**SE 2014**

**What are the two different uses of public key cryptography related to key distribution?**

**Encryption/decryption:** The sender encrypts a message with the recipient’s public key, and the recipient decrypts the message with the recipient’s private key.

**Digital signature:** The sender “signs” a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

**Key exchange:** Two sides cooperate to exchange a session key, which is a secret key for symmetric encryption generated for use for a particular transaction (or session) and valid for a short period of time.

Some algorithms are suitable for all three applications, whereas others can be used only for one or two of these applications.

**Define Stream Cipher. Write the specific function of MAC in network security.**

A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. Examples of classical stream ciphers are the auto-keyed Vigenère cipher and the Vernam cipher.

**MAC IN NS**

Typically, MACs are used between two parties that share a secret key to authenticate information exchanged between those parties.

- A MAC function takes as input a secret key and a data block and produces a hash value, referred to as the MAC, which is associated with the protected message.

- If the integrity of the message needs to be checked, the MAC function can be applied to the message and the result compared with the associated MAC value.

**List out the two methods of operation in AH and ESP.**

**Transport Mode:** Transport mode, the default mode for IPSec, provides for end-to-end security. It can secure communications between a client and a server. When using the transport mode, only the IP payload is encrypted. AH or ESP provides protection for the IP payload.

**Tunnel Mode:** Tunnel Mode means that one outgoing IP packet is encapsulated in another packet with typically a different IP destination.

**What is the role of compression function in hash function? What is the difference between weak and strong collision resistance?**

A compression function takes a fixed-length input and returns a shorter, fixed-length output.

Given a compression function, a hash function can be defined by repeated applications of the compression function until the entire message has been processed.

In this process, a message of arbitrary length is broken into blocks whose length depends on the compression function, and “padded” (for security reasons) so the size of the message is a multiple of the block size. The blocks are then processed sequentially, taking as input the result of the hash so far and the current message block, with the final function.

**WEAK AND STRONG COLLISION**

For any given value of h, it is computationally infeasible to find y = x with H(y) = H(x). This is “weak collision resistance.” It is easy to generate a code from a given message but almost impossible to do the reverse.

It is computationally infeasible to find any pair (x, y) such that H(x) = H(y). This is “strong collision resistance.” This guarantees that an alternative message hashing to the same values as given message can’t be found. This prevents forgery.

**For the following assets, assign a low, moderate or high impact level for the loss of confidentiality, availability, and integrity respectively. Justify your answers:**

1. **An organization managing public information on its web servers**
2. **A law enforcement organization managing extremely sensitive investigative information**
3. **Financial organization managing routine administrative information (not privacy related information)**

**(i) Confidentiality:**

Web server contains the public information. So everyone can access that information.

So there is no confidentiality is provided.

So impact of confidentiality level is low

**Integrity:**

Server maintains public information. So there may be anyone can modify that is either authorized user or intruder.

So impact of integrity level is moderate.

**Availability:**

Loss of information is not a biggest issue in this server.

So impact of availability level is moderate.

**(ii)**

**Confidentiality:**

Web server contains the sensitive information.

If any of data loss is occurred then it gives high loss.

So impact of the confidentiality level is high.

**Integrity:**

Server maintains private information.

If any modifications occurred it gives huge loss.

So impact of integrity level is high.

**Availability:**

Information is only available to organization that is stored at a single location.

So impact of availability level is high.

**(iii)**

**Confidentiality:** Web server contains only routine information not privacy related information.

So everyone can access that information.

So there is no confidentiality is provided.

So impact of confidentiality level is low

**Integrity:**

Server maintains routine information.

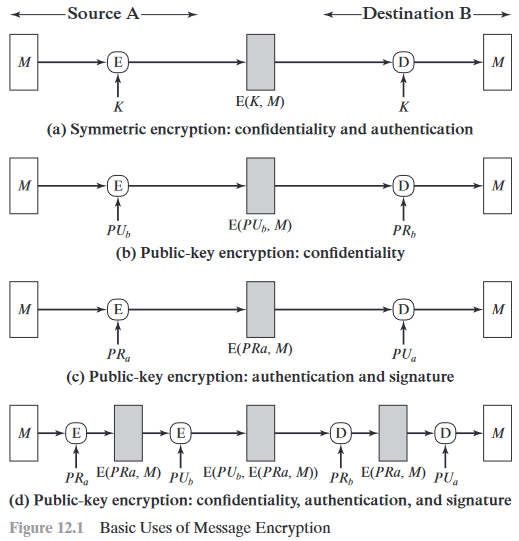
If data loss is occurred, it is not a big issue.

