Introduction to IS

Def:

- Định nghĩa chung: Các quy trình & công cụ bảo vệ thông tin khỏi:
  - Truy cập trái phép
  - Sử dụng sai mục đích
  - Tiết lộ
  - Gián đoạn
  - Sửa đổi
  - Phá hủy

  → Bao gồm cả thông tin đang lưu trữ, xử lý, và truyền tải

CIA:

- **Confidentiality** – Chỉ thực thể được phép mới truy cập được dữ liệu.
- **Integrity** – Dữ liệu không bị sửa đổi trái phép.
- **Availability** – Người dùng hợp lệ có thể truy cập dữ liệu khi cần / **Recoverability** – Khôi phục khi sự cố xảy ra.
- Gồm cả bảo mật vật lý

Tiêu chí	Thực trạng	Mong muốn	Mục Tiêu
Time to Compromise	vài phút	nhiều tháng	**Tăng** →triển khai phòng thủ nhiều lớp, kiểm soát truy cập, vá lỗi nhanh.
Time to Discover	vài tháng đến vài năm	vài giờ	**Giảm** →nâng cao giám sát, cảnh báo thời gian thực, threat hunting.
Time to Recover	vài tuần đến vài tháng	vài phút	**Giảm** →quy trình ứng cứu sự cố (IRP) chuẩn, tự động hóa khôi phục, backup tốt.
	Tấn công nhanh – phát hiện rất chậm – khắc phục lâu → thiệt hại nghiêm trọng	Tấn công khó – phát hiện nhanh – khắc phục cực nhanh → thiệt hại nhỏ	

Asset – Threat – Vulnerability – Risk (A + T + V = R)

- **Asset** – Tài sản cần bảo vệ (người, tài sản vật lý & phi vật lý, thông tin, uy tín, db, code).
- **Threat** – Mối đe dọa có thể khai thác lỗ hổng.
- **Vulnerability** – Lỗ hổng / điểm yếu bảo mật.

- **Risk** – Nguy cơ mất mát do mối đe dọa khai thác lỗ hổng

Action

- **Security Assessment** – Đánh giá rủi ro, điểm yếu, đề xuất biện pháp giảm thiểu.
- **Security Application** – Chuyên gia + tiếp cận đa lớp (multi-layered) + chính sách/quy trình.
- **Security Awareness** – Đào tạo liên tục, mọi cấp, tạo văn hóa bảo mật

Principles

- **Principle of Least Privilege** – Người dùng/chương trình chỉ có quyền tối thiểu để thực hiện nhiệm vụ
- **Defense in Depth** – Nhiều lớp bảo vệ, không có giải pháp duy nhất
- **Authentication** – Xác minh danh tính.
- **Authorization** – Cấp quyền truy cập.
- **Accounting** – Ghi nhận hoạt động.
- **Access control** – Cơ chế giới hạn truy cập.
- **Non-repudiation** – Không thể chối bỏ hành vi

Framework

- **ISO 27001/27002** – Hệ thống quản lý an toàn thông tin (ISMS).
- **COBIT** – Quản trị CNTT.
- **ITIL** – Quản lý dịch vụ CNTT.
- **RMF** – Quy trình quản lý rủi ro.
- **CSA STAR** – Tiêu chuẩn bảo mật điện toán đám mây

Crypto

Khái quát về Cryptology

- **Cryptology** = Cryptography (thiết kế mã) + Cryptanalysis (phá mã).
- **Mục tiêu chính**:
  - **Confidentiality**: Bảo mật nội dung.
  - **Integrity**: Đảm bảo toàn vẹn dữ liệu.
  - **Authentication**: Xác minh nguồn gốc.
  - **Non-repudiation**: Không thể chối bỏ.
- **Kerckhoffs' Principle**: Hệ thống vẫn phải an toàn ngay cả khi kẻ tấn công biết toàn bộ thuật toán, chỉ khóa là bí mật.

