CompTIA Security+

Domain 6: Cryptography

Objective 6.1

- Given a scenario, utilize general cryptography concepts.

Cryptographic Concepts

Symmetric vs. Asymmetric vs. Hashing

- Symmetric uses a Private key to encrypt / decrypt data
- Asymmetric uses a key pair to encrypt / decrypt data
- Hashing uses algorithm to provide a message digest

Cryptographic Concepts

- Encryption ---> Confidentiality
- Digital Signatures ---> Non-repudiation
- Hashing ---> Integrity

Cryptography

The science of hiding information

Greek

- kryptos = hidden
- graphein = to write

Cryptographic Terms

Encryption:
A cryptographic technique that converts data from plaintext (cleartext) into code (ciphertext)

Ciphers:
A specific set of actions used to encrypt data
Enciphering vs. deciphering

Cryptanalysis:
The science of breaking codes and ciphers

Cryptographic Terms

One-way Function:

Mathematical operation that easily produces an output for each possible combination of inputs but makes it impossible to retrieve input values

Cryptographic Terms

- Confidentiality: Ensures that data remains private while at rest or in motion
- Integrity: Ensures that data isn't altered while in transit or while at rest
- Authentication: Verifies the claimed identity of a user. Authentication is a major component of a cryptosystem.

Cryptographic Terms

- Cryptographic Keys AKA Cryptovariables
- Different cryptosystems have different keys
- Symmetric cryptosystems use one key (called a private-key or secret-key cryptosystem.)
- Asymmetric cryptosystems uses two keys (called a key pair)

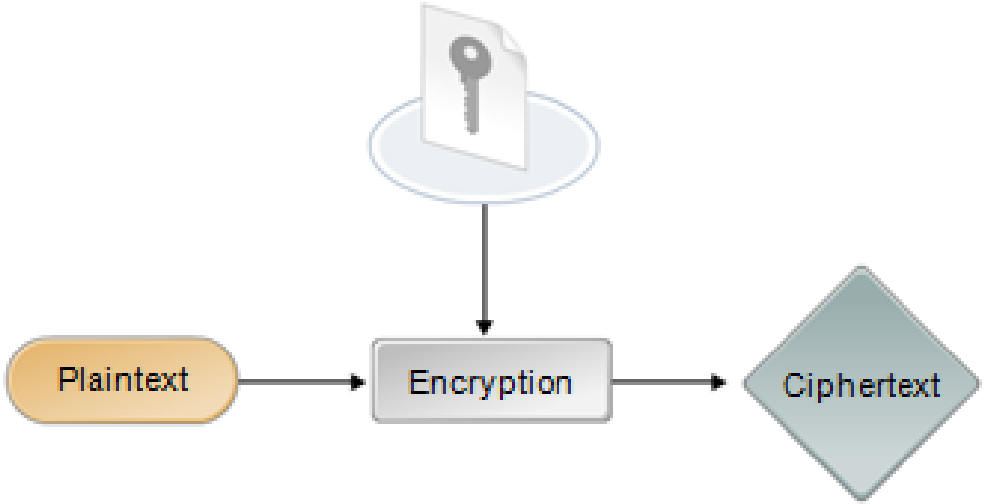
Cryptographic Terms

Keyspace:
Number of values that are valid for use as a key for a specific algorithm.

- Keyspace is defined by its *bit size*
  (# of 1's or 0's in the key)

Keys

A specific piece of information that is used in conjunction with an algorithm to perform encryption and decryption



Kerckhoff's Principle

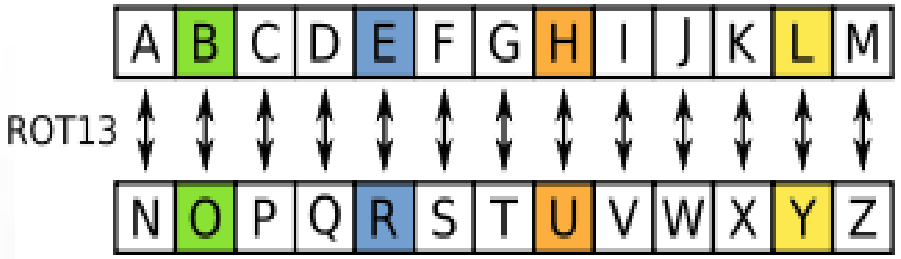
Kerckhoff's principle states that a cryptosystem should be secure even if everything about the system is known, except for the key

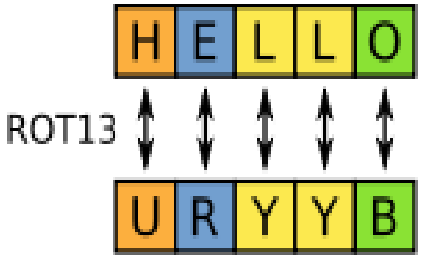
Cryptographic Types

- Substitution Cipher
  - ROT 13
- Transposition Cipher
  - Rail Fence
- Mathematical Cipher
  - Algorithm (symmetric and asymmetric)
- Quantum Ciphers
  - Lattice-based Cryptography, Multivariate Cryptography, Hash-based Cryptography, Code-based Cryptography, Supersingular Elliptic Curve Isogeny Cryptography, Symmetric Key Quantum Resistance

Substitution Cipher

- ROT13 (Caesar Cipher)
  - the Alphabet is shifted by 13 letters





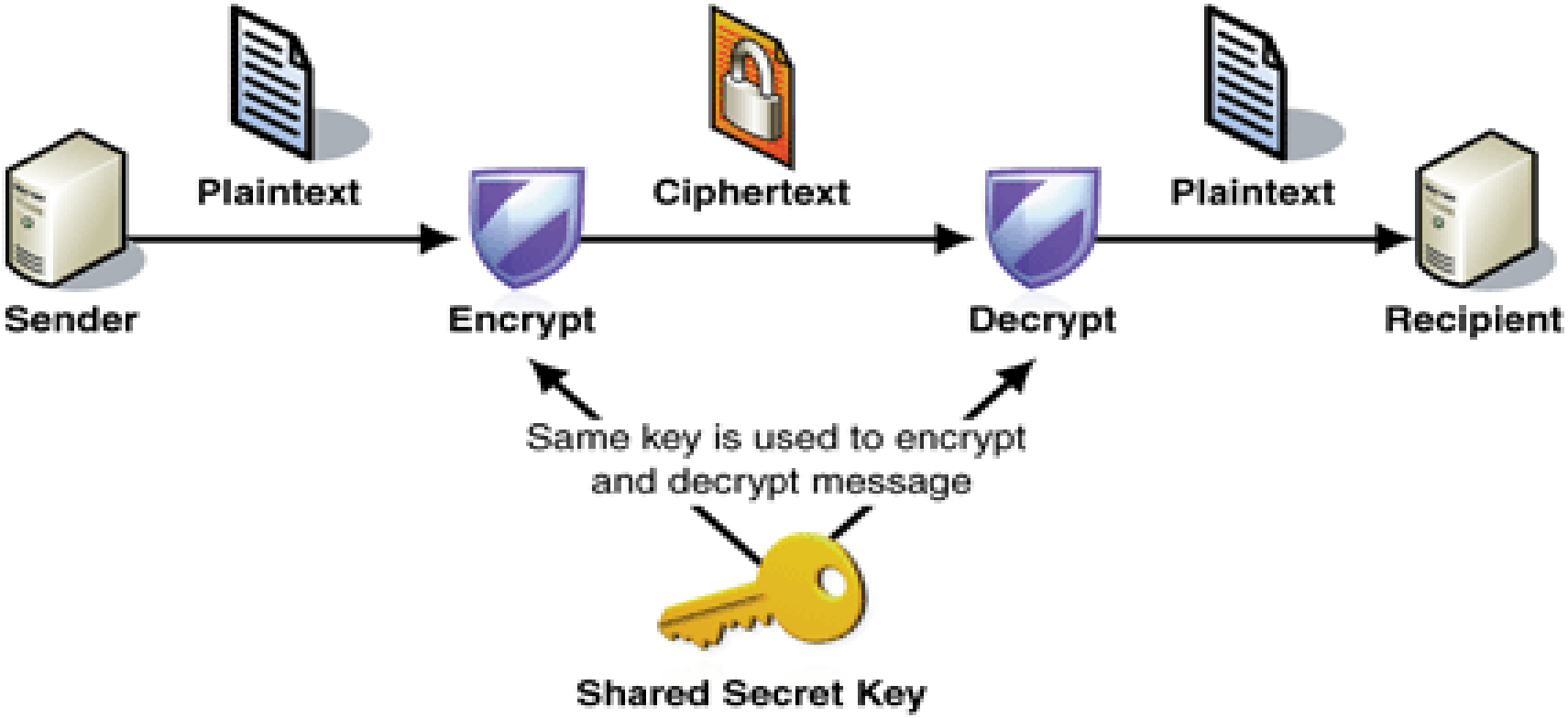
Transposition Cipher

- Rail Fence

Message: JAMESBONDNEEDSBACKUP
Code: JEONDAUASNESCPMBDEBK

J	E	O	N	D	A	U
A	S	N	E	S	C	P
M	B	D	E	B	K	

Symmetric Encryption



Symmetric Encryption

- Two-way encryption
- A single, shared key, secret-key, private-key encryption
- Encrypt and decrypt with the same Public key
- The key can be configured in software or coded in hardware
- The key must be securely transmitted between two parties prior to communications

Symmetric Encryption

- Secret key
  - If key is compromised, you will need new key
- Doesn't scale well
- Used to encrypt large sized bulk data
- Very fast to use
  - Often combined with asymmetric encryption

Symmetric Cryptographic Algorithms

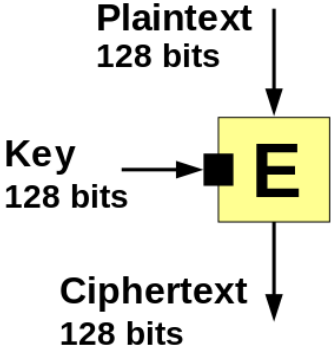
TABLE 6.1 Common symmetric cryptography solutions

Name	Block Size	Key Size (in Bits)
Advanced Encryption Standard (AES; uses the Rijndael block cipher algorithm)	128	128, 192, and 256
Triple Data Encryption Standard (3DES)	64	168
Data Encryption Standard (DES)	64	56
International Data Encryption Algorithm (IDEA)	64	128
Blowfish	64	32 to 448
Twofish	128	128, 192, or 256
Rivest Cipher 5 (RC5)	32, 64, 128	0–2040
Rivest Cipher 6 (RC6)	128	128, 192, or 256
Carlisle Adams/Stafford Tavares (CAST-128)	64	40 to 128 in increments of 8

Symmetric Encryption Types

Block Cipher

- Encrypt in fixed-length blocks of data
- 64-bit, 128-bit, 256-bit
- Pads the data to fill up a block



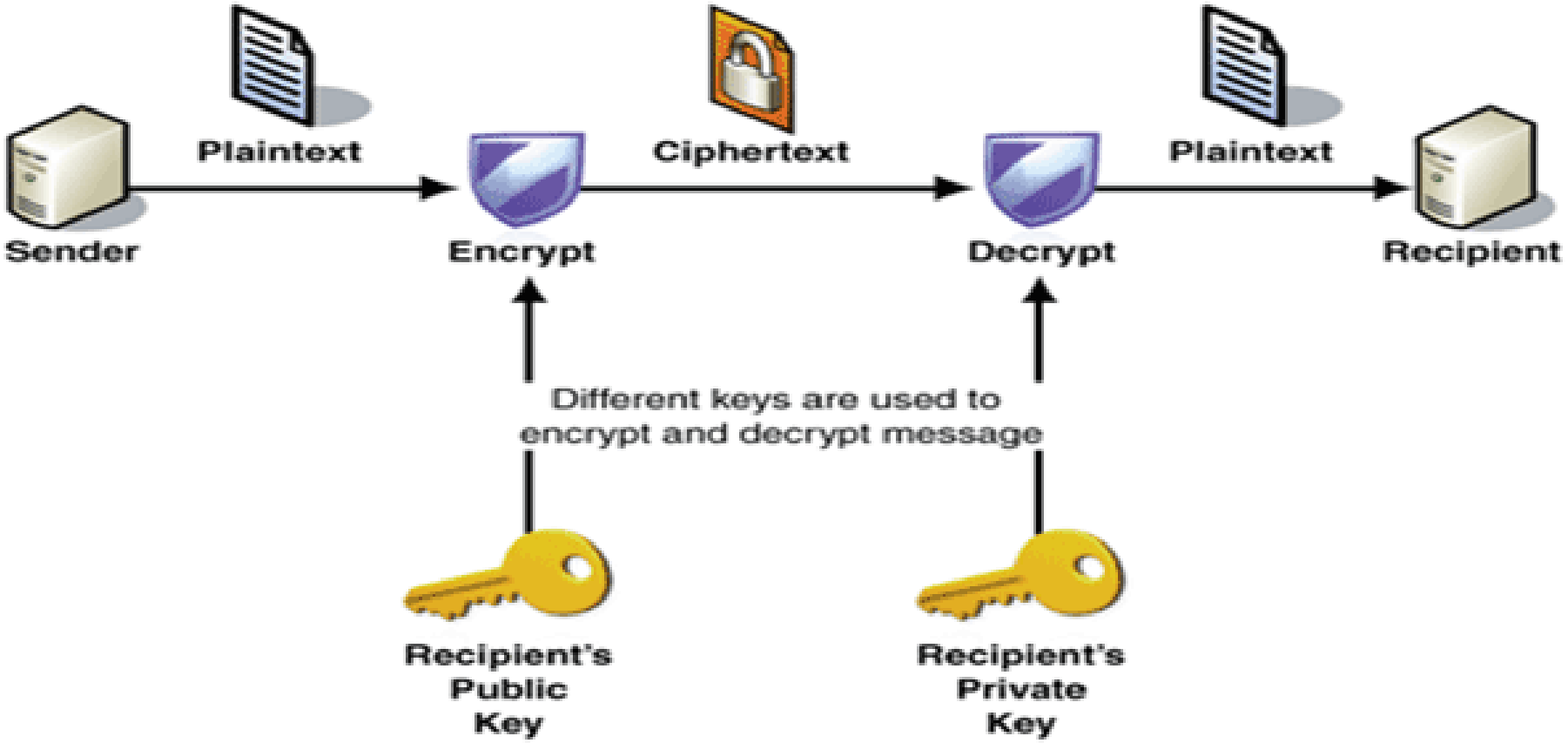
Stream Cipher

- Encrypt one bit or byte at a time
- High speed

Symmetric Cryptographic Algorithms

Symmetric	
Algorithm	**Cipher Type**
DES	Block
3DES	Block
AES (Rijndael)	Block
Blowfish	Block
IDEA	Block
RC2	Block
RC4	Stream
RC5	Block
RC6	Block
CAST	Block
MARS	Block
Serpent	Block
Twofish	Block
Kerberos	
SSL	Cipher*