So impact of integrity level is low.

**Availability:**

Loss of information is not a biggest issue in this server.

So impact of availability level is low.

**Consider the straightforward use of symmetric encryption. A message M is transferred from source A to destination B is encrypted using keys? Complete the blank spaces and also identify which type of functions are performed. (Authentication, Confidentiality, Signature etc.)**

**List and briefly define categories of passive and active attacks. List and briefly define the categories of security services.**

**Passive Attacks**

- A passive attack attempts to learn or make use of information from the system but does not affect system resources.

Two types of passive attacks are the **release of message contents** and **traffic analysis**.

- The **release of message contents** is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

- A second type of passive attack, **traffic analysis**, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message.

**Active Attacks**

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

- A masquerade takes place when one entity pretends to be a different entity.

- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

- Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

- The denial of service prevents or inhibits the normal use or management of communications facilities.

**Security Services**

ACCESS CONTROL: The prevention of unauthorized use of a resource.

AUTHENTICATION: The assurance that the communicating entity is the one that claims to be.

DATA CONFIDENTIALITY: The protection of data from unauthorized disclosure.

DATA INTEGRITY: The assurance that the data received are exactly as sent by an authorized entity.

NONREPUDIATION: Provide protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

**Describe the MD5 algorithm with necessary block diagram.**

**STEP 01: APPEND PADDING BITS**

The message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512

**Padding is performed as follows:**

* a single "1" bit is appended to the message, and
* then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448, modulo 512.
* In all, at least one bit and at most 512 bits are appended.

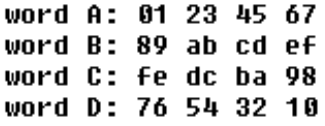
**STEP 02: APPEND LENGTH**

* A 64-bit representation of b is appended to the result of the previous step.
* In the unlikely event that b is greater than 2^64, then only the low-order 64 bits of b are used.

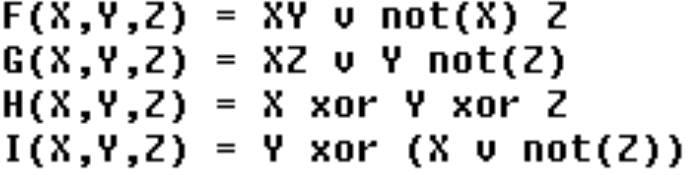
**STEP 03: INITIALIZE MD BUFFER**

* A four-word buffer (A,B,C,D) is used to compute the message digest.

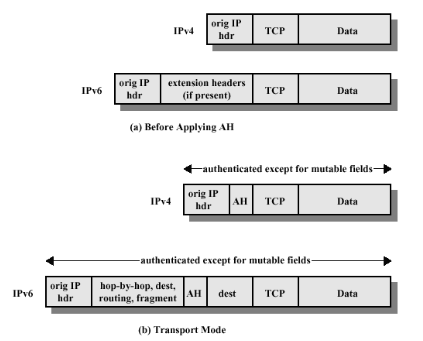
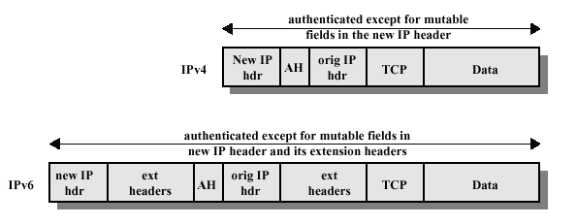
Here each of A, B, C, D is a 32-bit register.

* These registers are initialized to the following values in hexadecimal, low-order bytes first:

**STEP 04: PROCESS MESSAGE IN 16-WORD BLOCK (4 ROUNDS)**

Four functions will be defined such that each function takes an input of 32 bit words and produces 32 bit word output.

**Explain very briefly how transport and tunnel mode operations operates on AH packets for IPv4. Support your answer using AH packets figures for tunnel and transport mode of operations.**

****

**Transport Mode:** Transport mode, the default mode for IPSec, provides for end-to-end security. It can secure communications between a client and a server. When using the transport mode, only the IP payload is encrypted. AH or ESP provides protection for the IP payload.

