**Advanced Security Topics**

**Secure email systems**

**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.

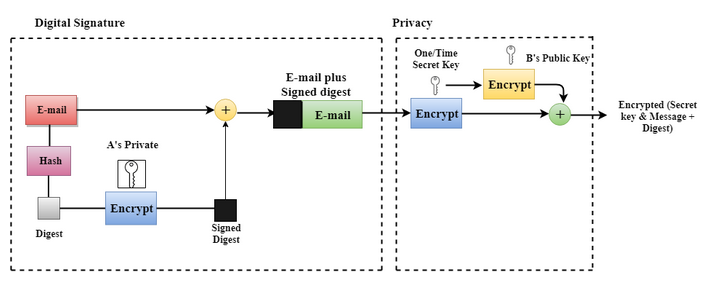
PGP provides authentication through the use of Digital Signature.

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

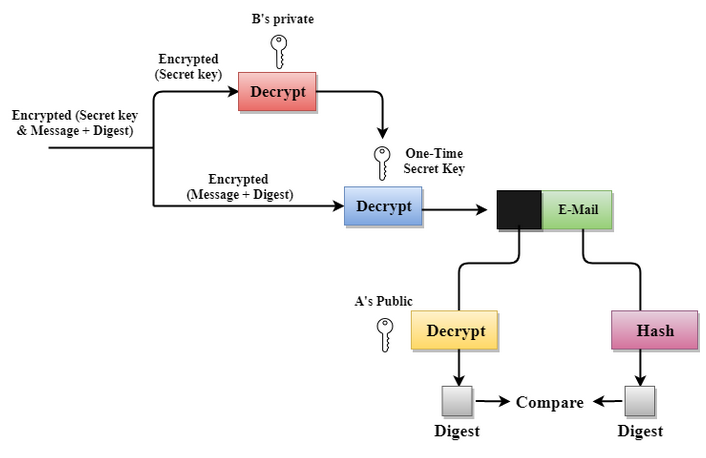
**Following are the steps taken by PGP to create secure e-mail at the sender site:**

* 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.



**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.



**Secure/Multipurpose Internet Mail Extensions (S/MIME)**

**Secure/Multipurpose Internet Mail Extensions (S/MIME)** is an end-end encryption protocol for sending digitally signed and encrypted emails that support data confidentiality, authenticity, and integrity.

To understand how S/MIME works we need to understand the following first:

* Digital signatures and signature verification
* Message encryption and decryption
* Public key
* Digital certificates

**Digital signatures and verification**

With digital signature, S/MIME verifies the identity of the sender of the email.

This verification ensures the following:

* Message in the email is the exact message sent by the sender.
* Message is received from the right sender and not someone pretending to be the sender.

**Message encryption and decryption**

S/MIME uses encryption to protect the content of the email, which ensures that only the receiver can decrypt the content.

Encryption creates coded information so that it cannot be read or understood until it is decoded and readable.

Message encryption helps with the two key security factors of confidentiality and data integrity.

**Public key**

S/MIME uses key pairs and asymmetric cryptography.

A private key in a key pair belongs only to the sender.

If the private key has been used, the owner of that key has used it.

Public key cryptography ensures secure communication between the sender and the receiver.

Both have a key-pair, with one being private and the other public​.

Public keys are shared between the sender and the receiver.

A public key is paired to only one private key.

The corresponding public key is used to identify its paired private key and only its paired private key.

A public key can be used by multiple recipients.

A key pair can be used to

* Sign and verify a signature
* Encrypt and decrypt the content of an email

S/MIME digital signatures and encryption require each sender and recipient to have it enabled.

They also need to send or exchange public keys though digital certificates to identify each other.

**Digital certificates**

Digital certificates help in delivering the public key in the key pair.

A digital certificate is a digital credential that provides information about the identity, validity, and any other required information.

Digital certificates are issued by a **certification authority (CA)** and are valid for only a specific period of time.

**How does S/MIME work?**

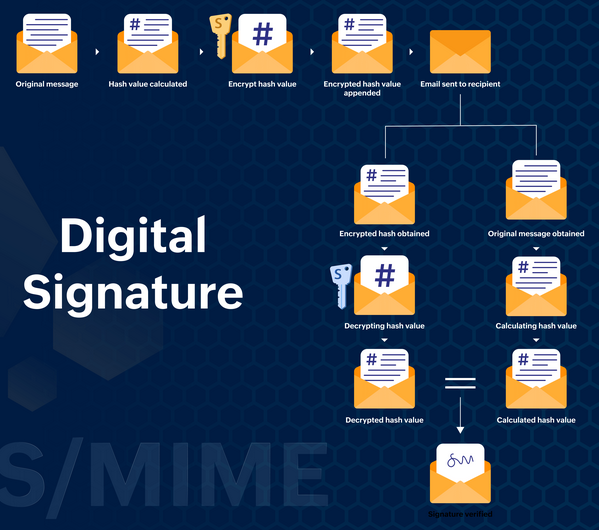
S/MIME works based on asymmetric encryption.

