**<u>BÀI TẬP</u>: Chọn 3 trong số 4 bài sau**

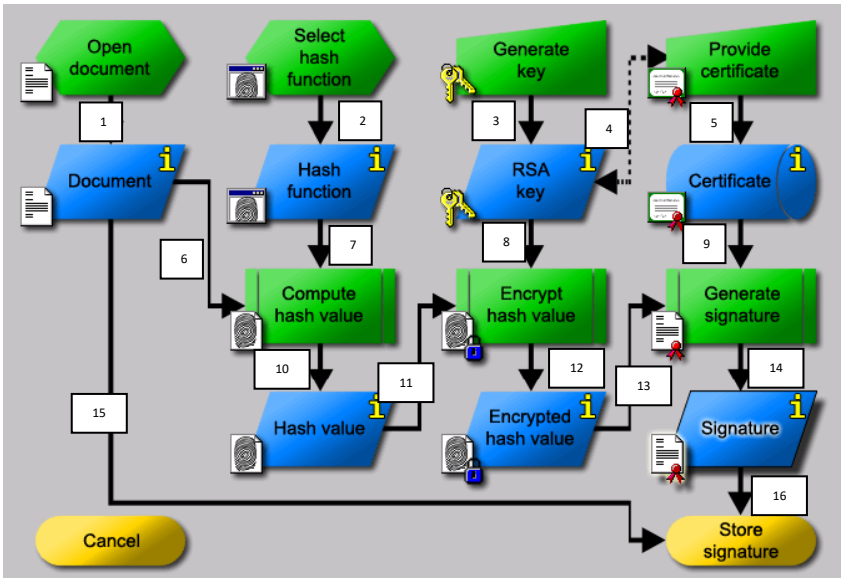
**Bài 1: Chứng thực với hàm băm**

Từ 6 mô hình cơ bản của hàm băm đã học, tiến hành xây dựng một mô hình "bảo mật - chứng thực – chữ ký số" mới. Bao gồm:

- Lưu đồ hoạt động của mô hình
- Biểu thức minh hoạ mô hình
- Phân tích hoạt động
- Nêu ưu và nhược điểm của mô hình so với các mô hình cơ bản

**BÀI 2: Chứng thực thông điệp và chữ ký số**

Đánh số thứ tự cho các mũi tên rồi phân tích chi tiết các bước thực hiện của quá trình sau:




**BÀI 3: Giao thức bảo mật mạng**

Lập bảng tổng hợp các giao thức bảo mật mạng (tên gọi, tầng hoạt động, đặc điểm, công dụng, các thành phần chính…)

**BÀI 4: Mã hoá và giải mã**

Cho đoạn văn bản (Cyphertext) được mã hoá bởi giải thuật Subtitution. Phân tích Ciphertext để tìm ra văn bản gốc (Plaintext):

**EGIDJSMGTDNI NTH T GSXQ JS DXTI BA ZTAI TGQTH. XBCQ HQTJ RQXJH, BJ PBXX ASJ ESZDXQJQXI DGSJQEJ KH. BA JNQ ENTDJQGH JNTJ USXXSP, B PBXX WQLQXSD JNQ RTHBE BWQTH TRSKJ EGIDJSMGTDNI TAW JNQA BXXKHJGTJQ HSZQ SU JNQ PTIH BJ BAJQGTEJH PBJN TAW DGSJQEJH KH.**