

CISSP® Common Body of Knowledge Review: Cryptography Domain – Part 2

Version: 5.9.2



CISSP Common Body of Knowledge Review by Alfred Ouyang is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Cryptography Domain

The Cryptography domain addresses the principles, means, and methods of applying mathematical algorithms and data transformations to information to ensure its integrity, confidentiality, and authentication.

The candidate is expected to know basic concepts within cryptography; public and private key algorithms in terms of their applications and uses; algorithm construction, key distribution and management, and methods of attack; the applications, construction and use of digital signatures to provide authenticity of electronic transactions, and non-repudiation of the parties involved; and the organization and management of the Public Key Infrastructure (PKIs) and digital certification and management.

Review of Part 1

- Classic ciphers:
 - Substitution cipher
 - Transposition cipher
 - Polyalphabetic (or running key) cipher
 - Concealment
- Modern ciphers:
 - Block cipher
 - Stream cipher
 - Steganography
 - Combination

Review of Part 1

- Hash Function Cryptography
 - Non-keyed Digest (for integrity)
 - Keyed Digest (for authentication)
 - Digital Signature (for non-repudiation)
- Symmetric Cryptography
 - Block Ciphers
 - Confusion & Diffusion
 - Confusion: S-box
 - Diffusion: Feistel network & Columnar transposition
 - Stream Ciphers
 - XOR operation
 - Modes of operation
 - Block mode: ECB and CBC
 - Stream mode: CFB, OFB, CTR

Review of Part 1

- Asymmetric Cryptography
 - Diffie-Hellman Algorithm
 - Factorization Algorithm
 - Discrete Logarithm Algorithm



- Hybrid Cryptography
 - Make use of asymmetric cryptography to keep the ephemeral secret key secret.
 - Make use of hash functions to ensure integrity and non-repudiation of the ephemeral secret key

Discussion on Part 2

- Utilization of Cryptography
 - Public Key Infrastructure (PKI)
 - HTTP, S-HTTP, IPsec, SSH, SET
 - Single Sign-On (SSO)
 - Secured E-mail
- Types of Crypto Attacks
 - Cryptoanalytic Attacks
 - Cryptographic Attacks
- Discussion on export of crypto technologies

Cryptography Domain – Part 2

- Utilization of Cryptography



- Public Key Infrastructure (PKI)
- HTTP, S-HTTP, IPsec, SSH, SET
- Single Sign-On (SSO)
- Secured E-mail
- Quantum Cryptography

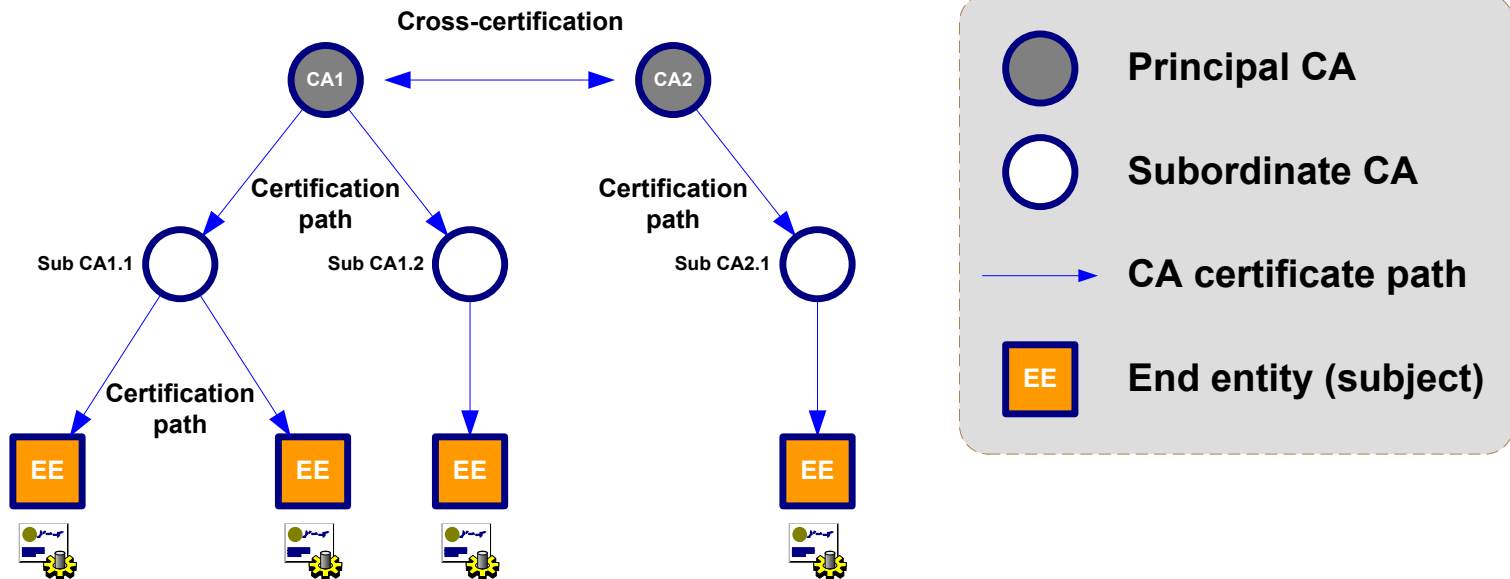
- Types of Crypto Attacks

- Cryptanalytic Attacks
- Cryptographic Attacks

- Discussion on export of crypto technologies

Public Key Infrastructure (PKI)

- PKI is a certificate-based public key hybrid cryptosystem
- PKI uses a “3rd party trust model”.
- Certification Authorities (CAs) provide verification of “end entity’s” (EE) certificate (identity, public key, and associated credentials).



Public Key Infrastructure (PKI)

For CISSP Exam...

PKI provides four (4) core services:

- Authentication
 - Provide assurance the person is who he/she claims to be.
- Integrity
 - Provide assurance that data received has not been altered, either intentionally or unintentionally.
- Confidentiality
 - Provide assurance that no one can read a particular piece of data except the intended receiver.
- Non-Repudiation
 - Provide assurance that the message sent cannot be disputed.

