BỘ CÔNG THƯƠNG
TRƯỜNG ĐẠI HỌC SAO ĐỎ
*****

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN
BẢO MẬT THÔNG TIN

Số tín chỉ: 03
Trình độ đào tạo: Đại học
Ngành đào tạo: Công nghệ thông tin

Năm 2020

TRƯỜNG ĐẠI HỌC SAO ĐỎ
KHOA: ĐIỆN TỬ - TIN HỌC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

Trình độ đào tạo: Đại học
Ngành đào tạo: Công nghệ thông tin

1. Tên học phần: Bảo mật thông tin
2. Mã học phần: CNTT 202
3. Số tín chỉ: 3 (2, 1)
4. Trình độ cho sinh viên: Năm thứ tư
5. Phân bổ thời gian
- Lên lớp: 30 tiết lý thuyết, 30 tiết thực hành.
- Tự học: 90 giờ.

6. Điều kiện tiên quyết: Ngôn ngữ Java; Mạng máy tính
7. Giảng viên

STT	Học hàm, học vị, họ tên	Số điện thoại	Email
1	ThS. Phạm Thị Hường	0972.306.806	PTHuong@saodo.edu.vn
2	ThS. Hoàng Thị Ngọc Diệp	0969.803.788	HTNDiep@saodo.edu.vn

8. Mô tả nội dung của học phần

Học phần Bảo mật thông tin gồm các kiến thức cơ bản về bảo mật thông tin, bảo mật mạng; giới thiệu các phương pháp mã hóa, giải mã và ứng dụng của chúng trong bảo mật thông tin.

9. Mục tiêu và chuẩn đầu ra học phần

9.1. Mục tiêu

Mục tiêu học phần thỏa mãn mục tiêu của chương trình đào tạo:

Mục tiêu	Mô tả	Mức độ theo thang đo Bloom	Phân bổ mục tiêu học phần trong CTĐT
MT1	**Kiến thức**		
MT1.1	Trình bày nội dung của an toàn và bảo mật thông tin, các chiến lược an toàn hệ thống, các mức bảo vệ trên mạng, ý tưởng chung của an toàn thông tin bằng mật mã và tiêu chuẩn để đánh giá một hệ mật mã.	2	[1.2.1.2a]
MT1.2	Trình bày các giải thuật mã hóa, giải mã, thám mã các hệ bất đối xứng, đối xứng, sơ đồ chữ ký số, hàm băm vào mã hóa, giải mã thông tin.	2	[1.2.1.2b]

Mục tiêu	Mô tả	Mức độ theo thang đo Bloom	Phân bổ mục tiêu học phần trong CTĐT
MT1.3	Tính toán các khóa, bản mã, bản rõ, chữ ký của từng hệ mật mã.	3	[1.2.1.2b]
MT2	**Kỹ năng**		
MT2.1	Áp dụng các phương pháp mã hóa, giải mã, thám mã các hệ mật mã vào thực hành cài đặt chương trình để bảo mật thông tin.	3	[1.2.2.1]
MT2.2	Phân tích kỹ thuật mã hóa, giải mã của hệ mật mã; kỹ thuật ký và xác minh của các hệ chữ ký.	4	[1.2.2.1]
MT2.3	Đánh giá các hệ mật mã và ứng dụng bảo mật thông tin dùng hệ mật mã và chữ ký số.	5	[1.2.2.2]
MT3	**Mức tự chủ và trách nhiệm**		
MT3.1	Có thái độ nghiêm túc, tự giác, tích cực, khoa học, độc lập, cẩn thận, tuân thủ trong công việc.	3	[1.2.3.1]
MT3.2	Có năng lực giải quyết các công việc liên quan đến bảo mật thông tin dữ liệu.	4	[1.2.3.2]

9.2. Chuẩn đầu ra

Sự phù hợp của chuẩn đầu ra học phần với chuẩn đầu ra của chương trình đào tạo:

CĐR học phần	Mô tả	Thang đo Bloom	Phân bổ CĐR học phần trong CTĐT
CĐR1	**Kiến thức**		
CĐR1.1	Giải thích được nội dung bí mật, xác thực, trách nhiệm của an toàn thông tin; 6 chiến lược an toàn hệ thống, 6 mức bảo vệ trên mạng; ý nghĩa 5 thành phần của an toàn thông tin bằng mật mã và 3 tiêu chuẩn để đánh giá một hệ mật mã.	2	[2.1.4]
CĐR1.2	Diễn giải được các giải thuật mã hóa, giải mã, thám mã hệ mật mã đối xứng, bất đối xứng, chữ ký, hàm băm, quản lý khóa.	2	[2.1.4]
CĐR1.3	Phân tích được bản rõ, bản mã, phương pháp mã hóa, giải mã, thám mã ứng với từng hệ mật mã.	4	[2.1.4]

CĐR học phần	Mô tả	Thang đo Bloom	Phân bổ CĐR học phần trong CTĐT
CĐR2	**Kỹ năng**		
CĐR2.1	Áp dụng các phương pháp mật mã cổ điển, mã khối, mã công khai, chữ ký số, hàm băm, quản lý khóa vào thực tế bảo mật thông tin.	3	[2.2.1]
CĐR2.2	Phân biệt được các hệ mật mã công khai về ý tưởng, giải thuật và áp dụng so với hệ mã bí mật.	4	[2.2.1]
CĐR2.3	Đánh giá được các chương trình sử dụng hệ chữ ký số để kiểm tra tính toàn vẹn và tính không chối cãi của file dữ liệu.	5	[2.2.7]
CĐR3	**Mức tự chủ và trách nhiệm**		
CĐR3.1	Nghiêm túc, tự giác, tích cực, khoa học, độc lập, cẩn thận, tuân thủ trong công việc.	3	[2.3.1]
CĐR3.2	Định hướng, hướng dẫn và đưa ra kết luận liên quan đến công việc bảo mật thông tin.	4	[2.3.2]

10. Ma trận liên kết nội dung với chuẩn đầu ra học phần

Chương	Nội dung học phần	Chuẩn đầu ra của học phần							
		CĐR1			CĐR2			CĐR3	
		CĐR 1.1	CĐR 1.2	CĐR 1.3	CĐR 2.1	CĐR 2.2	CĐR 2.3	CĐR 3.1	CĐR 3.2
1	**Chương 1. Tổng quan về an toàn và bảo mật thông tin** 1.1. Nội dung của an toàn và bảo mật thông tin 1.2. Các chiến lược an toàn hệ thống 1.3. Các mức bảo vệ trên mạng 1.4. An toàn thông tin bằng mật mã 1.5. Vai trò của hệ mật mã 1.6. Phân loại hệ mật mã	x						x	

Chương	Nội dung học phần	Chuẩn đầu ra của học phần							
		CĐR1			CĐR2			CĐR3	
		CĐR 1.1	CĐR 1.2	CĐR 1.3	CĐR 2.1	CĐR 2.2	CĐR 2.3	CĐR 3.1	CĐR 3.2
	1.7. Tiêu chuẩn đánh giá hệ mật mã								
2	**Chương 2. Các phương pháp mã hóa cổ điển** 2.1. Các hệ mật mã cổ điển 2.2. Thám mã các hệ mã cổ điển		x	x	x			x	
3	**Chương 3. Mật mã khối** 3.1. Mật mã khối 3.2. Hệ mã DES 3.3. Các điểm yếu của DES 3.4. Triple DES 3.5. Hệ mã AES 3.6. Các cơ chế, hình thức sử dụng của mã hóa khối		x	x	x			x	
4	**Chương 4. Mật mã công khai** 4.1. Giới thiệu về hệ mật mã khóa công khai 4.2. Hệ mật RSA 4.3. Hệ mật mã Rabin 4.4. Hệ mật Elgamal và các hệ tương tự 4.5. Các hệ mật mã dựa trên các bài toán NP- đầy đủ		x	x	x	x		x	
5	**Chương 5. Các sơ đồ chữ ký số**		x	x	x		x		x

Chương	Nội dung học phần	Chuẩn đầu ra của học phần							
		CĐR1			CĐR2			CĐR3	
		CĐR 1.1	CĐR 1.2	CĐR 1.3	CĐR 2.1	CĐR 2.2	CĐR 2.3	CĐR 3.1	CĐR 3.2
	5.1. Định nghĩa sơ đồ chữ ký số 5.2. Sơ đồ chữ ký RSA 5.3. Sơ đồ chữ ký ELGAMAL 5.4. Sơ đồ chữ ký không phủ định được 5.5. Hàm băm và chữ ký số								
6	**Chương 6. Quản lý khóa** 6.1. Quản lý khóa trong các mạng truyền tin 6.2. Một số hệ phân phối khóa 6.3. Trao đổi khóa và thỏa thuận khóa		x	x	x	x			x

