IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 12, December 2021

DOI: 10.17148/IARJSET.2021.81263

Network Security Technique - Digital Signature And PGP

SANKAR K

HOD of Computer Science, Lal Bahadur Shastri Government First Grade College,

R T Nagar , Bangalore-560032, India.

Abstract: The Digital Signature is a technique which is used to validate the authenticity and integrity of the message. We know that there are four aspects of security: privacy, authentication, integrity, and non-repudiation. We have already discussed the first aspect of security and other three aspects can be achieved by using a digital signature.

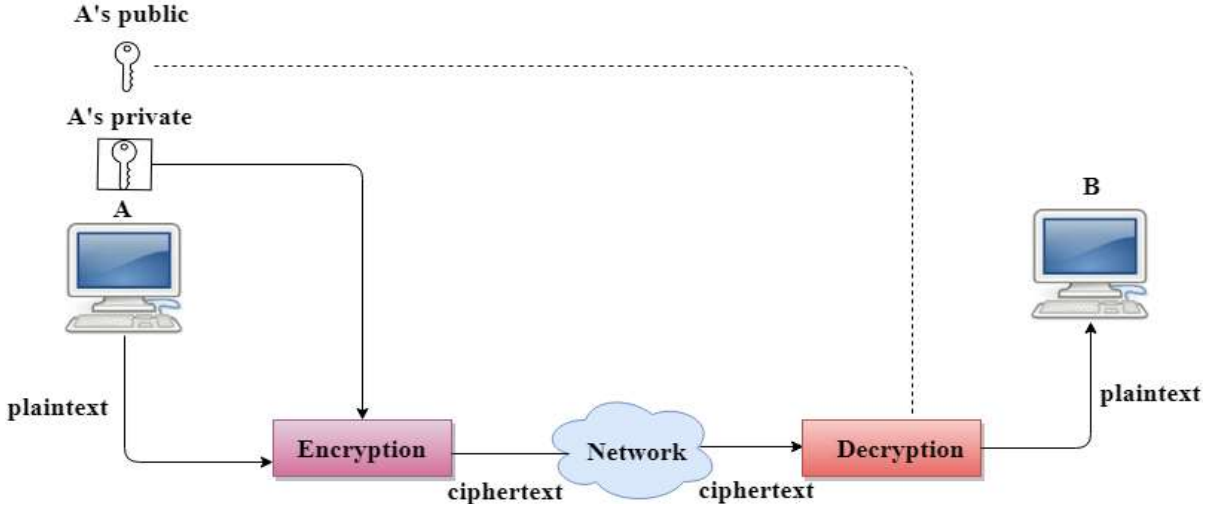
Keywords- Private key, public key, encryption, technique, digital Signature, Pretty Good Privacy

1. INTRODUCTION

The basic idea behind the Digital Signature is to sign a document. When we send a document electronically, we can also sign it. We can sign a document in two ways: to sign a whole document and to sign a digest.

2. SIGNING THE WHOLE DOCUMENT

- In Digital Signature, a public key encryption technique is used to sign a document. However, the roles of a public key and private key are different here. The sender uses a private key to encrypt the message while the receiver uses the public key of the sender to decrypt the message.
- In Digital Signature, the private key is used for encryption while the public key is used for decryption.
- Digital Signature cannot be achieved by using secret key encryption.



3. DIGITAL SIGNATURE IS USED TO ACHIEVE THE FOLLOWING THREE ASPECTS

- **Integrity:** The Digital Signature preserves the integrity of a message because, if any malicious attack intercepts a message and partially or totally changes it, then the decrypted message would be impossible.
- **Authentication:** We can use the following reasoning to show how the message is authenticated. If an intruder (user X) sends a message pretending that it is coming from someone else (user A), user X uses her own private key to encrypt the message. The message is decrypted by using the public key of user A. Therefore, this makes the message unreadable. Encryption with X's private key and decryption with A's public key results in garbage value.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 12, December 2021

DOI: 10.17148/IARJSET.2021.81263

- **Non-Repudiation:** Digital Signature also provides non-repudiation. If the sender denies sending the message, then her private key corresponding to her public key is tested on the plaintext. If the decrypted message is the same as the original message, then we know that the sender has sent the message.
- Digital Signature does not provide privacy. If there is a need for privacy, then another layer of encryption/decryption is applied.