Asymmetric


Plaintext
Ciphertext
Plaintext
Sender
Encrypt
Decrypt
Recipient
Different keys are used to
encrypt and decrypt message
Recipient's
Public
Key
Recipient's
Private
Key

Asymmetric Encryption

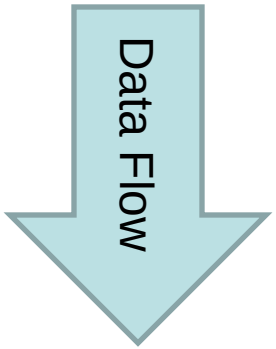
- Public key cryptography
- Key Generation
  - Application that generates a pair of public and private key. Key pair has a mathematical relationship which can not be spoofed.
- Private key
  - Must keep private (located on your CAC)
- Public key
  - Everyone you want to has access to your Public Key. (located on the CA)

Asymmetric Cryptographic Algorithms

Asymmetric - Non-repudiation
Rivest, Shamir & Aldeman Encryption Algorithm (**RSA**)
Diffie-Hellman Key Exchange
El Gamal Encryption Algorithm
Elliptic Curve Cryptography (**ECC**)
SSL – Handshake*
PKI

Student Alert

People encrypt data using your **Public key**



You decrypt that data with your **Private key**

Session Key

- Encrypted key that is used for a communication session
- Randomly selected (or generated) and then used only for one session
- Are often a symmetric key, however, Session Keys can also be asymmetric
- SSL / TLS uses Session Key
- Secure Session Key by using secure key-exchange mechanism

In-band vs. out-of-band key exchange

In-band key exchange takes place in the existing and established communication channel or pathway

Out-of-band key exchange takes place outside of the current communication channel or pathway, such as through a secondary channel, via a special secured exchange technique in the channel, or with a complete separate pathway technology

Transport Encryption

- Used to ensure the security of information while it is transmitted between two end points

- Protocols that support Transport Encryption

VPN – PPTP, L2TP, IPSec
SSL / TLS
HTTPS
SSH
S/MIME, PGP

Virtual Private Network

- VPN is a communications “tunnel” between two devices across an intermediary, usually untrusted network.
- VPN can connect two networks across the internet or allow distant clients to connect into a LAN across the Internet.
- Benefits:
  - Eliminate the need for expensive dial-up modem banks
  - They do away with long-distance toll charges
  - Any user in the world can connect to your local network
  - Provide security for both authentication and data transmission

VPN Protocols cont.

- There are several VPN protocols.
  - PPTP – Point-to-Point Tunneling Protocol
  - L2TP – Layer 2 Tunneling Protocol
    - Cisco Proprietary
  - IPsec – Internet Protocol Security

VPN cont.

- VPN's provide the following functions
- *Access Control* restricts users from resources
- *Authentication* proves the identity of users
- *Confidentiality* prevents unauthorized disclosure
- *Data Integrity* prevents unwanted changes to data

VPN Protocols

- Also known as Tunneling Protocols
- VPN's are possible due to a process called *encapsulation.*
  - As data is transmitted from one system to another across VPN link, the TCP/IP traffic is encapsulated (encased, or enclosed) in the VPN protocol.
- Firewalls, intrusion detection systems, antivirus scanners, or other packet-filtering and -monitoring security mechanisms can not observe encrypted traffic.

PPTP (*RFC* 2637)

- Originally developed by Microsoft
- After the user authenticates, typically with MSCHAPv2, a point-to-point protocol (PPP) session is created and tunneled using generic routing encapsulation (GRE).
- PPTP can use any of the authentication methods supported by PPP. Examples include CHAP and EAP

L2TP (RFC 2661)

- L2TP was developed by combining features of Microsoft's proprietary implementation of PPTP and Cisco's Layer 2 Forwarding (L2F) VPN protocols.

Internet Protocol Security (IPsec)

- IPsec provides security for the Internet Protocol (IP) via its open framework.
- Can provide both authentication and confidentiality.
- From an application perspective, IPsec is used for a secure point-to-point link across an unsecure network such as the Internet.
- EX: A company may use an IPsec connection for secure communication between two remote branches or offices

IPsec

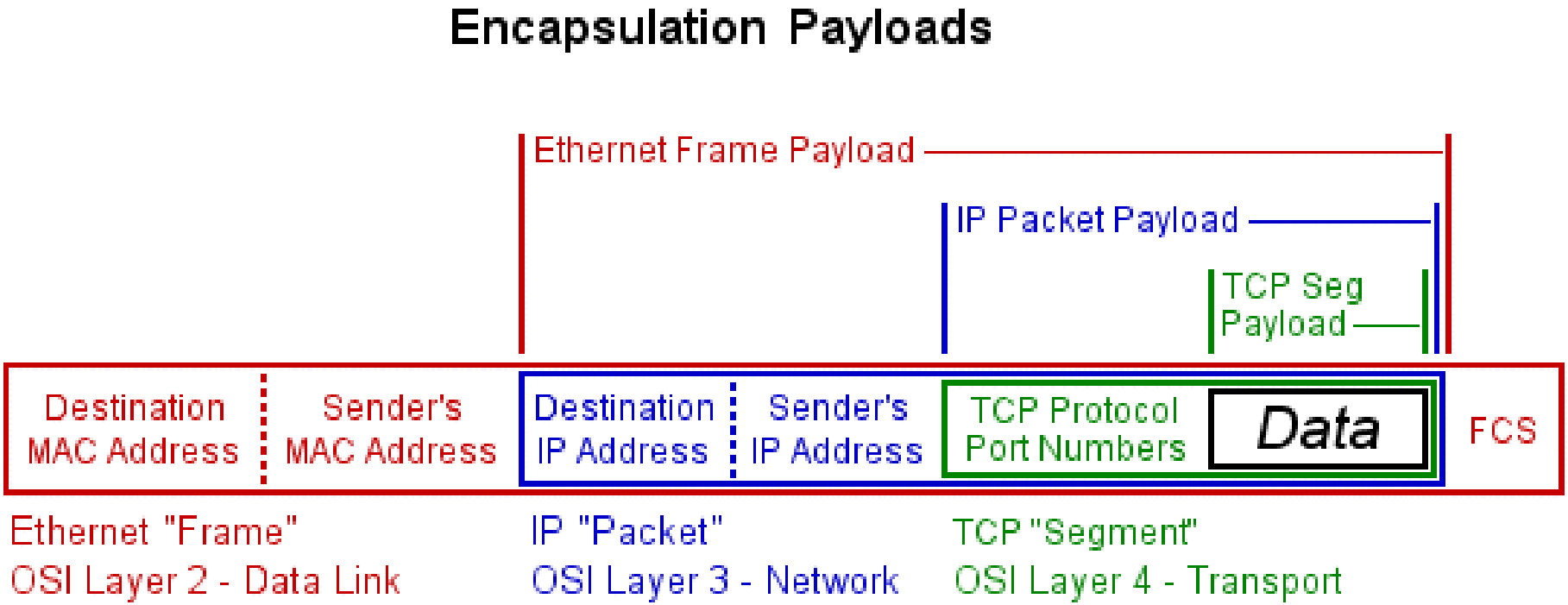
- The IPsec protocol provides a complete infrastructure for secured network communications.
- IPsec relies on security associations which has two main components:
  - Authentication Header (AH): provides assurance of message integrity and non-repudiation. Also provides authentication and access control and prevents replay attacks
  - Encapsulating Security Payload (ESP): provides confidentiality and integrity of packet contents. Provides encryption and limited authentication and also prevents replay attacks.

IPsec modes of operation

IPsec provides two modes of operation

- Transport Mode – Only packet payload is encrypted. This mode is used for P2P communications
- Tunnel Mode – The entire packet, including the header, is encrypted.

Ethernet Frame



Secure Socket Layer (SSL)

- Primarily used for secure online transactions such as online shopping or banking.
- SSL 1.0 was originally created by Netscape in 1995.
- Netscape released the source code for SSL version 2.0
- SSL is currently at version 3.0 and is still in use today, but its use is declining.
- Public desire for a completely open-source alternative finally found fruition in TLS, discussed next

Transport Layer Security (TLS)

- Performs a similar function to SSL. Both are used for secure connections over the Internet.
- They are so similar that TLS was created to be backward compatible with SSL, and newer TLS releases are often referred to as SSL versions
- TLS 1.0 is referred to as SSL 3.1, TLS 1.1 is referred to as SSL 3.2

HTTPS

- HTTPS is a secure form of the ever-popular HTTP
- The *S* stands for secure
- Uses Port # 443
- HTTPS provides the secure means for web-based transactions by utilizing protocols such as SSL and TLS

Secure Shell (SSH)

- Replacement for Telnet and uses Port # 22
- SSH transmissions are ciphertext and thus are protected from eavesdropping.
- SSH is the protocol most frequently used with a terminal editor program such as HyperTerminal in Windows, Minicom on Linux, or PuTTY on both.
- An example of SSH use would involve remotely connecting to a switch or router in order to make configuration changes.

SSH vs. SSL

- SFTP uses SSH
  - Port # 22
- FTPS & HTTPS uses SSL
  - FTPS – Port # 990 Controls / 991 Data
  - HTTPS – Port # 443
- Pay attention to the position of the “s”
  - If the “s” is before the protocol then it uses SSH
  - If the “s” is after the protocol then it uses SSL

Encrypting Email

- Because email is natively unsecure, several encryption options have been developed to add security to email used over the Internet.

- S/MIME and PGP / GPG

S/MIME

- Multipurpose internet Mail Extensions (S/MIME)
- Internet standard for encrypting and digitally signing email.
- S/MIME works by taking the original message from the server, encrypting it, and then attaching it to a new blank email as an attachment.
- The new blank email includes the sender's and receiver's email addresses to control routing of the message to its destination.
- The receiver must then strip off the attachment and decrypt it in order to extract the original message.

PGP and GPG

- Publicly available email security and authentication utility
- A **hybrid algorithm**, uses both symmetric and asymmetric cryptography to encrypt email
- Difference between PGP and GPG
  - Pretty Good Privacy (PGP) – Proprietary
  - GNU Privacy Guard (GPG) – Open Source

PGP and GPG


Professor Messer's
CompTIA Security+
Certification Training Course
Professor Messer
SY0-301: CompTIA Security+
Section 6.2 - Using Cryptography
Asymmetric
Encryption with
PGP and GPG
gtslearning
Content provided by:
http://www.gtslearning.com
Picture Credit: heliosphan (April)
http://www.flickr.com/photos/ryustar/2655110948/
http://creativecommons.org/licenses/by/2.0/
© 2011 Messer Studios, LLC

