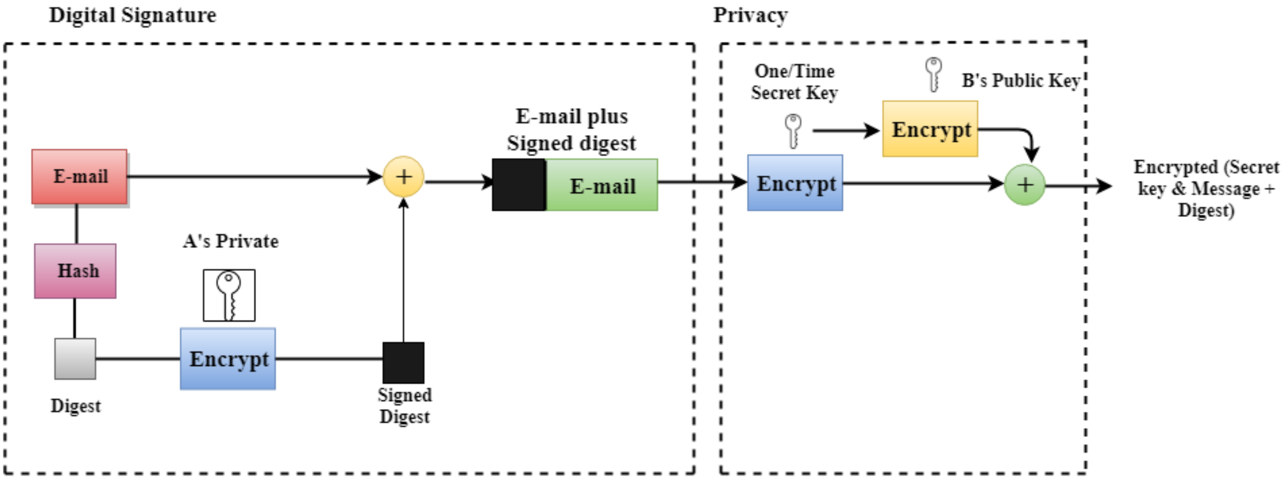
UNIT V

PGP (Pretty Good Privacy)

- 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.

