Understanding Cryptography and Auditing Public Key Infrastructures

Rami Elkinawy, Senior Audit Manager, eBay

Professional Strategies – S31

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

THE HISTORY OF CRYPTOGRAPHY

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

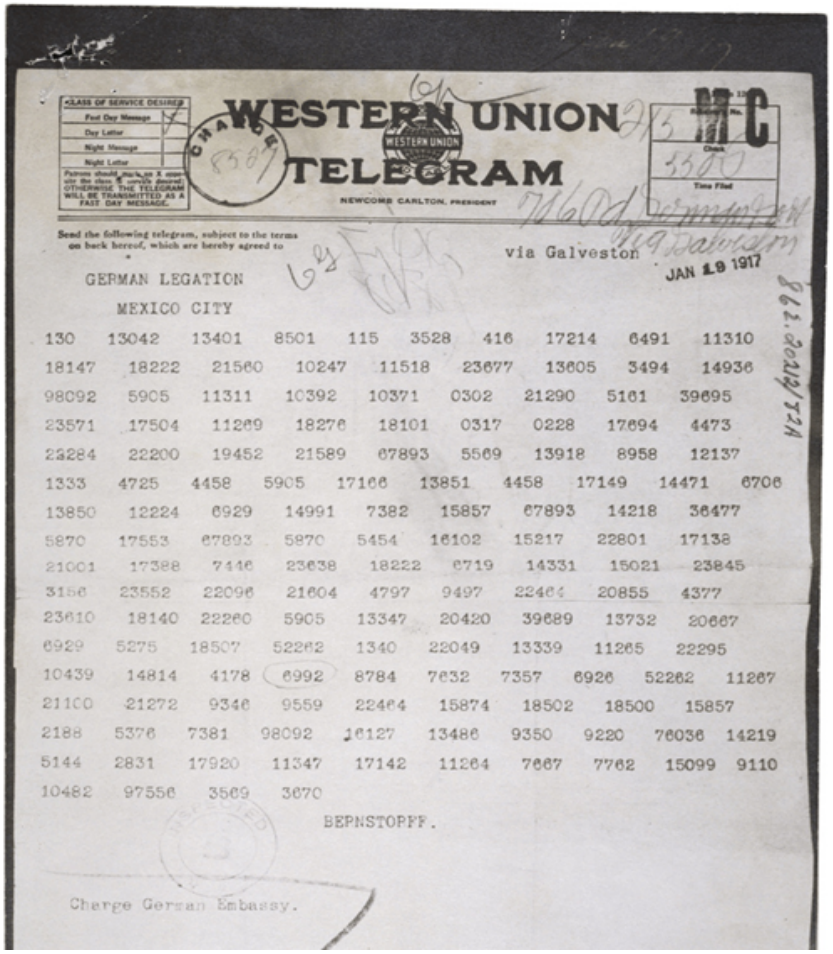
The History of Cryptography

- Before the modern era, cryptography was concerned solely with message confidentiality
- Encryption was used to (attempt to) ensure secrecy in communications, such as those of spies, military leaders, and diplomats
- In recent decades, the field has expanded beyond confidentiality, including message integrity checking, sender/receiver identity authentication, digital signatures etc.

The History of Cryptography

- The discovery and application of reading encrypted communications has, on occasion, altered the course of history
- Thus the Zimmermann Telegram triggered the United States' entry into World War I
- Until the 1970s, secure cryptography was largely the preserve of governments
- Two events have since brought it into the public domain: the creation of a public encryption standard (DES), and the invention of public-key cryptography

The History of Cryptography



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

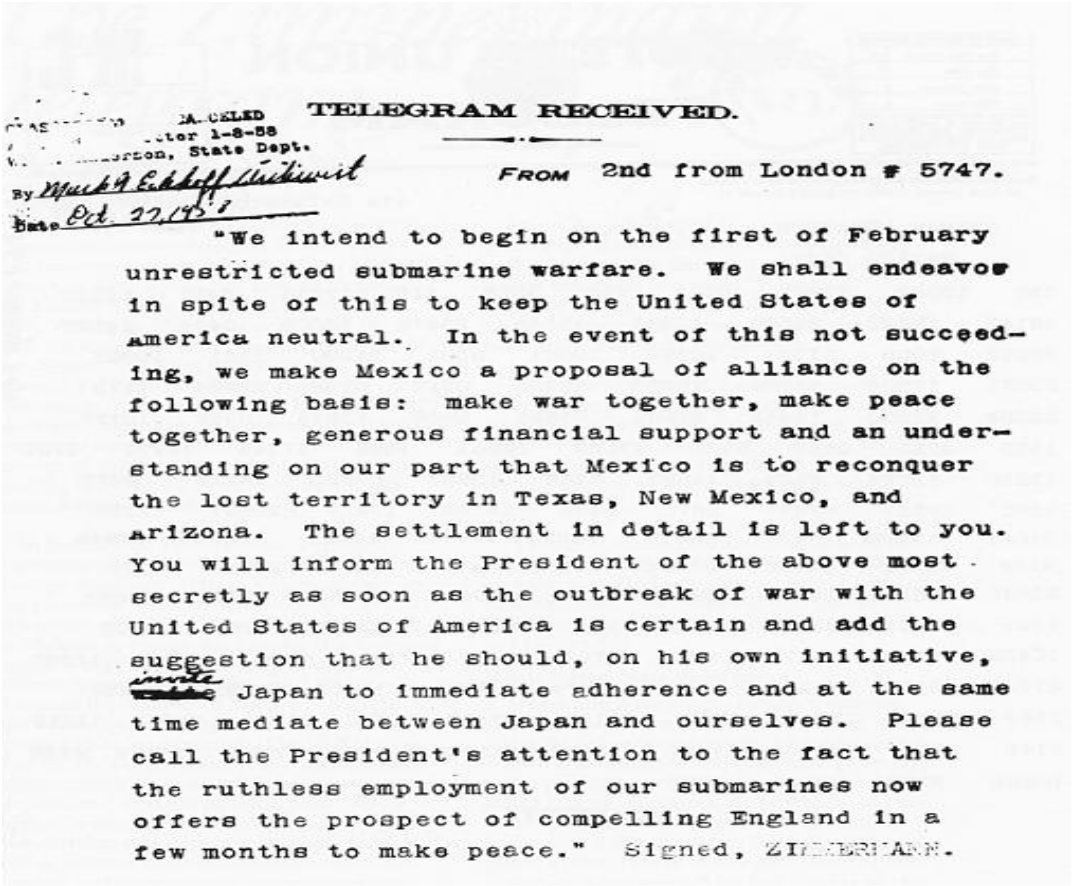
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