**Tunnel Mode:** Tunnel Mode means that one outgoing IP packet is encapsulated in another packet with typically a different IP destination

**Consider an automated teller machine in which users provide a personal identification number and a card for account access. Give examples of confidentiality, integrity and availability requirements associated with the system. In each case indicate the degree of importance for the requirement.**

CONFIDENTIALITY: Personal Identification Number (PIN) is an asset whose confidentiality is considered to be highly important by an individual. PIN information should only be available to individual. DOI 🡪 High

INTEGRITY: An individual should be able to trust that the card provided for account access is current and correct. And an individual should be able to withdraw amount she wishes to and from her available account. Now suppose bank staff is authorized to view and update individuals account deliberately falsifies the data in it. Integrity is lost. DOI 🡪 High

AVAILABILITY: ATM provides a way for individuals to withdraw money whenever and from wherever they want. Therefore, an individual should be able to withdraw money from ATM (i.e. ATM should always be available for withdrawal) provided s/he has PIN and Card for account access. However, this is the facility provided by banks to facilitate its customer for easy access to their bank account. This is not critical component of the banks information system, but unavailability of this service will cause some embarrassment to the customer. DOI 🡪 Moderate.

**ABBREVIATION**

|  |  |
| --- | --- |
| **RSA** | Rivest, Shamir, Adleman |
| **DES** | Data Encryption Standard |
| **AES** | Advanced Encryption Standard |
| **IKE** | Internet Key Exchange |
| **CHAP** | Challenge Handshake Authentication Protocol |
| **AAA** | Authentication, Authorization, & Accounting |
| **CSPRNG** | Cryptographically Secure Pseudocode Random Number Generator |
| **L2TP** | Layer 2 Tunneling Protocol |
| **MAC** | Message Authentication Code |
| **SSL** | Secure Socket Layer |
| **IP** | Internet Protocol |
| **PKS** | Public Key Schemes |
| **MD5** | Message Digest 5 |
| **ESP** | Encapsulating Security Payload |
| **SNMP** | Simple Network Management Payload |

**CS 2013:**

**Describe the types of vector attacks**

The method or way by an adversary can breach or infiltrate an entire network/system. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

**1. Compromised Credentials**

1. Compromised credentials describe a case where user credentials, such as usernames and passwords, are exposed to unauthorized entities. This typically happens when unsuspecting users fall prey to phishing attempts and enter their login credentials on fake websites.

2. Malicious Insiders

A malicious insider is an employee who exposes private company information and/or exploits company vulnerabilities.

3. Misconfiguration

Misconfiguration is when there is an error in system configuration. For example, if setup pages are enabled or a user uses default usernames and passwords, this can lead to breaches.

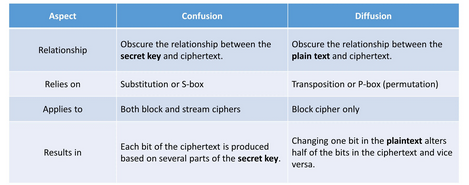
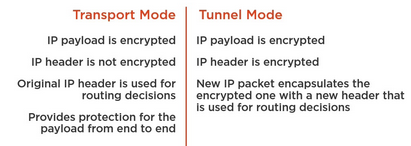
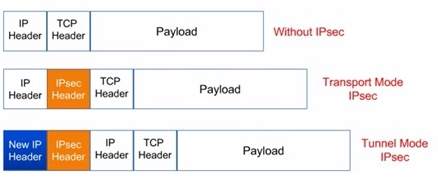
4. Ransomware

Ransomware is a form of cyber-extortion in which users are unable to access their data until a ransom is paid.

5. Phishing

Phishing is a cybercrime tactic in which the targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

**Differentiate between the following:**

1. **Confusion and Diffusion**
2. **Transport mode and Tunnel mode**
3. **Public Key Authority and Public Key Certificate**

|  |  |
| --- | --- |
| **Public Key Authority** | **Public Key Certificate** |
| It maintains a greater degree of security. | It is also known as digital signature or identity certificate. |
| It maintains a directory for each and every participant. | It is an electronic document used to prove the ownership of a key. |

**Give reason for two of the following:**

1. **Fabrication is an active attack.**

Yes, fabrication is an active attack. Active attacks are the attacks in which the attacker tries to modify the information or creates a false message.

Fabrication causes Denial of Service (DOS) attacks in which attacker strive to prevent licit users from accessing some services, which they are permitted to or in simple words the attacker gain access to the network and then lock the authorized user out.

