SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

COURSE NAME : 19EC625 – CYBER FORENSIC AND DATA SECURITY

III YEAR / VI SEMESTER

Unit II- E-MAIL SECURITY & FIREWALLS

Topic : PGP

INTRODUCTION

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is widely used for securing emails, files, and even disk partitions.

Encryption & Decryption: It uses a combination of **symmetric** and **asymmetric** encryption to secure data. The sender encrypts the message using the recipient's public key, and the recipient decrypts it with their private key.

Authentication: PGP ensures the authenticity of the sender through **digital signatures**. This helps verify that the message hasn't been tampered with.

Key Management: PGP uses a **web of trust** instead of a central authority to manage public keys. This means users verify and sign each other's keys to build trust, making it a decentralized system for secure communication.

INTRODUCTION

- PGP works on a hybrid cryptographic method that combines symmetric-key and public-key cryptography techniques. Symmetric-key cryptography uses one secret key for both encrypting and decrypting data. Public-key cryptography uses two keys: a public key (shared with everyone) for encryption and a private key (kept secret) for decryption.
- The following are the services offered by PGP:

1. Authentication
2. Confidentiality
3. Email Compatibility
4. Segmentation

Development of Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP), developed by Phil Zimmermann in 1991, has evolved significantly to enhance secure communication and privacy.

•Initially released as freeware, PGP used RSA for public-key encryption and IDEA for symmetric encryption. However, it faced legal challenges due to encryption export restrictions.

•Acquired by Network Associates Inc. in 1997, PGP gained global recognition for email encryption. The OpenPGP standard was introduced to ensure compatibility across different implementations.

•The OpenPGP Working Group developed GnuPG (GNU Privacy Guard), an open-source alternative to proprietary PGP, increasing transparency and security.

•PGP now supports elliptic curve cryptography (ECC), improved key management, cloud storage integration, and mobile compatibility, making it widely used in secure communication tools and enterprise security solutions

AUTHEMTICATION IN PGP

1. Authentication in PGP

Authentication means something that is used to validate something as true or real. To login into some sites sometimes we give our account name and password, that is an authentication verification procedure. In the email world, checking the authenticity of an email is nothing but to check whether it actually came from the person it says. In emails, authentication has to be checked as there are some people who spoof the emails or some spams and sometimes it can cause a lot of inconvenience.

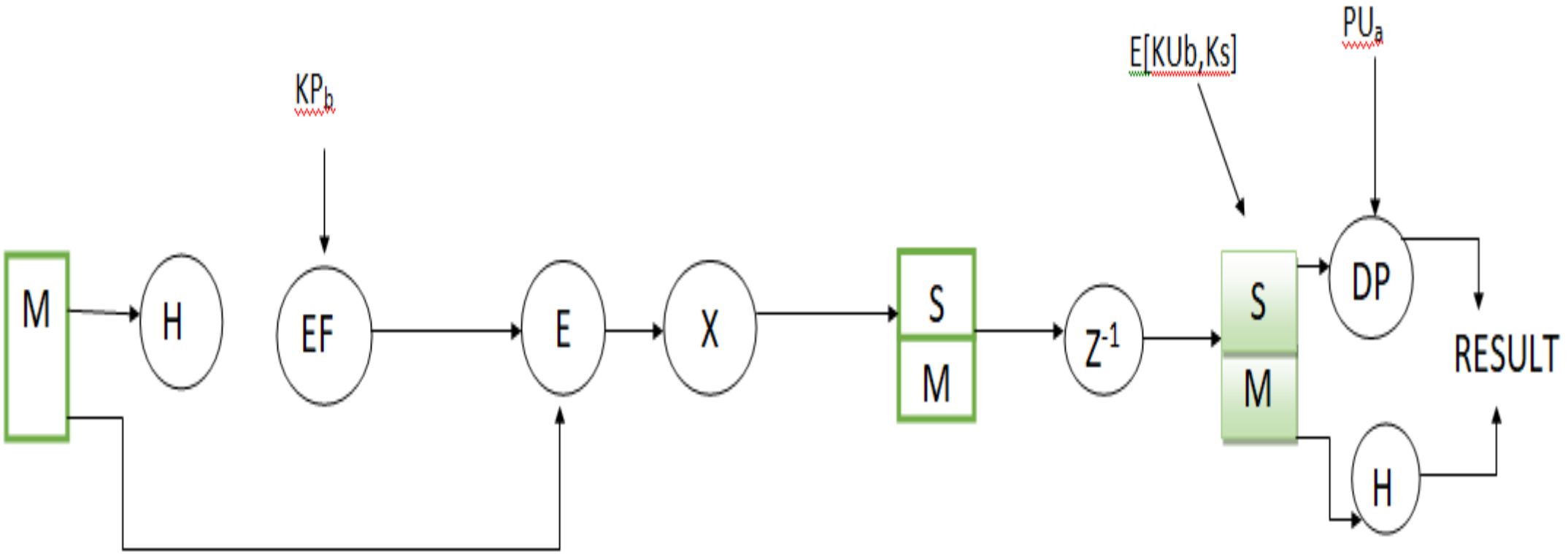
At the Sender's End:

1.A **hash function (SHA-1)** generates a **160-bit hash value** of the message.
2.This hash is **encrypted with the sender's private key (KPa)**, creating a **digital signature**.
3.The **message is appended to the signature**, compressed, and sent to the receiver.

At the Receiver's End:

1.The message is **decompressed**, and the signature is **decrypted using the sender's public key (PUa)** to retrieve the hash.
2.The message is **hashed again** using the same function.
3.If both hash values match, the message is verified as authentic and unaltered. If not, the message is likely tampered with or from an untrusted source.

AUTHENTICATION IN PGP



Confidentiality in PGP

2. Confidentiality in PGP

Sometimes we see some packages labelled as ‘Confidential’, which means that those packages are not meant for all the people and only selected persons can see them. The same applies to the email confidentiality as well. Here, in the email service, only the sender and the receiver should be able to read the message, that means the contents have to be kept secret from every other person, except for those two.

How PGP Provides Confidentiality:

1.The message is **compressed and encrypted** using a **random session key (Ks)** with **symmetric encryption (CAST-128, IDEA, or 3DES)**.

2.The session key (Ks) is then **encrypted using the receiver’s public key (PUb)** with **RSA encryption**.

3.The **encrypted message and encrypted session key** are sent together to the receiver.

At the Receiver’s End:

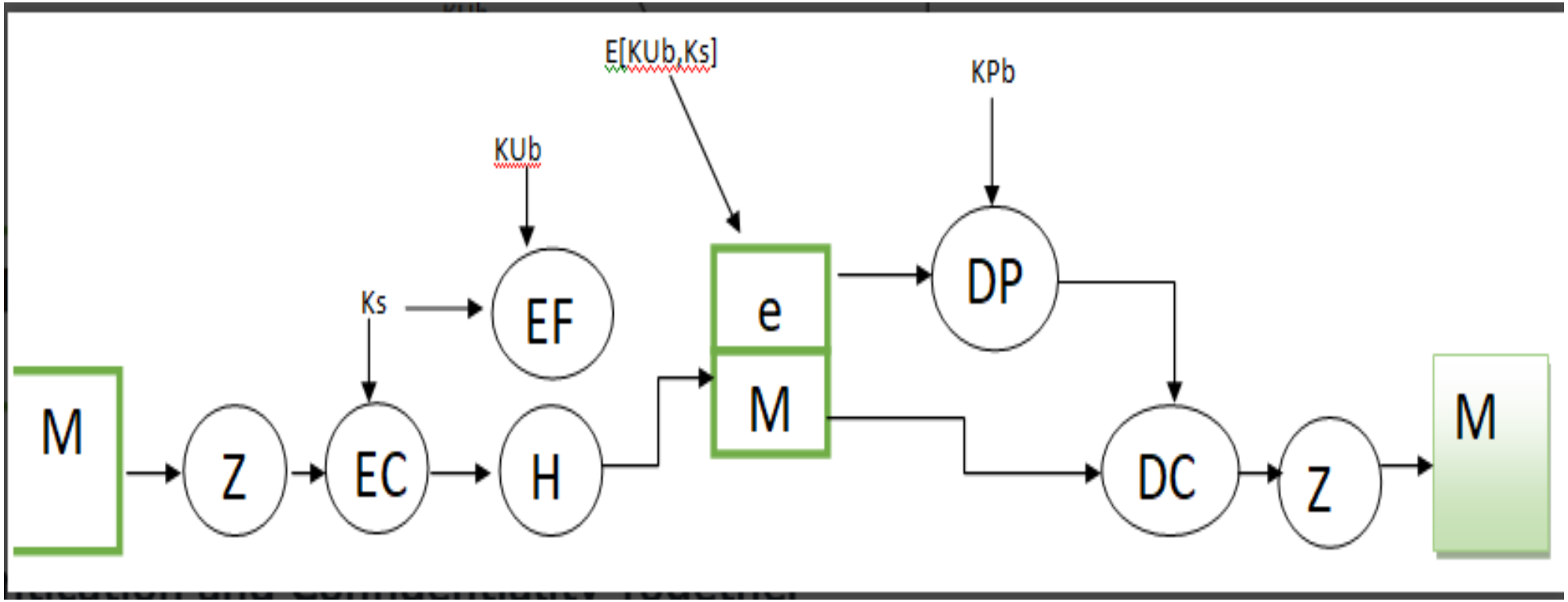
1.The **session key is decrypted** using the receiver’s private key (KPb).