The History of Cryptography



TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

KEY TERMS AND PRINCIPLES OF CRYPTOGRAPHY

Key Terms and Principles of Cryptography

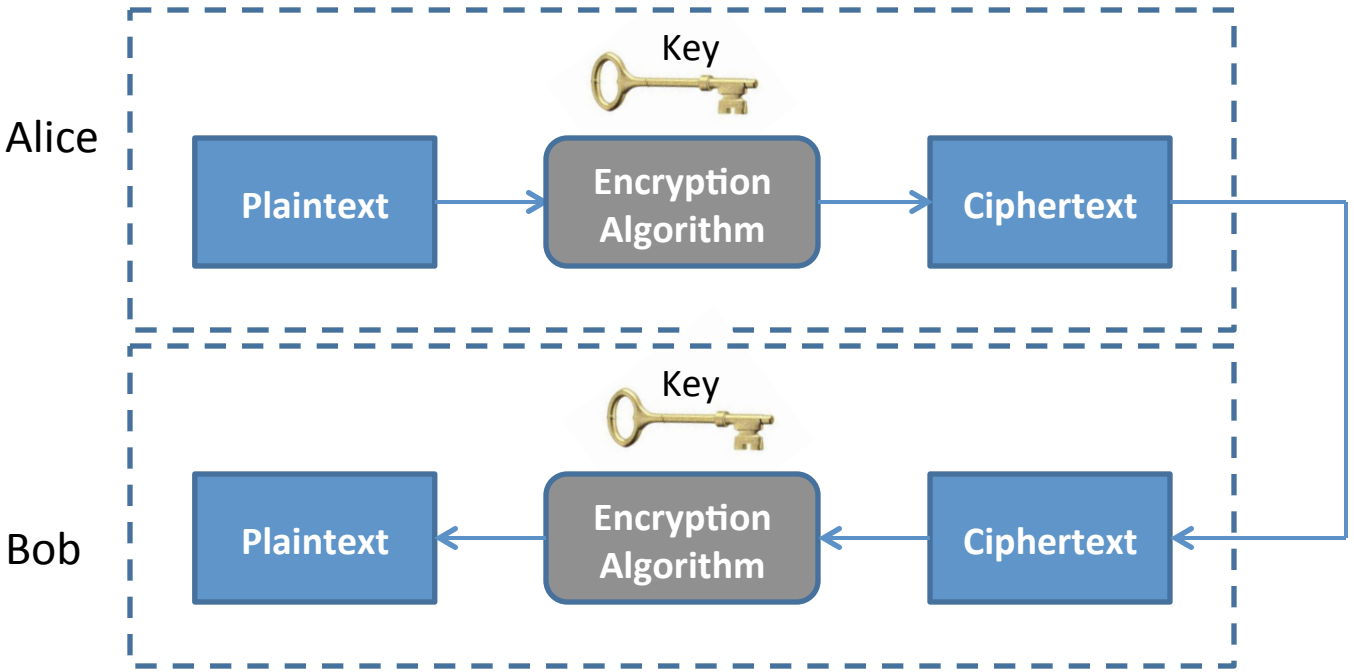
There are two general types of encryption methods that use keys: symmetric algorithms and public-key algorithms.

- When a symmetric algorithm is used, both the encryption key and decryption key are the same.
- A public-key algorithm uses different keys to encrypt and decrypt.
- The public-key can only be used to encrypt the message, not decrypt. The decryption key is called a private-key.

Key Terms and Principles of Cryptography

Symmetric Cryptography:

- Both the sender and receiver use the same key value *(shared secret key systems)*



Key Terms and Principles of Cryptography

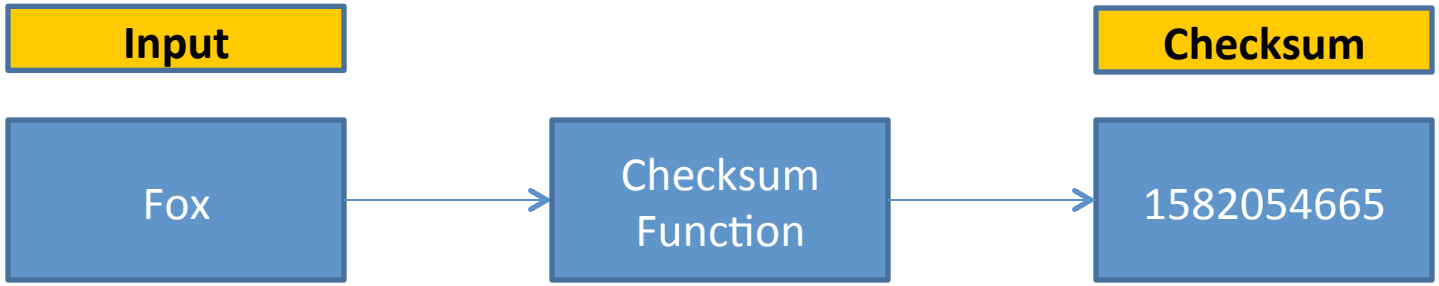
Symmetric Integrity Functions:

- A value is carried with the message and used to ensure that the message sent by Alice is the message received by Bob is called:
  - *Integrity Check Value (ICV)* or
  - *Message Authentication Code (MAC)*

Key Terms and Principles of Cryptography

Symmetric Integrity Functions:

- *Alice can transmit the last block of, or a portion of it, along with her message to Bob. Bob performs the same encryption on the received message. If the same check value and locally computed one match, then the message was not altered.*



Key Terms and Principles of Cryptography

Common Mode of Operation (Cipher Block Channeling):

- In order to encrypt arbitrary messages with a block cipher, the message is broken into a sequence of blocks, and the last block is padded to create a complete block if necessary.
- A random block, called the initialization vector, is generated
- The Initialization (IV) serves as the previous cipher text block for the first plaintext block

