**ASSIGNMENT QUESTIONS**

1. **Explain Diffie-Hellman Key Exchange algorithm?**

**Introduction to Diffie Hellman Key Exchange Algorithm**

Diffie Hellman key exchange Algorithms is developed by Whitefield Diffie and Martin Hellman in 1976 to overcome the problem of key agreement and exchange. It enables the two parties who want to communicate with each other to agree on symmetric key, key can be used for encrypting and decryption, note that Diffie Hellman key exchange algorithm can be used for only key exchange not for encryption and decryption process. The algorithm is based on mathematical principles.

**Diffie Hellman Key Exchange Algorithm for Key Generation**

The algorithm is based on Elliptic Curve Cryptography which is a method of doing public-key cryptography based on the algebra structure of elliptic curves over finite fields. The DH also uses the trapdoor function just like many other ways to do public-key cryptography. The simple idea of understanding to the DH Algorithm is the following

1. The first party picks two prime numbers g and p and tells them to the second party.

2. The second party then picks a secret number (let’s call it a) and then it computes gamod p and sends the result back to the first party, let’s call the result A. Keep in mind that the secret number is not sent to anyone, only the result is.

3. Then the first party does the same, it selects a secret number b and calculates the result B similor to the

4. step 2. Then, this result is sent to the second party.

5. The second party takes the received number B and calculates Bamod p

6. The first party takes the received number A and calculates Ab mod p

1. This is where it gets interesting, the answer in step 5 is the same as the answer in step 4. This means both parties will get the same answer no matter the order of exponentiation.
2. (ga *mod* p)b *mod* p = gab *mod* p  
   (gb *mod* p)a *mod* p = gba *mod* p
3. The number we came within steps 4 and 5 will be taken as the shared secret key. Now this key can be used to do any encryption of data that will be transmitted such as blowfish, [AES](https://www.educba.com/advanced-encryption-standard/), etc.

**Diffie Hellman Algorithm**

1. key =(YA)XBmod q -> this is the same as calculated by B

2. Global Public Elements

* Select a Private key XB    Here, XB<q
* Now, Calculation of Public key YBYB = aXb mod q

5. Calculation of Secret Key by A

* key =(YB)XAmod q

6. Calculation of Secret Key by B

* key =(YA)XBmod q

**Example**

1. Alice and Bob both use public numbers P = 23, G = 5

2. Alice selected private key a = 4 and Bob selected b = 3 as the private key

3. Both, Alice and bob now calculate the value of x and y as follows:

* Alice:    x = (54 mod 23) = 4
* Bob:    y = (53 mod 23) = 10

4. Now, both Alice and Bob exchange public numbers with each other.

5. Alice and Bob now calculate the symmetric keys

* Alice: ka = ya mod p = 104 mod 23 = 18
* Bob: kb = xb mod p = 43 mod 23 = 18

6. 18 is the shared secret key.

**2.** Explain RSA algorithm with example?

**Introduction to RSA Algorithm**

RSA algorithm is the most popular asymmetric key cryptographic algorithm based on the mathematical fact that it is easy to find and multiply large prime numbers but difficult to factor their product. It uses both private and public key (Keys should be very large prime numbers). Mathematical research suggests that if the value of keys is 100 digit number, then it would take more than 70 years for attackers to find the value of keys. The real challenge in RSA algorithm is to choose and generate the public and private keys.

**Working of RSA Algorithm**

Working of RSA algorithm is given as follows:

**Step 1:** Choose any two large prime numbers to say A and B.

**Step 2:** Calculate N = A \* B.

**Step 3**: Select public key says E for encryption. Choose the public key in such a way that it is not a factor of (A – 1) and (B – 1).

**Step 4:** Select private key says D for decryption. Choose the private key in such a way that it matches the below-mentioned equation

(D \* E) mod (A – 1) \* (B – 1) = 1.

**Step 5:** For encryption calculate the cipher text from the plain text using the below-mentioned equation

CT = PT^E mod N

**Step 6:** Send the cipher text to the receiver.

**Step 7:** For decryption calculate the plain text from the Cipher text using the below-mentioned equation

PT = CT^D mod N.