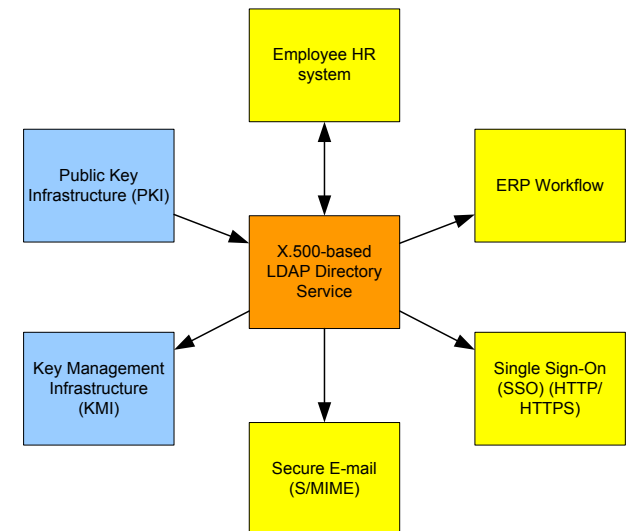
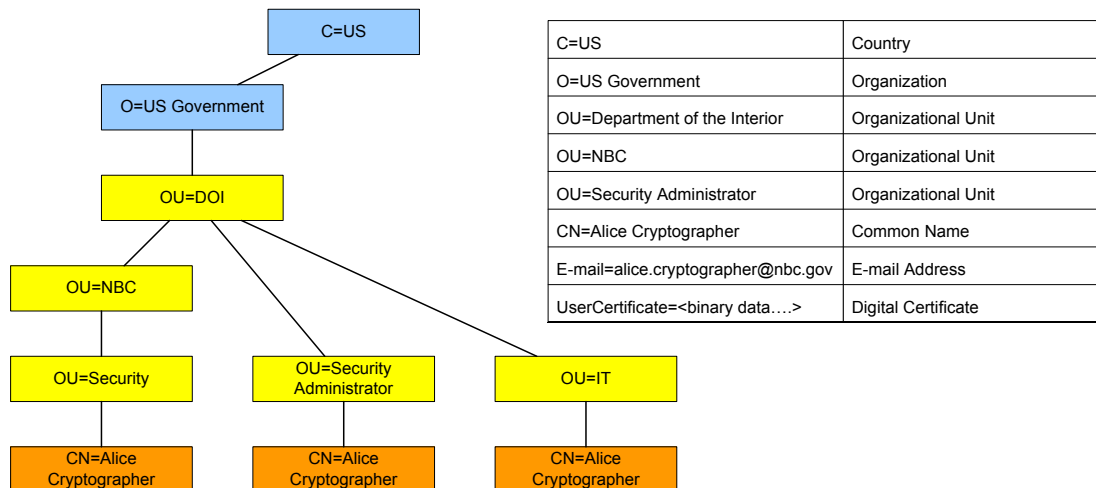
Public Key Infrastructure (PKI) – Functional Components

PKI consists of...

- Directory Service
 - Who are you? Who knows you?
- Certificate Management Service
 - Where is your credential? Who issued your credential? Is it valid?
- Key Management Service
 - Please make me a key. Your public key? My public key?
- Cryptography Service
 - Asymmetric, symmetric, and hash

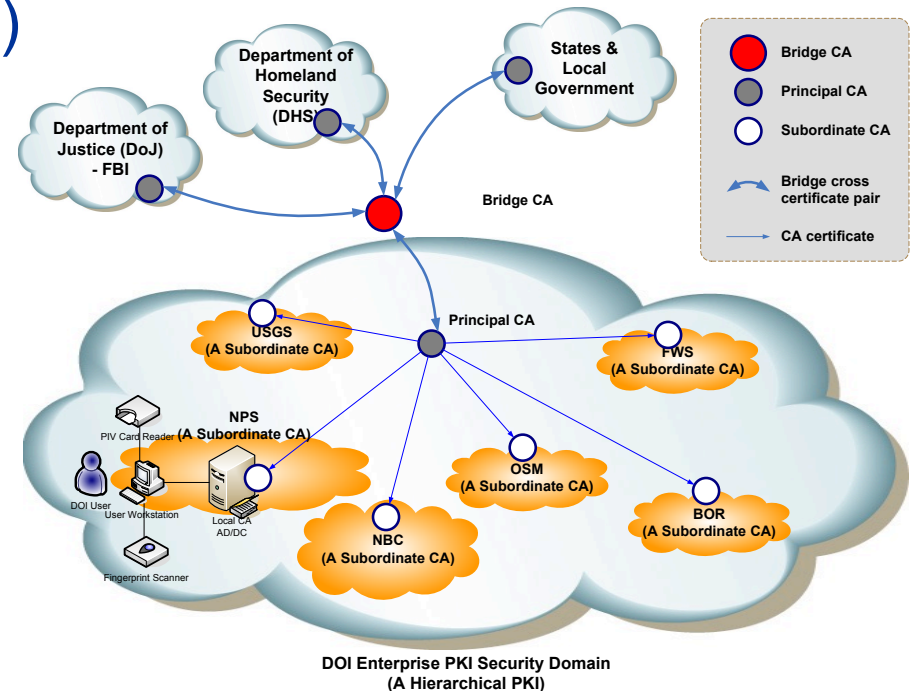
PKI Functional Component – Directory Service

- X.500-based LDAP directory service
 - A unified organizational information source that defines: Organization, Organizational Unit, IT systems, and Users... etc.
 - Store & distribute certificates (with keys and credentials) and certificate revocation list (CRL).
 - A central information hub to enterprise IT systems.



PKI Functional Component – Certificate Management Service

- Certificate Authority (CA)
 - Generate X.509-based digital certificates
 - Manages the life cycle of published certificates
 - Is a part of cross certification with other CAs
- Registration Authority (RA)
 - Interoperate with directory service to register subjects
 - Perform verification of certificates, certificate path



PKI Functional Component – Certificate Management Service

A X.509 digital certificate consist of...

- Version
- Serial Number
- Algorithm ID
- Issuer
- Validity
 - Not Before
 - Not After
- Subject
- Subject Public Key Info.
 - Public Key Algorithm
 - Subject Public Key
- Issuer Unique Identifier (Optional)
- Subject Unique Identifier (Optional)
- Certificate Signature Algorithm
- Certificate Signature

```

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
            OU=Certification Services Division,
            CN=Thawte Server CA/Email=server-certs@thawte.com
    Validity
      Not Before: Aug  1 00:00:00 1996 GMT
      Not After : Dec 31 23:59:59 2020 GMT
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
            OU=Certification Services Division,
            CN=Thawte Server CA/Email=server-certs@thawte.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
        68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
        85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
        6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
        6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
        29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
        6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
        5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
        3a:c2:b5:66:22:12:d6:87:0d
      Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
      CA:TRUE
    Signature Algorithm: md5WithRSAEncryption
    07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
    a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
    3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
    4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
    8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
    e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
    b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
    70:47
  
```

PKI Functional Component – Key Management Service

- Key establishment function – after a private key (or secret key in symmetric key crypto. operation) has been generated using RNG, a public key is then generated from the private key using an asymmetric key algorithm. (i.e., key generation)
- Key exchange function – composed of a set of key agreement protocols and key distribution rules, executing exchange of encryption keys.
- Key backup & recovery function – excluding ephemeral keys, “seeds” for RNG, and shared secret keys.