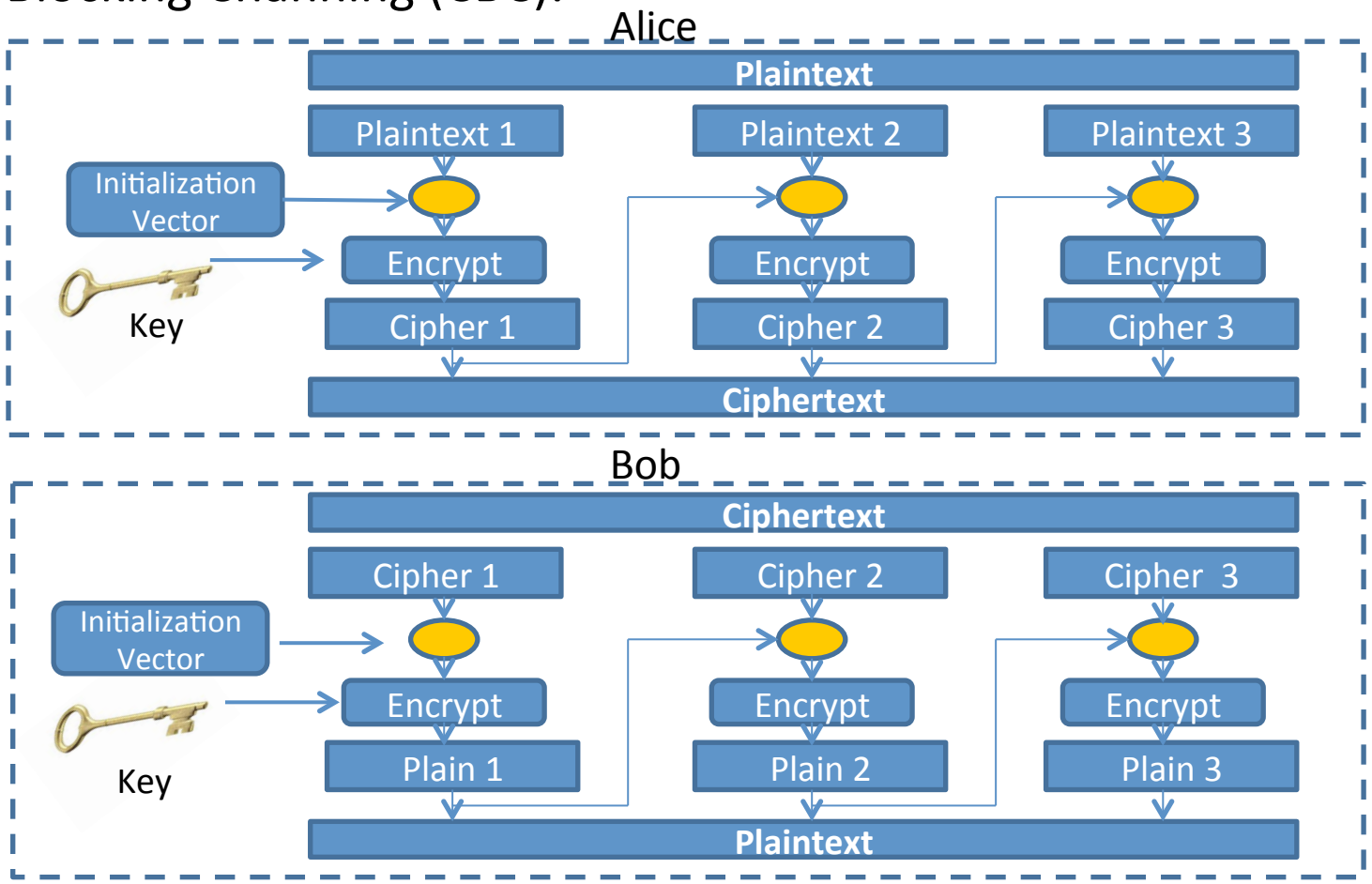
Key Terms and Principles of Cryptography

- XOR gains the name exclusive or. This is sometimes thought of as "one or the other but not both".
- The Truth Table of A XOR B shows that **it outputs true (1) whenever the inputs differ**:

XOR Truth Table		
Input		Output
0	0	0
0	1	1
1	0	1
1	1	0

Key Terms and Principles of Cryptography

Cipher Blocking Channing (CBC):



Key Terms and Principles of Cryptography

High Level Example of CBC:

1. CBC Coverts data and key to binary (example: 5 bits)

Plain Text: The Buck Stops Here

Key: Yeah

Plain Text: 10011 00111 00100 00001 10100 00010 01010 10010 10011 01110 01111 10010 00111 00100 10001 00100
Key: 11000 00100 00000 00111

2. Plaintext is broken into larger bits (12) and white space is removed from the key

Plaintext: 100110011100 100000011010 000010010101 001010011011 100111110010 001110010010 00100100

Key: 110000010000000000111

Last block is not a full 12 bits. To resolve this we will use padding

Key Terms and Principles of Cryptography

High Level Example of CBC:

3. We will alternate 1's and 0's until a complete block is made. Then, we will add an additional block that tells us how many bits were added.

Since four bits need to be added, the final block will be '**000000000100**',

This additional block is used to assist in deciphering the message. Without it, there is no way to determine how many extra bits were added.

4. Each block is encrypted by reversing the block and XOR each bit with the corresponding bit of the key

Plaintext: 100110011100
100000011010 000010010101
001010011011 100111110010
001110010010 001001001010
000000000100

Here is how the first block is encrypted:

Plaintext:	100110011100
Reversed:	001110011001
First 12 bits of key:	110000010000
Ciphertext:	111110001001

(Exclusive or [XOR])

Key Terms and Principles of Cryptography

High Level Example of CBC:

5. Now, the standard method of cipher block chaining uses the ciphertext of one block to assist in encrypting the next block.

6. This is done by XORing the ciphertext of the previous block with the plaintext of the next block, before the normal encryption technique is executed on the plaintext.