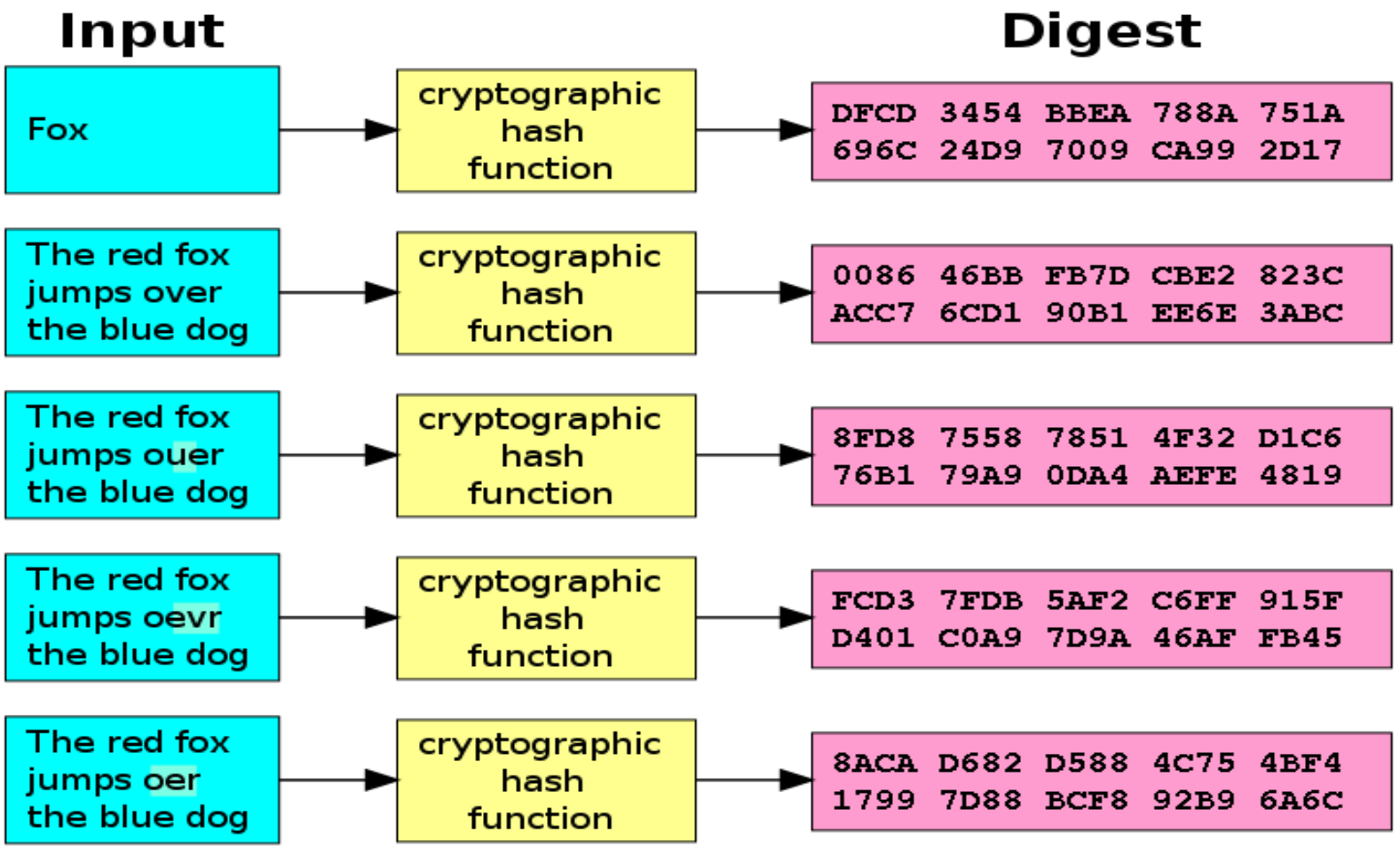
Non-repudiation

Non-repudiation prevents the sender of a message or the perpetrator of an activity from being able to deny that they sent the message or performed the activity

Hashing

- Represent data as a short string of text (fixed-length)
- Also called Message digest, checksum, hash value
- One-way hash – Never intended to be decrypted
- Used to store passwords
- Verify data integrity
- Digital signatures
  - Used in e-mails for data integrity and non-repudiation
- Avoid collisions
  - Different data having same message digest

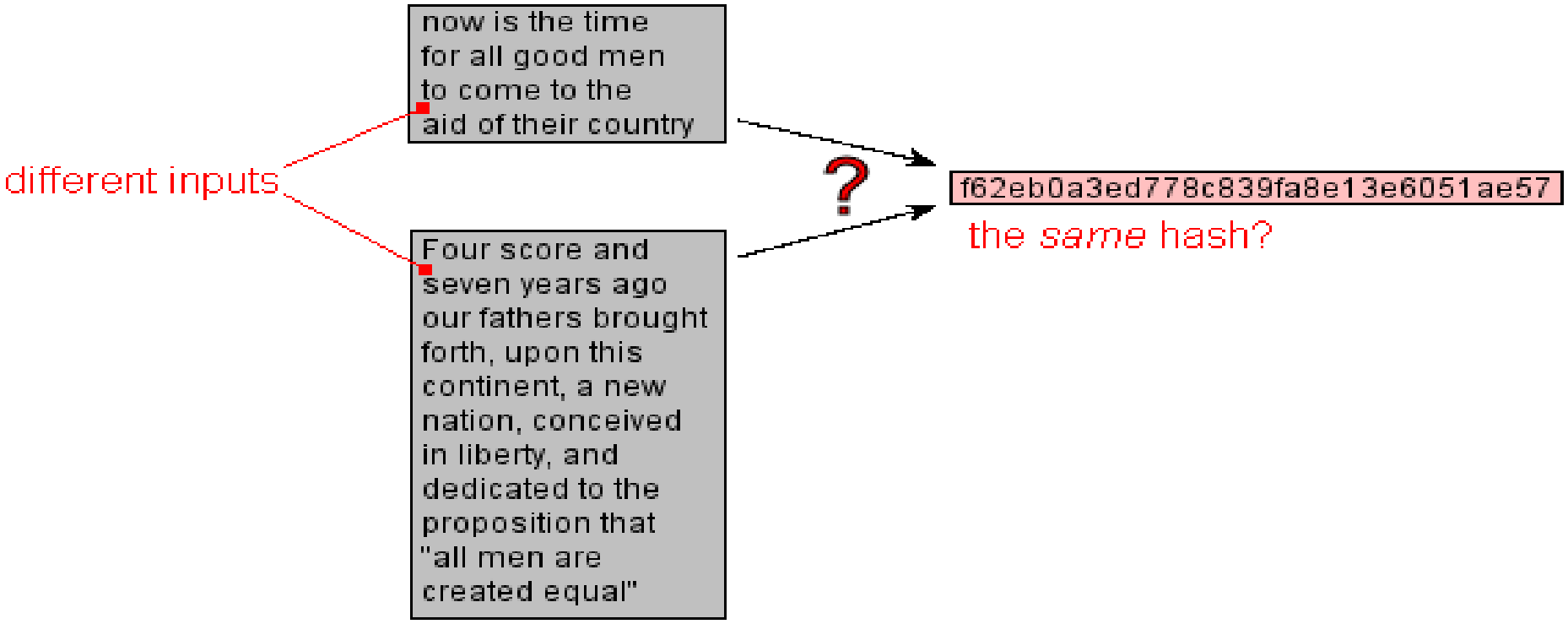
Hashing


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Collisions

Collisions

- Happens when two messages produce the same hash value



Hash Memorization Chart

TABLE 6.2 Hash algorithm memorization chart

Name	Hash Value Length
Secure Hash Algorithm (SHA-1)	160
SHA-224	224
SHA-256	256
SHA-384	384
SHA-512	512
Message Digest 5 (MD5)	128
Message Digest 4 (MD4)	128
Message Digest 2 (MD2)	128
RIPEMD	160
Hash Message Authentication Code (HMAC)	Variable
Hash of Variable Length (HAVAL)—an MD5 variant	128, 160, 192, 224, and 256 bits

Cryptographic Attacks

- **Birthday Attack:** Built on the premise that if 23 people are in a room, there is a probability that 2 people will have the same birthday
- **Brute Force:** Accomplished by applying every possible combination of characters that could be the key. 100% successful - time is the factor
- **Dictionary Attack:** Uses a dictionary of common words to reveal the users password

Cryptographic Attacks

- **Rainbow Tables:** pre calculated hashes
- **Frequency Analysis:** Analyzing blocks of an encrypted message to determine if any common patterns exist by using common occurrences in the English language
- **Hash Collision:** situation that occurs when two distinct inputs into a hash function produce identical outputs

Cryptographic Attacks

Frequencies of the letters in the English language

E	S	U	Y	Q
12.51%	6.54	2.71	1.73	0.11
T	R	M	B	Z
9.25	6.12	2.53	1.54	0.09
A	H	F	V	
8.04	5.49	2.30	0.99	
O	L	P	K	
7.60	4.14	2.00	0.67	
I	D	G	X	
7.26	3.99	1.96	0.19	
N	C	W	J	
7.09	3.06	1.92	0.16	

Cryptographic Attacks

The most common first letter in a word in order of frequency
T, O, A, W, B, C, D, S, F, M, R, H, I, Y, E, G, L, N, O, U, J, K

The most common second letter in a word in order of frequency
H, O, E, I, A, U, N, R, T

The most common third letter in a word in order of frequency
E, S, A, R, N, I

The most common last letter in a word in order of frequency
E, S, T, D, N, R, Y, F, L, O, G, H, A, K, M, P, U, W

More than half of all words end with
E ,T, D, S

http://scottbryce.com/cryptograms/stats.htm

Key escrow

- An alternative to key backups

- Used to store keys securely, while allowing one or more 3rd parties (key escrow agents) access to the keys under predefined conditions

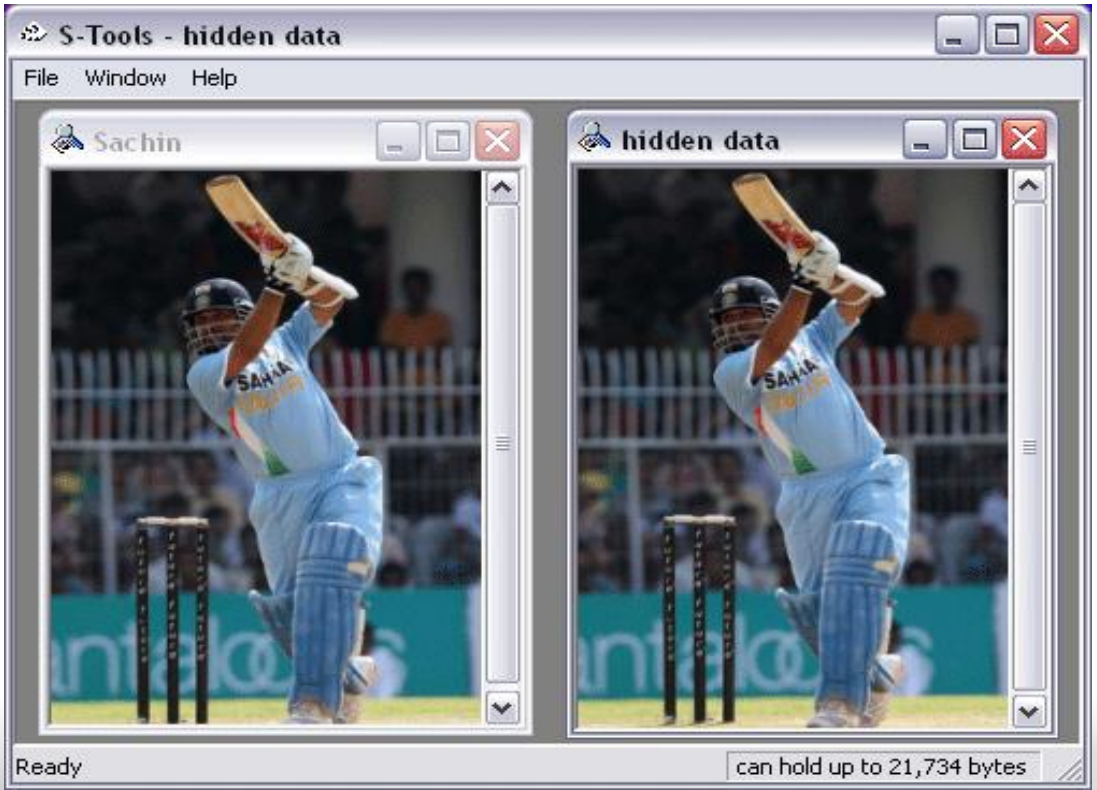
- M of N Control - Ensures no single administrator can abuse the key recovery process.

M of N Control

- This access-control mechanism creates a PIN number during the archive process and splits the number into two or more parts (N is the number of parts).
- Each part is given to a separate key-recovery agent (a person authorized to retrieve a user's private key).
- The recovery system can reconstruct the PIN number only if M number of agents provide their individual PIN numbers. For M of N Control to work, N must be greater than one and M must be less than or equal to N."

Steganography

- Concealed writing
- Hide data within other data
- Embedded in pictures, audio, document files



Steganography

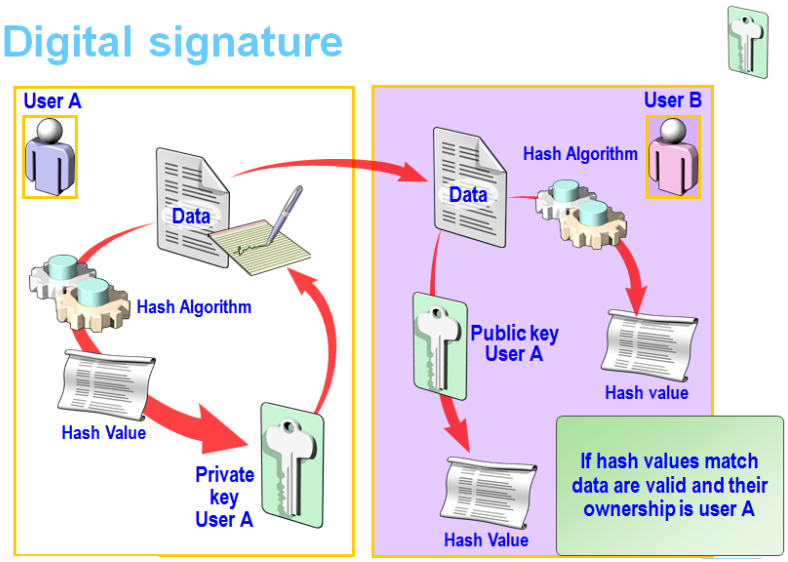
SilentEye

Exam Alert

- Steganography is **not** cryptography, but the two are related and often used in conjunction with one another
- Steganography seeks to hide the presence of a message
- Cryptography is to transform a message from its readable plain text into an unreadable form known as ciphertext.

Digital Signatures

- Similar in function to a standard signature on a document
- Sender signs with their Private key
- Receiver decrypts the hash and verifies the data with the sender's Public key
- Proof of origin
- Proof of submission
- Proof of delivery
- Proof of receipt
- Supports both Integrity and Nonrepudiation



Digital Signatures

1. You type an email

2. Using hashing software built in to your email client (SHA, MD5), you obtain a hash of the message

3. You use your private key to encrypt the hash. This encrypted hash is your digital signature for the message.

4. You send the message

Digital Signatures

5. The email recipient makes a hash of the received message

6. The email recipient uses your public key to decrypt the message hash

7.The email recipient hashes the message using the same hashing algorithm.