PKI Functional Component – Key Management Service

- Key revocation function – If a key has been compromised or subjected to a change, then...
 - the status of key-pair is revoked, and
 - the certificate status shall be listed in the certificate revocation list (CRL).
- Key destruction function – Key zero-ization is used in the destruction of key-pair.
- Key escrow function – Use of 3rd party agent (i.e. CA) to store “encrypted” key-pair.
 - Fair Cryptosystem, defined by FIPS 185 *Escrowed Encryption Standard*: SKIPJACK Algorithm and a Law Enforcement Access Field (LEAF) creation method.

Key Types Identified in NIST SP 800-57 ... (1/2)

Key Type	Crypto-period	
	Originator Usage Period (OUP)	Recipient Usage Period
1. Private Signature Key	1-3 years	
2. Public Signature Key	Several years (depends on key size)	
3. Symmetric Authentication Key	≤ 2 years	$\leq \text{OUP} + 3$ years
4. Private Authentication Key	1-2 years	
5. Public Authentication Key	1-2 years	
6. Symmetric Data Encryption Keys	≤ 2 years	$\leq \text{OUP} + 3$ years
7. Symmetric Key Wrapping Key	≤ 2 years	$\leq \text{OUP} + 3$ years
8. Symmetric and asymmetric RNG Keys	Upon reseeding	
9. Symmetric Master Key	About 1 year	
10. Private Key Transport Key	≤ 2 years	

Key Types Identified in NIST SP 800-57 ... (2/2)

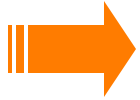
Key Type	Crypto-period	
	Originator Usage Period	Recipient Usage Period
11. Public key Transport Key	1-2 years	
12. Symmetric Key Agreement Key	1-2 years	
13. Private Static key Agreement Key	1-2 years	
14. Public Static Key Agreement Key	1-2 years	
15. Private Ephemeral Key Agreement Key	One key agreement transaction	
16. Public Ephemeral Key Agreement Key	One key agreement transaction	
17. Symmetric Authorization Key	≤ 2 years	
18. Private Authorization Key	≤ 2 years	
19. Public Authorization Key	≤ 2 years	

PKI Functional Component – Cryptography Service

- Asymmetric key cryptography operations in PKI
 - Because of crypto. operation speed, mostly used for key management function.
- Symmetric key cryptography operations in PKI
 - Because of speed, symmetric-key cryptosystems are used for crypto. operations. E.g. SSL/TLS at transport-level (communication path), e-mail & SOAP messages at message-level.
- Hash function
 - Message digest
 - Message authentication code (MAC)
 - Key-hashed MAC (HMAC)
 - Digital signature

Cryptography Domain – Part 2

- Utilization of Cryptography
 - Public Key Infrastructure (PKI)
 - HTTP, S-HTTP, IPsec, SSH, SET
 - Single Sign-On (SSO)
 - Secured E-mail
 - Quantum Cryptography
- Types of Crypto Attacks
 - Cryptanalytic Attacks
 - Cryptographic Attacks
- Discussion on export of crypto technologies

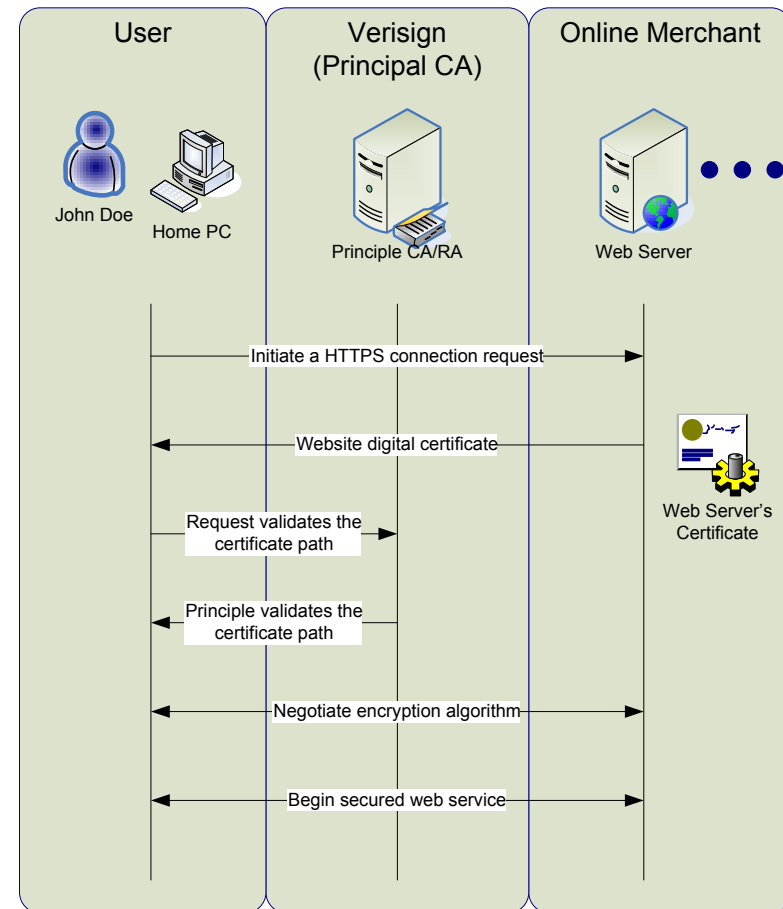
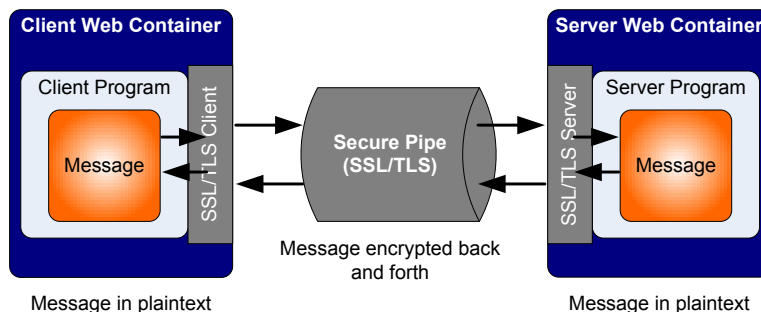


Cryptography for Internet Security

- HTTPS is a uniform resource identifier (URI) scheme that refers the use of HTTP over an encrypted Secured Socket Layer (SSL) or Transport Layer Security (TLS) session.
- S-HTTP – Secure Hypertext Transfer Protocol (RFC 2660)
 - a variation of HTTP providing encryption through a secure port using SSL/TLS.
 - Message oriented protocol – protects the message.
 - Supports encryption of Web documents employing RSA public key technology.
 - Provides confidentiality, integrity, non-repudiation and authentication for electronic payments.