4. SIGNING THE DIGEST

- Public key encryption is efficient if the message is short. If the message is long, a public key encryption is inefficient to use. The solution to this problem is to let the sender sign a digest of the document instead of the whole document.
- The sender creates a miniature version (digest) of the document and then signs it, the receiver checks the signature of the miniature version.
- The hash function is used to create a digest of the message. The hash function creates a fixed-size digest from the variable-length message.
- The two most common hash functions used: MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1). The first one produces 120-bit digest while the second one produces a 160-bit digest.

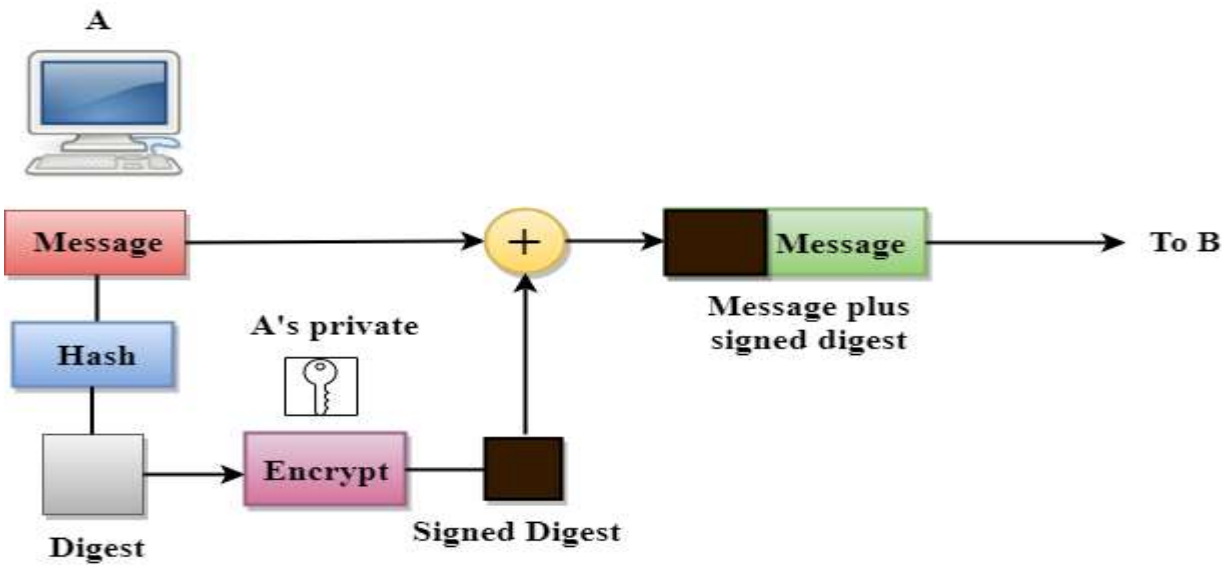
A hash function must have two properties to ensure the success:

- First, the digest must be one way, i.e., the digest can only be created from the message but not vice versa.
- Second, hashing is a one-to-one function, i.e., two messages should not create the same digest.

5. FOLLOWING ARE THE STEPS TAKEN TO ENSURE SECURITY:

- The miniature version (digest) of the message is created by using a hash function.
- The digest is encrypted by using the sender's private key.
- After the digest is encrypted, then the encrypted digest is attached to the original message and sent to the receiver.
- The receiver receives the original message and encrypted digest and separates the two. The receiver implements the hash function on the original message to create the second digest, and it also decrypts the received digest by using the public key of the sender. If both the digests are same, then all the aspects of security are preserved.