8. A comparison of the hashes is done. A match proves that the message is valid.

Use of proven technologies

- Because of the sensitive nature behind the uses of cryptography, the use of well-known, proven technologies is crucial

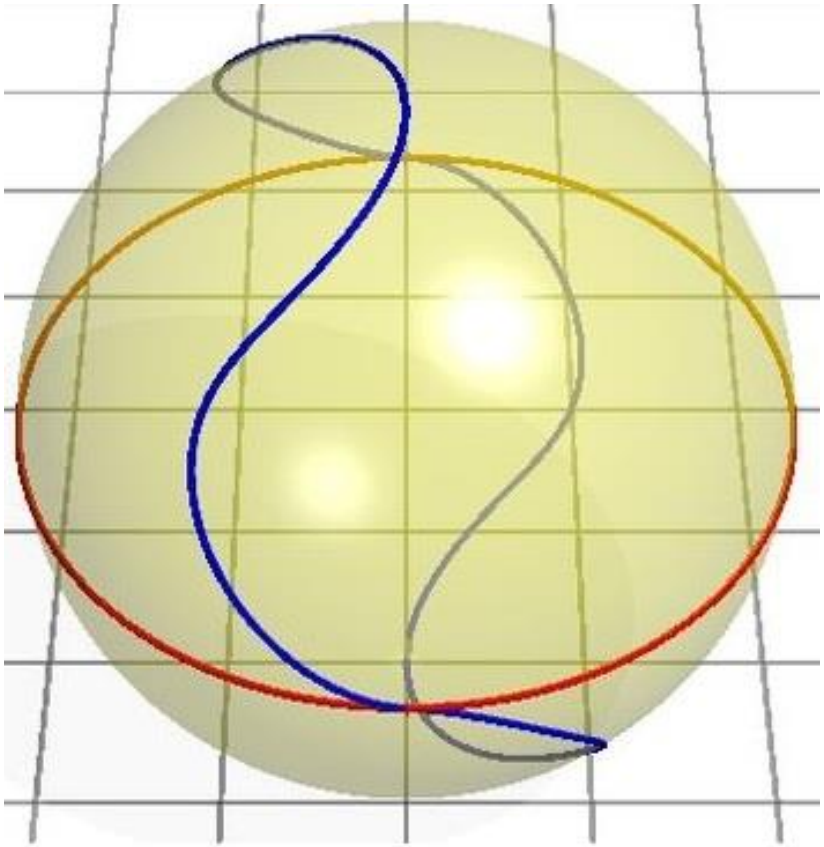
- Back doors and flaws can undermine any encryption algorithm

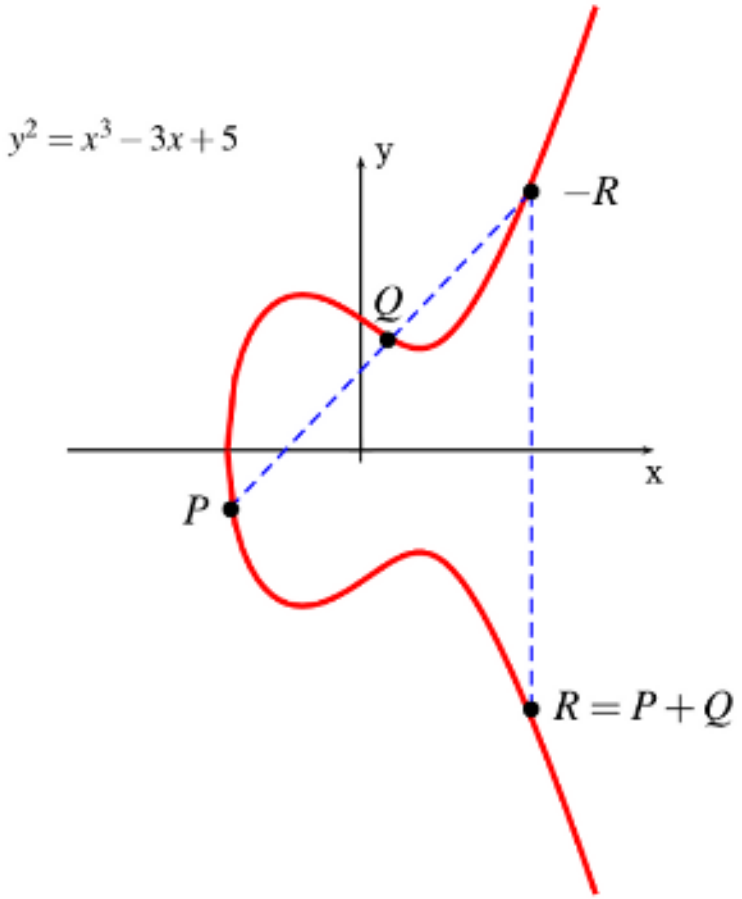
- Although various vendors might have their own encryption solutions, most of these depend upon well-known, time-tested algorithms, and generally speaking one should be skeptical of any vendor using a proprietary non-proven algorithm

Elliptic Curve Cryptography (ECC)

- ECC is a public-key cryptosystem based upon complex mathematical structures (asymmetric)
- ECC uses smaller key sizes than traditional public-key cryptosystem
- As a result, it is faster and consumes fewer resources, making it more ideal for mobile and wireless devices
- ECC RSA 160-bit key = RSA 1,024-bit

Elliptic Curve Cryptography (ECC)





Quantum Cryptography

- Unlike elliptic curves and other cryptosystems, quantum cryptography does not rely upon mathematics
- Although slower, the primary advantage provided by quantum cryptography is increased security
- Quantum mechanics protects against data being disturbed because one cannot measure the quantum state of the photons
- The mere observation of a quantum data stream changes the data

Ephemeral Key

- A key that is generated at the time of need for use in a short or temporary time frame
- Might be used once or could be used for a communication session before being discarded
- Session keys should be Ephemeral
- They are used uniquely and exclusively by end points of a single transaction or session.
- **Ephemeral keys are key to having *perfect forward secrecy***

Perfect Forward Secrecy

- Means of ensuring that the compromise of an entity's digital certificate or public/private key pairs does not compromise the security of any session keys
- Implemented by using ephemeral keys for each and every session
- The keys are generated at the time of need and used for only a specific period of time of volume of data transfer before being discarded and replaced
- Each subsequent rekeying operation in a session is performed independently of any previous keys, so each key is not dependent on other session keys and can not be used to determine any other key employed (No previous or future sessions)
- Technique ensures that the compromise of a session key would only result in the disclosure of a subsection of the encrypted conversation.

Student Check

In encryption, when data is broken into a single unit of varying sizes (depending on the algorithm) and the encryption is applied to those chunks of data, what type of algorithm is this?

- ❍ **A. Symmetric encryption algorithm**
- ❍ **B. Elliptic curve**
- ❍ **C. Block cipher**
- ❍ **D. All of the above**

Student Check

In encryption, when data is broken into a single unit of varying sizes (depending on the algorithm) and the encryption is applied to those chunks of data, what type of algorithm is this?

- ❍ A. Symmetric encryption algorithm
- ❍ B. Elliptic curve
- ❍ C. Block cipher
- ❍ D. All of the above

Student Check

Which type of algorithm generates a key pair (a public key and a private key) that is then used to encrypt and decrypt data and messages sent and received?

- ❍ **A. Elliptic curve**
- ❍ **B. Symmetric encryption algorithms**
- ❍ **C. Asymmetric encryption algorithms**
- ❍ **D. Paired algorithms**

Student Check

Which type of algorithm generates a key pair (a public key and a private key) that is then used to encrypt and decrypt data and messages sent and received?

- ❍ A. Elliptic curve
- ❍ B. Symmetric encryption algorithms
- ❍ C. Asymmetric encryption algorithms
- ❍ D. Paired algorithms

Objective 6.2

Use and apply appropriate cryptographic tools and products

WEP vs. WPA/WPA2 & Preshared Concepts

- WEP – Wired Equivalent Privacy
- Uses RC4 encryption to prevent eavesdropping
- Remember RC4 is not weak.
- WEP is weak due to small key space and static IV keys.
  - Because of such, we can brute force credentials using frequency analysis

WPA/WPA2

- WiFi Protected Access (WPA) – Replaced WEP
- WPA2 is currently the best encryption standard publically available.
- Only WPA2 should be used for securing wireless networks.
- Uses AES protocol for confidentiality
- WPA2 offers two options
  - Personal – uses a Preshared Key (PSK)
  - Enterprise – uses a certificates (ex: CA)

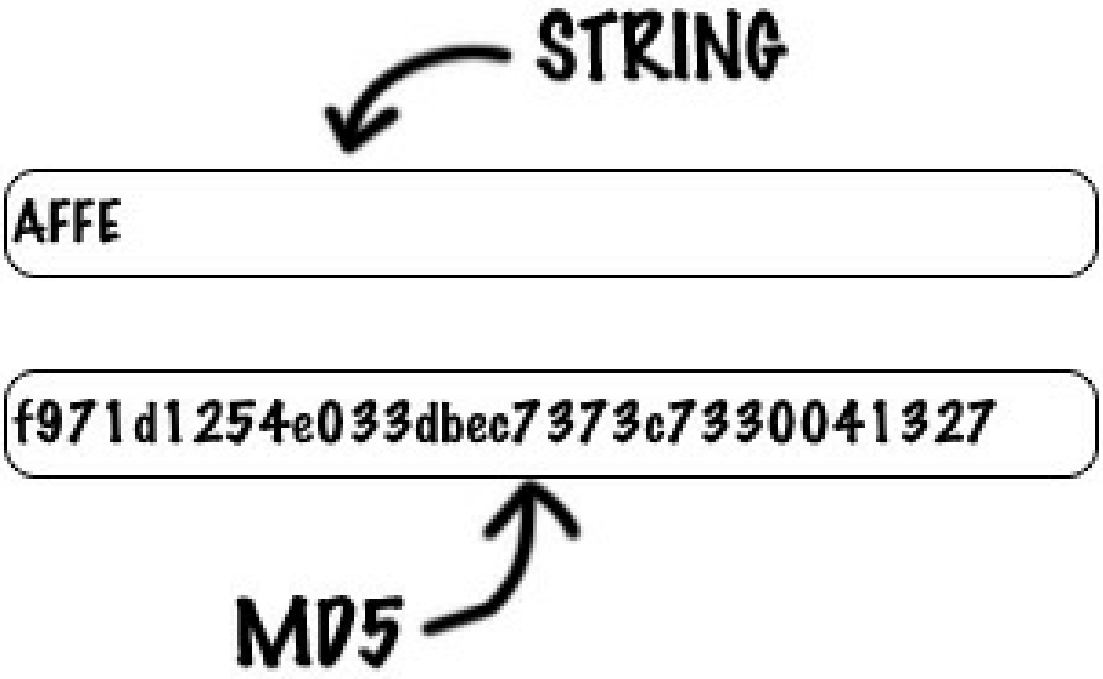
Preshared Key

- PSK is exactly what is sounds like. Two separate parties share a key via an out-of-band communication method prior to communication.
- This was part of the problem with WEP, because the same value used for encryption was also used for authentication.
- Under WEP, this is known as shared-key authentication (SKA).
- The PSK is still a fixed value; the difference is that it is a much stronger password than that of WEP.
  - PSK isn't involved in the key assignment for wireless encryption.

Message Digest 5 (MD5)

- Developed by Ronald Rivest in 1989
- Most widely used hashing algorithm in the world and will remain so for at least several more years to come.
  - Due to the fact that MD5 is coded into operating systems and popular software products
- Produces a 128-bit / 32 character message digest from variable length data
- Weakness: Does not have strong collision resistance

Message Digest 5 (MD5)



Secure Hash Algorithm (SHA)

- Modeled after MD5 but considered the stronger of the two
- Modeled SHA: 160 bit hash, but flawed and replaced
- SHA-1: 160 bit hash from any size of data
- SHA-2: 256 bit hash (32 bit word) and 512 bit hash (64 bit word) 224 bit and 384 bit are made by truncating the 256 bit and 512 bit versions
- SHA-1 Required by most US Government applications
- SHA-3: Chosen to replace SHA-2

Other Hashing Algorithms

- RACE Research and Development in Advanced Communications Technology (RACE)
- RACE Integrity Primitives Evaluation Message Digest **(RIPEMD)**
- RIPEMD Designed after MD4
- RIPEMD-160 Performs like SHA-1
- Used less than SHA-1 and MD5

Advanced Encryption Standard (AES) (Rinjdael)

- October 2000 NIST announced that the AES/Rinjdael block cipher had been chosen to replace DES
- (pronounced "rhine-doll")

- December 2000 U.S. Secretary of Commerce approved FIPS-197, mandating the use of AES for the encryption of all sensitive but unclassified data within the U.S. Government

- AES supports key sizes of 128, 192, 256 bit keys
  - 128-bit is the default

- The number of encryption rounds depends on the key size
  - 128-bit key requires 10 rounds of encryption
  - 192-bit key requires 12 rounds of encryption
  - 256-bit key requires 14 rounds of encryption

Data Encrypted Standard (DES)