1. **A New IP header is added to the packet IP Sec Tunnel Mode.**

Tunnel Mode means that one outgoing IP packet is encapsulated in another packet with typically a different IP destination and which is then enclosed in a new IP header for the identification of the particular packet.

**Step of MD5?**

STEP 01: Append Padding bits

STEP 02: Append Length

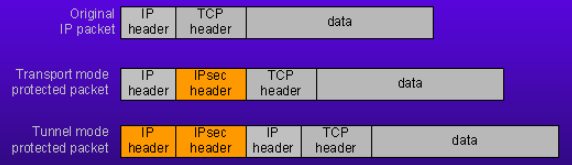
STEP 03: Initialize MD Buffer

STEP 04: Process Message in 16 word block

STEP 05: Output

**Transport and Tunnel mode and Draw their packet diagrams.**

**Transport Mode:** Transport mode, the default mode for IPSec, provides for end-to-end security. It can secure communications between a client and a server. When using the transport mode, only the IP payload is encrypted. AH or ESP provides protection for the IP payload.

**Tunnel Mode:** Tunnel Mode means that one outgoing IP packet is encapsulated in another packet with typically a different IP destination

**What happens if a router is under attack? What are the consideration to take or avoid/defend?**

* Hackers Can Steal Your Data — Once a hacker is in, they pretty much have free range to steal what data they want.
* You Could Be the Target of DNS Hijacking — Hackers can also perform something called DNS hijacking, which is a DNS attack that involves rerouting users to websites they weren’t intending to go to.
* You May Find Yourself on the Receiving End of Malware & DDoS Attacks — Hackers could inject malicious code snippets (malware), which could compromise your entire home network, or use your router in a DDoS attack (distributed denial of service).

Considerations to take:

Step 1 — Disconnect from The Internet

Step 2 — Reset Your Router

Step 3 — Change Your Passwords

**CS 2018:**

**Write about a few major applications of cryptography in the modern world.**

Secure communications: The most obvious use of cryptography, and the one that all of us use frequently, is encrypting communications between us and another system. This is most commonly used for communicating between a client program and a server.

Time Stamping: Time stamping is a technique that can certify that a certain electronic document or communication existed or was delivered at a certain time. Time stamping uses an encryption model called a blind signature scheme.

Anonymous Remailers: A remailer is a free service that strips off the header information from an electronic message and passes along only the content.

Storing Data: We all store a large amount of data, and any data is valuable to at least the person who generated it. Every operating system uses encryption in some of the core components to keep passwords secret, conceal some parts of the system, and make sure that updates and patches are really from the maker of the system

**What the prime objectives of modern cryptography are?**

The Main Goals of cryptography:

* Data Privacy(confidentiality)
* Data Authenticity(it came from where it claims)
* Data integrity(it has not been modified on the way) in the digital world

**What is meant by one-way property in hash function? Why is it so hard to generate an MD5 collision?**

A hash function H is said to be one-way if it is hard to invert, where ``hard to invert'' means that given a hash value h, it is computationally infeasible to find some input x such that H(x) = h.

Multiple messages can produce the same MD5 hash. When this happens, it is called a "hash collision." The algorithm is designed so that a collisions are unlikely, especially on similar messages with only a few bytes changed. You can't "decrypt" an MD5 since a lot of information is lost in producing a message digest

**Is there a size limit to the length of the string passed to an MD5 function?**

You can have any length, but of course, there can be a memory issue on the computer if the String input is too long. The output is always 32 characters. The algorithm has been designed to support arbitrary input length.

**What is the difference between encryption and hashing?**

|  |  |
| --- | --- |
| **Encryption** | **Hashing** |
| Encryption is the process of encoding a message or information in such a way that only authorized parties can access it. | Hashing is the process of using hash functions on data to map it to a fixed size numerical output. |
| Encryption uses encryption algorithms and a key to convert the message to transmit into an unrecognizable format. | Hashing converts the data to message digest or hash, which is a number generated from a string of text |
| The objective of encryption is to transmit data securely. | The objective of using hashing is to verify data |
| Encryption is used for transferring sensitive business information, etc. | Hashing is used for sending passwords, files and for searching. |
| C4, AES, DES, 3DES are some Symmetric Encryption algorithms. Diffie-Hellman and RSA algorithm are some Asymmetric Encryption algorithms. | MD5, SHA1 and SHA-256 are some hashing functions. |

**Distinguish between passive and active attacks. SE 2014**