Cryptography for Internet Security – HTTPS using PKI

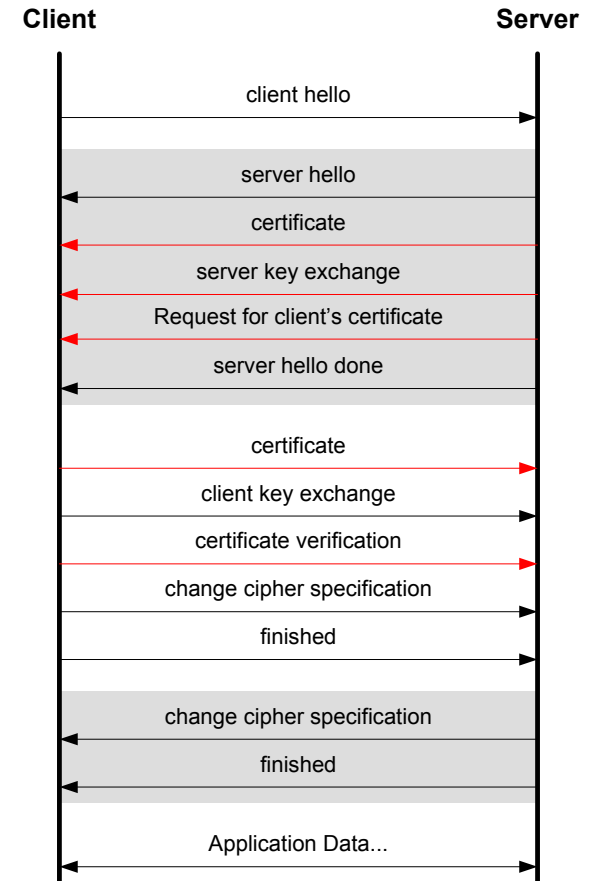
- X.509 certificate with public key is the key for implementing HTTPS...
 - SSL/TLS for Transport-Level security
 - Asymmetric key algorithm for key management operations
 - Symmetric key algorithm for cryptographic operations
 - Hash function & digital signature for integrity and non-repudiation
 - Principal CA is the “trusted third party” that enables the trusted relationships
 - PKI is the supporting IT infrastructure



Cryptography for Internet Security – SSL

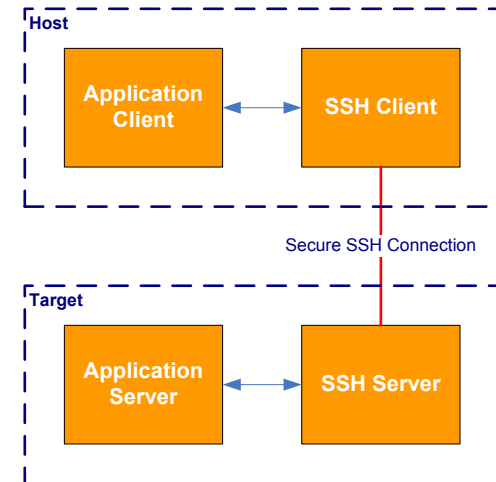
SSL (Secure Sockets Layer)

- Runs between the Application Layer (HTTP, SMTP, NNTP, etc) and the Transport Layer (TCP).
- Supports client/server's negotiation of cryptographic algorithms:
 - Public-key cryptography: RSA, Diffie-Hellman, DSA or Fortezza.
 - Symmetric ciphers: RC2, IDEA, DES, 3DES or AES.
 - One-way hash functions: MD5 or SHA.



Cryptography for Internet Security – SSH... (1/2)

- SSH (Secure Shell) is a secure replacement for the r* programs (rlogin, rsh, rcp, rexec, etc.) (RFC 4251)
- SSH consists of three major components:
 - Transport Layer Protocol [SSH-TRANS] provides server authentication, confidentiality, and integrity.
 - User Authentication Protocol [SSH-USERAUTH] authenticates the client-side user to the server.
 - Connection Protocol [SSH-CONNECT] multiplexes the encrypted tunnel into several logical channels.



Cryptography for Internet Security – SSH... (2/2)