6. AT THE SENDER SITE



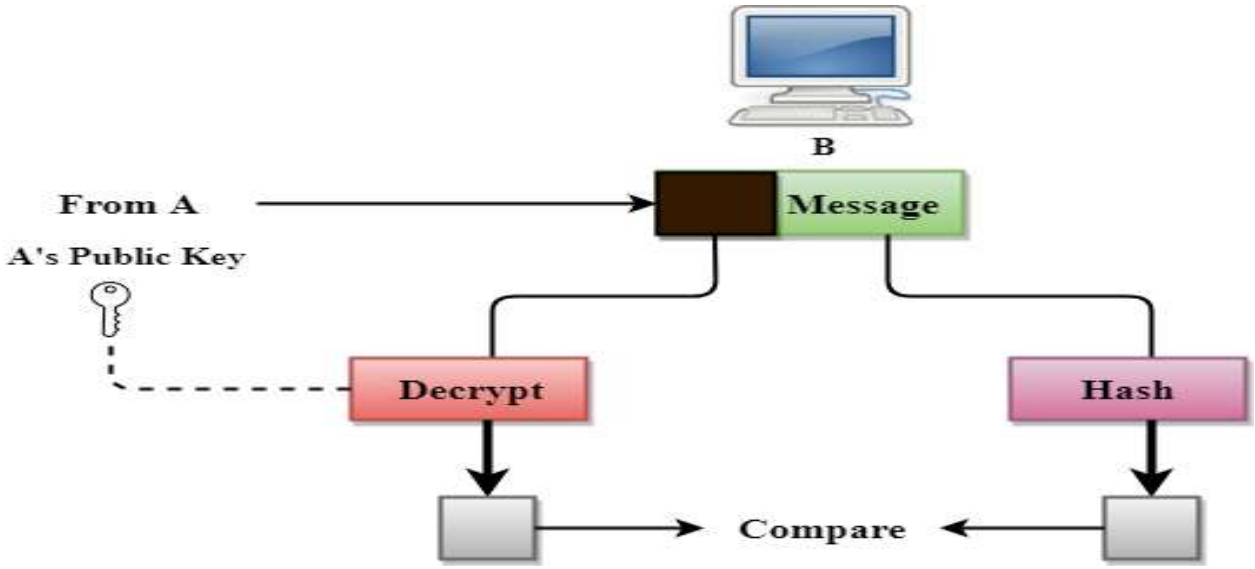
IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 12, December 2021

DOI: 10.17148/IARJSET.2021.81263

7. AT THE RECEIVER SITE



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.

8. 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.

IARJSET

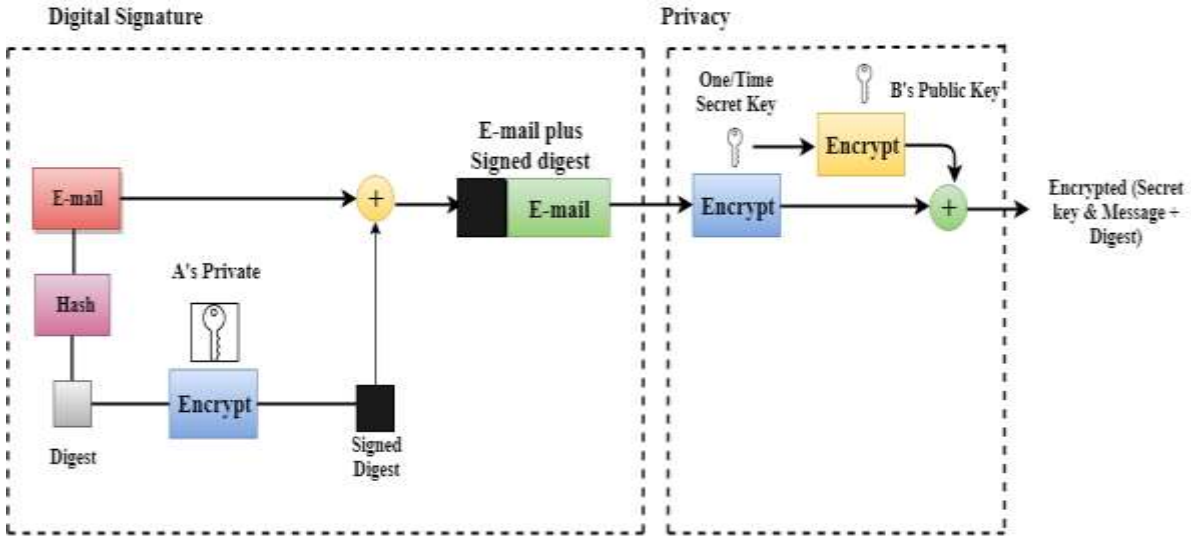
ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 12, December 2021