This means that this protocol uses **a two-key system (Public and Private)** that is mathematically related but different, to encrypt and decrypt an email.

The sender and receiver have their own pair of private and public keys in which the public keys are known to the other party.

A S/MIME certificate needs to be installed on the email clients of both the recipient and the sender to ensure email encryption at both ends.

When an email is sent, the sender encrypts the email using the recipient's public key and the recipient decrypts the email using the private key.



**Benefits of S/MIME**

The encryption and digital signing of an email ensure that the data transmitted through email is confidential, and true to its sender.

S/MIME protects an email in the following methods:

**Email Encryption**

The email content is encrypted using the recipient's public key, the moment the sender hits the Send button.

Even if the email gets intercepted by anyone, they cannot view the content of the email unless they have access to the private key of the recipient.

**Data Confidentiality**

The encryption of the email content ensures the confidentiality of the data and attachments sent through the email.

Any attempt to view the content of the email is made void as the data can be decrypted only with the help of a private key unique to the recipient.

**Digital Signature**

The email will be digitally signed along with encryption on installing the S/MIME certificate.

The email is signed using the private key of the sender and authenticated by the public key of the recipient.

An unaltered digital signature shows that the email content has not been compromised and tampered with.

**Signature Authentication**

When the sender digitally signs the email using their private key, the recipient validates and authenticates the signature using their public key to ensure that the email is received from a reliable source.

**Non-repudiation by the Sender**

The digital signature of each sender is unique and is assigned to the user and the domain when the S/MIME certificate is purchased and installed.

This voluntarily provides the non-repudiation of the signature by the sender in case of any legal proceedings.

**Content Integrity of the Email**

When the recipient of a digitally signed email is validated using the public key of the recipient, they're assured of the absence of any alterations in the content of the email and is intact as and when it was sent.

**Difference between PGP and S/MIME :**

| **S.NO** | **PGP** | **S/MIME** |
| --- | --- | --- |
| 1. | It is designed for processing the plain texts | It is designed to process email as well as many multimedia files. |
| 2. | PGP is less costly as compared to S/MIME. | S/MIME is comparatively expensive. |
| 3. | PGP is good for personal as well as office use. | It is good for industrial use. |
| 4. | PGP is less efficient than S/MIME. | It is more efficient than PGP. |
| 5. | It depends on user key exchange. | It relies on a hierarchically valid certificate for key exchange. |
| 6. | PGP is comparatively less convenient. | It is more convenient than PGP due to the secure transformation of all the applications. |
| 7. | PGP contains 4096 public keys. | It contains only 1024 public keys. |
| 8. | PGP is the standard for strong encryption. | It is also the standard for strong encryption but has some drawbacks. |
| 9. | PGP is also be used in VPNs. | It is not used in VPNs, it is only used in email services. |
| 10. | PGP uses **Diffie hellman digital signature**. | It uses **Elgamal digital signature**. |
| 11. | In PGP Trust is established using Web of Trust. | In S/MIME Trust is established using Public Key Infrastructure. |
| 12. | PGP doen’t  provides authentication. | S/MIME provides authentication. |
| 13. | PGP is used for   Securing text messages only. | S/MIME is used for Securing Messages and attachments. |
| 14. | Their is less use of PGP in industry . | S/MIME is widely used in industry. |
| 15. | Convenience of PGP is low. | Convenience of S/MIME is High. |
| 16. | Administrative overhead of PGP is high. | Administrative overhead of S/MIME is low. |

**Domain Keys Identified Mail (DKIM)**

Domain Keys Identified Mail (DKIM) is a digital signature added to every email sent from a given email address.

**Why use DKIM?**

Imagine the following scenario.

You’re sending a quick follow-up message to a potential investor after a meeting, “Yvonne, let me know if you would like to proceed with what we discussed earlier.”

Some time goes by, and you never got a reply from Yvonne but you bump into her in another meeting and discreetly mention that email.

Puzzled, Yvonne says, “Mark, I never heard from you back.”

There are many potential reasons for poor deliverability, but, as it turned out, Mark forgot to set up DKIM authentication for his email account.

As a result, Yvonne’s server wasn’t quite sure if it was really Mark emailing her and discarded the message.

The main purpose of DKIM is to prevent spoofing.

Email spoofing is changing the original message’s content and sending it from an alternative sender that looks like a trusted source.

This type of cyber attack is widely used for fraud — for example, someone sending payment request messages from an email address that looks like yours (mark@whatevercompany.io vs. mark@whatever-company.io).