Here is how we would XOR the plaintext of block 2 with the ciphertext of block 1:
Ciphertext (Block 1): 111110001001
Plaintext (Block 2): 100000011010
Exclusive or (XOR): 011110010011

Key Terms and Principles of Cryptography

High Level Example of CBC:

7. The result of the exclusive or is now treated as the plaintext, and encrypted normally with the technique we came up with earlier:

Reverse the plaintext (the result of the XOR) and XOR the result with the first 12 bits of the key:

Result of XOR (New Plaintext): 011110010011
Reversed: 110010011110
First 12 bits of key: 110000010000
Ciphertext (by XOR): 000010001110

8. Since each of these blocks (except the first one) was encrypted using the ciphertext of the previous block and the key, it becomes very difficult to decrypt without knowing the key.

Key Terms and Principles of Cryptography

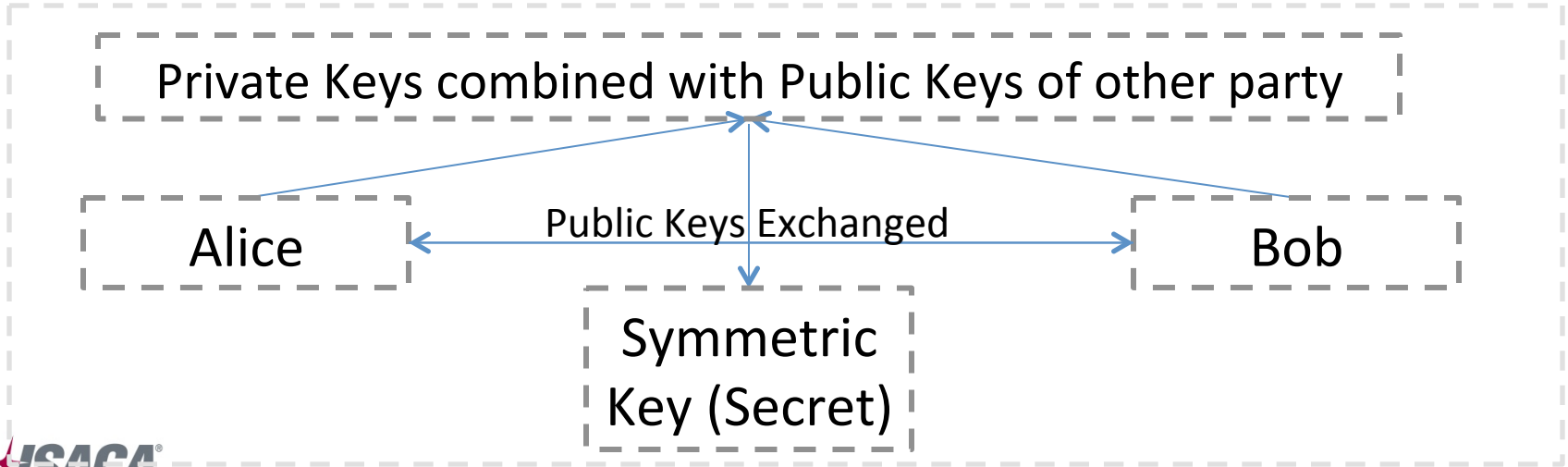
Asymmetric Key Management:

- When sharing multiple keys you need to ensure that the key remains associated with the correct party
- You can avoid many of the complexities associated with the distribution and storage of symmetric keys using asymmetric cryptography (public key cryptography)
- Public keys are not generally used to encrypt user data.

Key Terms and Principles of Cryptography

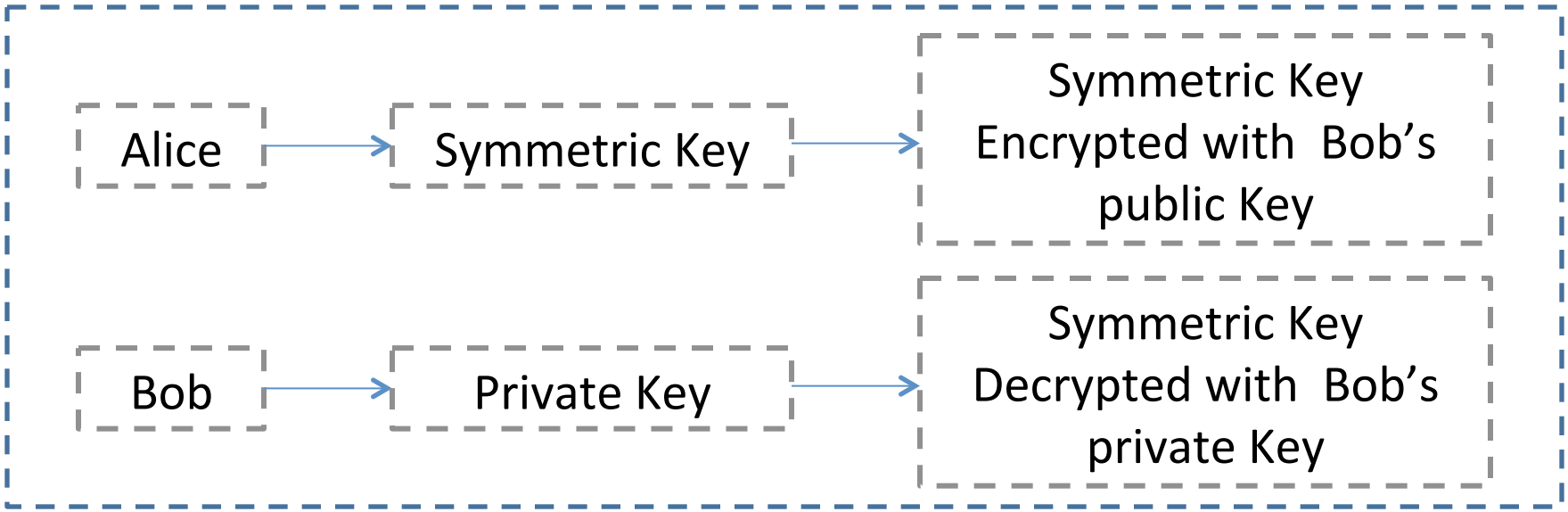
Two key management public key algorithms:

- **Key Agreement Algorithms**: Alice and Bob exchange public keys, and then combine their own private key with the public key of the other party to compute a symmetric key that is known only to the two parties



