THUẬT TOÁN TRONG AN TOÀN THÔNG TIN

I. THÔNG TIN CHUNG

Tên học phần	**Thuật toán trong an toàn thông tin**
Tên tiếng Anh	Informations Security Algorithms
Số tín chỉ	2
Số giờ học ở lớp	42 (18 LT, 24 TH)
Số giờ tự học ở nhà	60
Học phần học trước	Cấu trúc dữ liệu và giải thuật

II. MỤC TIÊU HỌC PHẦN

2.1. Mục tiêu chung

Học phần này trang bị cho sinh viên kiến thức về một số thuật toán để thực hiện các tính toán hiệu quả ứng dụng trong an toàn thông tin, đặc biệt là trong mật mã khóa công khai và trong phát hiện tấn công, mã độc.

2.2. Mục tiêu cụ thể

Mục tiêu	Mô tả	Chuẩn đầu ra CTĐT
M1	Nắm được, lập trình cài đặt được các phép tính toán hiệu quả trên số nguyên lớn	R5, R7, R18, R27
M2	Nắm được, lập trình cài đặt được một số thuật toán hiệu quả liên quan đến số nguyên tố	R5, R7, R18, R27
M3	Nắm được, lập trình cài đặt được một số thuật toán đối sánh mẫu hiệu quả trên chuỗi	R5, R7, R18, R27

III. MÔ TẢ HỌC PHẦN

Học phần này trình bày một số thuật toán được ứng dụng để thực thi các tính toán hiệu quả trong lĩnh vực an toàn thông tin, cụ thể là trong mật mã (các thuật toán tính toán trên số nguyên lớn, một số thuật toán về số nguyên tố) và trong phát hiện mã độc và tấn công mạng (các thuật toán đối sánh mẫu trên chuỗi).

IV. ĐỀ CƯƠNG CHI TIẾT

Chương 1. Tính toán trên số nguyên lớn trong trường Fp [1] (6 LT, 6 TH)

1.1. Phép tính cộng và trừ

1.2. Phép tính nhân

1.3. Phép tính bình phương

1.4. Phép lấy modulo

1.5. Phép tính lũy thừa

1.6. Phép tính nghịch đảo

1.7. Tính toán với modulo là số nguyên tố đặc biệt của NIST

Chương 2. Một số thuật toán về số nguyên tố [2] (6 LT, 6 TH)

2.1. Sàng Eratosthenes

2.1.1. Sàng Eratosthenes nguyên thủy

2.1.2. Sàng Eratosthenes phân đoạn

2.2. Phân tích ra thừa số nguyên tố

2.2.1. Thuật toán Pollard Rho

2.2.2. Thuật toán Baby-steps Giant-steps

2.3. Kiểm tra tính nguyên tố

2.3.1. Thuật toán kiểm tra tất định Adleman–Pomerance–Rumely

2.3.2. Thuật toán kiểm tra xác suất Fermat

2.3.3. Thuật toán kiểm tra xác suất Miller–Rabin

2.3.4. Thuật toán kiểm tra xác suất Solovay–Strassen

2.4. Sinh số nguyên tố

2.4.1. Thuật toán sinh số nguyên tố

2.4.2. Thuật toán sinh số giả nguyên tố

Chương 3. Đối sánh mẫu trên chuỗi [3] (6 LT, 6 TH)

3.1. Thuật toán vét cạn

3.2. Thuật toán Karp–Rabin

3.3. Thuật toán Knuth–Morris–Pratt

3.4. Thuật toán Boyer–Moore

3.5. Thuật toán Horspool

3.6. Thuật toán Aho–Corasick

V. KẾ HOẠCH GIẢNG DẠY

Giải thích ký hiệu: LT – lý thuyết; BT – bài tập/thảo luận; TH – Thực hành; ON – tự học ở nhà

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
1	***Chương 1. Tính toán trên số nguyên lớn trong trường Fp (Phần 1/2)*** **Giảng dạy trên lớp** – Phép tính cộng và trừ – Phép tính nhân – Phép tính bình phương – Phép lấy modulo **Phương pháp giảng dạy chính** – Trình chiếu Powerpoint – Thuyết giảng **Tài liệu tham khảo** [1] **Tự học ở nhà** – Nghiên cứu tài liệu tham khảo – Lập trình cài đặt thuật toán	M1	3	0	0	5
2	***Chương 1. Tính toán trên số nguyên lớn trong trường Fp (Phần 2/2)***	M1	3	0	0	5

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
	Giảng dạy trên lớp – Phép tính lũy thừa – Phép tính nghịch đảo – Tính toán với modulo là số nguyên tố đặc biệt của NIST **Phương pháp giảng dạy chính** – Trình chiếu Powerpoint – Thuyết giảng **Tài liệu tham khảo** [1] **Tự học ở nhà** – Nghiên cứu tài liệu tham khảo – Lập trình cài đặt thuật toán					
3	***Thực hành Chương 1: Lập trình cài đặt thuật toán tính toán trên số nguyên lớn trong trường Fp*** **Giảng dạy trên lớp** – Hướng dẫn giải bài tập – Giải đáp thắc mắc của sinh viên **Phương pháp giảng dạy chính** – Làm mẫu – Cho sinh viên tự làm bài tập – Tương tác, hỏi đáp với sinh viên **Tự học ở nhà** – Ôn lại kiến thức lý thuyết – Hoàn thành các bài tập được giao	M1	0	0	6	10
4	***Chương 2. Một số thuật toán về số nguyên tố (Phần 1/2)*** **Giảng dạy trên lớp** – Sàng Eratosthenes – Phân tích ra thừa số nguyên tố **Phương pháp giảng dạy chính** – Trình chiếu Powerpoint – Thuyết giảng **Tài liệu tham khảo** [2] **Tự học ở nhà** – Nghiên cứu tài liệu tham khảo – Đọc thêm [4] – Lập trình cài đặt thuật toán	M2	3	0	0	5
5	***Chương 2. Một số thuật toán về số nguyên tố (Phần 2/2)***	M2	3	0	0	5