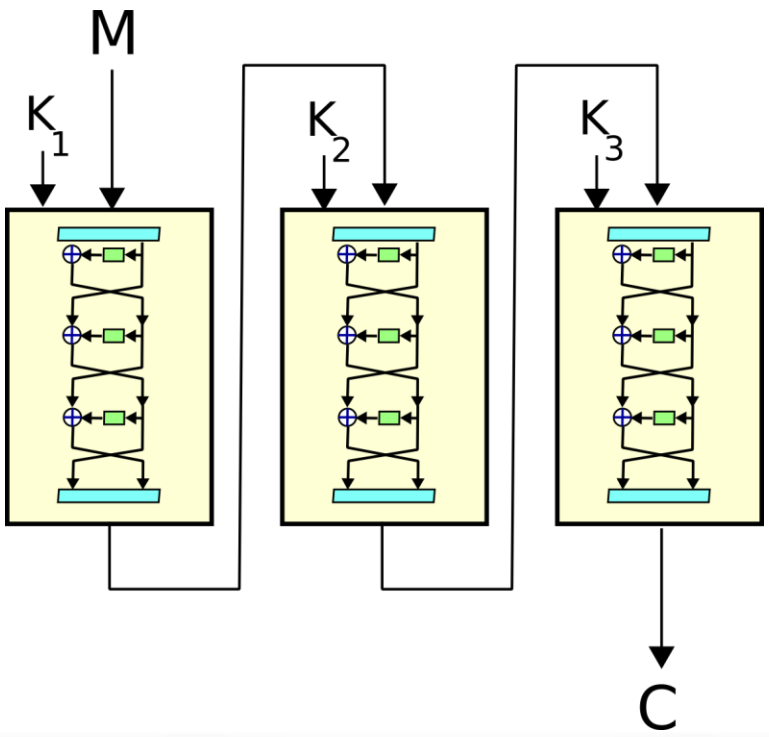
- Block-cipher
  - encrypts 64-bit blocks or chunks of data at a time
  - 16 rounds of encryption

- Uses a 56-bit Key
  - Short key length makes it weak

- Modes of Operation
  - Electronic Codebook (ECB) mode
  - Cipher Block Chaining (CBC) mode
  - Cipher Feedback (CFB) mode
  - Output Feedback (OFB) mode
  - Counter (CTR) mode

Triple-DES (3DES)

- Upgraded DES
- Uses 168-bit key
- Processes each block of data three times using a different key each time



Hash-based Message Authentication (HMAC)

- Combines a hash with a secret key
  - EX: Example, SHA-1 can be used to calculate an HMAC, which results in what's called HMAC-SHA1
- Verify data integrity and authenticity
- For example, IPsec uses HMAC to reduce the possibility of data collision to a near impossibility

Rivest Shamir Adelman (RSA)

- Designed in the late 1970's. Still used today. Only difference between original RSA and modern RSA implementations is the length of the public and private keys.
- Strength depends on the difficulty of factoring the product of prime numbers
- The most commonly used public key algorithm on the market
- Used for data encryption and digital signatures
- Used in many environments including SSL

Other Asymmetric Algorithms

- Diffie-Hellman Key Exchange
  - Provides for secure key exchange
  - Not used to encrypt/decrypt messages

- El Gamal
  - ElGamal is an extension of the Diffie-Hellman key-exchange algorithm that depends on modular arithmetic.
  - Used to transmit digital signatures and key exchanges

Rivest Cipher (RC)

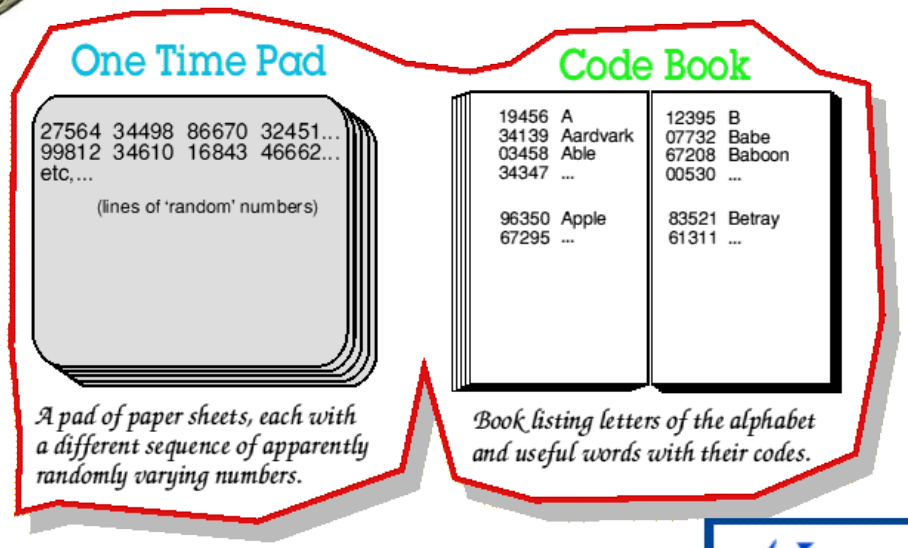
- A series of algorithms developed by Ronald Rivest
  - RC4, RC5, RC6
- RC4 uses a variable key-length
  - RC4 is a stream cipher (only RC that is a stream cipher)
- RC5 uses 128-bit key
- RC6 uses 128-bit or 256-bit key

One-Time-Pads (OTP)

- An algorithm that was developed under the assumption that if a key was used once, was completely random, and was kept secret, then it constitutes the perfect method of encryption, **unbreakable**

- Not practical because the key size has to be the same exact length as the data being encrypted.

OTP Cont.



the	cat	sat	on	the	mat
27173	75640	02166	44478	27173	99554
+			numbers from Code Book		
11743	98542	31318	42008	73192	50320
=			numbers from One time pad		
38816	63182	33474	86476	90265	49874

Encypted message

By adding the 'random' values from the pad we ensure that a word like "the" does not produce the same output every time it occurs in the message. Hence the encrypted pattern is protected from entropic attack.

NTLM

- LAN Manager
  - LM or LAN Manager, is a legacy storage mechanism developed by Microsoft to store passwords.
  - LM was replaced by NTLM on Windows NT 4.0 and should be disabled

- NTLM (UniCode Hash)
  - New Technology LAN Manager is a password hash storage system used on Microsoft Windows. NTLM exists in two versions
    - NTLMv1
    - NTLMv2

NTLM

- Results are nonreversible and thus much more secure than LM hashing.

- However, reverse-engineering password-cracking mechanisms can ultimately reveal NTLMv1 or v2 stored passwords if the passwords are relatively short (under 15 characters) and the hacker is given enough processing power and time.

Blowfish and Twofish

- Both developed by Bruce Schneier
- Both are symmetric block algorithms

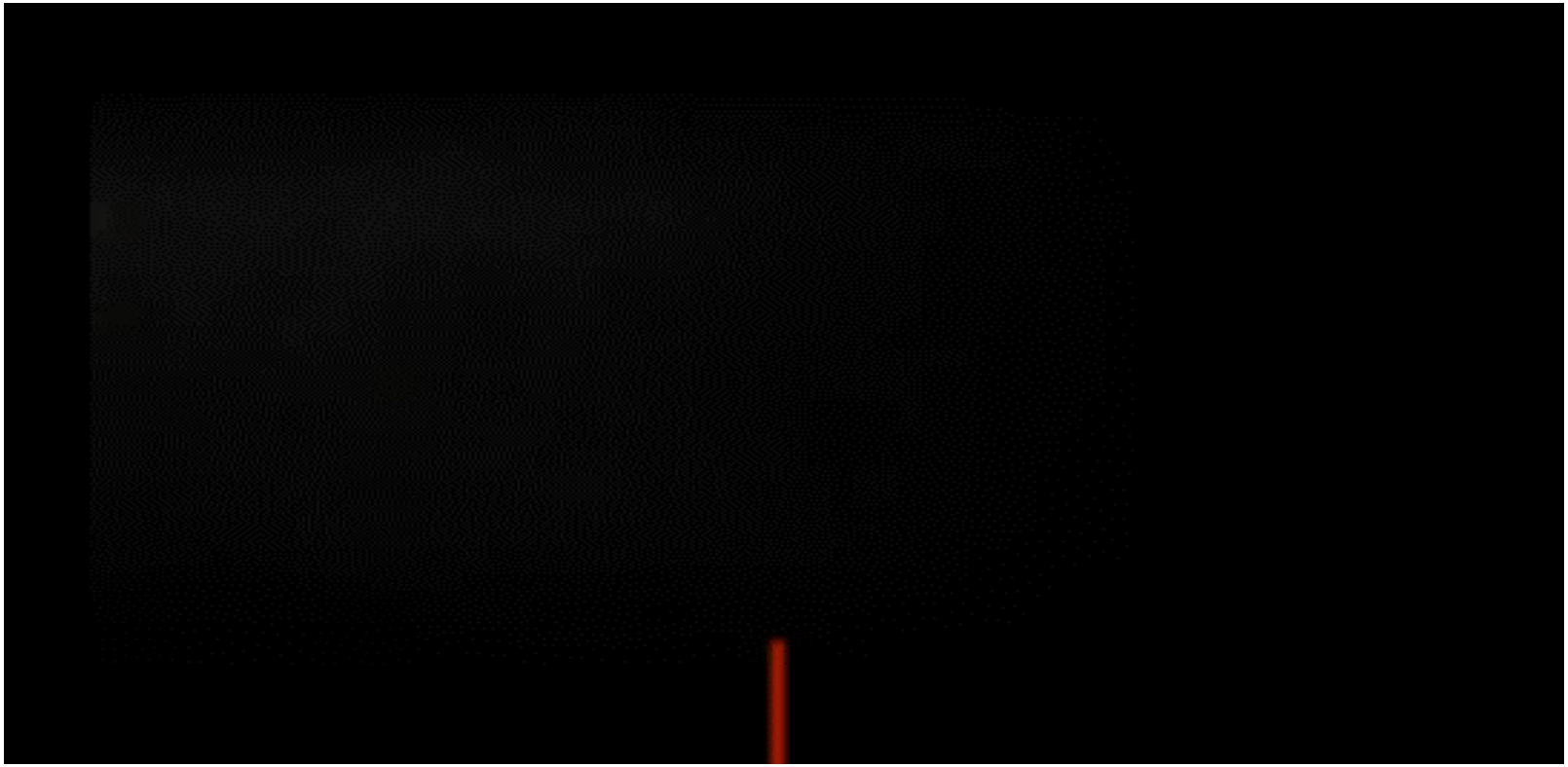
Blowfish and Twofish

- Blowfish
  - 64-bit key length
  - Alternative to DES and IDEA
  - Acceptable option for encryption, but only when you're using key lengths of at least 128 bits

- Twofish
  - 128-bit key length
  - Capable using cryptographic keys up to 256-bits in length
  - Twofish is a secure solution

Diffie-Hillman Key Exchange

- DHKE or DHE (as you may see it)



ECDHE

- Elliptic Curve Diffie-Hellman Ephemeral, or Elliptic Curve Ephemeral Diffie-Hellman
- implements perfect forward secrecy through the use of elliptic curve cryptography
- ECC has the potential to provide greater security with less computational burden than that of DHE.

Challenge Handshake Authentication Protocol (CHAP)

- Authentication protocol used primarily over dial-up connections (usually Point-to-Point Protocol [PPP]) as a means to provide a secure transport mechanism for logon credentials.

- It was developed as a secure alternative and replacement for PAP, which transmitted authentication credentials in cleartext

Challenge Handshake Authentication Protocol (CHAP)

- Uses an initial authentication-protection process to support logon and an ongoing verification process to ensure that the subject/client is still who they claim to be.

Challenge Handshake Authentication Protocol (CHAP)

1. The initial authentication process performs a one-way hash function (specifically, MD5) on the subject's password and then passes the username and hash value to the authentication server.

2. The authentication server compares the username to its accounts database and the hash value to that stored for the identified user in its database.

3. If there is a match, the server transmits a challenge to the client.

4. The client produces the correct response and transmits it back to the server.

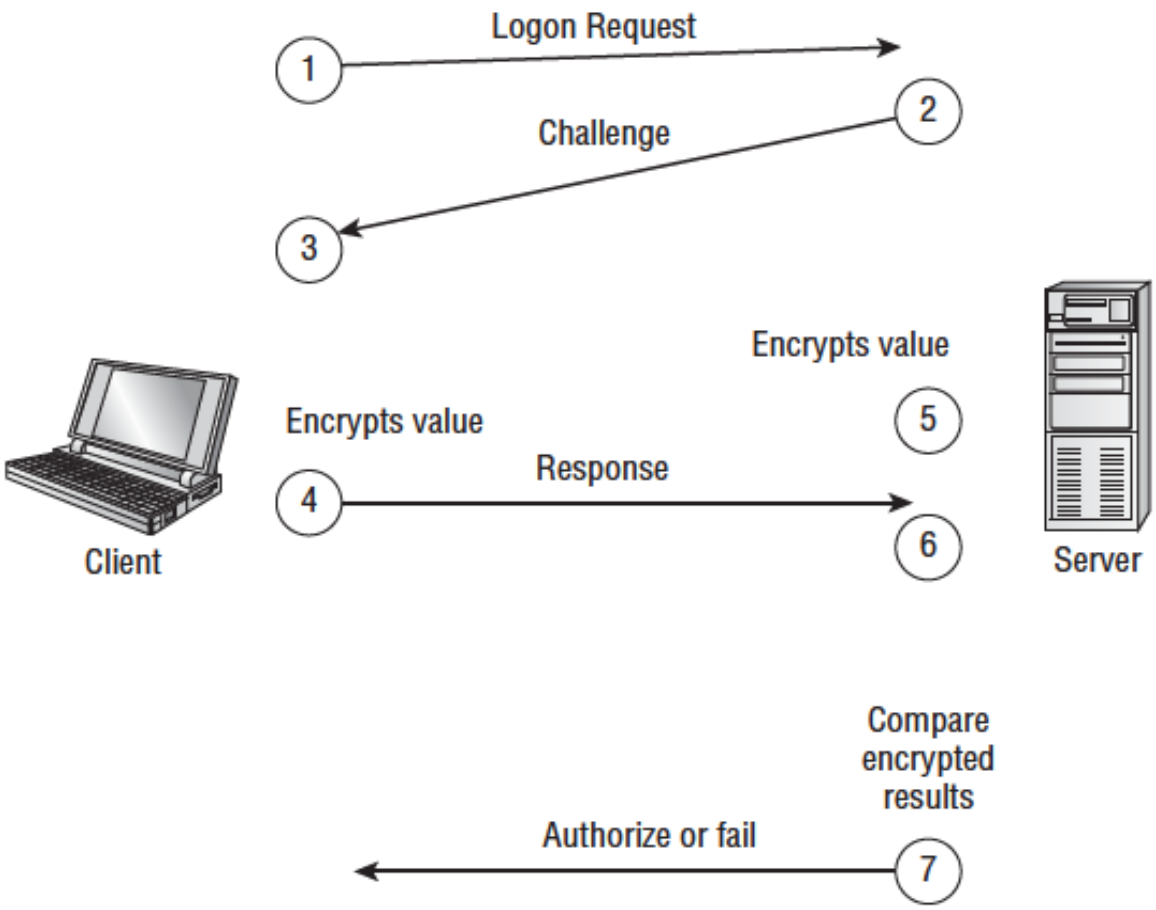
5. The server computes the response.