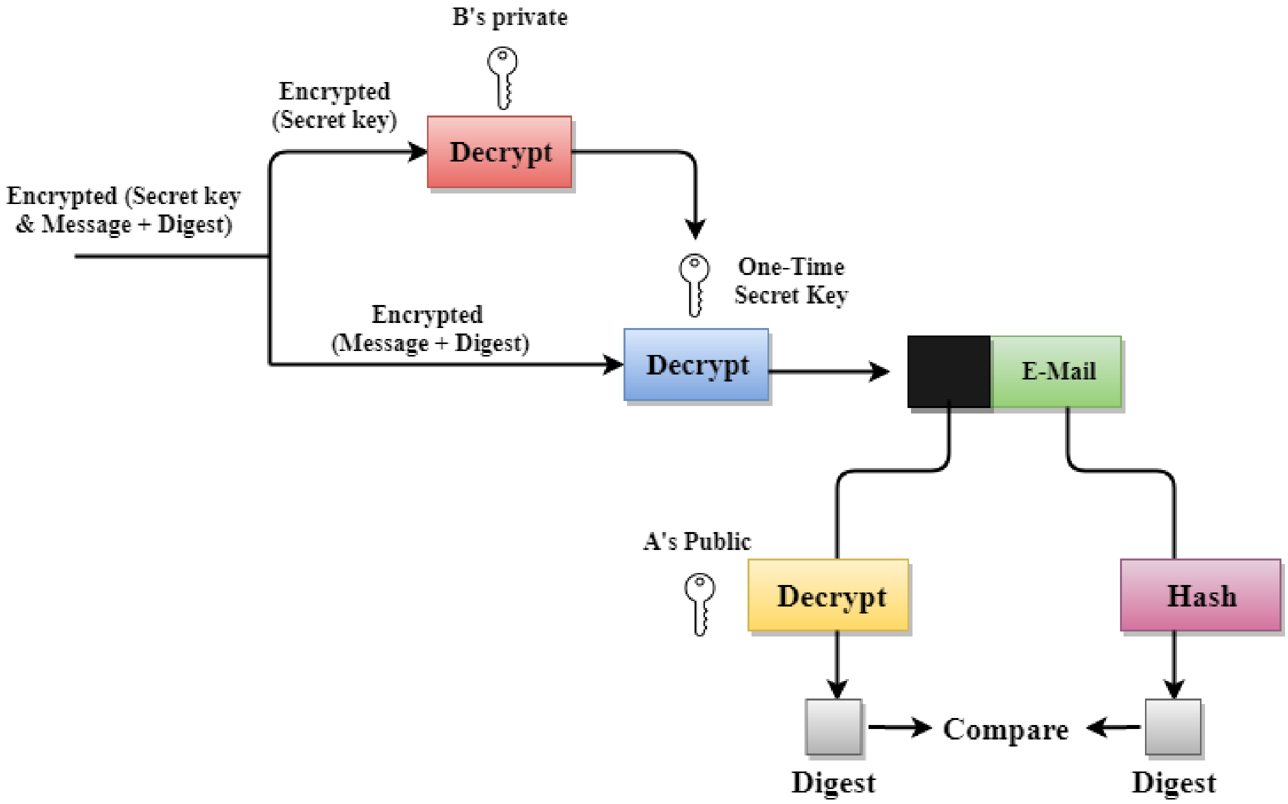


Following are the steps taken to show how PGP uses hashing and a combination of three keys to generate the original message:

- The receiver receives the combination of encrypted secret key and message digest is received.

- The encrypted secret key is decrypted by using the receiver'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)



What is IP Security (IPSec)?

IP Security (IPSec) refers to a collection of communication rules or protocols used to establish secure network connections. Internet Protocol (IP) is the common standard that controls how data is transmitted across the internet. IPSec enhances the protocol security by introducing encryption and authentication. IPSec encrypts data at the source and then decrypts it at the destination. It also verifies the source of the data. In this article we will see IPSec in detail.

Why is IPSec Important?

IPSec (Internet Protocol Security) is important because it helps keep your data safe and secure when you send it over the Internet or any network. Here are some of the important aspects why IPSec is Important:

- IPSec protects the data through Data Encryption.
- IPSec provides Data Integrity.
- IPSec is often used in Virtual Private Networks (**VPNs**) to create secure, private connections.
- IPSec protects from **Cyber Attacks**.

Features of IPSec

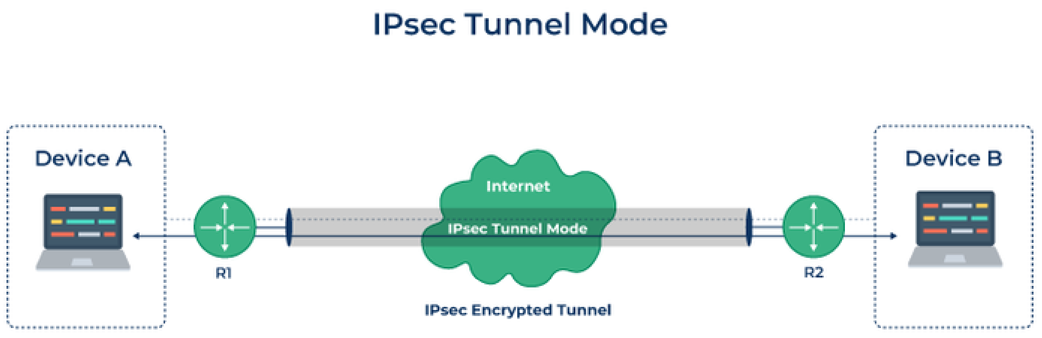
- **Authentication:** IPSec provides authentication of IP packets using **digital signatures** or shared secrets. This helps ensure that the packets are not tampered with or forged.
- **Confidentiality:** IPSec provides confidentiality by encrypting IP packets, preventing **eavesdropping** on the network traffic.
- **Integrity:** IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.
- **Key management:** IPSec provides key management services, including key exchange and key revocation, to ensure that cryptographic keys are securely managed.
- **Tunneling:** IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or **L2TP (Layer 2 Tunneling Protocol).**
- **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.

- **Interoperability:** IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

How Does IPSec Work?

IPSec (Internet Protocol Security) is used to secure data when it travels over the Internet. IPSec works by creating secure connections between devices, making sure that the information exchanged is kept safe from unauthorized access. IPSec majorly operates in two ways i.e. **Transport Mode** and **Tunnel Mode**.
To provide security, IPSec uses two main protocols: **AH (Authentication Header)** and **ESP (Encapsulating Security Payload)**. Both protocols are very useful as **Authentication Header** verifies the data that whether it comes from a trusted source and hasn't been changed, and **ESP** has the work of performing authentication and also encrypts the data so that it becomes difficult to read.
For Encryption, IPSec uses cryptographic keys. It can be created and shared using a process called **IKE (Internet Key Exchange)**, that ensures that both devices have the correct keys to establish a secure connection.