**Example of RSA algorithm**

Here I have taken an example from an Information technology book to explain the concept of the RSA algorithm.

**Step 1:** In this step, we have to select prime numbers.

suppose A is 7 and B is 17

**Step 2:** Calculate N

N = A \* B

N = 7 \* 17

N = 119

**Step 3:** Select public key such that it is not a factor of f (A – 1) and (B – 1).

= (7 – 1) \* (17 – 1)

= 6 \* 16

= 96

factor of 96 is 2 \* 2 \* 2 \* 2 \* 2 \*3

So here we select encryption key E as 5 because it is not a factor of both 2 and 3.

**Step 4:** Select private key in such way that it match following equation

(D \* E) mod (A – 1) \* (B – 1) = 1.

(D \* 5) mod (7 – 1) \* (17 – 1) = 1

(D \* 5) mod (6) \* (16) = 1.

(D \* 5) mod 96 = 1

After some mathematical computation, i have select D as 77

( 77 \* 5) mod 96 = 1.

385 mod 96 = 1

1 = 1

Hence the equation is equal.

**Step 5:** Calculate cipher text

let’s take plain text as 10

CT = PT^E mod N

CT = 10^5 mod 119

CT = 100000 mod 119

CT = 40

**Step 6:** send cipher text to the receiver.

**Step 7:** calculate plain text

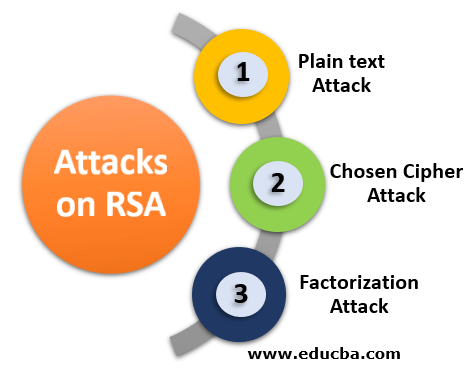
PT = CT^D mod N.

PT = 40^77 mod 119.

PT = 10 which is the original plain text.

**Attacks on RSA**

Below is the list of some possible attacks on RSA algorithm:



**1. Plain text Attack**

Plain text attacks are classified into three categories

* **Short message attack:** In this type of attack, the assumption is that the attacker knows some blocks of the plain text message. If an attacker knows some block of plain text, then he could try to encrypt the blocks of plain text using the information and try to convert it into cipher text. To prevent a short message attack, we can use the [padding bits for encryption](https://www.educba.com/what-is-encryption/).
* **Cycling attack:** In cycling attack, the reverse process is done. An attacker assumes that the ciphertext is formed using some permutations operations. If the attacker assumption becomes true, then he can try the reverse process to obtain the plain text from the cipher text.
* **Unconcealed message attack:** In some rare cases, it is found that some encrypted cipher text is the same as the plain text i.e original text. This means that the plain text is not hidden. Such type of attack is called an unconcealed message attack

**2. Chosen cipher Attack**

In this type of attack, the attacker can find out the plain text from cipher text using the extended euclidean algorithm.

**3. Factorization Attack**

In factorization Attack, the attacker impersonates the key owners, and with the help of the stolen cryptographic data, they decrypt sensitive data, bypass the security of the system. This attack occurs on An RSA cryptographic library which is used to generate RSA Key. By doing this, Attackers can have the private keys of n number of security tokens, smartcards, Motherboard Chipsets by having a target’s public key.