Key Terms and Principles of Cryptography

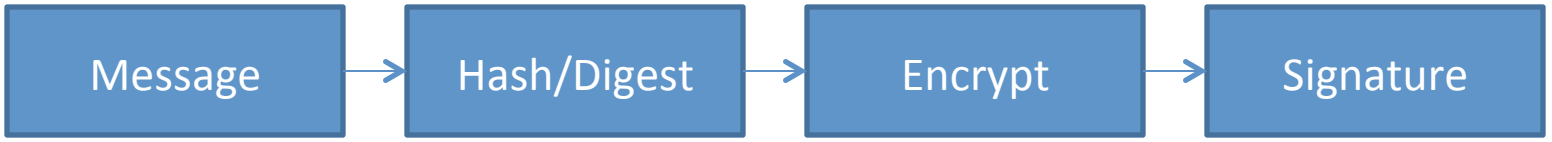
- **Key Transport Algorithms:** Alice creates a symmetric key and encrypts it with Bob's public key, and then Bob uses his own private key to decrypt the value and recover the symmetric key.



Key Terms and Principles of Cryptography

Digital Signatures:

- The private key is used to generate signatures, and the public key validates them
- In real-world applications, the message is hashed, and then signed,
- If Alice uses her private key to sign a message, Bob can validate it with her public key



Key Terms and Principles of Cryptography

Simple Certificates:

- The problem with public key cryptography is determining who holds the corresponding private key
- To answer this, PKI relies on the concept of a public key certificate
- Each certificate contains a public key and identifies the user with the corresponding private key

Key Terms and Principles of Cryptography

Simple Certificates:

- A certificate is like a credit card, it provides you with the name of the user and his account number
- Characteristics of an ideal certificate:
  - Digital Object
  - Contains the name of the user that holds the private key
  - Contains issue date
  - Created by a trusted party
  - Tamper proof

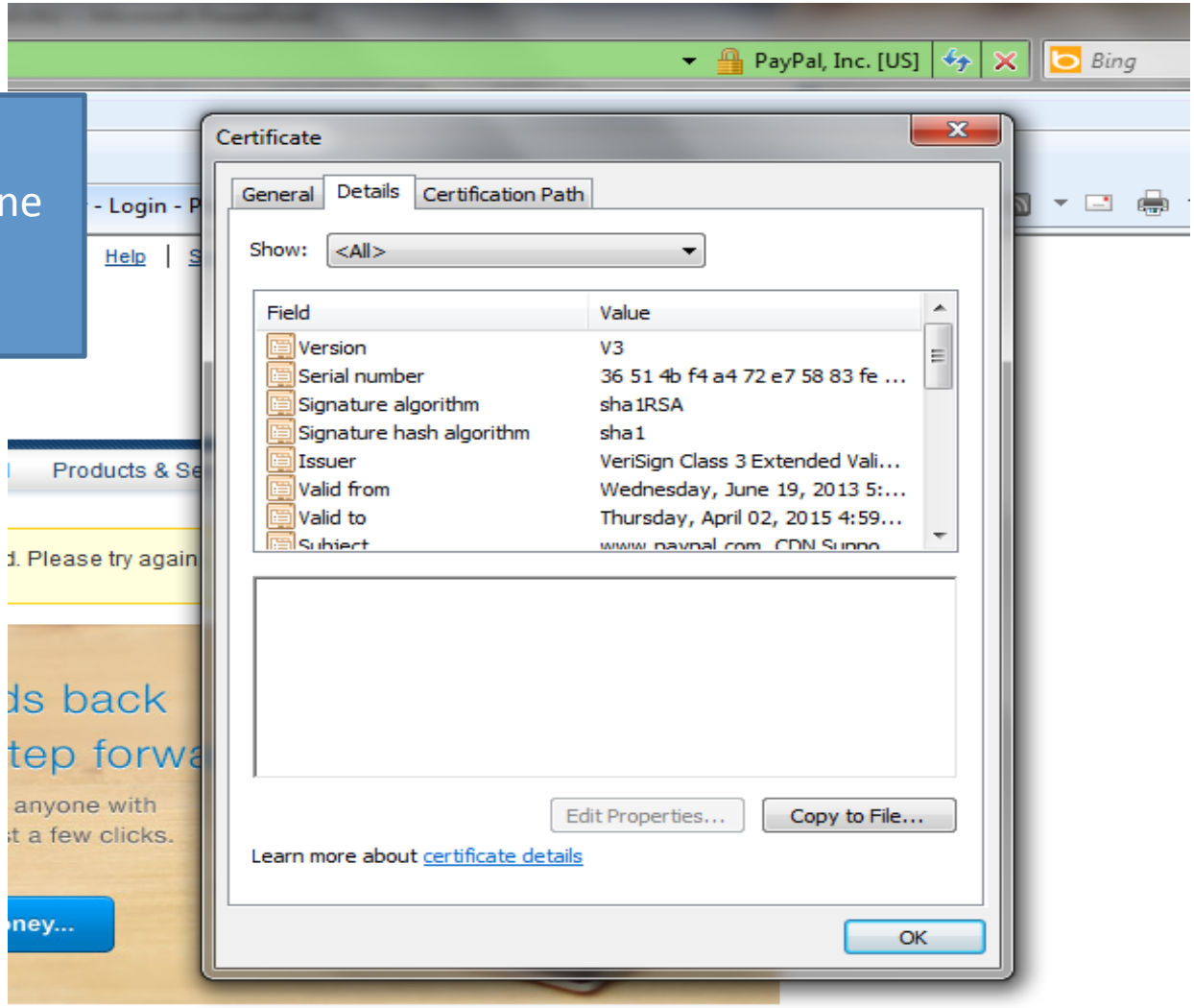
Key Terms and Principles of Cryptography

Public Key Certificates:

- Contains fields for:
  - Name
  - Company
  - Contact info
  - Activation and expiration date
  - Name of trusted party who created the certificate (issuer)
  - Unique serial number in every certificate
  - Public Key
  - Contents of Certificate are protected by the issuer's digital signature