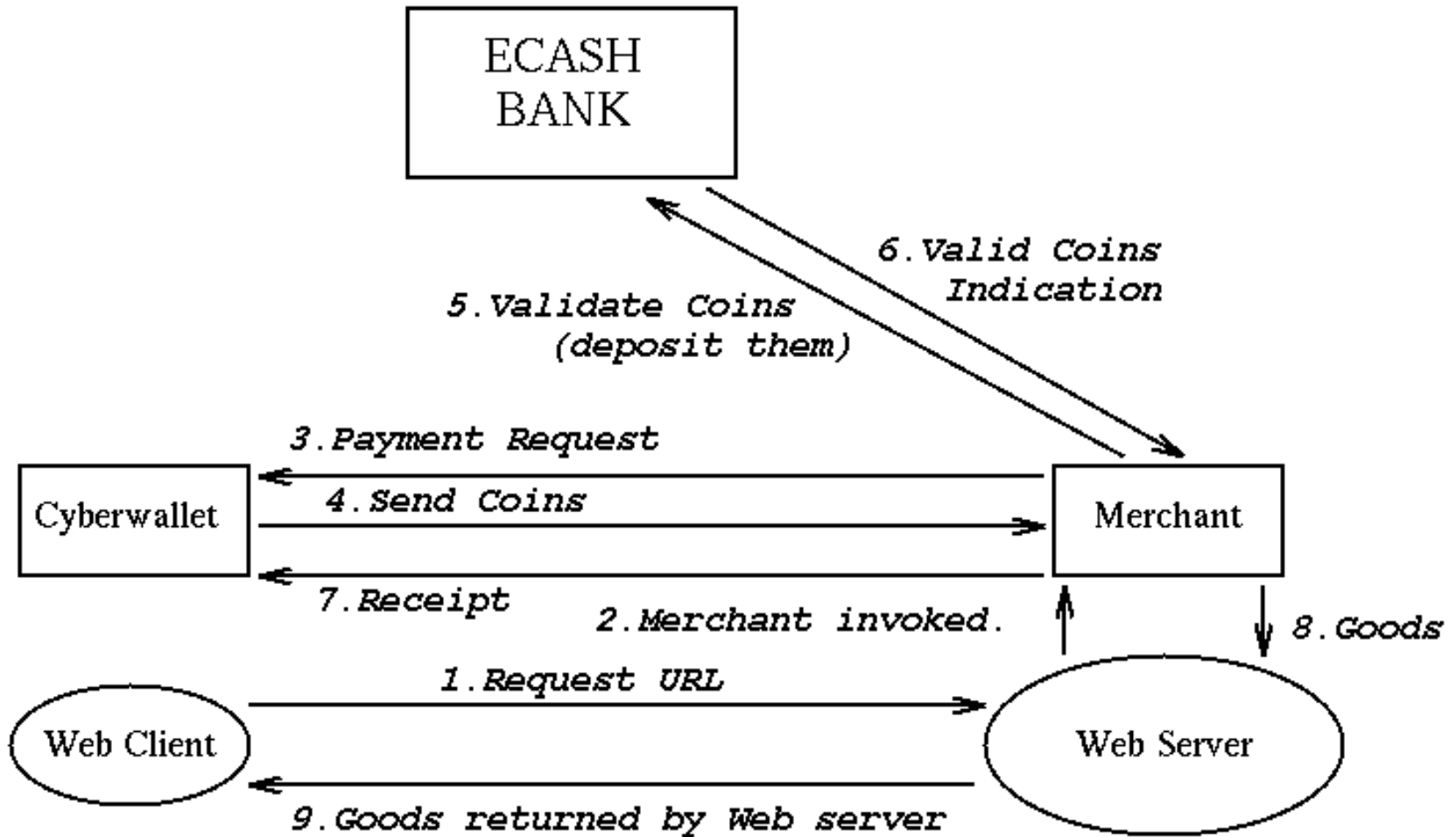
- SSH has an open architecture (RFC 4251):
 - Uses public-key trust model to authenticate users
 - “Web of trust”: Client has a local database of public keys
 - “3rd party of trust”: Public keys are certified by CAs
 - Supports variety of cryptography algorithms:
 - Blowfish, TDES, AES, IDEA, etc.
- SSH protects:
 - Eavesdropping of data transmitted over the network.
 - Manipulation of data at intermediate elements in the network (e.g. routers).
 - IP address spoofing where an attack hosts pretends to be a trusted host by sending packets with the source address of the trusted host.
 - DNS spoofing of trusted host names/IP addresses.
 - IP source routing.

Cryptography for Internet Security – SET

Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. It was supported initially by Mastercard, Visa, Microsoft, Netscape, and others.

- A user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signature among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and confidentiality.
 - SET uses Netscape's SSL, Microsoft's STT (Secure Transaction Technology), and Terisa System's S-HTTP.
 - SET uses some but not all aspects of a PKI.

Cryptography for Internet Security – SET - 2



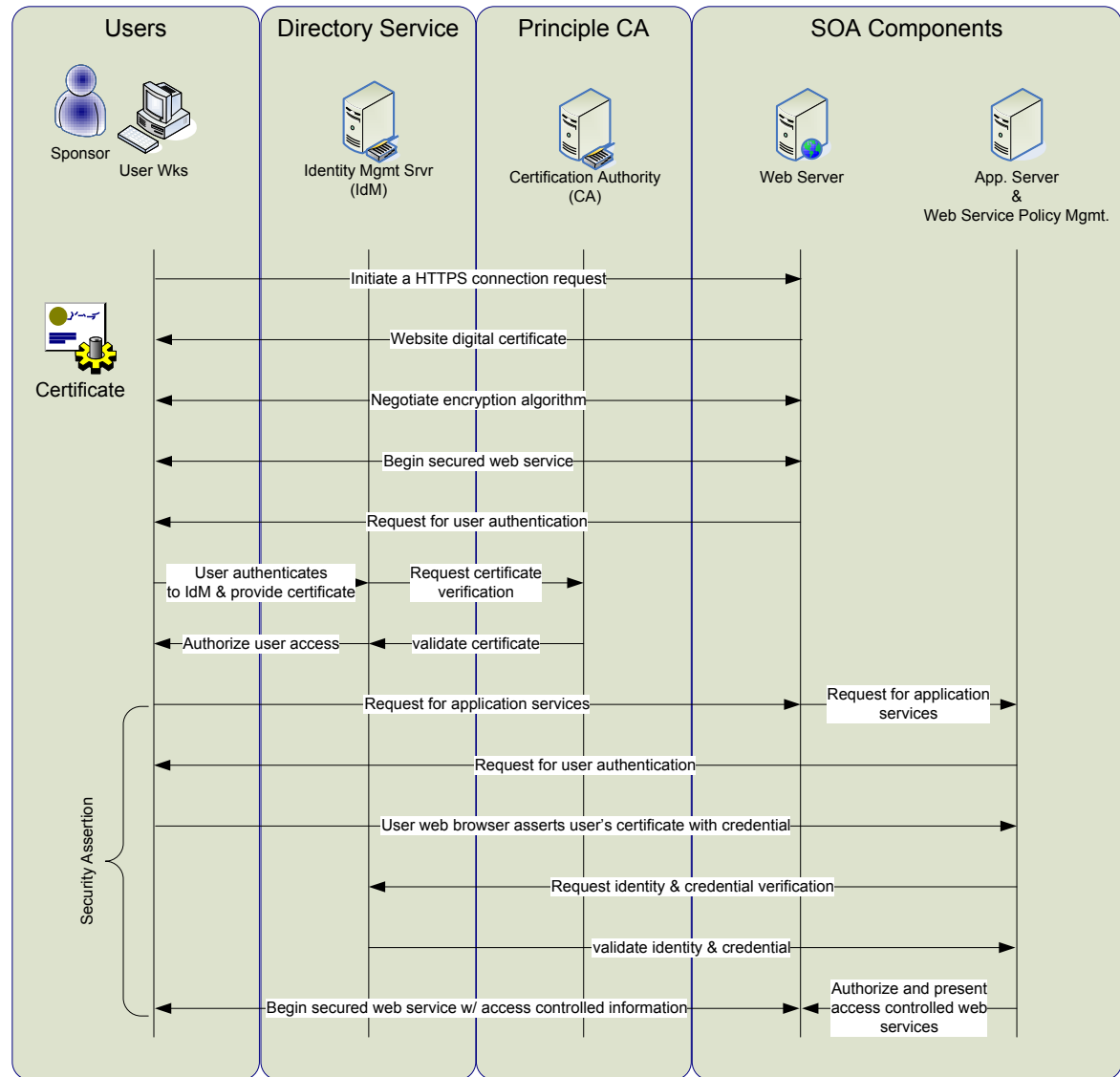
Cryptography Domain – Part 2

- Utilization of Cryptography
 - Public Key Infrastructure (PKI)
 - HTTP, S-HTTP, IPsec, SSH, SET
 - ➔ – Single Sign-On (SSO)
 - Secured E-mail
 - Quantum Cryptography
- Types of Crypto Attacks
 - Cryptanalytic Attacks
 - Cryptographic Attacks
- Discussion on export of crypto technologies

Cryptography for Single Sign-On (SSO) – Using PKI

Security Assertion is the key for implementing SSO...