11. Đánh giá học phần

11.1. Kiểm tra và đánh giá trình độ

Chuẩn đầu ra	Mức độ thành thạo được đánh giá bởi
CĐR1	Kiểm tra thường xuyên, kiểm tra thực hiện nhiệm vụ về nhà, kiểm tra giữa học phần, thi kết thúc học phần.
CĐR2	Bài tập thực hành, thực hiện nhiệm vụ về nhà, kiểm tra giữa học phần, thi kết thúc học phần.
CĐR3	Kiểm tra thường xuyên, kết quả thực hiện nhiệm vụ của cá nhân và theo nhóm, thi kết thúc học phần.

11.2. Cách tính điểm học phần: Tính theo thang điểm 10 sau đó chuyển thành thang điểm chữ và thang điểm 4.

STT	Điểm thành phần	Quy định	Trọng số	Ghi chú
1	Điểm kiểm tra thường xuyên; điểm đánh giá nhận thức và thái độ tham gia thảo luận; điểm đánh giá phần bài tập; điểm chuyên cần	01 điểm	20%	Điểm trung bình của các lần đánh giá

STT	Điểm thành phần	Quy định	Trọng số	Ghi chú
2	Điểm kiểm tra giữa học phần	01 điểm	30%	
3	Điểm thi kết thúc học phần	01 điểm	50%	

11.3. Phương pháp đánh giá

- Kiểm tra thường xuyên; đánh giá nhận thức và thái độ tham gia thảo luận; đánh giá nhiệm vụ tự học; chuyên cần: Vấn đáp.

- Kiểm tra giữa học phần: Tự luận (01 bài kiểm tra, thời gian làm bài: 90 phút).

- Thi kết thúc học phần: Tự luận (01 bài thi, thời gian làm bài: 90 phút).

12. Yêu cầu học phần

- Tham gia tối thiểu 80% số tiết học trên lớp dưới sự hướng dẫn của giảng viên.

- Đọc và nghiên cứu tài liệu phục vụ học phần, hoàn thành các bài tập cá nhân và bài tập nhóm.

- Chủ động ôn tập theo đề cương ôn tập được giảng viên cung cấp.

- Tham gia kiểm tra giữa học phần, thi kết thúc học phần.

- Dụng cụ học tập: Máy tính, vở ghi, bút,...

13. Tài liệu phục vụ học phần

- Tài liệu bắt buộc:

[1] - Trường ĐH Sao Đỏ (2019), *Giáo trình Bảo mật thông tin.*

- Tài liệu tham khảo:

[2] - Trương Tiến Tùng (2011), *Mật mã an toàn thông tin*, NXB Thông tin và truyền thông.

[3] - Douglas R. Stinson (1995), *Cryptography Theory and practice*. CRC Press.

14. Nội dung chi tiết học phần và phương pháp dạy-học

TT	Nội dung giảng dạy	Số tiết	Phương pháp dạy-học	CĐR học phần
1	**Chương 1. Tổng quan về an toàn và bảo mật thông tin** **Mục tiêu chương:** Sau khi học xong chương này, sinh viên giải thích được các nội dung về an toàn và bảo mật thông tin, các chiến lược an toàn hệ thống, các mức bảo vệ trên mạng, cách phân loại và đánh giá một hệ mật mã.	4 (2LT, 2TH)	**Thuyết trình; Tổ chức học theo nhóm; Thực hành trên máy tính** **- Giảng viên:** + Giải thích các khái niệm, định nghĩa về an toàn và bảo mật thông tin. + Giao bài tập, nội dung thực hành cho cá nhân, các nhóm. + Hướng dẫn sinh viên thực hành, đánh giá, nhận xét.	CĐR1.1; CĐR3.1.