Key Terms and Principles of Cryptography

Example of an online certificate



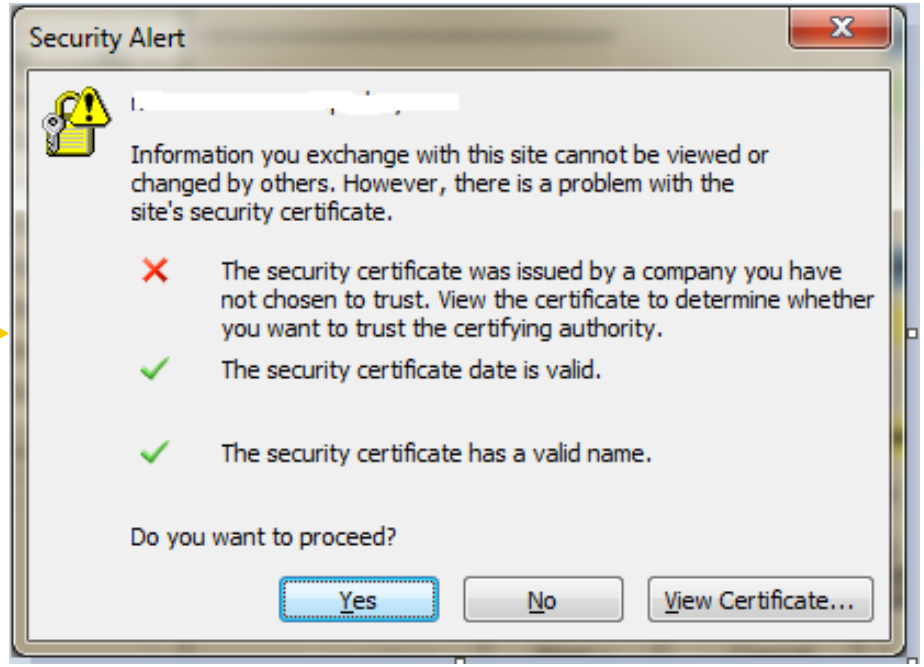
CERTIFICATE TYPES AND SELF-SIGNED CERTIFICATES

Certificate Types and Self-Signed Certificates

- Self issued certificates are a special class of CA certificates
- The issuer and the subject are the same. A self-signed certificate is commonly used to distribute a public key and establish a trust point
- The signature on the self-signed certificate proves that the issuer has both the public and private key. It does not prove anything else regarding the content of the certificate

Certificate Types and Self-Signed Certificates

Error message when accessing a site that utilizes a self-signed Certificate



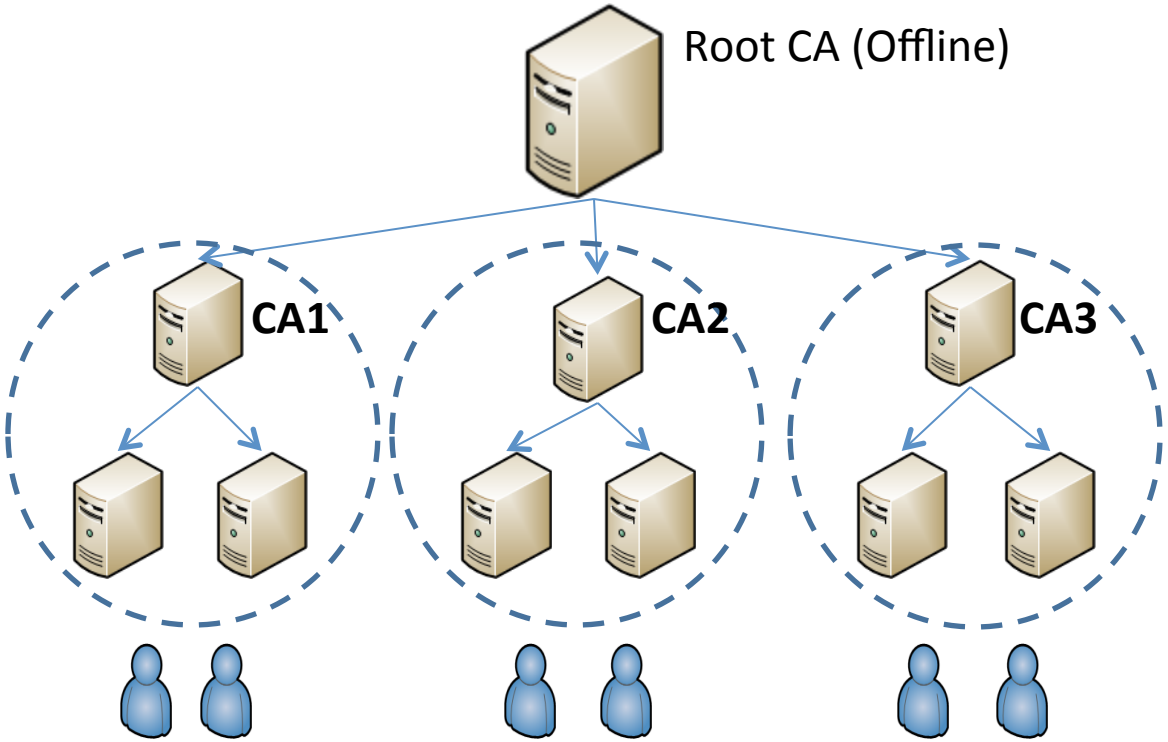
Certificate Types and Self-Signed Certificates

Examples of different certificate types:

- SSL certificates for web application servers (packet encryption)
- Encrypting File System (EFS) certificates for users laptops and desktops
- 802.1x certificates for wireless connections
- Mobile authentication certificates

PUBLIC KEY INFRASTRUCTURE (PKI)

Public Key Infrastructure



- Hierarchical PKIs handle the compromise of a single CA within the infrastructure easily, as long as its not the root CA. If a CA is compromised, its superior simply revokes its certificate

Public Key Infrastructure

Public Key Certificates:

- While we cannot make the certificate tamper proof they are tamper evident
- The issuers signature of the certificate makes it tamper evident If the signature does not verify
- Issuer links public key with user's identity in a trustworthy fashion

Public Key Infrastructure

Public Key Certificates:

