**NỘI DUNG ÔN TẬP THI CUỐI KỲ**

**AN TOÀN BẢO MẬT THÔNG TIN**

**A. Cấu trúc đề**

* Thời gian: 60 phút
* Không sử dụng tài liệu
* 3-4 câu bài tập, 1-2 câu lý thuyết

**B. Nội dung ôn tập bài tập (bài tập lý thuyết và bài tập lập trình)**

1. Mã hóa đối xứng cổ điển
   1. Bài tập mã hóa Ceasar
   2. Bài tập mã hóa Vigenere: Bảng Vigenere được cho trong đề
   3. Bài tập mã hóa hoán vị
2. Mã hóa đối xứng hiện đại
   1. Bài tập mã hóa TinyA5/1: cách quay thanh ghi được cho trong đề
   2. Bài tập mã hóa TinyDES: các hàm Expand, Sbox, Pbox, Collapse được cho trong đề
3. Mã hóa khóa công khai
   1. Bài tập thuật toán Euclid mở rộng tìm nghịch đảo
   2. Bài tập thuật toán bình phương liên tiếp tính lũy thừa modulo
   3. Bài tập tìm cặp khóa công khai, khóa riêng của thuật toán RSA, mã hóa và giải mã
4. Các hình thức tấn công ứng dụng Web
   1. Tấn công SQL Injection
   2. Tấn công XSS

**C. Nội dung ôn tập lý thuyết**

1. So sánh giữa mã hóa đối xứng cổ điển và mã hóa đối xứng hiện đại
2. So sánh giữa mã hóa đối xứng và mã hóa khóa công khai
3. Mục đích sử dụng của hàm băm
4. Sơ đồ chữ ký điện tử
5. Giao thức bảo mật, Chứng thư số X509, Giao thức SSL
6. Tấn công SQL Injection
7. Tấn công XSS
8. Tường lửa Web (WAF)