TT	Nội dung giảng dạy	Số tiết	Phương pháp dạy-học	CĐR học phần
	Nội dung cụ thể: 1.1. Nội dung của an toàn và bảo mật thông tin 1.2. Các chiến lược an toàn hệ thống 1.3. Các mức bảo vệ trên mạng 1.4. An toàn thông tin bằng mật mã 1.5. Vai trò của hệ mật mã 1.6. Phân loại hệ mật mã 1.7. Tiêu chuẩn đánh giá hệ mật mã Bài thực hành số 1.		**- Sinh viên:** + Đọc trước tài liệu: [1]: Chương 1; + Lắng nghe, ghi chép, quan sát. + Làm bài tập cá nhân, theo nhóm trong [1]: Chương 1. + Thực hành bài thực hành số 1.	
2	**Chương 2. Các phương pháp mã hóa cổ điển** **Mục tiêu chương:** Sau khi học xong chương này, sinh viên đạt được các yêu cầu cơ bản sau: - Giải thích được các phương pháp mã hóa, giải mã và thám mã các hệ mật mã cổ điển như mã dịch vòng, mã thay thế, mã affine, mã Vigenère, mã Hill, các hệ mã dòng. - Phân tích được bản rõ, bản mã, phương pháp mã hóa, giải mã, thám mã ứng với từng hệ mật mã trong hệ mã cổ điển. - Áp dụng vào thực hành cài đặt các hệ mật mã cổ điển trong vấn đề bảo mật thông tin. **Nội dung cụ thể:** 2.1. Các hệ mật mã cổ điển	16 (8LT, 8TH)	**Thuyết trình; Phương pháp động não; Tổ chức cho sinh viên tranh luận; Tổ chức học theo nhóm; Thực hành trên máy tính** **- Giảng viên:** + Giải thích và minh họa các giải thuật mã hóa, giải mã, phá mã của phương pháp mã hóa cổ điển. + Nêu nội dung vấn đề cần giải quyết. + Nêu nội dung tranh luận. + Giao bài tập, nội dung thực hành cho cá nhân và các nhóm. + Hướng dẫn sinh viên thực hành, đánh giá, nhận xét. **- Sinh viên:** + Đọc trước tài liệu: [1]: Chương 2; [2]: Chương 1. + Lắng nghe, ghi chép, quan sát, tranh luận và phản biện.	CĐR1.2; CĐR1.3; CĐR2.1; CĐR3.1.

TT	Nội dung giảng dạy	Số tiết	Phương pháp dạy-học	CĐR học phần
	2.1.1. Mã dịch vòng (Shift Cipher) 2.1.2. Mã thay thế 2.1.3. Mã Affine 2.1.4. Mã Vigenère 2.1.5. Mật mã Hill 2.1.6. Các hệ mã dòng 2.2. Thám mã các hệ mã cổ điển 2.2.1. Thám mã dịch vòng 2.2.2. Thám mã Affine 2.2.3. Thám mã thay thế 2.2.4. Thám mã Vigenère 2.2.5. Tấn công với bản rõ đã biết trên hệ mật Hill 2.2.6. Thám mã hệ mã dòng xây dựng trên LFSR Bài thực hành số 2 - 5.		+ Làm bài tập theo nhóm trong [1]: Chương 2. + Thực hành bài thực hành số 2 - 5.	
3	**Chương 3. Mật mã khối** **Mục tiêu chương:** Sau khi học xong chương này, sinh viên đạt được các yêu cầu cơ bản sau: - Giải thích được nguyên tắc hoạt động của mã dữ liệu DES: Thuật toán, hoán vị khởi đầu, khóa chuyển đổi, hoán vị mở rộng, hộp thay thế S, hộp hoán vị P, hoán vị cuối cùng, giải mã DES, AES; phần cứng và phần mềm thực hiện DES, sự an và các chế độ hoạt động của DES. - Phân tích được bản rõ, bản mã, phương pháp tạo khóa, mã hóa, giải mã, thám mã DES, AES.	16 (6LT, 8TH, 2KT)	**Thuyết trình; Dạy học dựa trên vấn đề; Tổ chức cho sinh viên tranh luận; Tổ chức học theo nhóm Thực hành trên máy tính** **- Giảng viên:** + Giải thích ý tưởng và giải thuật mã hóa, giải mã, phá phá hệ mã khối DES. + Nêu vấn đề, hướng dẫn sinh viên giải quyết vấn đề. + Nêu nội dung tranh luận. + Giao bài tập, nội dung thực hành cho cá nhân, các nhóm. + Hướng dẫn sinh viên thực hành, đánh giá, nhận xét. **- Sinh viên:** + Đọc trước tài liệu: [1]: Chương 3;	CĐR1.2; CĐR1.3; CĐR2.1; CĐR3.1.