3. Explain E-Mail Security**--** Pretty Good Privacy

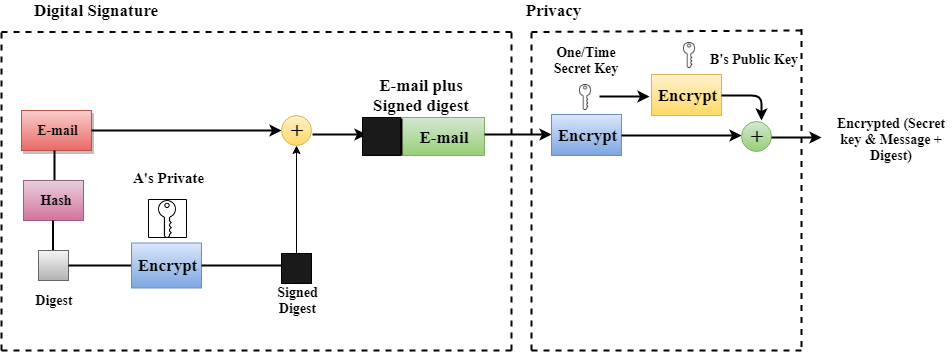
PGP

* PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
* PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
* PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
* PGP is an open source and freely available software package for email security.
* PGP provides authentication through the use of Digital Signature.
* It provides confidentiality through the use of symmetric block encryption.
* It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

Following are the steps taken by PGP to create secure e-mail at the sender site:

* The e-mail message is hashed by using a hashing function to create a digest.
* The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
* The original message and signed digest are encrypted by using a one-time secret key created by the sender.
* The secret key is encrypted by using a receiver's public key.
* Both the encrypted secret key and the encrypted combination of message and digest are sent together.

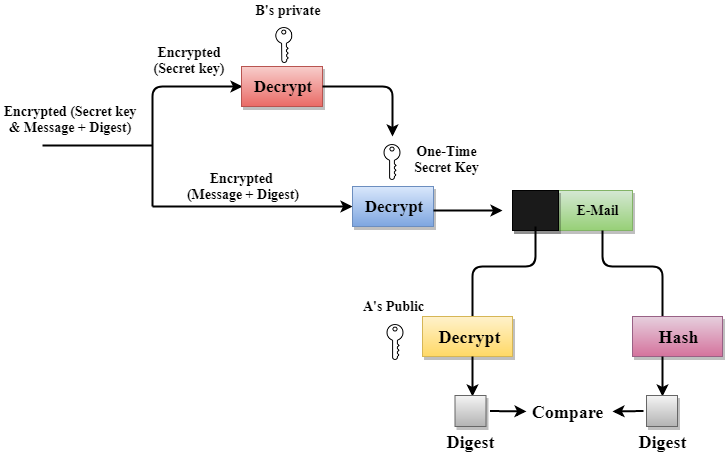
PGP at the Sender site (A)



Following are the steps taken to show how PGP uses hashing and a combination of three keys to generate the original message:

* The receiver receives the combination of encrypted secret key and message digest is received.
* The encrypted secret key is decrypted by using the sender's private key to get the one-time secret key.
* The secret key is then used to decrypt the combination of message and digest.
* The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
* Both the digests are compared if both of them are equal means that all the aspects of security are preserved.

PGP at the Receiver site (B)



Disadvantages of PGP Encryption

* **The Administration is difficult:** The different versions of PGP complicate the administration.
* **Compatibility issues:** Both the sender and the receiver must have compatible versions of PGP. For example, if you encrypt an email by using PGP with one of the encryption technique, the receiver has a different version of PGP which cannot read the data.
* **Complexity:** PGP is a complex technique. Other security schemes use symmetric encryption that uses one key or asymmetric encryption that uses two different keys. PGP uses a hybrid approach that implements symmetric encryption with two keys. PGP is more complex, and it is less familiar than the traditional symmetric or asymmetric methods.
* **No Recovery:** Computer administrators face the problems of losing their passwords. In such situations, an administrator should use a special program to retrieve passwords. For example, a technician has physical access to a PC which can be used to retrieve a password. However, PGP does not offer such a special program for recovery; encryption methods are very strong so, it does not retrieve the forgotten passwords results in lost messages or lost files.