- **SSL/TLS** for layer 4-7 security.
- **SAML** asserts user authentication credential & X.509 certificates from one system to another.
- **Principal CA** is the “trusted 3rd party” that enables the trusted relationships.
- **PKI** is the supporting IT infrastructure.



Cryptography Domain – Part 2

- Utilization of Cryptography
 - Public Key Infrastructure (PKI)
 - HTTP, S-HTTP, IPsec, SSH, SET
 - Single Sign-On (SSO)
 - Secured E-mail
 - Quantum Cryptography
- Types of Crypto Attacks
 - Cryptanalytic Attacks
 - Cryptographic Attacks
- Discussion on export of crypto technologies



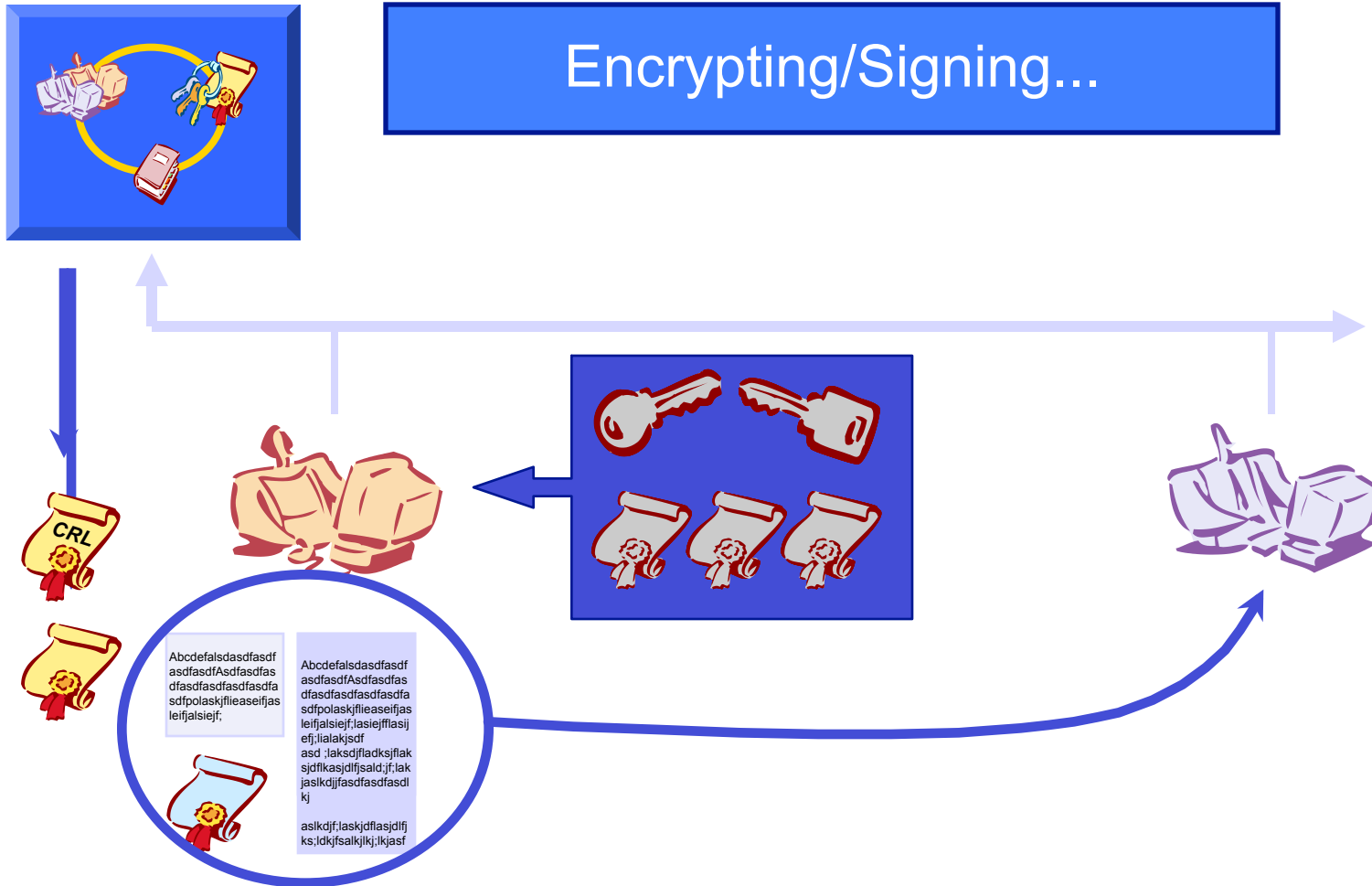
Cryptography for Secure E-mail Service

- Security Objectives (operational requirements)
 - Message origin – verify sender of message.
 - Content integrity – verify integrity of message.
 - Content confidentiality – verify secrecy of message.
 - Proof of delivery – verify delivery.
 - Message sequence integrity – verify proper segment order.
 - Non-repudiation of origin – verify sender to receiver.
 - Non-repudiation of delivery – verify receipt of message.