DOI: 10.17148/IARJSET.2021.81263

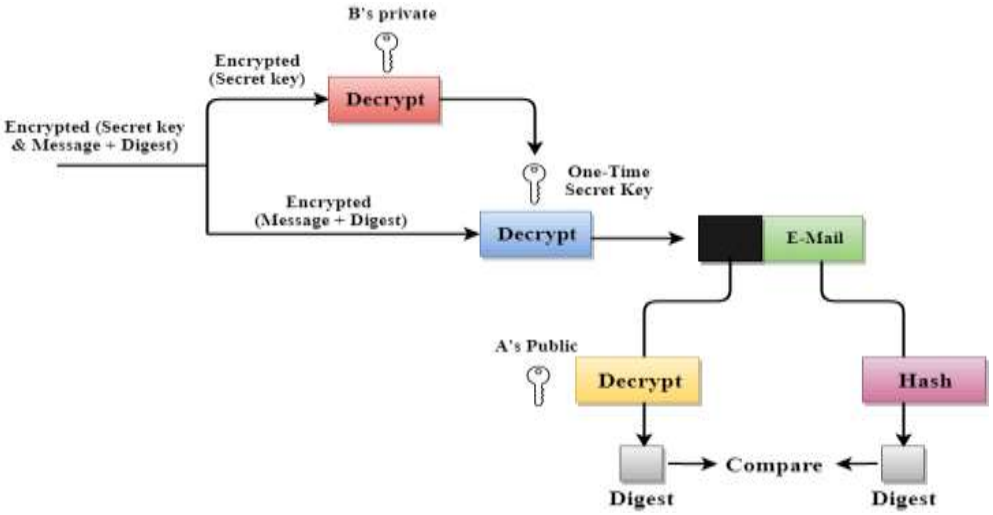
9. PGP AT THE SENDER SITE (A)



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.

10. PGP AT THE RECEIVER SITE (B)



11. 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.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 12, December 2021

DOI: 10.17148/IARJSET.2021.81263

- **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.

12. THE PHP COMPONENT OFFERS THE FOLLOWING KEY FEATURES:

- Completely written in the interpreted PHP language
- Compatible with all available PDF versions
- Digital sign PDF documents with any Certificate, that is useable with OpenSSL (CLI or PHP build in functions)
- Sign or Certify Documents
- Create PAdES-BES/B-B conform PDF signatures in PHP
- Optional signature modules on request
- Visible signatures
- RFC 3161 compatible timestamping
- Easy to understand usage
- Extendable via individual modules.

13. DIGITAL SIGNATURES OF DOCUMENTS USING GPG

- A digital signature certifies and timestamps a document.
- If the document is subsequently modified in any way, a verification of the signature will fail. A digital signature can serve the same purpose as a hand-written signature with the additional benefit of being tamper-resistant.
- Creating and verifying signatures uses the public/private keypair in an operation different from encryption and decryption. A signature is created using the private key of the signer. The signature is verified using the corresponding public key.
- we know what it is all about we can take a look at how you can sign your document.
- To sign a document with PGP, run this in the command-line:
- gpg --output document.sig --sign document.pdf
- Where "document.pdf" is the path to the document you want to sign and compress. It doesn't need to be a .pdf; in fact, it can be any type of file you want. After you have entered your password for your private key, GPG will output the "document.sig" file into C:\Users\YourPCName (on Windows).

To verify a document that has been signed with PGP, run this in the command line:
gpg --output document.pdf --decrypt document.sig
This will output the decrypted "document.pdf" into C:\Users\YourPCName if you have the person who signed the document's public key. In the command line you will see something like this:
gpg: Signature made 03/12/16 12:02:38 Coordinated Universal Time using DSA key ID ABD907D3 gpg: Good signature from "Person < person@domain.tld >"
Now, on to an example:
Bob wants to send Kate a sensitive document, and he wants to make sure that it isn't tampered with along the way. The document is called "classifiedinfo.docx" and it is located at D:\Users\Bob. He types this into the command line:
gpg --output classifiedinfo.sig --sign D:\Users\Bob\classifiedinfo.docx
Note that you can choose any name you like for the .sig file.
Now he types in his private key's password, retrieves the signed file from D:\Users\Bob and sends it to Kate. He also tells her that it is a .docx file. Kate has already imported Bob's public key into GPG.
Kate verifies and decompresses Bob's file by running this in the command line:
gpg --output classifiedinfo.docx --decrypt C:\Users\Kate\Downloads\classifiedinfo.siggpg --output classifiedinfo.docx --decrypt C:\Users\Kate\Downloads\classifiedinto.sig
She gets this message in the command line:
gpg: Signature made 02/12/2016 15:39:05 Central African Time using DSA key ID A657BC83 gpg: Good signature from "Bob < bob@pgp.com >"
The document is untampered and genuine.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 12, December 2021