When two devices communicate using IPSec, the devices first initiate the connection by sending a request to each other. After that, they mutually decide on protection of data using **passwords** or **digital certificates**. Now, they establish the secure tunnel for communication. Once the tunnel is set up, data can be transmitted safely, as IPSec is encrypting the data and also checking the integrity of the data to ensure that data has not been altered. After the communication is finished, the devices can close the secure connection. In this way, the IPSec works.



Difference Between IPSec Tunnel Mode and IPSec Transport Mode

- **Tunnel:** The **IPSec tunnel mode** is appropriate for sending data over public networks because it improves data security against unauthorised parties. The computer encrypts all data, including the payload and header, and adds a new header to it.

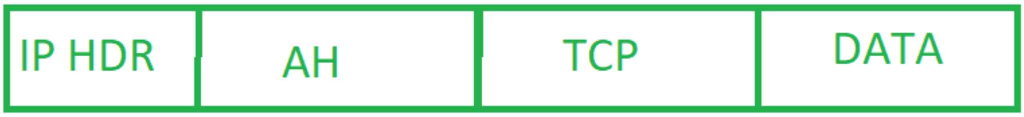
- **Transport:** **IPSec transport mode** encrypts only the data packet’s payload while leaving the IP header unchanged. The unencrypted packet header enables **routers** to determine the destination address of each data packet. As a result, IPSec transport is utilized in a closed and trusted network, such as to secure a direct link between two computers.

Protocols Used in IPSec

It has the following components:

- Encapsulating Security Payload (ESP)
- Authentication Header (AH)
- Internet Key Exchange (IKE)

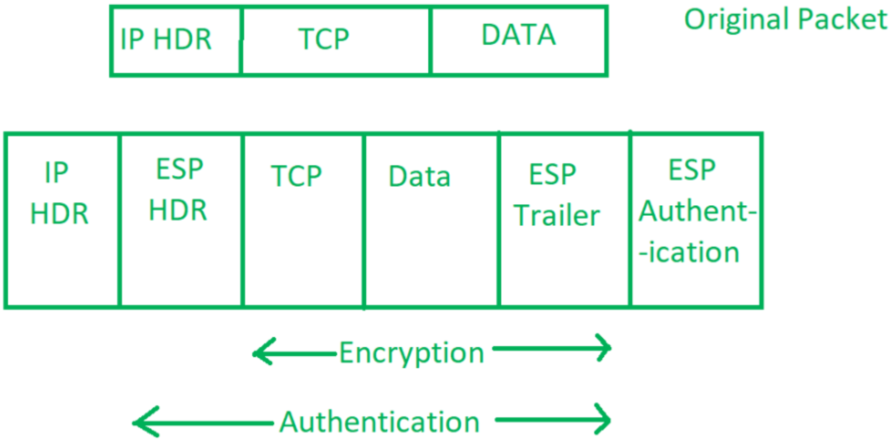
1. Encapsulating Security Payload (ESP): It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.
2. Authentication Header (AH): It also provides data integrity, authentication, and anti-replay and it does not provide encryption. The anti-replay protection protects against the unauthorized transmission of packets. It does not protect data confidentiality.



3.

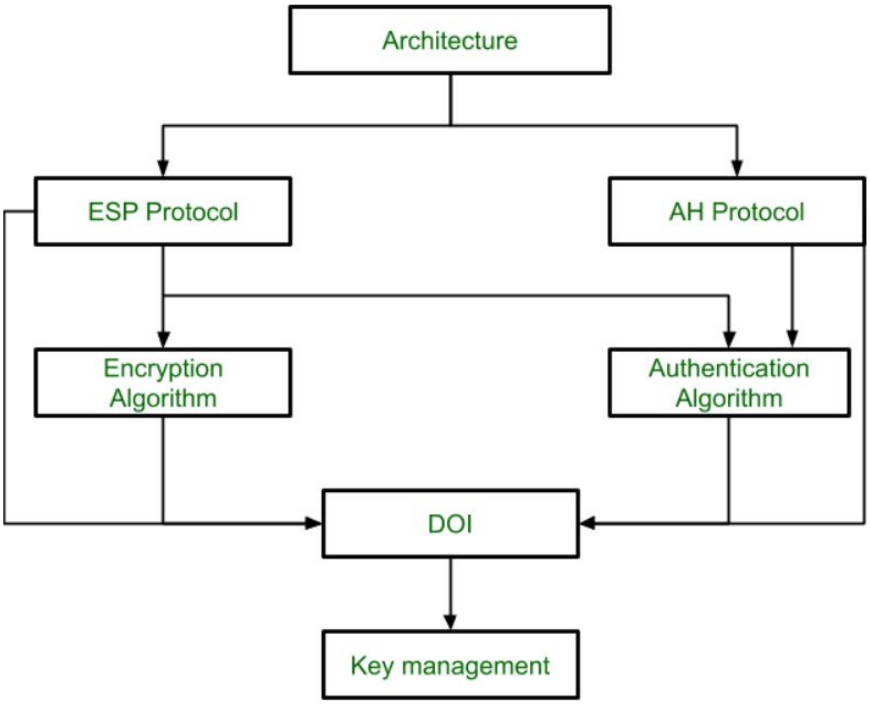
Internet Key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication.

