**Kế hoạch giảng dạy An toàn Bảo mật thông tin 2022**

Buổi 1: Nhập môn ATBMTT

1. Vị trí môn học
2. Một số ví dụ đơn giản
3. Tấn công, cơ chế, dịch vụ, mô hình
4. Đánh giá môn học

Mã cổ điển

1. Các khái niệm mật mã
2. Một số mã thế cổ điển
3. Một số mã hoán vị, mã kết hợp
4. EncryptTrans, DecryptTrans

Buổi 2, 3: Mã đối xứng hiện đại

1. DES
2. AES
3. Mã dòng
4. Cài đặt 1: DES, RC4, AES

Buổi 4, 5, 6, 7: Số học modulo

1. Trường modulo
2. Các Định lý Fecma, Euler, Phần dư Trung hoa
3. Căn nguyên thủy, Logarit rời rạc
4. Cài đặt 2: Euclide mở rộng, Lũy thừa nhanh, Radix64, Milner-Rabin, Primitive roots, Discrete logarithms

Buổi 8: Mã công khai RSA

1. Khái niệm mã công khai
2. Thiết lập RSA
3. Mã và giải mã RSA

Buổi 9: Trao đổi khóa Diffie-Hellman, mã Elgamal

1. Trao đổi công khai khóa mã
2. Sơ đồ Diffie-Hellman
3. Elgamal

Buổi 10: Xác thực thông điệp và Chữ ký điện tử

1. Mac, Hash
2. Khái niệm chữ ký điện tử
3. Chữ ký RSA
4. DSA

Buổi 11: Cài đặt 3

1. RSA
2. D-H
3. DSA
4. Elgamal
5. Knapsack

Buổi 12: Cài đặt 4:

ATBMTT-Client: Sử dụng các gói an ninh của Java, mã đối xứng: DES, AES, SHA

Buổi 13: Cài đặt 5

ATBMTT-Client: Sử dụng các gói an ninh của Java, mã công khai: RSA, DSA, Elgamal

Buổi 14: Ứng dụng xác thực

1. Phân phối khóa
2. Xác thực trung tâm Kerberos
3. PKI
4. Hệ thống Email
5. WebSecurity – TLS
6. Thanh toán điện tử an toàn

Buổi 15: An ninh hệ thống

1. Phần mềm có hại và các giải pháp chống
2. Chống xâm nhập trái phép
3. Phân quyền truy cập

Buổi 16: An ninh mạng

1. IPSec
2. Tường lửa
3. SNMP

Buổi 17: Ôn tập 1

1. Mã cô điển
2. Modulo, Định lý Ferma, Euler
3. Phần dư Trung hoa
4. Căn nguyên thủy, Logarit rời rạc

Buổi 18-19: Ôn tập 2

1. RSA
2. D-H
3. DSA

**Buổi 20, 21, 22: Nghiệm thu thực hành (50%)**

1. Hoàn thiện các chương trình, chạy và đưa giao diện kết quả vào báo cáo
2. Tách hàm main đưa vào chương trình client, xây dựng các lớp độc lập để tạo thành gói thư viện An ninh của riêng mình.
3. Project ATBMTT: hoàn thiện chạy các thuật toán sau, tách hàm main ra bên ngoài, tạo thành các phương thức api của các lớp để gọi sử dụng:
4. ModExp, ModStuff, RC4; tạo các phương thức api của các lớp
5. DiscLog, Milner-Rabin, PrimitiveRoots; tách hàm main, tạo các phương thức api của các lớp
6. DES, AES; bổ sung code còn thiếu, hoàn thiện và chạy chương trình.
7. BigInterger, RSABigInt, RSA2BigInt, RSAtext; tách hàm main, tạo các phương thức api của các lớp
8. Diffie-Hellman, Elgamal, DSA; tách hàm main, tạo các phương thức api của các lớp
9. StringToBase64, Base64ToString: tách hàm main, tạo các phương thức api của các lớp
10. Project ATBMTT-CLIENT: Hiểu code ứng dụng các gói an ninh trong Java như trong ATBM\_client. Biết cách sử dụng các gói an ninh với các lựa chọn khác nhau.
11. Ứng dụng mã, giải mã DES, AES, RSA, Elgamal, GenSig, VerSig trên file văn bản Radix 64 và Unicode.
12. Xây dựng các ứng dụng mở rộng các dự án ATBMTT và ATBMTT-Client cho các file văn bản tiếng Anh và file văn bản tiếng Việt.
13. Thêm một bước: tạo các lớp ứng dụng XXX\_App, sử dụng thư viện và tách hàm main ra đưa vào các lớp XXX\_Client, ở đó khởi tạo các đối tượng XXX\_App và gọi các phương thức của các đối tượng đó

**Nội dung thi viết (50%):**

1. Mã cổ điển: Cesar, Vigenere, Play Fair, Rail Fence, Mã dịch chuyển dòng (EncryptTrans)
2. Mã DES, AES
3. Số học Modulo: Lũy thừa (Fecma, Euler), nghịch đảo, số học modulo, hàm Euler, phần dư Trung hoa, logarit rời rạc, căn nguyên thủy
4. Mã công khai: RSA, Elgamal
5. Trao đổi khóa công khai: Diffie-Hellman
6. Chữ ký điện tử: DSA

Điều chỉnh kế hoạch:

1-2-3: Mã cổ điển, đối xứng

4-5-6-7: Số học modulo

8-9-10-11: Mã hóa công khai

12-13-14: Ứng dụng mã hóa

15-16-17: Ôn tập

Cấu trúc đề thi

1. Mã hóa cổ điển 1 câu - 1 điểm

2. Mã hóa hiện đại 3 điểm (1 câu trong 3 câu ở trên)

3. Giải hệ phương trình đồng dư (2) + kiểm tra số có là căn nguyên thủy, logarit rời rạc (1 điểm)

4. Mã hóa khóa công khai <3 điểm> 1 trong 4 câu ở trên