Mật mã đối xứng (Symmetric Cryptography)

- **Đặc điểm**: Cùng một khóa cho mã hóa và giải mã.
- **Loại**:
  - **Block Cipher**: AES, DES, 3DES – làm việc theo khối.
  - **Stream Cipher**: RC4, Salsa20 – tạo key stream kết hợp với dữ liệu.
- **Nguyên lý Shannon**:
  - **Confusion**: Che giấu quan hệ giữa key và ciphertext.
  - **Diffusion**: Phân tán ảnh hưởng của bit plaintext trên nhiều bit ciphertext.
- **Modes of operation**:
  - **ECB**: Nhanh nhưng lộ mẫu dữ liệu → tránh dùng.
  - **CBC**: Dùng IV ngẫu nhiên, bảo mật cao hơn.
  - **CFB/OFB/CTR**: Chuyển block cipher thành stream cipher, hỗ trợ xử lý song song (CTR).
- **One-Time Pad**: Bảo mật tuyệt đối, nhưng không thực tế vì yêu cầu khóa dài = thông điệp và chỉ dùng 1 lần
- **Ưu điểm**
  - Tốc độ nhanh, hiệu suất cao, phù hợp xử lý lượng dữ liệu lớn.
  - Thuật toán đơn giản hơn bất đối xứng → dễ triển khai trong phần cứng và thiết bị hạn chế tài nguyên.
  - Bảo mật cao nếu dùng thuật toán mạnh + khóa đủ dài + quản lý khóa tốt.
- **Khuyết điểm**
  - Vấn đề phân phối khóa: cả hai bên phải có cùng khóa bí mật, việc trao đổi khóa an toàn khó khăn.
  - Không cung cấp non-repudiation: vì các bên dùng chung một khóa.
  - Nếu một khóa bị lộ → toàn bộ dữ liệu mã hóa bằng khóa đó đều nguy hiểm.
- **Tính chất khóa**
  - Cùng một khóa cho mã hóa và giải mã.
  - Khóa phải bí mật tuyệt đối (trái ngược với thuật toán có thể công khai).
  - Không được sử dụng lại key stream (đối với stream cipher).
- **Độ dài khóa khuyến nghị**
  - Tối thiểu: 112-bit an toàn (NIST), 80-bit đang bị loại bỏ
  - Thông dụng: AES-128, AES-192, AES-256.
  - Nguyên tắc: Độ dài khóa tăng → không gian khóa (key space) tăng theo 2^n → tấn công brute-force khó hơn.

Mật mã bất đối xứng (Asymmetric Cryptography)

- **Đặc điểm**: Public key và private key khác nhau.
- **Cơ sở toán học**:
    - **RSA**: Khó khăn trong phân tích thừa số nguyên lớn.
    - **ElGamal, ECC**: Khó khăn của bài toán logarithm rời rạc.
- **Ứng dụng**:
    - Gửi khóa đối xứng (key exchange)
    - Chữ ký số (digital signature).
- **Ưu điểm**
    - Giải quyết vấn đề phân phối khóa: chỉ cần gửi khóa công khai, không lo lộ khóa riêng.
    - Hỗ trợ non-repudiation: chữ ký số gắn liền với cá nhân/tổ chức.
    - Dễ dàng quản lý nhiều bên nhờ PKI (Public Key Infrastructure).
- **Khuyết điểm**
    - Chậm hơn rất nhiều so với đối xứng → không thích hợp để mã hóa dữ liệu lớn.
    - Yêu cầu kích thước khóa lớn hơn để đạt mức an toàn tương đương đối xứng.
    - Bảo mật phụ thuộc vào tính khó của bài toán toán học (factoring, discrete log) → có thể bị ảnh hưởng nếu có đột phá toán học hoặc máy tính lượng tử.
- **Tính chất khóa**
    - Hai khóa toán học liên quan: public key (công khai) và private key (bí mật).
    - Bảo mật dựa trên việc không thể tính khóa riêng từ khóa công khai trong thời gian khả thi.
    - Public key có thể được phân phối rộng rãi, private key phải được bảo vệ tuyệt đối.
- **Độ dài khóa khuyến nghị**
    - RSA: tối thiểu 2048-bit (tương đương AES-112), khuyến nghị 3072-bit cho bảo mật dài hạn.
    - ECC: 256-bit ECC ≈ 3072-bits RSA về mức an toàn.
    - Nguyên tắc: Asymmetric cần khóa dài hơn nhiều lần để chống brute-force do không gian khóa nhỏ hơn tương ứng về độ bảo mật.

