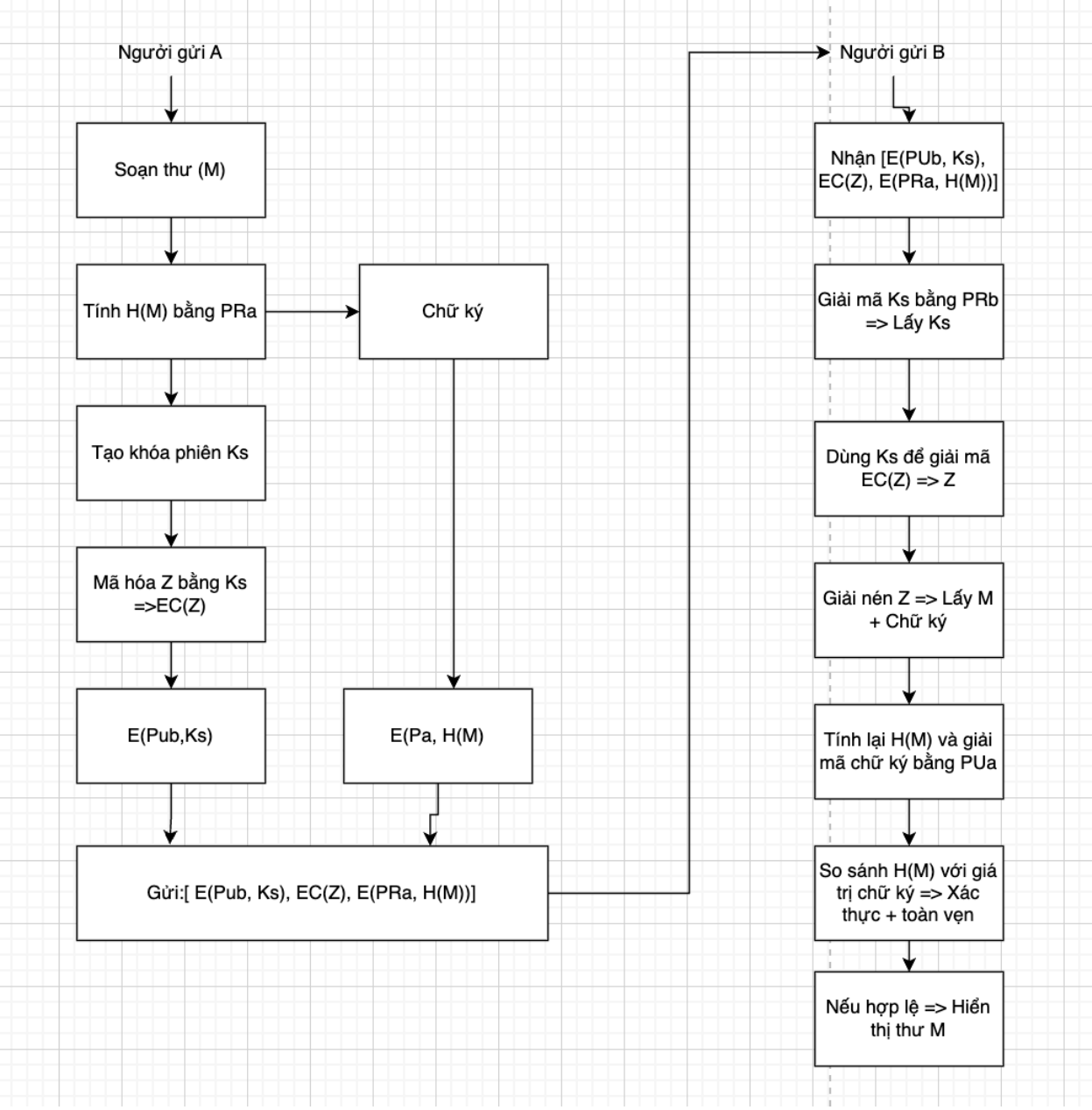
Bài tập ngày 14/04/2025

1. Từ các sơ đồ đã học, hãy xây dựng một lưu đồ mới có đầy đủ chức năng chứng thực, chữ ký số, bảo mật cho thư điện tử.

a. Vẽ lưu đồ mới này



b. Mô tả hoạt động của lưu đồ

Bên gửi:

1. Người gửi soạn nội dung thư M.
2. Tính hàm băm (hash) của M để tạo H(M).
3. Mã hóa H(M) bằng khóa riêng (PRa) để tạo chữ ký số.
4. Ghép M và chữ ký, nén toàn bộ bằng thuật toán ZIP thành Z.
5. Sinh Khóa phiên (Ks) → mã hóa Z bằng Ks (EC).
6. Mã hóa Ks bằng khóa công khai của người nhận (PUb).
7. Gửi 3 phần:

- EC(Z): nội dung thư đã mã hóa
- E(PUb, Ks): khóa phiên được mã hóa
- Chữ ký: H(M) mã hóa bằng Pra

Bên nhận:

1. Giải mã E(PUb, Ks) bằng khóa riêng PRb để lấy khóa phiên Ks.
2. Dùng Ks để giải mã nội dung thư EC(Z).
3. Giải nén để lấy ra M và chữ ký.
4. Giải mã chữ ký bằng khóa công khai của người gửi (PUa) → Lấy lại H(M).
5. Tính lại H(M) từ nội dung M và so sánh → nếu khớp → thư hợp lệ, không bị thay đổi, đúng người gửi

c. Nêu các ưu nhược điểm của lưu đồ đã tạo

Ưu điểm:

- Xác thực người gửi: thông qua chữ ký số.
- Đảm bảo toàn vẹn dữ liệu: nhờ cơ chế băm và so sánh hash.
- Bảo mật nội dung: nhờ mã hóa đối xứng với khóa phiên.
- Chống tấn công trung gian, giả mạo.

Nhược điểm:

- Cần hệ thống quản lý khóa công khai (PKI): khó triển khai ở quy mô lớn nếu không có CA.
- Khó dùng với người không rành kỹ thuật.
- Tốn tài nguyên xử lý: do sử dụng cả mã hóa đối xứng và bất đối xứng.
- Phụ thuộc vào độ tin cậy của khóa công khai.
- Nén dữ liệu: giúp tiết kiệm băng thông.

2. Xây dựng một bảng tổng hợp các giao thức bảo mật mạng đã học (tên gọi, tầng hoạt động, công dụng, đặc điểm, cơ chế hoạt động...).

Tên giao thức	Tầng hoạt động	Công dụng	Đặc điểm	Cơ chế hoạt động
IPSec	Tầng mạng	Bảo mật kết nối VPN, mã hóa dự liệu truyền trên mạng	Cung cấp xác thực, toàn vẹn và bảo mật dữ liệu	Sử dụng Authentication Header, Encapsulating Security, Internet Key Change
SSL/TLS	Tầng vận chuyển	Bảo mật giao tiếp web (HTTPS), email, ứng dụng mạng	Mã hóa đầu cuối, bảo vệ dữ liệu khỏi nghe lén	Thực hiện handshake để trao khóa, sử dụng mã hóa RSA, AES
PGP	Tầng ứng dụng	Bảo mật email và dữ liệu cá nhân	Kết hợp mã hóa bất đối xứng và đối xứng, sử dụng khóa công khai	Chứng thực, nén, mã hóa, truyền thông điệp an toàn
S/MIME	Tầng ứng dụng	Bảo mật email bằng chữ ký số và mã hóa	Được tích hợp vào các ứng dụng email phổ biến	Sử dụng PKI để quản lý khóa công khai
Kerberos	Tầng ứng dụng	Chứng thực người dùng trong mạng nội bộ	Dựa trên mô hình chứng thực trung gian (TGS – Ticket Granting Server)	Sử dụng mật mã khóa đối xứng, cấp vé chứng thực giữa máy khách và máy chủ
SSH	Tầng ứng dụng	Bảo mật đăng nhập từ xa, truyền tập an toàn	Mã hóa đầu cuối, chống tấn công trung gian	Sử dụng trao đổi khóa, mã hóa phiên làm việc, chứng thực danh tiến