Cryptography for Secure E-mail Service – Standards

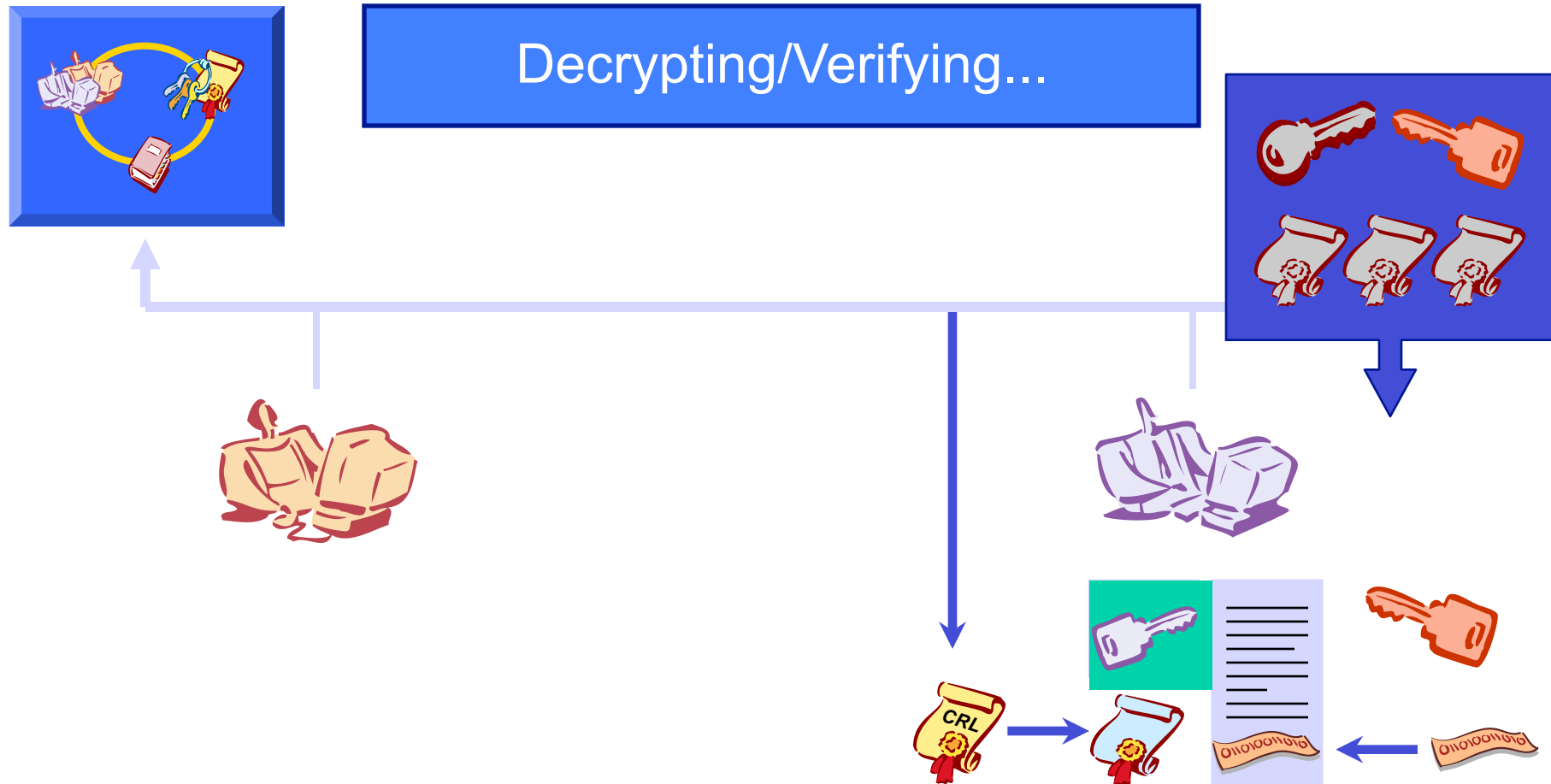
- Privacy Enhanced Mail (PEM) (RFC 822, 1421, 1422, 1423, 1424)
 - Internet standard to provide secure e-mail over the Internet or in-house.
 - Supports DES in CBC mode, RSA PKCS, X.509 digital certificate.
- Secure/Multipurpose Internet Mail Extension (S/MIME) (RFC 2633, RFC 2311)
 - Extension of MIME that supports encryption of e-mail and attachments.
 - Encryption and hashing algorithms can be defined by the user.
 - Supports X.509 Certificate format is used.
- Pretty Good Privacy (PGP)
 - Uses “web-of-trust” model, users create their own key-pair.
 - Supports a variety of Asymmetric and Symmetric algorithms.
 - PGP also does file/disk encryption.

Cryptography for Secure E-mail Service – S/MIME – Encrypting & Signing



- **ANALOGY: A lock is used to secure the message. The lock is a public key, and the key is a private key. The lock is used to encrypt the message, and the key is used to decrypt the message.**

Cryptography for Secure E-mail Service – S/MIME – Decrypting & Verifying

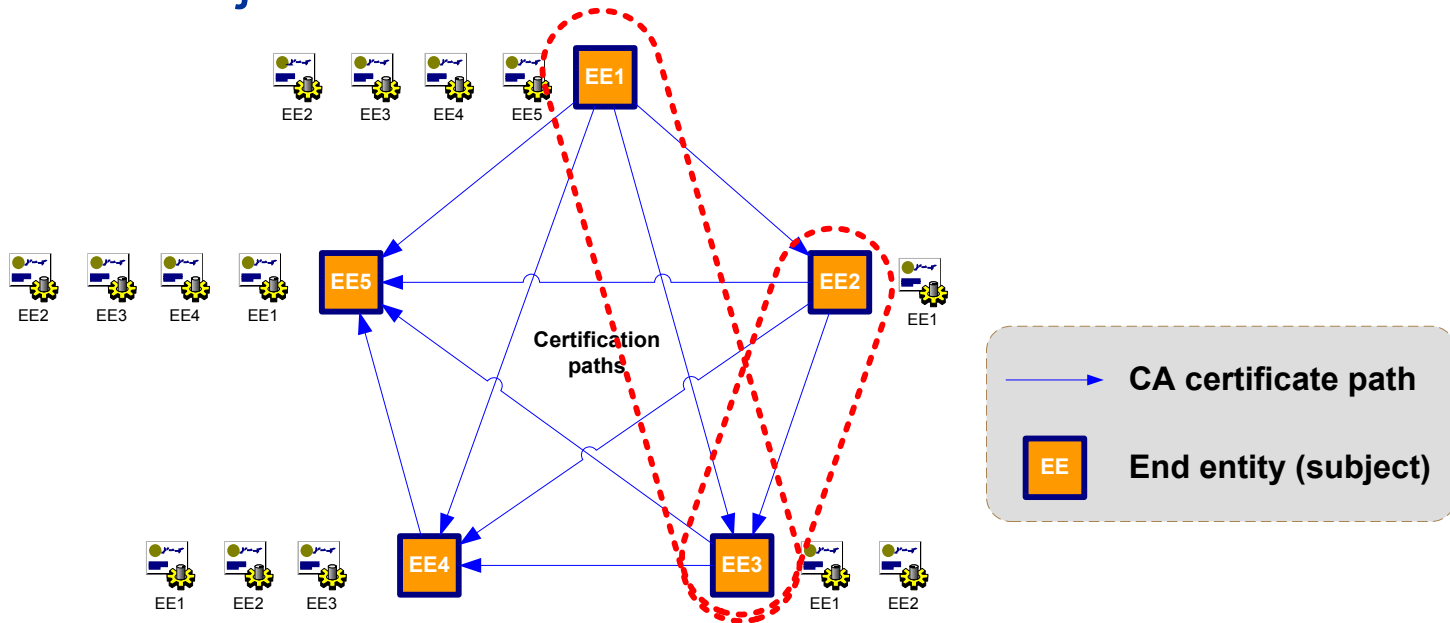


- Bob imports the public key from Alice's certificate and uses it to decrypt the message and verify the signature. He also imports the certificate from Alice's email and uses it to verify the signature.

