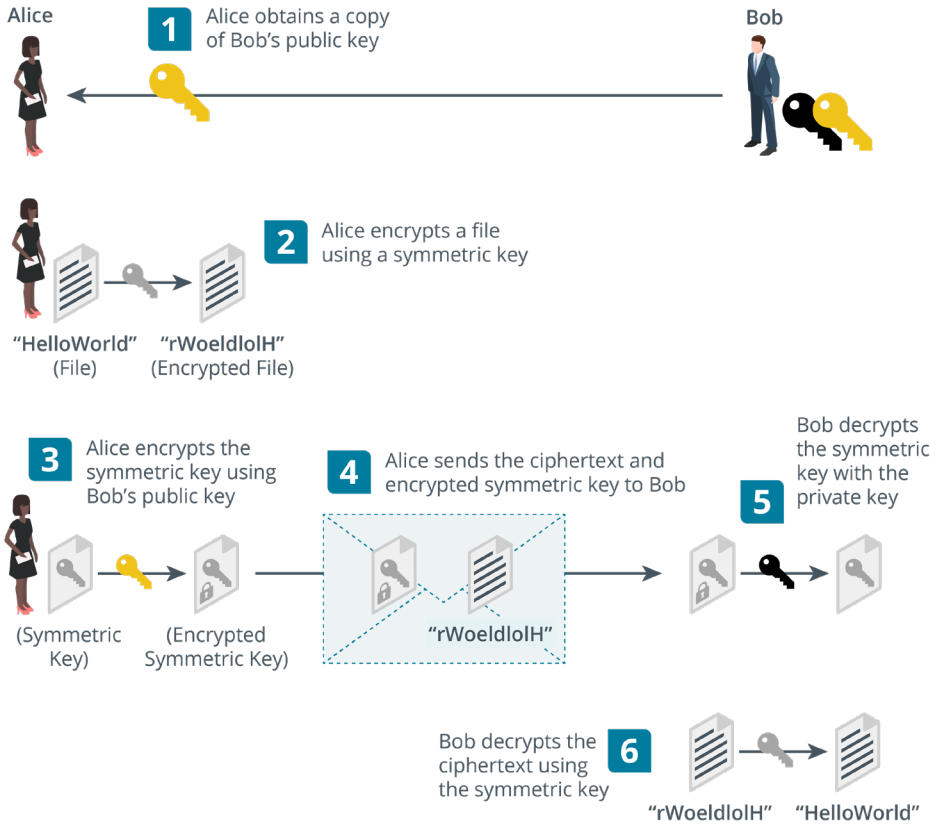
Disk and File Encryption

- Data at rest storage levels
- Full disk and partition encryption
  - Encrypt whole disk or partition on disk
  - Often performed by drive firmware (self-encrypting)
- Volume and file encryption
  - Often performed by OS/software
  - Usually requires file system support

Database Encryption

- Structured data
  - Tables, columns (fields), and rows (records)
  - Database Management System (DBMS)
    - Structured Query Language (SQL)
- Database-level encryption
  - Page-level decryption and encryption as data is moved from disk to memory
- Record-level encryption
  - Cell/column versus record-level
  - Enforce fine-grained access controls to support compliance requirements for privacy/security

Transport Encryption and Key Exchange



Perfect Forward Secrecy

Salting and Key Stretching

- Password hashes
- User-generated data is low entropy
  - Brute force attack discovers value by generating every possible value and finding a match
- Salting
  - Add a random value to each password when hashing it for storage
  - Prevents use of pre-computed hash tables
- Key stretching
  - Use additional rounds to strengthen keys
  - Makes attacker do more work, so slows down brute force

Blockchain

- Expanding list of transactional records (blocks)
- Each block is linked by hashing
- Open public ledger
- Ledger of transactions performed on a digital asset
- Peer-to-peer so transactions are public
- Transactions cannot be deleted or reversed
- Widely used for cryptocurrencies
- Potential uses for financial transactions, online voting systems, identity management systems, notarization, data storage, …

Obfuscation

- Steganography
  - Concealing messages within a covertext
  - Often uses file data that can be manipulated without introducing obvious artifacts
  - Covert channels
- Data masking
  - Redacting information from fields
- Tokenization
  - Substituting data with token
  - Reversible with access to the token server
- De-identification

Review Activity: Cryptographic Solutions

- Encryption supporting confidentiality
- Disk and file encryption
- Database encryption
- Transport encryption and key exchange
- Perfect forward secrecy
- Salting and key stretching
- Blockchain
- Obfuscation

Lab Activity

- Assisted Lab: Using Hashing and Salting

Lesson 3

Summary