TT	Nội dung giảng dạy	Số tiết	Phương pháp dạy-học	CĐR học phần
	- Áp dụng vào thực hành cài đặt mã DES, AES trong bảo mật thông tin. **Nội dung cụ thể:** 3.1. Mật mã khối 3.2. Hệ mã DES 3.2.1. Sơ đồ mã DES 3.2.2. Hoán vị IP và hoán vị ngược 3.2.3. Thuật toán sinh khóa con 3.2.4. Mô tả hàm f 3.2.5. Hàm mở rộng E 3.2.6. Hộp S-Box 3.2.7. Hộp P-Box 3.2.8. Thuật toán giải mã DES 3.3. Các điểm yếu của DES 3.4. Triple DES 3.5. Hệ mã AES 3.6. Các cơ chế, hình thức sử dụng của mã hóa khối 3.6.1. Hình thức sử dụng 3.6.2. Cơ chế bảng tra mã điện tử ECB 3.6.3. Cơ chế mã móc xích CBC 3.6.4. Chế độ mã phản hồi CFB Kiểm tra giữa học phần Bài thực hành số 6 - 9.		[2]: Chương 2; [3]: Chương 3. + Lắng nghe, ghi chép, quan sát, tranh luận, phản biện và giải quyết các vấn đề. + Làm bài tập cá nhân, theo nhóm trong [1]: Chương 3. + Làm bài kiểm tra. + Thực hành bài thực hành số 6 - 9.	
4	**Chương 4. Mật mã công khai** **Mục tiêu chương:** Sau khi học xong chương này, sinh viên đạt được các yêu cầu cơ bản sau: - Giải thích được nguyên tắc hoạt động của hệ mật mã khóa công khai, hệ mật mã RSA, hệ mật mã Rabin, hệ mật mã Elgamal và các	8 (4LT, 4TH)	**Thuyết trình; Dạy học dựa trên vấn đề; Tổ chức học theo nhóm; Thực hành trên máy tính** **- Giảng viên:** + Giải thích ý tưởng, giải thuật má hóa, giải mã, phá phá của các hệ mã khóa công khai.	CĐR1.2; CĐR1.3; CĐR2.1; CĐR2.2; CĐR3.1.

TT	Nội dung giảng dạy	Số tiết	Phương pháp dạy-học	CĐR học phần
	hệ tương tự, các hệ mật mã dựa trên các bài toán NP-đầy đủ. - Phân tích được bản rõ, bản mã, phương pháp mã hóa, giải mã, thám mã hệ công khai. - Áp dụng hệ mật mã công khai vào thực hành cài đặt chương trình nhằm bảo mật thông tin. **Nội dung cụ thể:** 4.1. Giới thiệu về hệ mật mã khóa công khai 4.2. Hệ mật RSA 4.2.1. Thuật toán RSA 4.2.2. Một số thuật toán triển khai trong RSA 4.2.3. Độ an toàn của hệ mật RSA 4.3. Hệ mật mã Rabin 4.4. Hệ mật Elgamal và các hệ tương tự 4.5. Các hệ mật mã dựa trên các bài toán NP-đầy đủ Bài thực hành số 10 – 11.		+ Nêu vấn đề, hướng dẫn sinh viên giải quyết vấn đề. + Giao bài tập, nội dung thực hành cho cá nhân, các nhóm. + Hướng dẫn sinh viên thực hành, đánh giá, nhận xét. **- Sinh viên:** + Đọc trước tài liệu: [1]: Chương 4; [2]: Chương 4; [3]: Chương 5; + Lắng nghe, ghi chép, quan sát và giải quyết các vấn đề. + Làm bài tập cá nhân, theo nhóm trong [1]: Chương 4. + Thực hành bài thực hành số 10 - 11.	
5	**Chương 5. Các sơ đồ chữ ký số** **Mục tiêu chương:** Sau khi học xong chương này, sinh viên đạt được các yêu cầu cơ bản sau: - Giải thích được sơ đồ chữ ký số, sơ đồ chữ ký RSA, sơ đồ chữ ký Elgamal, sơ đồ chữ ký không phủ định được, hàm băm và chữ ký số.	8 (4LT, 4TH)	**Thuyết trình; Tổ chức cho sinh viên tranh luận; Tổ chức học theo nhóm; Thực hành trên máy tính** **- Giảng viên:** + Giải thích các giai đoạn ký, xác minh của sơ đồ chữ ký và hàm băm. + Nêu nội dung tranh luận. + Tổ chức thảo luận	CĐR1.2; CĐR1.3; CĐR2.1; CĐR2.3; CĐR3.2.