- The basic tool to update status about public Key Certificates is the CRL
- The CRL contains a list of serial numbers from unexpired certificates that should not be trusted
- The CRL is tamper evident because the issuer signs it
- CRL includes public signatures
- By adopting the concept of a trusted party issuing certificates, Alice can establish trust with users she has never met

Public Key Infrastructure

Authentication Mechanisms:

- PKI-based authentication can provide unilateral or mutual authentication
- Several protocols provide authentication based on certificates:
  - SSL (Secure Socket Layer),
  - TLS (Transport Layer Security),
  - IKE (Internet Key Exchange),
  - PGP and Open PGP,

Public Key Infrastructure

The Certificate Authority:

- The CA is the collection of computer hardware, software and the people who operate it
- Performs the following:
  - Issues certificates (creates and signs them)
  - Maintains Certificate Status Information and issues CRLs
  - Maintains archives of status information about the expired or revoked certificates that it issued
  - To satisfy certain functions, the CA may delegate certain functions to other components of the infrastructure

Public Key Infrastructure

Issuing Certificates:

- A CA may issue certificates to users, other CAs or both
- When it issues a certificate, it assumes that the subject (entity) has the private key that corresponds to its public key
- When the subject of the certificate is another CA, the issuer is asserting that the certificates issued by the other CA are trustworthy

Public Key Infrastructure

Issuing Certificates:

- The primary responsibility of the CA is to protect its private key from disclosure
- To meet this requirement, the CA relies on cryptographic modules, which generate keys, protect private keys and implement cryptographic algorithms
- Software cryptographic modules are programs that run on the computer system
- Cryptographic modules generate keys, protect private keys, and implement cryptographic algorithms

Public Key Infrastructure

Issuing Certificates:

- Cryptographic modules may be implemented in software or hardware (smart cards on external processors). Software cryptographic modules are programs that run on the computer system.
- NIST and the Canadian Communications Security Establishment accredit third party's against the **FIPS140-2 standard**

Public Key Infrastructure

Issuing Certificates:

- A CA's private key is at risk when stored in host memory or an unvalidated cryptographic module
- The second responsibility of the certificate is to verify the information in a certificate before it is issued
- The CA can use the digital signature mechanism to ensure that a user actually has the private key corresponding to the public in the certificate. This is called *proof of procession*

Public Key Infrastructure

Issuing Certificates:

- A CA specifies the type of information that it will include in the certificate
- The third responsibility is to ensure that all certificates and CRLs it issues conform to its profile
- To do this, it must:
  - Protect the integrity of the profile
  - And it must verify each and every certificate and CRL it generates conforms to the profile
  - To ensure that they conform, the CA must examine them and compare them to the profile before signing them
  - To protect the integrity, the CA restricts access to the CA components

Public Key Infrastructure

Issuing Certificates:

- The fourth responsibility, accurately maintain the list of certificates that should no longer be trusted
- Fifth, distributes its certificates and CRLs
- Sixth, maintenance of a sufficient archival information to establish the validity of certificates after they expired

Note: An attacker could deny service to Alice and Bob, by deleting or modifying information, but cannot make them trust the altered information without obtaining the CA's private key

Public Key Infrastructure

The Registration Authority:

- This is the entity that verifies certificate content (especially identifying users). Also assumes responsibility of certificate revocation decisions
- Each CA will have an accredited list of RAs (Operated by one person)
- Each RA is known to the CA by name and public key. By verifying the RA ‘s signature on a message, the CA assure that an accredited RA provided the information

Public Key Infrastructure

The entity that distributes certificates and CRLs is called a repository:

- A repository distributes certificates and CRLs for one or more CAs and makes them available to parties that need them to implement security services
- System know by its address and access protocol. Provides certs and CRLs upon request
- Repositories are not trusted entities, user accepts the cert and CRL because the CA signed them

Public Key Infrastructure

The entity that provides long term secure storage for the archival information is called an archive:

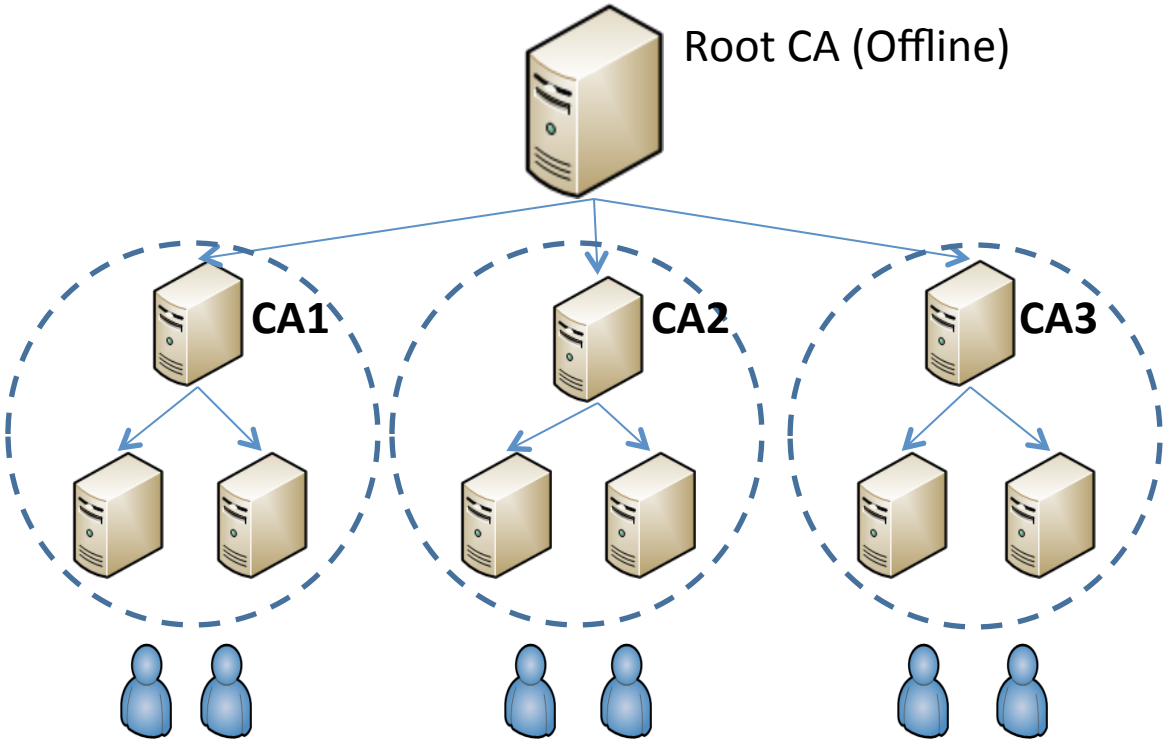
- Responsible for long term storage of archival information on behalf of the CA
- Archive asserts that information was good at the time it was received, and has not been modified while in archive
- Info provided by the CA to the repository must be sufficient to determine if a certificate was actually issued by the CA