2.The **message is decrypted** using the retrieved session key.

3.Finally, the message is **decompressed** to restore the original content.

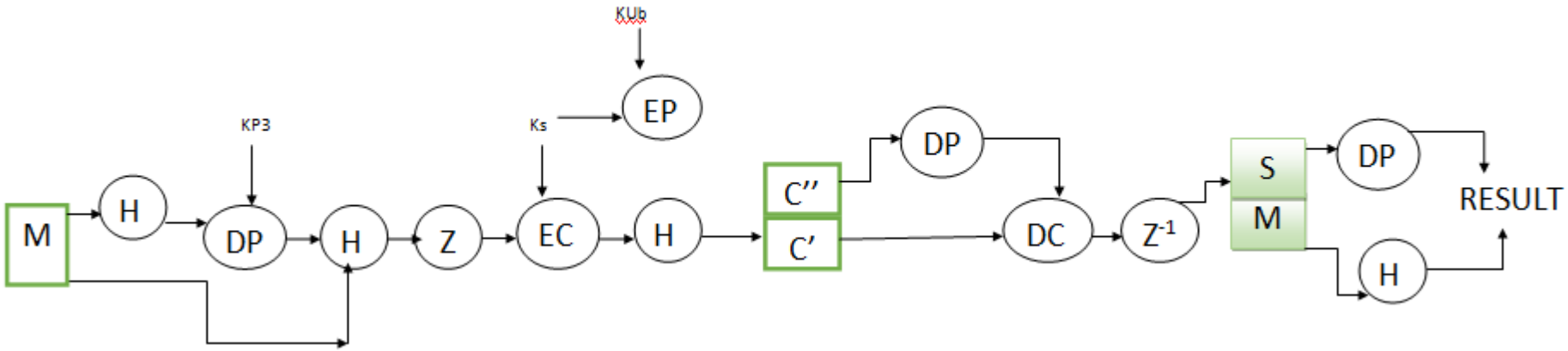
Since the session key is transmitted in **encrypted form** even if intercepted, it remains unreadable without the private key (KPb).

Confidentiality in PGP



Authentication and Confidentiality Together

Practically, **both** the Authentication and Confidentiality services are provided in parallel as



Key Terms:

- **M** – Message
- **H** – Hash Function
- **K**s– Session Key (for Symmetric Encryption)
- **KP_a, KP_b** – Private Keys of Sender (A) and Receiver (B)
- **PU_a, PU_b** – Public Keys of Sender (A) and Receiver (B)
- **EC / DC** – Symmetric Encryption & Decryption Algorithms
- **EP / DP** – Public Key Encryption & Decryption Algorithms
- **| |** – Concatenation
- **Z / Z^{-1}** – Compression & Decompression Functions

Advantages of PGP

•The primary benefit of PGP encryption lies in its unbreakable algorithm.

•It is regarded as a top technique for improving cloud security and is frequently utilised by users who need to encrypt their private conversations.

•This is due to PGP's ability to prevent hackers, governments from accessing files or emails that are encrypted with PGP.

Disadvantage of PGP

•The main drawback of PGP encryption is that it is usually not intuitive to use. PGP requires time and effort to fully encrypt data and files, which might make messaging more difficult for users. If an organisation is thinking about deploying PGP, it has to train its employees.

•It is imperative that users comprehend the intricacies of the PGP system to prevent unintentionally weakening their security measures. This may occur from using PGP incorrectly or from losing or corrupting keys, endangering other users in situations where security is at an extreme.

•PGP encrypts user messages but does not provide users with any anonymity. This makes it possible to identify the source and recipient of emails sent using a PGP solution.

Any Query????

Thank you……