6. The server compares the response to that received by the client.

7. If everything matches, the subject is authenticated and allowed to communicate over the link.

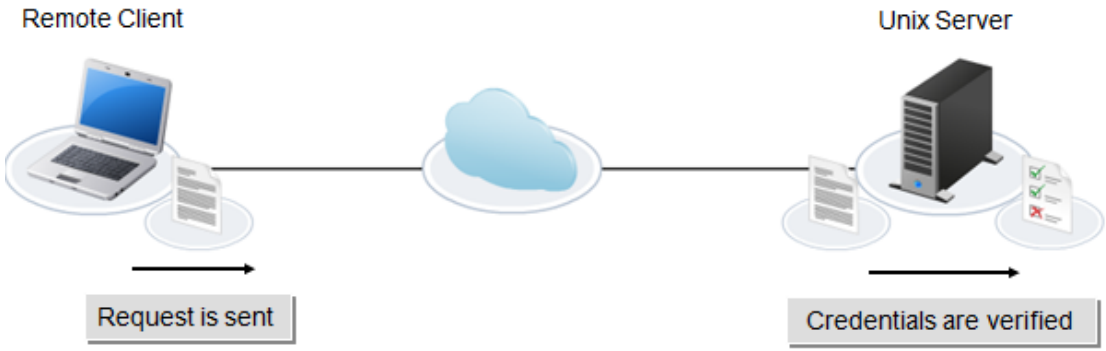
Challenge Handshake Authentication Protocol (CHAP)

FIGURE 6.11 CHAP authentication



Password Authentication Protocol (PAP)

- Offers no true security
- Sends user IDs and passwords in cleartext
- Generally used for a remote client to connect to a non-Windows server that does not support stronger password encryption, such as CHAP



Comparative Strengths of Algorithms

- The following list reveals why symmetric algorithms are favored for most applications and why asymmetric algorithms are widely considered very secure but often too complex and resource-intensive for every environment

  - 64-bit symmetric key strength = 512-bit asymmetric key strength
  - 112-bit symmetric key strength = 1792-bit asymmetric key strength
  - 128-bit symmetric key strength = 2304-bit asymmetric key strength

Cipher Suites

- Standardized collection of authentication, encryption, and hashing algorithms used to define the parameters for a security network communication.
- Most often *cipher suite* is used in relation to SSL/TLS connections.
- An official TLS Cipher Suite Registry is maintained by the International Assigned Numbers Authority (IANA)
- www.iana.org/assignments/tls-parameters/tls-parameters.xhtml.

Cipher Suites

- A cipher suite consists of and is named by four elements
- EX: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384):
- A key-exchange mechanism (TLS_ECDHE)
- An authentication mechanism (RSA)
- A cipher (AES_256_GCM)
- A hashing or message-authenticating code (MAC) mechanism (SHA384)
- A client requesting a TLS session sends a preference-ordered list of client-side supported cipher suites as part of the initiation handshake process. The server replies and negotiates with the client based on the highest-preference cipher suite they have in common.

Cipher Suite
Strong vs. weak ciphers

- Not all ciphers or other algorithm elements in a cipher suite are secure.
- Many older algorithms or implementations of algorithms have known flaws, weaknesses, or means of compromise.
- These weaker ciphers should be avoided and disabled in preference of stronger cipher suites with no or fewer issues.

Key Stretching

- A collection of techniques that can potentially take a weak key or password and stretch it to become more secure.
- Protects against brute-force attacks.
- Often, key stretching involves adding iterative computations that increase the effort involved in creating the improved key result
- A common example of key stretching is to convert a user's password into an encryption key.

Key Stretching – PBKDF2

- *Password-Based Key Derivation Function 2*
- It uses a hashing operation, an encryption cipher function, or an HMAC operation
- (a symmetric key is used in the hashing process) on the input password, which is combined with a salt.
- This process is then repeated thousands of times

Key Stretching - Bcrypt

- Bcrypt is another example of a key-stretching technology.
- It's based on the Blowfish cipher
- it uses salting, and it includes an adaptive function to increase iterations over time

Student Check

Which of the following protocols are used to manage secure communication between a client and a server over the Web? (Select two correct answers.)

- ❍ A. SSL
- ❍ B. ISAKMP
- ❍ C. PGP
- ❍ D. TLS

Student Check

Which of the following protocols are used to manage secure communication between a client and a server over the Web? (Select two correct answers.)

- ❍ A. SSL
- ❍ B. ISAKMP
- ❍ C. PGP
- ❍ D. TLS

Student Check

Which of the following algorithms are examples of a symmetric encryption algorithm? (Choose three answers.)

- ❍ A. 3DES
- ❍ B. Diffie-Hellman
- ❍ C. RC4
- ❍ D. AES

Student Check

Which of the following algorithms are examples of a symmetric encryption algorithm? (Choose three answers.)

- ❍ A. 3DES
- ❍ B. Diffie-Hellman
- ❍ C. RC4
- ❍ D. AES

Student Check

Which of the following algorithms are examples of an asymmetric encryption algorithm? (Choose two answers.)

- ❍ A. Elliptic curve
- ❍ B. 3DES
- ❍ C. AES
- ❍ D. RSA

Student Check

Which of the following algorithms are examples of an asymmetric encryption algorithm? (Choose two answers.)

- ❍ A. Elliptic curve
- ❍ B. 3DES
- ❍ C. AES
- ❍ D. RSA

Student Check

Which of the following is a type of cipher that has earned the distinction of being unbreakable?

- ❍ **A. RSA**
- ❍ **B. One-time pad**
- ❍ **C. 3DES**
- ❍ **D. WPA**

Student Check

Which of the following is a type of cipher that has earned the distinction of being unbreakable?

- ❍ A. RSA
- ❍ B. One-time pad
- ❍ C. 3DES
- ❍ D. WPA

Student Check

Which of the following is most directly associated with providing or supporting perfect forward secrecy?

- ❍ A. PBKDF2
- ❍ B. ECDHE
- ❍ C. HMAC
- ❍ D. OCSP

Student Check

Which of the following is most directly associated with providing or supporting perfect forward secrecy?

- ❍ A. PBKDF2
- ❍ B. ECDHE
- ❍ C. HMAC
- ❍ D. OCSP

Student Check

Which of the following symmetric-encryption algorithms offers the strength of 168-bit keys?

- ❍ A. Data Encryption Standard
- ❍ B. Triple DES
- ❍ C. Advanced Encryption Standard
- ❍ D. IDEA

Student Check

Which of the following symmetric-encryption algorithms offers the strength of 168-bit keys?

- ❍ A. Data Encryption Standard
- ❍ B. Triple DES
- ❍ C. Advanced Encryption Standard
- ❍ D. IDEA

Student Check

Which of the following is a description of a key-stretching technique?

❍ A. Salting input before hashing

❍ B. Generating a random number, and then using a trapdoor one-way function to derive a related key

❍ C. Adding iterative computations that increase the effort involved in creating the improved result

❍ D. Using a challenge-response dialogue

Student Check

Which of the following is a description of a key-stretching technique?

❍ A. Salting input before hashing

❍ B. Generating a random number, and then using a trapdoor one-way function to derive a related key

❍ C. Adding iterative computations that increase the effort involved in creating the improved result

❍ D. Using a challenge-response dialogue

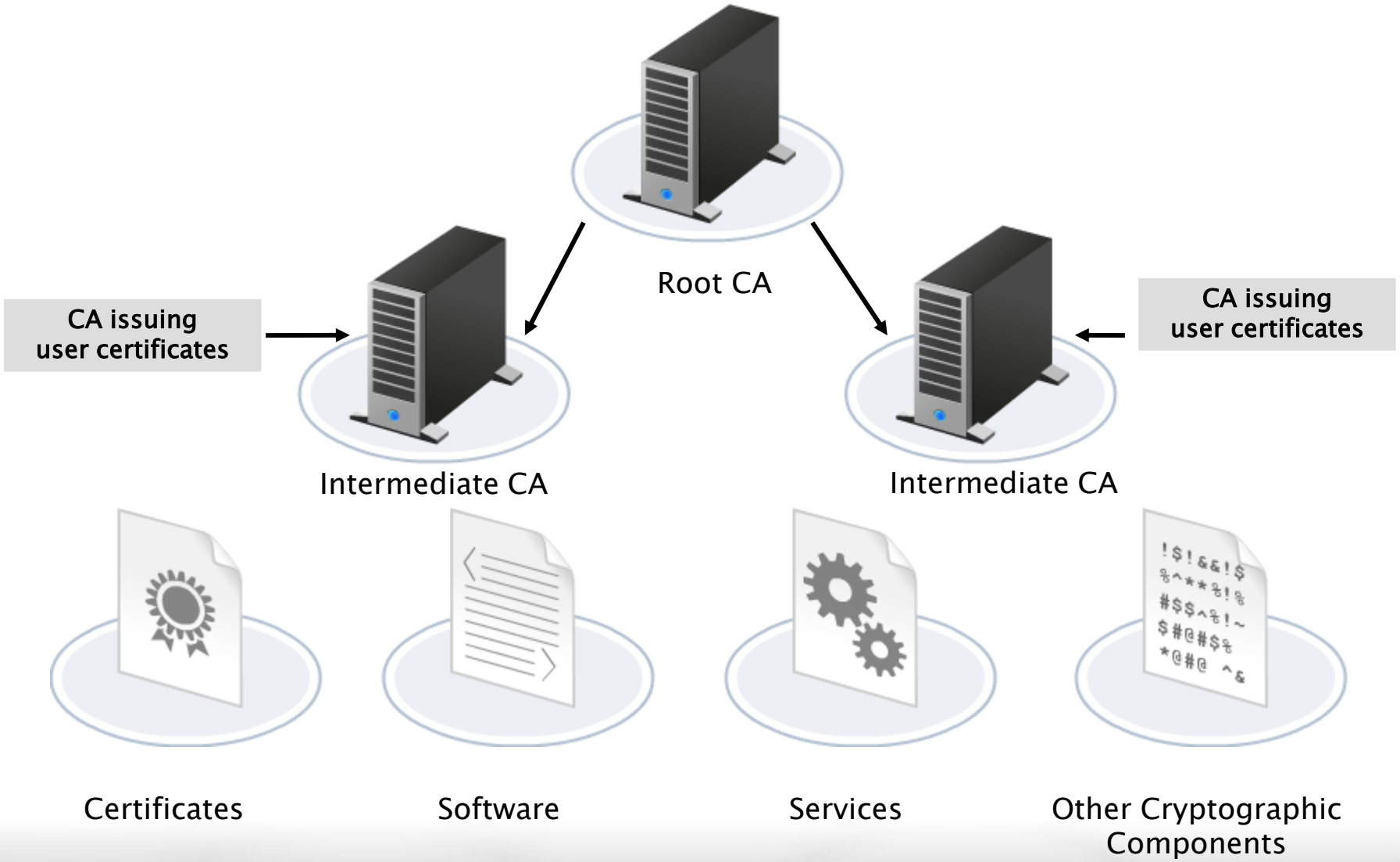
Objective 6.3

- Explain the core concepts of Public Key infrastructure

Public Key Infrastructure (PKI)

- A system that is composed of the following
  - Certificate Authority (CA)
  - Registration Authority
  - Certificates (OCSP
  - Certificate Revocation List (CRL)

PKI


Root CA
CA issuing
user certificates
Intermediate CA
CA issuing
user certificates
Intermediate CA
Certificates
Software
Services
Other Cryptographic
Components

PKIX and PKCS

- PKIX Develops Internet standards based on X.509
- PKCS – Public Key Cryptography Standards Defacto cryptography message standards.
- Developed and published by RSA Labs
- Provides a basic and widely accepted framework for the development of PKI solutions

Digital Certificates

- Digitally signed block of data by the Issuing CA
- Signed with the CA's private key and associates the user's credentials with a public key
- Both users and devices can hold certificates
- The certificate validates the certificate holder's identity

X.509 Standard

Defines the format of required data for Digital Certificate:

Version – Version of X.509
Serial Number – Unique Serial number assigned by the CA
Signature Algorithm Identifier – Algorithm used to sign by the CA
Issuer – Name of the CA
Validity Period – How long the certificate is valid
Subject Name – Who the certificate is for
Subject Public Key Information – Public Keys of the Subject Name