Public Key Infrastructure

Hierarchical PKI:

- In this architecture, multiple CAs are related through a superior-subordinate relationship
- All users trust the same central *root CA*
- Each CA trust relationship is represented by a single certificate
- The issuer is the superior CA and the subject is the subordinate
- Widely accepted standard format for public key certificates is the X.509 public key certificate.

Public Key Infrastructure



- Hierarchical PKIs handle the compromise of a single CA within the infrastructure easily, as long as its not the root CA. If a CA is compromised, its superior simply revokes its certificate

Public Key Infrastructure

Key Usage:

- The key usage extension identifies the security services that a public key may be used to provide:
  - KeyCertSign
  - cRLSign
  - Non-Repudiation
  - digitalSignature
  - KeyEncipherment
  - DataEncipherment
  - keyAgreement
  - encipherOnly
  - decipherOnly

Public Key Infrastructure

PKI Enabled Applications:

- S/MIME: Provides security for internet electronic mail. It can be used to digitally sign and encrypt mail messages
- TLS: Transport Layer Security provides authentication and encryption for a communications stream (Client to server)
- IPSEC: Internet Protocol Security, provides authentication and encryption for individual datagrams

Public Key Infrastructure

PKI Enabled Applications:

- SSL and TLS provide authentication, integrity and confidentiality in communication between two communicating applications
- The protocols are composed of two layers: The handshake protocol and the record protocol
- The handshake authenticates the server and the client, negotiates an encryption algorithm, and establishes cryptographic keys before any application protocol data is transferred

Public Key Infrastructure

PKI Enabled Applications:

- SSL/TLS provide stream oriented security with three properties:
  - Authentication: The identity of the peer is confirmed. The handshake protocol uses certificates and digital signature verification to confirm the identity of the remote application
  - Integrity: The application protocol data is protected from undetected modification. The record protocol employs an integrity check value, computed HMAC, to confirm that the data stream is unaltered
  - Confidentiality: The connection is private. After the handshake protocol establishes a symmetric encryption key, the record protocol encrypts the remainder of the session.

Public Key Infrastructure

The Handshake Protocol:

- The Handshake protocol is responsible for negotiating a session for the Record Protocol, which consists of the following items:
  - Session identifier: An arbitrary byte sequence chosen by the server to identify a session
  - Peer certificate. X.509 certificate of the peer. The element may be absent if authentication is not performed
  - Compression method. The algorithm used to compress data prior to encryption
  - Cipher spec. Specifies the bulk data encryption algorithm such as 3DES and HMAC one way hash algorithm (SHA1). It also defines cryptographic attributes (such as hash size).
  - MasterSecret, a large secret value shared between the client and server.
  - IsResumable, a flag indicating whether the session can be used to initiate new connections.

METHODS OF AUDITING A PUBLIC KEY INFRASTRUCTURE (PKI)

Methods of Auditing A PUBLIC KEY INFRASTRUCTURE (PKI)

CA key generation controls:

- Inspect the CPS to obtain an understanding of the CA key generation controls
- Understand and evaluate the root key ceremony
- For a selection of key ceremonies, inspect detailed key generation scripts to determine whether:
  - the script is followed and any exceptions documented
  - Ceremony complied with stated CP/CPS requirements
- Observe a key ceremony and determine whether scripts were followed, any exceptions were documented, and keys were handled in accordance to the CPS

Methods of Auditing A PUBLIC KEY INFRASTRUCTURE (PKI)

Certificate Issuance, Certificate Profiles and Certificate Revocation:

- List of all certificates issued, renewed, and revoked by certificate type and issuer CA
- Understand the Certificate distribution process and certificate revocation
- Test the sample of selected certificates to determine the following:
  - Issued Certificates are appropriately approved
  - Certificates issued to external domains are appropriately vetted
  - Certificate profiles are compliant with the minimal established requirements in the CPS
- Revoked certificates were appropriately revoked within a timely manner as defined within the CPS

Methods of Auditing A PUBLIC KEY INFRASTRUCTURE (PKI)

Physical Security:

- Perform an onsite observation of PKI facilities to determine whether required physical security controls such as the following are in place:
  - Number of security zones
  - Two factor authentications using card readers
  - Two person access requirements
  - DVR device and video cameras
- Identify the relevant personnel who are responsible for administering and maintaining the physical access system to obtain an understanding of how access is restricted to that system
- Inspect management approval documentation to determine whether management approval exists for granting physical access to PKI facilities
- In addition, please obtain and inspect a list of authorized approvers
- Obtain a list of individuals that have access to the PKI facilities within the data center

Methods of Auditing A PUBLIC KEY INFRASTRUCTURE (PKI)

Physical Security:

- Simulate the physical security response process by generating a physical access alarm
- Obtain the events logged by the physical security system; this should include activities like successful attempts, unsuccessful attempts and alarms (two year period)
- Evaluate whether incidents were appropriately documented and resolved
- Review the Physical Security Controls:
  - System generated physical access lists to CA facilities
  - Documentation of most recent review of physical access lists and logs for all restricted access locations within Tempe,
  - Email request the revocation of physical access to the PKI secure room
  - Quarterly Security Audit report
  - Documentation of authorized signers for badges and property removal for PKI
- PKI Site Access Policy

Understanding Cryptography and Auditing Public Key Infrastructures

Sources:

- Planning for PKI (Best Practice Guide for Deploying PKI) – Russ Housley and Tim Polk
- Thinkquest.org

Understanding Cryptography and Auditing Public Key Infrastructures

Thank You!

Questions?