# Crypto & Security Concepts

## Privacy vs Secret vs Confidential

- Privacy: Quyền cá nhân, kiểm soát thông tin cá nhân.  
- Secret: Thông tin bị giữ kín, không công khai.  
- Confidential: Thông tin được chia sẻ trong phạm vi hạn chế, cần bảo mật.

## Coding vs Encoding vs Encrypting

- Coding: Biểu diễn dữ liệu theo một quy tắc (ví dụ: ASCII).  
- Encoding: Chuyển đổi để truyền/đọc (ví dụ: Base64).  
- Encrypting: Mã hóa để bảo mật, cần key để giải mã.

## Cryptology vs Cryptography vs Cryptanalysis

- Cryptology: Khoa học nghiên cứu về mật mã.  
- Cryptography: Tạo hệ mã để bảo mật.  
- Cryptanalysis: Phá mã, tìm điểm yếu (codebreaking).

## System, Scheme, Protocol, Primitive, Building Block

- System: Toàn bộ hệ thống bảo mật.  
- Scheme: Phương án/hệ mã cụ thể.  
- Protocol: Quy trình trao đổi, gồm nhiều bước và chuẩn.  
- Primitive: Thành phần cơ bản (RSA, AES).  
- Building block: Khối nền để xây dựng hệ thống.

## RSA: Chọn số nguyên tố

Trong RSA, cần chọn 2 số nguyên tố lớn p, q:  
- Độ lớn: Ít nhất 1024 bit (hiện khuyến nghị 2048 hoặc 3072 bit).  
- Cách chọn: Ngẫu nhiên, kiểm tra tính nguyên tố bằng Miller-Rabin.  
- Mục tiêu: Khó factor n = p\*q để bảo mật.

## Naming (System + Notes)

- RSA Pitfall: Chọn p, q quá nhỏ, dễ bị factor.  
- RSA Recommendation: Sử dụng prime đủ lớn, random, khác biệt.  
- AES Good Practice: Khóa dài, tránh reuse.  
- AES Bad Practice: Dùng ECB mode.