Cryptography for Secure E-mail Service – Pretty Good Privacy (PGP)

Like PKI, PGP is also a hybrid cryptosystem, but unlike PKI, PGP uses a “web-of-trusts” model.

- There is no trusted CA to verify the identity and associated credential.
- Each “end entity” collects certificates from other trusted subjects.



Cryptography for Secure E-mail Service – Pretty Good Privacy (PGP)

PGP accepts both

- X.509 digital certificate and
- PGP certificate (consists of)

...

- PGP version number
- Algorithm ID
- Issuer
- Validity
 - Not Before
 - Not After
- Subject
- Subject Public Key Info.
 - Public Key Algorithm
 - Subject Public Key
- Certificate Signature Algorithm
- Certificate Signature

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 1 (0x1)
  Signature Algorithm: md5withRSAEncryption
  Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
        OU=Certification Services Division,
        CN=Thawte Server CA/Email=server-certs@thawte.com
  Validity
    Not Before: Aug  1 00:00:00 1996 GMT
    Not After : Dec 31 23:59:59 2020 GMT
  Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
        OU=Certification Services Division,
        CN=Thawte Server CA/Email=server-certs@thawte.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
        68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
        85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
        6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
        6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
        29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
        6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
        5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
        3a:c2:b5:66:22:12:d6:87:0d
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Basic Constraints: critical
    CA:TRUE
  Signature Algorithm: md5withRSAEncryption
    07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
    a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
    3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
    4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
    8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
    e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
    b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
    70:47
```

Cryptography Domain – Part 2

- Utilization of Cryptography
 - Public Key Infrastructure (PKI)
 - HTTP, S-HTTP, IPsec, SSH, SET
 - Single Sign-On (SSO)
 - Secured E-mail
 - Quantum Cryptography



Types of Crypto Attacks

- Cryptanalytic Attacks
- Cryptographic Attacks

Crypto Attacks

- Types of cryptanalytic attacks:
 - Ciphertext-only attack
 - Known-plaintext attack
 - Chosen-plaintext attack
 - Chosen-ciphertext attack
 - Adaptive-chosen-plaintext attack
 - Adaptive-chosen-ciphertext attack
- Types of cryptographic attacks
 - Brute-force attack
 - Symmetric block cipher attacks
 - Stream cipher attacks
 - Hash function attack
 - Message authentication code (MAC) attack
 - Birthday attack
 - Man-in-the-middle attack

Reference:

- *Cryptography Engineering*, N. Ferguson, B. Schneier, T. Kohno, Wiley Publishing, 2010.
- http://en.wikipedia.org/wiki/Category:Cryptographic_attacks

Types of Cryptanalytic Attacks... (1/2)

- Ciphertext-only attack (or known-ciphertext attack)
 - Attacker has: ciphertext messages
 - Goal: discover the key
- Known-plaintext attack
 - Attacker has: ciphertext and plaintext messages
 - Goal: discover the key
- Chosen-ciphertext attack
 - Attacker selects: a series of same ciphertext messages
 - Goal: discover the key
- Chosen-plaintext attack
 - Attacker selects: a series of ciphertext and corresponding plaintext messages
 - Goal: discover the key

Reference:

- *Cryptography Engineering*, N. Ferguson, B. Schneier, T. Kohno, Wiley Publishing, 2010.
- http://en.wikipedia.org/wiki/Category:Cryptographic_attacks

Types of Cryptanalytic Attacks... (2/2)

- Adaptive-chosen-ciphertext attack
 - Attacker is able to choose: ciphertext sample dynamically, depending on previous outcomes of the attack.
 - Goal: discover key
- Adaptive-chosen-plaintext attack
 - Attacker choose: plaintext samples dynamically, and alter his or her choice based on the results of the previous operations.
 - Goal: discover key

Reference:

- *Cryptography Engineering*, N. Ferguson, B. Schneier, T. Kohno, Wiley Publishing, 2010.
- http://en.wikipedia.org/wiki/Category:Cryptographic_attacks

Types of Cryptographic Attacks... (1/5)

- Brute-force attack
 - Exhaustive search of possible combination (key) until the correct one is identified.
 - Can be applied to any type of cipher because the advance technologies in computing performance has made brute-force attacks practical against keys of a fixed length.

Bits	Number of keys	Brute Force Attack Time
56	7.2×10^{16}	20 hours
80	1.2×10^{24}	54,800 years
128	3.4×10^{38}	1.5×10^{19} years
256	1.15×10^{77}	5.2×10^{57} years

Types of Cryptographic Attacks... (2/5)

- Symmetric block cipher attacks
 - Differential cryptanalysis – A chosen-plaintext attack that relies on the analysis of the evolution of the differences between the two related plaintext samples as they are encrypted using the same key.
 - Linear cryptanalysis – A known-plaintext attack using linear approximations to describe the behavior of the block cipher.
 - Weak keys – Secret keys with a certain value for which the block cipher in question will exhibit certain regularities in encryption, or in other cases, a poor level of encryption.
 - Algebraic attacks – A class of techniques that rely on the block ciphers exhibiting a high degree of mathematical structure. (i.e., “pattern”)

Types of Cryptographic Attacks... (4/5)

- Hash function attack
 - Brute-force attack. Attacker chooses random inputs to the hash function until a targeted output is produced.
 - Differential attack. Attacker uses the difference in term of integer modular subtraction as inputs to MD5 until a targeted output is produced.
- Message authentication code (MAC) attack
 - Unlike digital signature, MAC value is generated and verified using same secret key (i.e. symmetric). Attacker performs chosen-plaintext attack on MAC to find the secret key.

Reference: *How to Break MD5 and Other Hash Functions*, Xiaoyun Wang and Hongbo Yu, Shandong University, 2005

Types of Cryptographic Attacks... (5/5)

- Birthday attack

- A class of brute-force attack used against hashing functions based on birthday paradox: probability that two or more people in a group of 23 share the same birthday is greater than 50%.
- Attacker is to find two messages with the same digest value instead of matching a specific value.

- Man-in-the-middle attack

- Relevant for cryptographic communications and key exchange protocols.
- Attacker is between two internetworking entities on a communications line. (i.e. a proxy.)