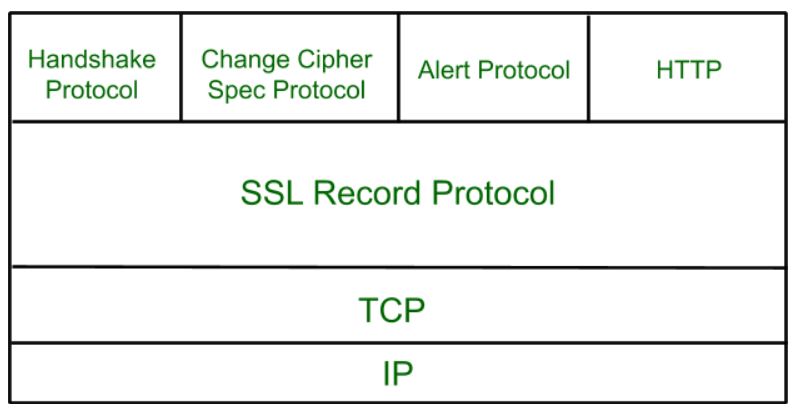
1. Explain Secure Socket Layer (SSL)?

[Secure Socket Layer (SSL)](https://practice.geeksforgeeks.org/problems/what-is-ssl) provide security to the data that is transferred between web browser and server. SSL encrypt the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

**Secure Socket Layer Protocols:**

* SSL record protocol
* Handshake protocol
* Change-cipher spec protocol
* Alert protocol

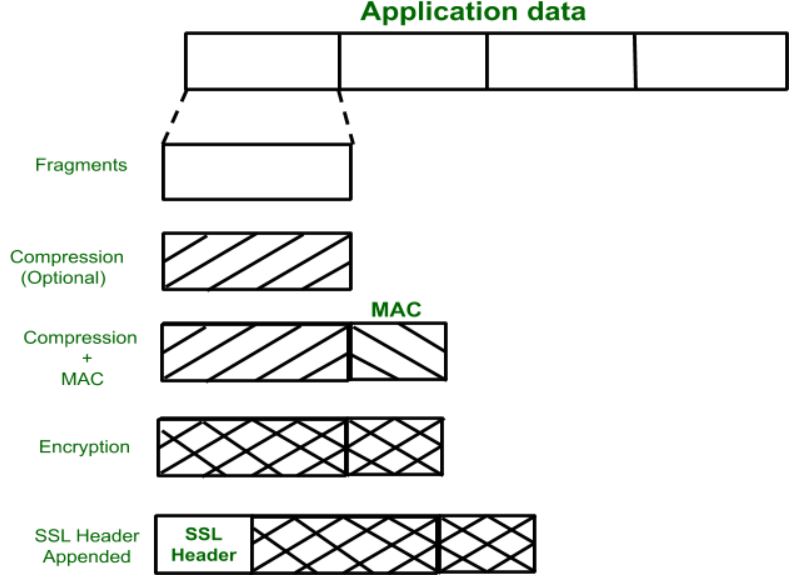
**SSL Protocol Stack:**



**SSL Record Protocol:**  
SSL Record provide two services to SSL connection.

* Confidentiality
* Message Integerity

In SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.



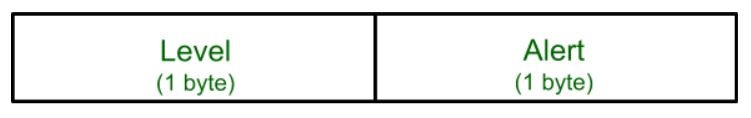
**Handshake Protocol:**  
Handshake Protocol is used to establish sessions. This protocol allow client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

* **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purpose.
* **Phase-2:** Server send his certificate and Server-key-exchange. Server end the phase-2 by sending Server-hello-end packet.
* **Phase-3:** In this phase Client reply to the server by sending his certificate and Client-exchange-key.
* **Phase-4:** In Phase-4 Change-cipher suite occurred and after this Handshake Protocol ends.

**Change-cipher Protocol:**  
This protocol uses SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in pending state. After handshake protocol the Pending state is converted into Current state.  
Change-cipher protocol consists of single message which is 1 byte in length and can have only one value. This protocol purpose is to cause the pending state to be copied into current state.