TT	Nội dung giảng dạy	Số tiết	Phương pháp dạy-học	CĐR học phần
	- Phân tích được bản rõ, bản mã, phương pháp mã hóa, giải mã hệ chữ ký và hàm băm. - Áp dụng sơ đồ chữ ký số, hàm băm vào cài đặt chương trình thử nghiệm. **Nội dung cụ thể:** 5.1. Định nghĩa sơ đồ chữ ký số 5.2. Sơ đồ chữ ký RSA 5.3. Sơ đồ chữ ký ELGAMAL 5.4. Sơ đồ chữ ký không phủ định được 5.5. Hàm băm và chữ ký số Bài thực hành số 12 – 13.		+ Giao bài tập, nội dung thực hành cho cá nhân và các nhóm. + Hướng dẫn sinh viên thực hành, đánh giá, nhận xét. **- Sinh viên:** + Đọc trước tài liệu: [1]: Chương 5; [2]: Chương 5; [3]: Chương 7; + Lắng nghe, ghi chép, quan sát, thảo luận, tranh luận và phản biện. + Làm bài tập cá nhân, theo nhóm trong [1]: Chương 5. + Thực hành bài thực hành số 12 - 13.	
6	**Chương 5. Quản lý khóa** **Mục tiêu chương:** Sau khi học xong chương này, sinh viên đạt được các yêu cầu cơ bản sau: - Giải thích được nguyên tắc quản lý khóa, trung tâm phân phối khóa, trao đổi khóa. - Phân tích được trung tâm phân phối khóa, trao đổi khóa. - Áp dụng sơ đồ trao đổi khóa Diffie Hellman vào cài đặt chương trình nhằm bảo mật thông tin. **Nội dung cụ thể:** 6.1. Quản lý khóa trong các mạng truyền tin 6.2. Một số hệ phân phối khóa	8 (4LT, 4TH)	**Thuyết trình; Tổ chức cho sinh viên tranh luận; Tổ chức học theo nhóm; Thực hành trên máy tính** **- Giảng viên:** + Giải thích nguyên tắc quản lý khóa. + Nêu nội dung tranh luận. + Tổ chức thảo luận + Giao bài tập, nội dung thực hành cho cá nhân và các nhóm. + Hướng dẫn sinh viên thực hành. **- Sinh viên:** + Đọc trước tài liệu: [1]: Chương 5; [2]: Chương 3.	CĐR1.2; CĐR1.3; CĐR2.1; CĐR2.2; CĐR3.2.

TT	Nội dung giảng dạy	Số tiết	Phương pháp dạy-học	CĐR học phần
	6.2.1. Sơ đồ phân phối khoá Blom 6.2.2. Hệ phân phối khoá Kerberos 6.2.3. Hệ phân phối khóa Diffe-Hellman 6.3. Trao đổi khóa và thỏa thuận khóa 6.3.1. Giao thức trao đổi khoá Diffie-Hellman 6.3.2. Giao thức trao đổi khoá Diffie-Hellman có chứng chỉ xác nhận 6.3.3. Giao thức trao đổi khoá Matsumoto-Takashima-Imai 6.3.4. Giao thức Girault trao đổi khoá không chứng chỉ Bài thực hành số 14 - 15.		+ Lắng nghe, ghi chép, thảo luận, tranh luận và phản biện. + Làm bài tập cá nhân, theo nhóm trong [1]: Chương 6. + Thực hành bài thực hành số 14 - 15.	

Hải Dương, ngày 24 tháng 09 năm 2020

KT.HIỆU TRƯỞNG PHÓ HIỆU TRƯỞNG	KT.TRƯỞNG KHOA PHÓ TRƯỞNG KHOA	TRƯỞNG BỘ MÔN
TS. Nguyễn Thị Kim Nguyên	Phạm Văn Kiên	Phạm Văn Kiên