Registration Authority (RA)

- Responsible for verifying users' identities and approving or denying requests for digital certificates
- RAs do **not** issue certificates
- Goes to CA on a businesses behalf

Certificate Authority (CA)

- The server that issues and signs digital certificates and generates the public/private key pair
- Key pair is based on a mathematical relationship that can not be spoofed
- You can only trust a certificate if you can trust the CA that issued it

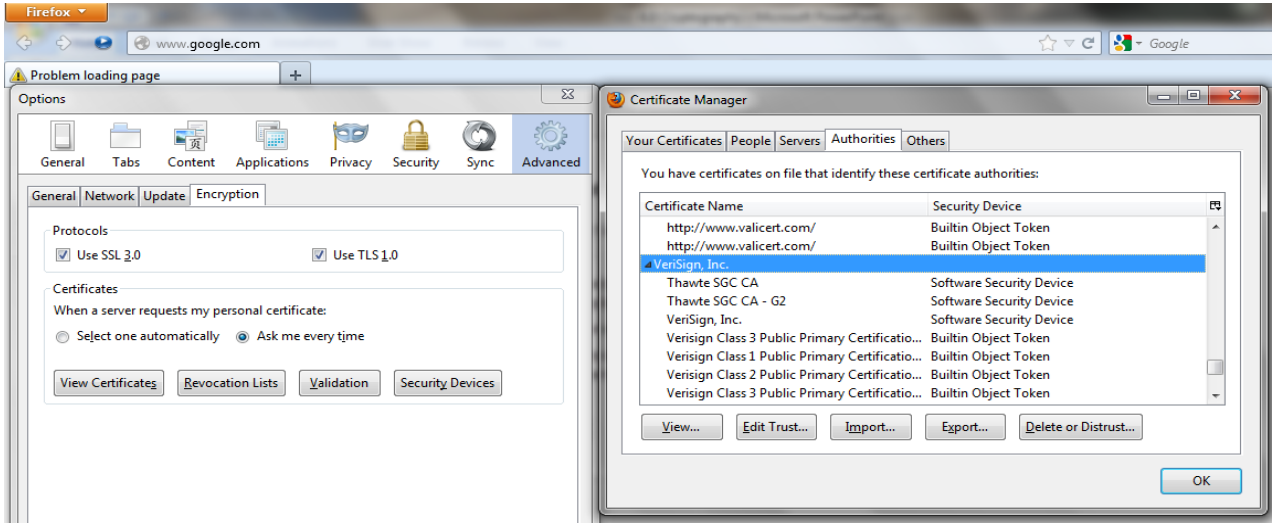
Commercial CAs

VeriSign

Comodo

GlobalSign

Entrust



Certificate Policies

- Provides the rules that indicate how the certificate will be used and its purpose
- Acceptable-use policies for certificates
- They dictate what is and isn't acceptable with regard to how certificates can be used in an organization
- Focused on the Certificate

Certificate Practice Statement (CPS)

- Provides the general practices followed by the CA issuing certificates and customer-related information about certificates, responsibilities, and problem management
- Details how certificate management is performed, how security is maintained, and the procedures the CA must follow to perform any type of certificate management from creation to revocation
- Focused on the CA and the way the CA issues certificates

Certificate Revocation List (CRL)

- List of certificates that were revoked before expiration date
- Each CA has its own CRL that can be accessed through directory services of the network operating system
- Generally contains entity's name, ID number, and the reason why the certificate was revoked
- Many applications will check the CRL for the status of a certificate before accepting it
- OCSP – Online Certificate Status Protocol

Revoke Certificates

Certificates can be revoked before expiration for one of several reasons:

- Private key compromised
- Fraudulent certificate
- Holder no longer trusted
- Employee leaves organization
- System intrusion

Certificates can also be suspended

Certificate Signing Request (CSR)

- A message sent to a certificate authority from a user or organization to request and apply for a digital certificate
- Often follows the PKCS#10 specification or the Signed Public Key and Challenge (SPKAC) format

Private Key Protection Methods

- Back up to removable media and store securely
- Delete from unsecure media
- Require restoration password
- Never share a key
- Never transmit a key on the network
- Use key escrow

Recovery Agent

- Also be called key-recovery agents or key-escrow agents

- Key backup
  - Restore from backup media

- Key escrow
  - One or more escrow agents can restore

Registration

Process of obtaining a certificate from the CA.

1. A subject crafts a private key and then generates a public key

2. The public key is sent to the CA along with proof-of-subject identity

3. The CA verifies the subject's identity using whatever level of due diligence is warranted

4. The CA crafts the certificate by digitally signing the subject's public key with the CA's private key, and then it adds a text file containing the details mandated by the X.509 v3 certificate standard

5. The CA sends the certificate to the subject via a secured pathway

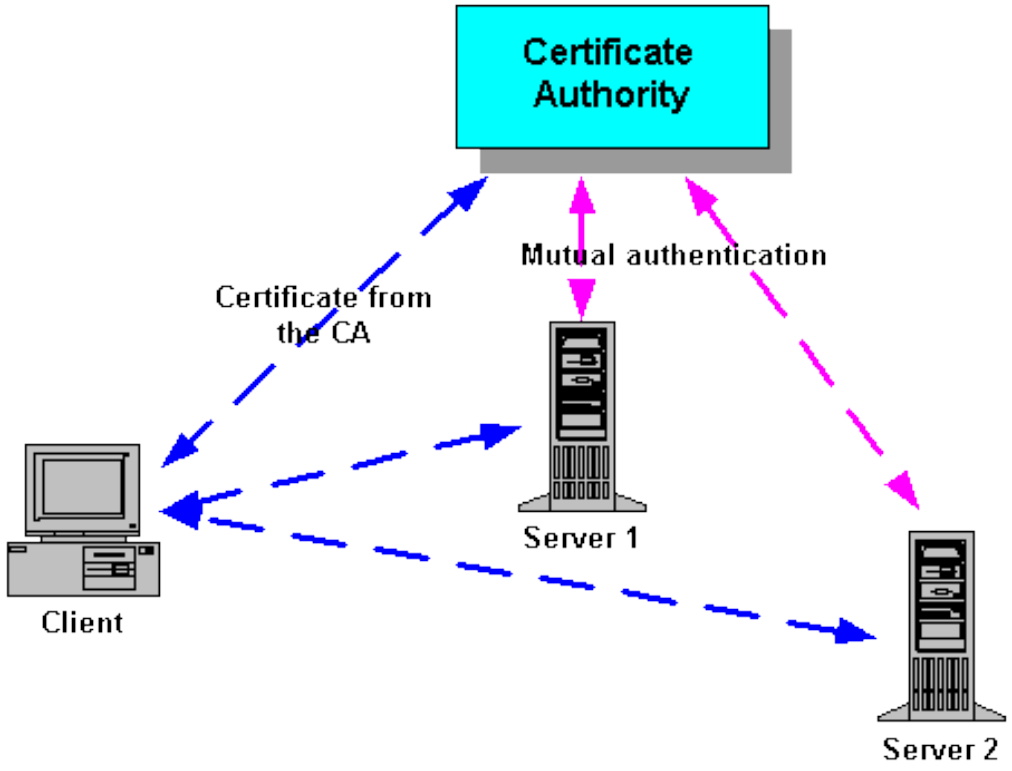
Private Key Replacement Process

1. Recover key
2. Decrypt data
3. Destroy original key
4. Obtain new key pair
5. Encrypt data with new key

Trust Models

- Single-CA Model
  - Single CA that issues digital certificates
  - Simplest model used mostly by small organizations
- Hierarchical CA Model
  - One Root CA and Subordinate CA
  - Subordinate CAs provide redundancy and load balancing
  - Most common model used today
- Cross-Certification CA Model (Web of Trust)
  - More than one Single-CA models that trust each other as peers
  - When a small company starts off with one Single-CA model and adds more
- Bridge CA Model
  - One CA becomes the Bridge CA and the central point of trust
  - Used in a large Cross-Certificate CA model

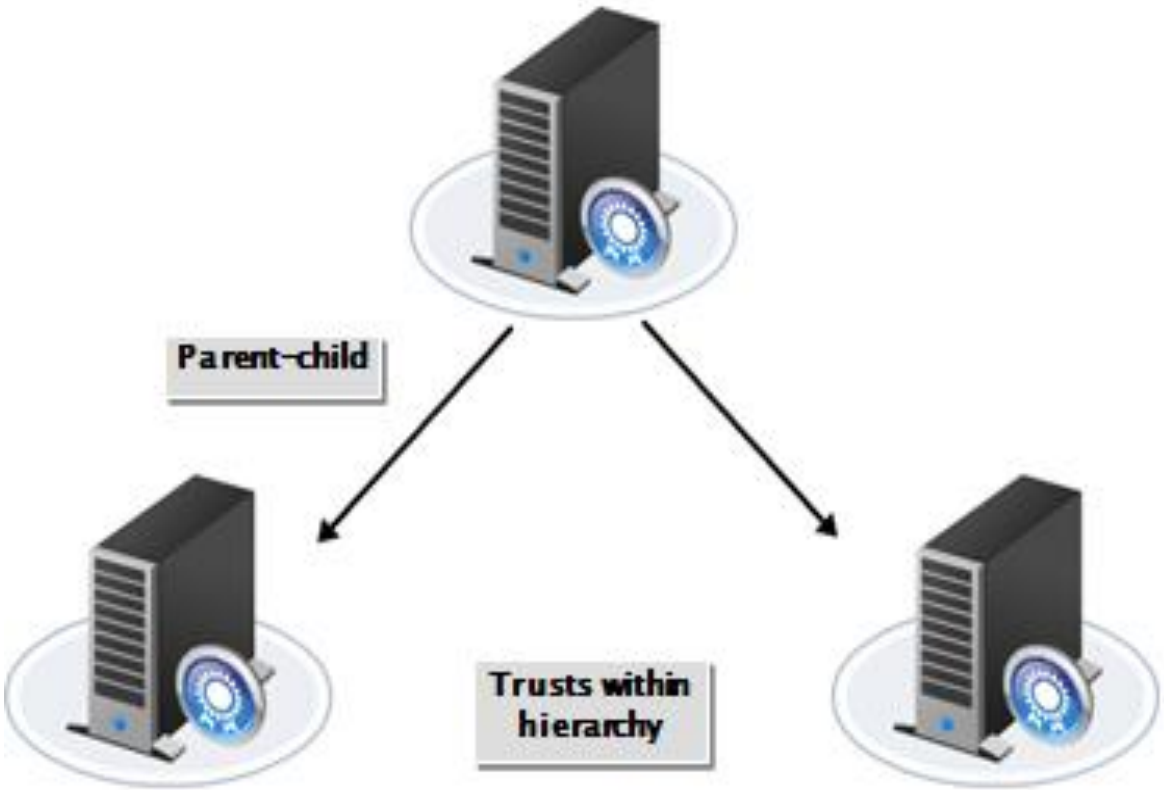
Single CA Model



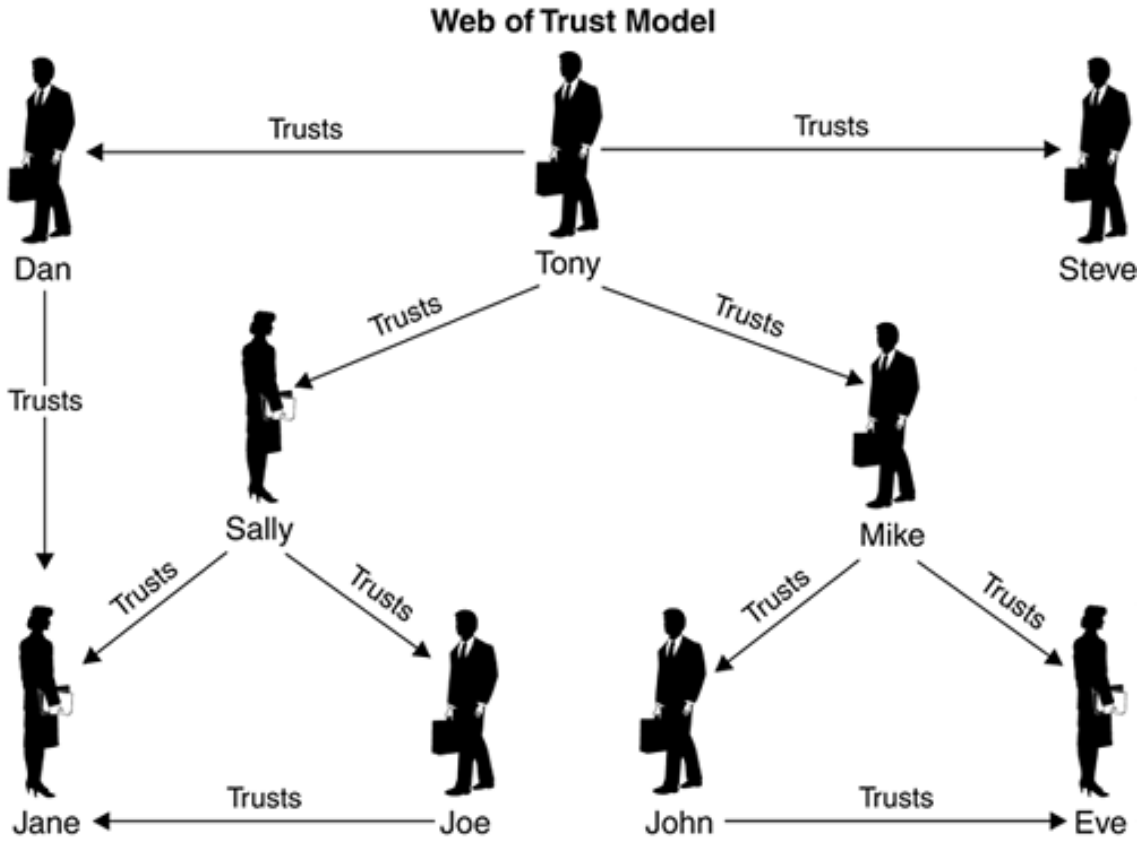
Hierarchical CA Model

- A single group of CAs that work together to issue digital certificates
- Each CA in the hierarchy has a parent-child relationship with the CA directly above it
- Helps distribute workload
- If a CA is compromised only the certificates issued by that particular CA and its children are invalid