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
	Giảng dạy trên lớp – Thuật toán kiểm tra tính nguyên tố – Sinh số nguyên tố **Phương pháp giảng dạy chính** – Trình chiếu Powerpoint – Thuyết giảng **Tài liệu tham khảo** [2] **Tự học ở nhà** – Nghiên cứu tài liệu tham khảo – Đọc thêm [4] – Lập trình cài đặt thuật toán					
6	***Thực hành Chương 2: Lập trình cài đặt thuật toán tính toán liên quan đến số nguyên tố*** **Giảng dạy trên lớp** – Hướng dẫn giải bài tập – Giải đáp thắc mắc của sinh viên **Phương pháp giảng dạy chính** – Làm mẫu – Cho sinh viên tự làm bài tập – Tương tác, hỏi đáp với sinh viên **Tự học ở nhà** – Ôn lại kiến thức lý thuyết – Hoàn thành các bài tập được giao	M2	0	0	6	10
7	***Thi giữa kỳ*** Hình thức thi: thực hành lập trình trên máy tính		0	0	6	0
8	***Chương 3. Đối sánh mẫu trên chuỗi (Phần 1/2)*** **Giảng dạy trên lớp** – Thuật toán vét cạn – Thuật toán Karp–Rabin – Thuật toán Knuth–Morris–Pratt – Thuật toán Boyer–Moore **Phương pháp giảng dạy chính** – Trình chiếu Powerpoint – Thuyết giảng **Tài liệu tham khảo** [3] **Tự học ở nhà**	M3	3	0	0	5

TT	Nội dung và phương pháp dạy học	Mục tiêu	LT	BT	TH	ON
	– Nghiên cứu tài liệu tham khảo – Đọc thêm [5] – Lập trình cài đặt thuật toán					
9	***Chương 3. Đối sánh mẫu trên chuỗi (Phần 2/2)*** **Giảng dạy trên lớp** – Thuật toán Horspool – Thuật toán Aho-Corasick **Phương pháp giảng dạy chính** – Trình chiếu Powerpoint – Thuyết giảng **Tài liệu tham khảo** [3] **Tự học ở nhà** – Nghiên cứu tài liệu tham khảo – Đọc thêm [5] – Lập trình cài đặt thuật toán	M3	3	0	0	5
10	***Thực hành Chương 3: Lập trình cài đặt thuật toán đối sánh mẫu trên chuỗi*** **Giảng dạy trên lớp** – Hướng dẫn giải bài tập – Giải đáp thắc mắc của sinh viên **Phương pháp giảng dạy chính** – Làm mẫu – Cho sinh viên tự làm bài tập – Tương tác, hỏi đáp với sinh viên **Tự học ở nhà** – Ôn lại kiến thức lý thuyết – Hoàn thành các bài tập được giao	M3	0	0	6	10
	Tổng		**18**	**0**	**24**	**60**

VI. GIÁO TRÌNH VÀ TÀI LIỆU THAM KHẢO

6.1. Tài liệu chính

[1] Darrel Hankerson, Alfred Menezes and Scott Vanstone, Chapter 2. Finite Field Arithmetic // Guide to Elliptic Curve Cryptography, Springer, 2004

[2] Richard Crandall and Carl Pomerance, Prime Numbers - A Computational Perspective (2nd edition), Springer, 2005

[3] Mikhail J. Atallah and Marina Blanton (editors), Chapter 13. Pattern Matching in Strings // Algorithms and Teory of Computation Handbook: General Concepts and Techniques, CRC Press, 2010

6.2. Tài liệu bổ sung

[4] Hans Riesel, Prime Numbers and Computer Methods for Factorization (2nd edition), Springer, 2012

[5] Alberto Apostolico and Zvi Galil (editors), Pattern Matching Algorithms, Oxford University Press, 1997

VII. TRANG THIẾT BỊ DẠY HỌC

7.1. Giảng đường cho các buổi học lý thuyết

- Máy chiếu
- Bảng viết

7.2. Phòng máy cho các buổi học thực hành

- Máy chiếu
- Máy tính chạy hệ điều hành Windows, có kết nối Internet
- Công cụ lập trình: C/C++, Java

VIII. ĐÁNH GIÁ KẾT QUẢ HỌC TẬP

8.1. Chấm điểm

Điểm đánh giá	Căn cứ đánh giá	Công thức tính
Điểm chuyên cần	Đi học đầy đủ, tham gia xây dựng bài; Kết quả các bài thực hành	(1)
Điểm thi giữa kỳ	Bài thi giữa kỳ	(2)
Điểm quá trình	(1), (2)	(3) = 0,3×(1) + 0,7×(2)
Điểm thi kết thúc học phần	Bài thi kết thúc học phần	(4)
Điểm học phần	(3), (4)	(5) = 0,3×(3) + 0,7×(4)

8.2. Điều kiện để được thi kết thúc học phần

- Dự lớp tối thiểu 75% số giờ học
- Điểm quá trình đạt tối thiểu 4,0 (thang điểm 10)

8.3. Hình thức thi kết thúc học phần

Thực hành lập trình trên máy