**Alert Protocol:**  
This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contain 2 bytes.



Level is further classified into two parts:

* **Warning:**  
  This Alert have no impact on the connection between sender and receiver.
* **Fatal Error:**  
  This Alert breaks the connection between sender and receiver.

**Silent Features of Secure Socket Layer:**

* Advantage of this approach is that the service can be tailored to the specific needs of the given application.
* Secure Socket Layer was originated by Netscape.
* SSL is designed to make use of TCP to provide reliable end-to-end secure service.
* This is two-layered protocol.

5. What is Firewall and List and explain different types of firewalls in detail?

The firewall acts as a guard. It guards a corporate network acting as a shield between the inside network and the outside world. All the traffic in either direction must pass through the firewall. It then decides whether the traffic is allowed to flow or not. The firewall can be implemented as hardware and software, or a combination of both. // The standard firewall definition shows that firewalls are systems that are put in place to provide [network security](https://www.extnoc.com/blog/network-security-checklist-for-businesses/). It does this by filtering any network traffic – both in and out – based on rules defined by the user. They reduce and in some cases, eliminate the occurrence of unwanted communications in the network, and at the same time, allow any genuine communication and information to flow in and out freely. Firewalls aren’t an option – they are essential for any business. They work hard to prevent attackers from accessing your servers and data maliciously.//



**Types of Firewalls:**

1. **Packet Filters –**  
   It works in the **network layer** of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.

For example, a rule could specify to block all incoming traffic from a certain IP address or disallow all traffic that uses UDP protocol. If there is no match with any predefined rules, it will take default action. The default action can be to ‘discard all packets’ or to ‘accept all packets’.

**Security threats** to Packet Filters:

* 1. **IP address Spoofing:**  
     In this kind of attack, an intruder from the outside tries to send a packet towards the internal corporate network with the source IP address set equal to one of the IP address of internal users.  
     **Prevention:**  
     Firewall can defeat this attack if it discards all the packets that arrive at the incoming side of the firewall, with source IP equal to one of the internal IPs.
  2. **Source Routing Attacks:**  
     In this kind of attack, the attacker specifies the route to be taken by the packet with a hope to fool the firewall.  
     **Prevention:**  
     Firewall can defeat this attack if it discards all the packets that use the option of source routing aka path addressing.
  3. **Tiny Fragment Attacks:**  
     Many times, the size of the IP packet is greater than the maximum size allowed by the underlying network such as Ethernet, Token Ring etc. In such cases, the packet needs to be [fragmented](https://www.geeksforgeeks.org/fragmentation-network-layer/), so that it can be carried further. The attacker uses this characteristic of TCP/IP protocol. In this kind of attack, the attacker intentionally creates fragments of the original packet and send it to fool the firewall.  
     **Prevention:**  
     Firewall can defeat this attack if it discards all the packets which use the TCP protocol and is fragmented. *Dynamic Packet Filters* allow incoming TCP packets only if they are responses to the outgoing TCP packets.

1. **Application Gateways –**  
   It is also known as **Proxy server**. It works as follows:
   1. **Step-1:** User contacts the application gateway using a TCP/IP application such as HTTP.
   2. **Step-2:** The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.
   3. **Step-3:** After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.
2. **Stateful Inspection Firewalls –**  
   It is also known as ‘Dynamic Packet Filters’. It keeps track of the state of active connections and uses this information to decide which packets to allow through it, i.e., it adapts itself to the current exchange of information, unlike the normal packet filters/stateless packet filters, which have hardcoded routing rules.
3. **Circuit-Level Gateways –**  
   It works at the **session layer** of the OSI Model. It is the advanced variation of *Application Gateway*. It acts as a virtual connection between the remote host and the internal users by creating a new connection between itself and the remote host. It also changes the source IP address in the packet and puts its own address at the place of source IP address of the packet from end users. This way, the IP addresses of the internal users are hidden and secured from the outside world.