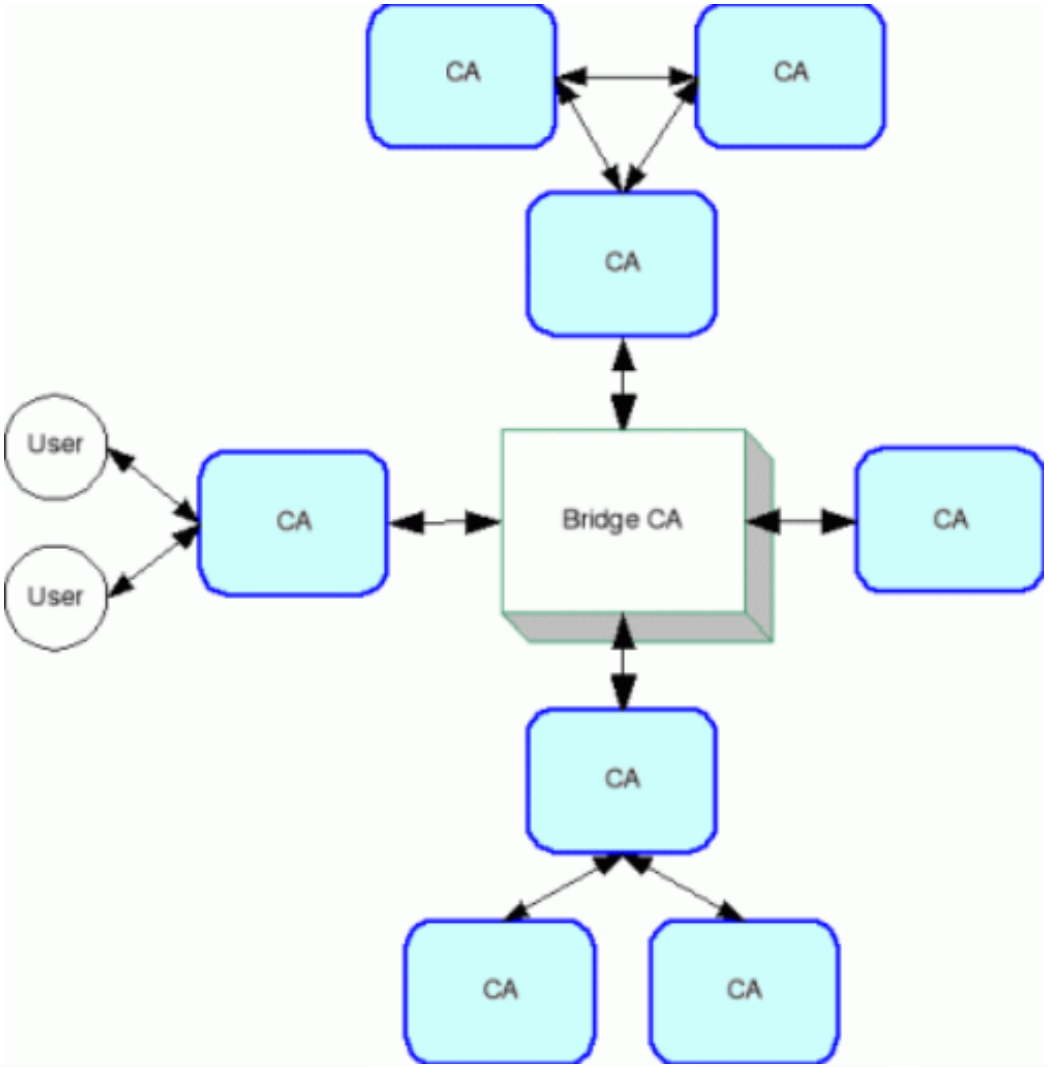
Hierarchical CA Model



Cross-Certification CA Model (Web of Trust)



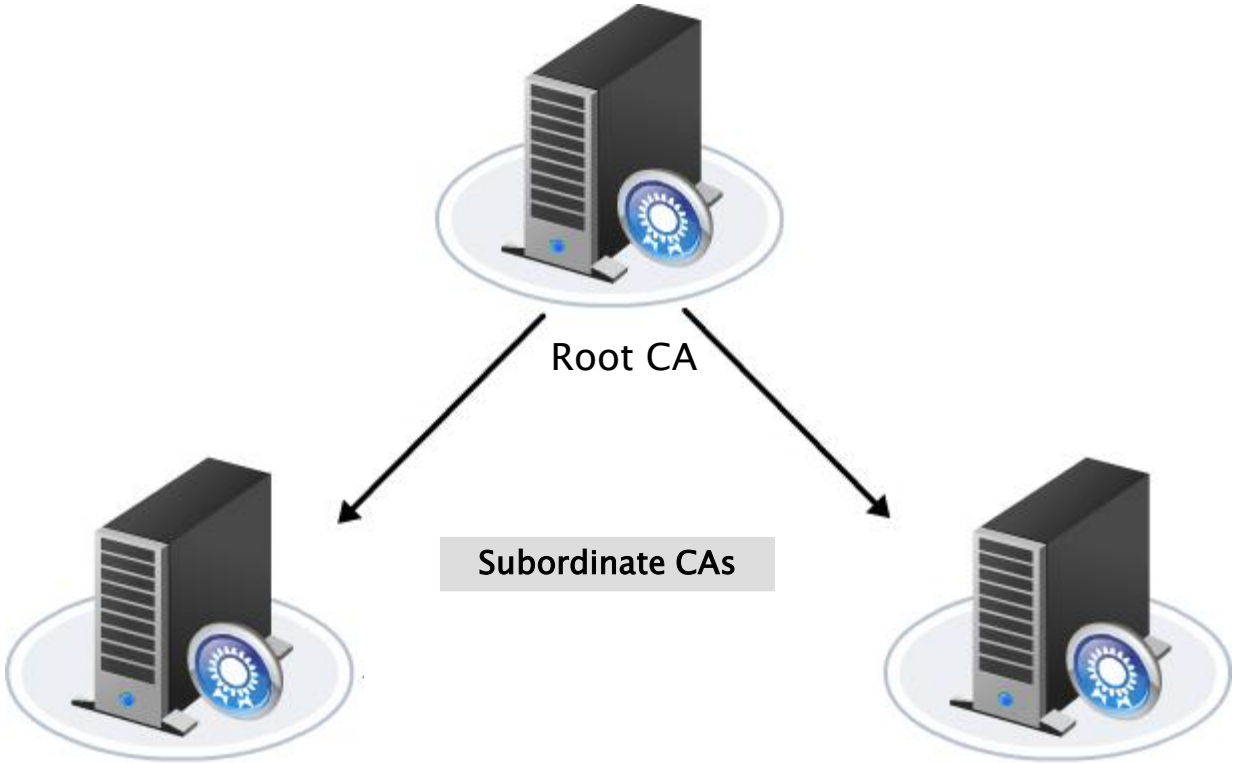
Bridge CA Model



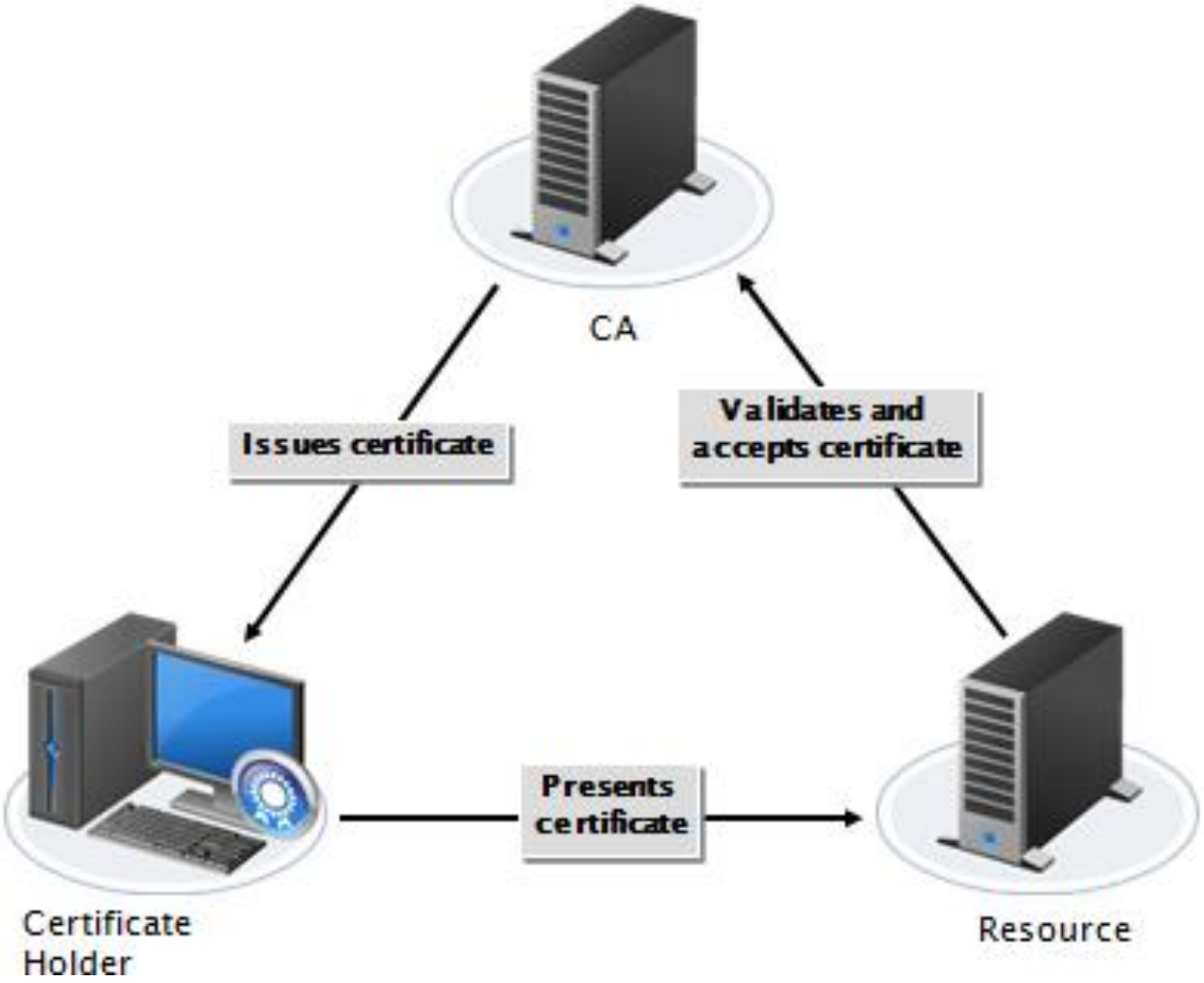
The Root CA

- The top-most CA in the hierarchy and the most trusted authority
- Must be secured, if compromised, all other certificates become invalid
- Common practice to take root CA offline

Subordinate / Intermediate CAs



Certificate Authentication



Student Check

To check the validity of a digital certificate, which one of the following would be used?

- ❍ A. Corporate security policy
- ❍ B. Certificate policy
- ❍ C. Certificate revocation list
- ❍ D. Expired domain names

Student Check

To check the validity of a digital certificate, which one of the following would be used?

- A. Corporate security policy
- B. Certificate policy
- C. Certificate revocation list
- D. Expired domain names

Student Check

Which of the following is not a certificate trust model for the arranging of certificate authorities?

- ❍ A. Bridge CA architecture
- ❍ B. Sub-CA architecture
- ❍ C. Single-CA architecture
- ❍ D. Hierarchical CA Architecture

Student Check

Which of the following is not a certificate trust model for the arranging of certificate authorities?

- ❍ A. Bridge CA architecture
- ❍ B. Sub-CA architecture
- ❍ C. Single-CA architecture
- ❍ D. Hierarchical CA Architecture

Student Check

Which of the following are included within a digital certificate? (Select the correct answers.)

- ❍ A. User's public key
- ❍ B. User's private key
- ❍ C. Information about the user
- ❍ D. Digital signature of the issuing CA

Student Check

Which of the following are included within a digital certificate? (Select the correct answers.)

- ❍ A. User's public key
- ❍ B. User's private key
- ❍ C. Information about the user
- ❍ D. Digital signature of the issuing CA

Student Check

When a subject or end user requests a certificate, they must provide which of the following items? (Choose all that apply.)

- ❍ A. Proof of identity
- ❍ B. A hardware storage device
- ❍ C. A public key
- ❍ D. A private key

Student Check

When a subject or end user requests a certificate, they must provide which of the following items? (Choose all that apply.)

- ❍ A. Proof of identity
- ❍ B. A hardware storage device
- ❍ C. A public key
- ❍ D. A private key

Student Check

When should a key or certificate be renewed?

- ❍ A. Every year
- ❍ B. Every quarter
- ❍ C. Just before it expires
- ❍ D. Just after it expires

Student Check

When should a key or certificate be renewed?

- ❍ A. Every year
- ❍ B. Every quarter
- ❍ C. Just before it expires
- ❍ D. Just after it expires