Lab07

1. Cleartext vs. Encrypted SMTP

During the test with an unencrypted SMTP server (port 1025, no TLS), the entire email was visible in Wireshark.

It was possible to read:

- sender and recipient addresses
- subject
- message body
- SMTP commands

This means that anyone on the same network could intercept, read, or even alter the message.

With SMTP using STARTTLS (port 587), the captured traffic only showed packet metadata (IP, ports), but the actual email content was encrypted.

In this case, the attacker can see that communication is happening but cannot read or modify the message.

2. Why is fingerprinting in PGP to prevent man-in-the-middle attacks?

Fingerprinting in PGP allows you to confirm that the public key you are encrypting with actually belongs to the correct person.

By comparing fingerprints through a trusted channel, you make sure the key was not replaced.

This prevents a man-in-the-middle attacker from inserting their own key and secretly intercepting or changing encrypted messages.

3. When to Use PGP vs. Signal

PGP is best for:

- email encryption
- exchanging sensitive files
- long-term communication where messages must remain accessible

Signal is best for:

- fast, everyday messaging (text, audio, video)
- mobile communication
- situations where usability is important and messages do not need long-term archival

PGP offers strong security for documents and emails, while Signal is designed for real-time encrypted chat.

4. Should End-to-End Encryption Be the Default?

Yes, end-to-end encryption should be the default for most communication apps.

Security:

It protects messages from interception and tampering.

Privacy:

Only the sender and receiver can access the content, not even the service provider.

User Experience:

Modern apps handle encryption automatically, so users don’t need any advanced knowledge.

The experience feels the same as normal messaging, just with better protection.

Although it may complicate law-enforcement access or moderation, from a user's security and privacy standpoint, E2EE should be the standard.