Packet-Filtering Firewalls

This is the oldest firewall type out there. They are designed to create checkpoints at individual routers or switches. The packet-filtering firewalls will check the data packets that try to come through, without inspecting the contents. If the information trying to come through looks suspicious, it cannot get through the network. This is a simple firewall that does not impact network performance too much.

Circuit-Level Gateways

Circuit-level gateways are much like packet-filtering firewalls in that they quickly and easily check and approve or deny traffic. They do it without being heavy on resources, too. Circuit-level gateways work by verifying the transmission control protocol handshake. It doesn’t check the packet directly, so there is a risk of malware getting through. These are not the best ones to protect your business.

Stateful Inspection Firewalls

A combination of the two firewalls above, the stateful inspection firewalls offer a higher level of protection for your business. The problem with these is that they take up more resources, which can slow down the legitimate packet transfer.

Proxy Firewalls (Application-Level Gateways/Cloud Firewalls)

If you want firewalls that operate at the application layer to filter traffic, proxy firewalls do the job. These are cloud-based most of the time, and they establish traffic connections and examine data packets coming through. The difference between these and the stateful inspection firewalls is that the proxy firewalls can also do a more in-depth inspection to check the packet contents. The drawback to these is that they can create a [network slowdown](https://www.extnoc.com/blog/denying-the-true-cost-of-network-downtime/) because of all the extra steps – but it’s all in the name of the security for your business.

Next-Generation Firewalls

There’s no real insight into what makes a firewall today “next-generation” besides the time it was created. There are commonalities between these firewalls and the originals, and those include TCP handshakes and packet inspections. Next-generation firewalls also use IPS – intrusion prevention systems – to stop network attacks.

Software Firewalls

These are any firewalls installed on local devices. The biggest draw for these in that they can create a useful, in-depth defense path. Maintaining these on more than one device is not easy, though, so you may need more than one for each asset.

Hardware Firewalls

Hardware firewalls use physical appliances, and they act like a traffic router. The intercept data packets before they are connected to a network server. The weakness here is that they can be easily bypassed, which goes against your need for a firewall.

Cloud Firewalls

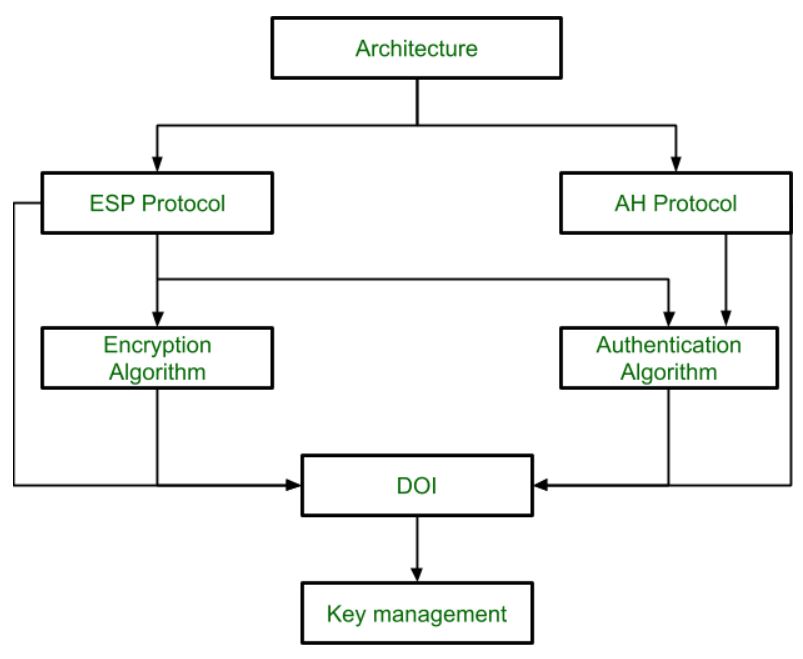
Cloud solutions are also called FaaS – firewalls as a service. They often go hand in hand with proxy firewalls, and the most significant benefit to these is that they grow with your business. They work to filter large amounts of traffic away from your company, where it’s malicious.