IP Security 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 includes protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

- Confidentiality
- Authenticity
- Integrity



Advantages of IPSec

- **Strong security:** IPSec provides strong **cryptographic** security services that help protect sensitive data and ensure network privacy and integrity.

- **Wide compatibility:** IPSec is an open standard protocol that is widely supported by vendors and can be used in heterogeneous environments.
- **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including **point-to-point**, site-to-site, and remote access connections.
- **Scalability:** IPSec can be used to secure large-scale networks and can be scaled up or down as needed.
- **Improved network performance:** IPSec can help improve network performance by reducing network congestion and improving network efficiency.

ESP(Encapsulating Security Payload)

Encapsulating Security Payload (ESP) provides all encryption services in IPSec based on integrity for the payload and not for the IP header, confidentiality and authentication that using encryption, without authentication is strongly discouraged because it is insecure.

Any translations in readable message format into an unreadable format are encrypted and used to hide the message content against data tampering.

IPSec provides an open framework, such as SHA and MD5 for implementing industry standard algorithms.

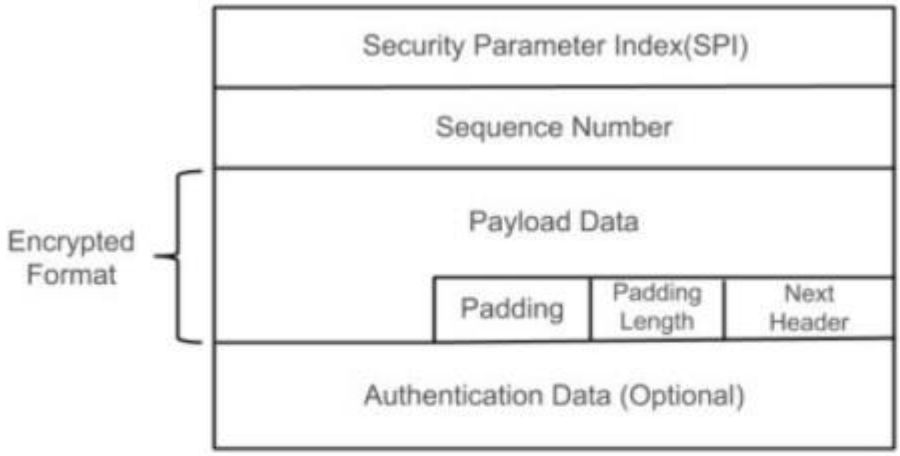
Encryption/decryption allows only the sender and the authorised receiver to make the data to be received in readable form and only after the integrity verification process is complete, the data payload in the packet is decrypted.

IPSec uses a unique identifier for each packet, which is a data equivalent of a fingerprint and checks for packets that are authorised or not. It doesn't sign the entire packet unless it is being tunnelled—ordinarily, for this IP data payload is protected, not the IP header. In Tunnel Mode, where the entire original IP packet is encapsulated with a new packet header added.

ESP in transport mode does not provide integrity and authentication for the entire IP packet.

ESP Format

The ESP format is diagrammatically represented as follows −



Explanation

Security Parameters Index (32 bits) − Identifies a security association. This field is mandatory. The value of zero is reserved for local, implementation- specific use and MUST NOT be sent on the wire.

Sequence Number (32 bits) − A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH. The first packet sent using a given SA will have a Sequence number of 1.

Payload Data (variable) − This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption. The type of content that was protected is indicated by the Next Header field.