Hàm băm (Hash Functions)

- **Chức năng**: Tạo "dấu vân tay số" cho dữ liệu, không đảo ngược được.
- **Thuộc tính an toàn**:
    - **Collision resistance**: Khó tìm 2 đầu vào khác nhau cho cùng 1 giá trị băm.
    - **Preimage resistance**: Khó tìm đầu vào từ giá trị băm.
    - **Second preimage resistance**: Khó tìm đầu vào thứ hai cùng giá trị băm với đầu vào cho trước.
- **Tấn công Birthday**: Xác suất tìm collision tăng nhanh theo số mẫu thử (mốc ~2^(n/2) với n-bit hash).

MAC & Digital Signatures

- **MAC (Message Authentication Code)**:
  - Dùng khóa đối xứng + hash để đảm bảo **tính toàn vẹn + xác thực**.
  - Không cung cấp non-repudiation (do các bên dùng chung khóa).
- **Chữ ký số**:
  - Dùng khóa riêng ký dữ liệu hoặc hash của dữ liệu.
  - Cung cấp **authentication** + **integrity** + **non-repudiation**.

Quản lý khóa & Giao thức

- **Vấn đề phân phối khóa**:
  - **KDC/Kerberos**: Trung tâm phân phối khóa tin cậy.
  - **PKI/CA**: Hạ tầng khóa công khai với Certificate Authority.
  - **Diffie–Hellman**: Thỏa thuận khóa công khai, dễ bị MITM nếu không xác thực.
- **Trust models**: Hierarchical, Web of Trust, Cross-certification.

Cryptanalysis (Phân tích phá mã)

- **Brute-force**: Thử toàn bộ khóa → yêu cầu keyspace đủ lớn.
- **Ciphertext-only / Known-plaintext / Chosen-plaintext / Chosen-ciphertext attacks**.
- **Attacks trên symmetric**:
  - **Linear cryptanalysis**: Tìm quan hệ tuyến tính giữa plaintext, ciphertext, key.
  - **Differential cryptanalysis**: Phân tích khác biệt đầu vào – đầu ra.
- **Attacks trên asymmetric**:
  - Phân tích thừa số (RSA).
  - Giải logarithm rời rạc (DH, ECC).
- **Implementation attacks**:
  - Side-channel: timing attack, power analysis, EM analysis.
- **Social engineering**: Phishing, policy attacks.

Case Studies & Sai lầm phổ biến

- **WEP**: IV ngắn, dùng lại key stream, CRC32 yếu → dễ bị phá.
- **EMV (Chip & PIN)**: Lỗ hổng xác thực cho phép bypass PIN.
- **VOIP**: Độ dài gói tiết lộ thông tin giọng nói.
- **KeeLoq**: Bị phá qua power analysis, clone remote.

Chuẩn & Tổ chức

- **NIST**: AES, SHA-2, SHA-3.
- **IETF**: TLS, SSH, Kerberos.
- **PKCS**: Chuẩn RSA, ECC, Diffie–Hellman.
- **Quy trình chọn chuẩn hiện đại**: thi tuyển công khai (AES, SHA-3).

Bài học nâng cao

- **Chỉ khóa là bí mật** – thuật toán phải công khai, kiểm chứng được.

- **An toàn là tạm thời** – mọi thuật toán sẽ bị phá, chỉ là sớm hay muộn.
- **Crypto ≠ Security** – bảo mật hệ thống phải tính cả con người, triển khai, chính sách.
- **Right crypto, right way** – chọn thuật toán phù hợp mục tiêu và môi trường.