IPSec Architecture

**IPSec (IP Security) architecture** uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture include protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

* Confidentiality
* Authentication
* Integirity

**IP Security Architecture:**

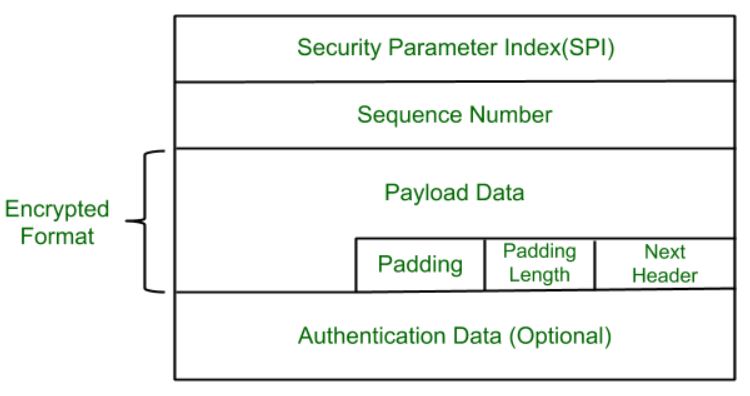


**1. Architecture:**  
Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms and security requirements of IP Security technology.

**2. ESP Protocol:**  
ESP(Encapsulation Security Payload) provide the confidentiality service. Encapsulation Security Payload is implemented in either two ways:

* ESP with optional Authentication.
* ESP with Authentication.

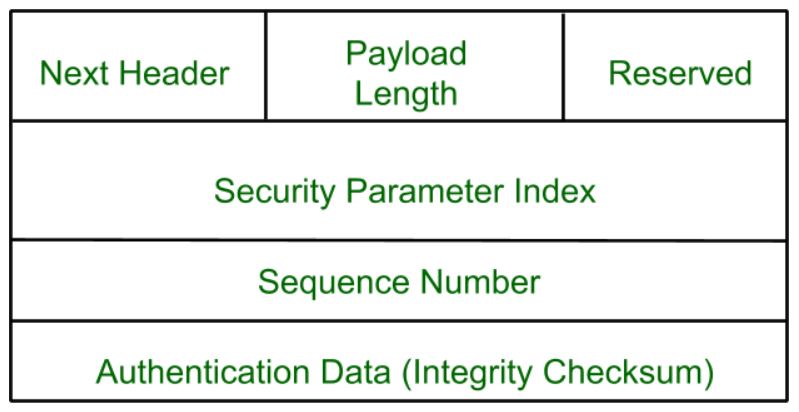
**Packet Format:**



* **Security Parameter Index(SPI):**  
  This parameter is used in Security Association. It is used to give a unique number to the connection build between Client and Server.
* **Sequence Number:**  
  Unique Sequence number are allotted to every packet so that at the receiver side packets can be arranged properly.
* **Payload Data:**  
  Payload data means the actual data or the actual message. The Payload data is in encrypted format to achieve confidentiality.
* **Padding:**  
  Extra bits or space added to the original message in order to ensure confidentiality. Padding length is the size of the added bits or space in the original message.
* **Next Header:**  
  Next header means the next payload or next actual data.
* **Authentication Data**  
  This field is optional in ESP protocol packet format.

**3. Encryption algorithm:**  
Encryption algorithm is the document that describes various encryption algorithm used for Encapsulation Security Payload.

**4. AH Protocol:**  
AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.



Authentication Header covers the packet format and general issue related to the use of AH for packet authentication and integrity.

**5. Authentication Algorithm:**  
Authentication Algorithm contains the set of the documents that describe authentication algorithm used for AH and for the authentication option of ESP.

**6. DOI (Domain of Interpretation):**  
DOI is the identifier which support both AH and ESP protocols. It contains values needed for documentation related to each other.

**7. Key Management:**  
Key Management contains the document that describes how the keys are exchanged between sender and receiver.