Padding (0-255 bytes) − Padding for encryption, to extend the payload data to a size that fits the encryption's cipher block size, and to align the next field.

Pad Length (8 bits) − Indicates the number of pad bytes immediately preceding this field.

Next Header (8 bits) − Identifies the type of data contained in the payload data field by identifying the first header in that payload.

Authentication Data (variable) − A variable-length field (must be an integral number of 32-bit words) that contains the Integrity. Check Value computed over the ESP packet minus the Authentication Data field. This field is optional and is included only if the authentication service has been selected for the SA in question.

What is Secure Multiparty Computation?

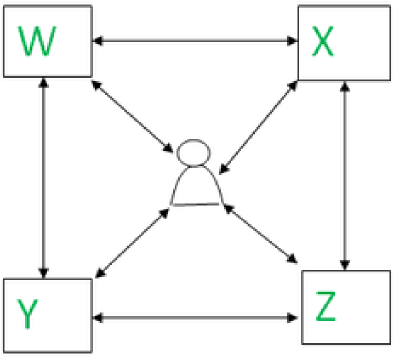
Data Security and privacy have grown to be everyone’s top worries over the past few decades. Data security and privacy in distributed networks have become a major concern with the growth of the internet and technology. By enabling partners to compute a function on their private inputs without disclosing them to third parties, Secure Multiparty Computation (SMPC) presents a viable solution to this problem.

What is Secure Multiparty Computation?

With the use of the cryptographic approach known as "secure multiparty computation," "n" parties can securely compute a function together without disclosing each other's unique inputs. This preserves data privacy while enabling computations and analysis. When privacy is important, whether in financial transactions, healthcare data, or personal information shared between various institutions, SMPC is used.

Architecture

The secure multiparty computation provides a protocol where no individual can see the other parties data while distributing the data across multi parties. It enables the data scientists and analysts to compute privately on the distributed data without exposing it.



The co-workers want to compute the maximum salary without revealing their salary to others. To perform such a computation, secure multiparty computation is implemented to calculate the maximum salary. The parties in a distributed manner jointly perform a function to calculate it without revealing the salary. Data in use is kept in encrypted form, broken up, and distributed across parties, there are no chances of quantum attacks. It is impossible to have a trusted party in the real world, as all parties communicate with each other in one or the other way In such a scenario, the parties may get corrupted. The corrupted parties have behavior like semi-honest and malicious.

1.A semi-honest opponent is one who follows the specified protocol but corrupts the parties corrupted. The protocol is run honestly, but they try to extract information from the messages exchanged between parties.

2.A malicious adversary attempts to breach security and does not follow the specified protocol. The adversary can make the changes during the execution process of the protocol. While using multiparty computation, we assume the party is honest and follows all the protocols.

In today's digital world, electronic transactions have become an integral part of our lives. Whether it's using a credit card, making a debit card payment, transferring money through UPI, or conducting online banking, we rely on these transactions for convenience and efficiency. However, with the increasing prevalence of online fraud and security threats, ensuring the safety of inter-branch payment transactions has become crucial.

Inter-branch payment transactions, also known as online transactions, involve the transfer of funds between different branches of the same bank or even between different banks. These transactions encompass a wide range of electronic payment methods, including credit cards, debit cards, net banking, mobile banking, and more.

2. What are Inter-branch Payment Transactions?

Inter-branch payment transactions refer to the transfer of funds between different branches of a bank or between different banks. These transactions can be conducted through various electronic payment methods such as credit cards, debit cards, net banking, and mobile banking. Whether it's making a purchase online, transferring money to another account, or paying bills electronically, all these transactions fall under the purview of inter-branch payment transactions.

Examples of Inter-branch Payment Transactions

To better understand inter-branch payment transactions, let's explore a few examples:

- Using a credit card to make a purchase on an e-commerce Website.
- Making a debit card payment at a retail store.
- Transferring money to another bank account using net banking.
- Conducting a mobile banking transaction through a banking app.

4. Importance of Secure Inter-branch Payment Transactions

Ensuring the security of inter-branch payment transactions is of utmost importance for several reasons:

1. Protection against Fraud: Secure transactions prevent unauthorized access and protect sensitive financial information, reducing the risk of fraudulent activities.
2. Customer Confidence: When customers feel secure during transactions, they are more likely to engage in online payments, boosting overall customer trust and satisfaction.
3. Streamlined Operations: Secure payment systems facilitate smooth and efficient transactions, improving operational processes for both banks and customers.