DOI: 10.17148/IARJSET.2021.81263

14. HOW DO DIGITAL SIGNATURES WORK?

Familiarize yourself with the following terms to better understand how digital signatures work:

- **Hash function** – A hash function (also called a "hash") is a fixed-length string of numbers and letters generated from a mathematical algorithm and an arbitrarily sized file such as an email, document, picture, or other type of data. This generated string is unique to the file being hashed and is a one-way function- a computed hash cannot be reversed to find other files that may generate the same hash value. Some of the more popular hashing algorithms in use today are Secure Hash Algorithm-1 (SHA-1), the Secure Hashing Algorithm-2 family (SHA-2 and SHA-256), and Message Digest 5 (MD5).
- **Public key cryptography** – Public key cryptography (also known as asymmetric encryption) is a cryptographic method that uses a key pair system. One key, called the public key, encrypts the data. The other key, called the private key, decrypts the data. Public key cryptography can be used several ways to ensure confidentiality, integrity, and authenticity. Public key cryptography can
- Ensure integrity by creating a digital signature of the message using the sender's private key. This is done by hashing the message and encrypting the hash value with their private key. By doing this, any changes to the message will result in a different hash value.
- Ensure confidentiality by encrypting the entire message with the recipient's public key. This means that only the recipient, who is in possession of the corresponding private key, can read the message.
- Verify the user's identity using the public key and checking it against a certificate authority.
- **Public key infrastructure (PKI)** – PKI consists of the policies, standards, people, and systems that support the distribution of public keys and the identity validation of individuals or entities with digital certificates and a certificate authority.
- **Certificate authority (CA)** – A CA is a trusted third party that validates a person's identity and either generates a public/private key pair on their behalf or associates an existing public key provided by the person to that person. Once a CA validates someone's identity, they issue a digital certificate that is digitally signed by the CA. The digital certificate can then be used to verify a person associated with a public key when requested.
- **Digital certificates** – Digital certificates are analogous to driver licenses in that their purpose is to identify the holder of a certificate. Digital certificates contain the public key of the individual or organization and are digitally signed by a CA. Other information about the organization, individual, and CA can be included in the certificate as well.
- **Pretty Good Privacy (PGP)/OpenPGP** – PGP/OpenPGP is an alternative to PKI. With PGP/OpenPGP, users "trust" other users by signing certificates of people with verifiable identities. The more interconnected these signatures are, the higher the likelihood of verifying a particular user on the internet. This concept is called the "Web of Trust."

Digital signatures work by proving that a digital message or document was not modified-intentionally or unintentionally-from the time it was signed. Digital signatures do this by generating a unique hash of the message or document and encrypting it using the sender's private key. The hash generated is unique to the message or document, and changing any part of it will completely change the hash.

Once completed, the message or digital document is digitally signed and sent to the recipient. The recipient then generates their own hash of the message or digital document and decrypts the sender's hash (included in the original message) using the sender's public key. The recipient compares the hash they generate against the sender's decrypted hash; if they match, the message or digital document has not been modified and the sender is authenticated.

CONCLUSION

A digital signature-a type of electronic signature-is a mathematical algorithm routinely used to validate the authenticity and integrity of a message (e.g., an email, a credit card transaction, or a digital document). Digital signatures create a virtual fingerprint that is unique to a person or entity and are used to identify users and protect information in digital messages or documents. In emails, the email content itself becomes part of the digital signature. Digital signatures are significantly more secure than other forms of electronic signatures.

Digital signatures increase the transparency of online interactions and develop trust between customers, business partners, and vendors.

REFERENCE

- https://medium.com/@hashelse/how-to-sign-and-verify-a-document-or-file-using-pgp-gpg-401d013d2405
- https://cran.r-project.org/web/packages/gpg/vignettes/intro.html
- https://www.linuxbabe.com/security/a-practical-guide-to-gpg-part-4-digital-signature