HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA ATTT

ĐỀ THI KẾT THÚC HỌC PHẦN
MÔN: CƠ SỞ ATTT
Thời gian làm bài thi: 90 phút

ĐỀ 01

Sinh viên viết đáp án ĐÚNG vào cột "ĐÁP ÁN"

STT	Câu hỏi	ĐÁP ÁN
1.	Khi thiết lập luật ACL cho bộ định tuyến, cần tuân thủ hướng dẫn chung nào? A. Không cho phép lưu lượng truy cập dựa trên địa chỉ IP. B. Không chặn lưu lượng dựa trên địa chỉ IP. C. Quy tắc đầu tiên phải là quy tắc từ chối tất cả. D. Quy tắc cuối cùng phải là quy tắc từ chối tất cả.	D
2.	Sắp xếp các phương pháp định danh theo thứ tự an toàn tăng dần? A. Thẻ thông minh, quét võng mạc, mật khẩu B. Quét võng mạc, mật khẩu, thẻ thông minh C. Tên người dùng và mật khẩu, thẻ thông minh, quét võng mạc D. ACL, tên người dùng và mật khẩu, quét võng mạc	C
3.	Giao thức nào sau đây không thể định tuyến? A. HTTP B. DNS C. NetBIOS D. Telnet	C
4.	Khi truy cập vào các tài liệu trong một thư mục trên máy tính của bạn, bạn nhận thấy tất cả các tệp đã bị đổi tên thành các tên tệp ngẫu nhiên. Ngoài ra, bạn thấy một tài liệu chứa các hướng dẫn thanh toán để giải mã các tệp tin. Trong trường hợp này bạn đã nhiễm mã độc nào? A. Encryptionware B. Mã độc C. Criminalware D. Ransomware	D
5.	Một máy trạm có địa chỉ IP là 169.254.46.86. Các quản trị viên máy chủ nhận ra dịch vụ DHCP đang ngoại tuyến, vì vậy họ bắt đầu dịch vụ DHCP. Lệnh nào sẽ được sử dụng tiếp theo trên máy trạm để ngay lập tức có được cấu hình TCP / IP hợp lệ? A. ping -t B. tracert C. netstat -a D. ipconfig / renew	D
6.	Một loại phần mềm độc hại thay thế một thư viện hợp lệ của chương trình bằng một thư viện khác chứa các mã điều khiển nhằm chiếm quyền kiểm soát chương trình đó. Mã độc này sử dụng kỹ thuật nào sau đây?	A

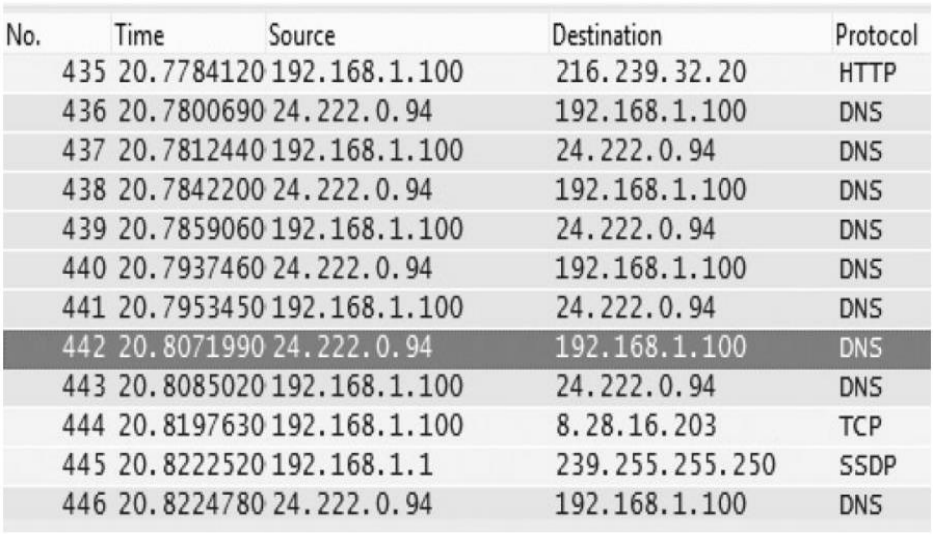
	A. DLL injection B. Pointer dereference C. Integer overflow D. Buffer overflow	
7.	Khi giám sát lưu lượng mạng, bạn nhận thấy rất nhiều kết nối IMAP giữa mạng của công ty bạn và địa chỉ IP không thuộc về máy chủ email của công ty. Nguyên nhân của những lưu lượng này là gì?? A. Các mã độc nâng cao B. Các ứng dụng nằm trong Whitelist C. DEP D. E-mail cá nhân	D
8.	Một hacker ngồi trong quán cà phê có điểm truy cập Internet và tiến hành thực hiện ARP poisoning mọi người kết nối với mạng không dây để tất cả lưu lượng truy cập qua máy tính xách tay hacker trước khi cô định tuyến lưu lượng truy cập vào Internet. Đây là loại tấn công nào? A. Rainbow tables B. Man in the middle C. DNS poison D. Spoofing	B
9.	Việc kiểm toán an ninh xác định thấy ba bộ định tuyến không dây không an toàn do sử dụng các cấu hình mặc định. Nguyên tắc bảo mật nào đã bị bỏ qua? A. Quản lý bản vá ứng dụng B. Kiện toàn an toàn thiết bị C. Xác thực đầu vào D. Nguyên tắc đặc quyền tối thiểu	B
10.	Có thể làm gì để bảo vệ dữ liệu sau khi thiết bị xách tay bị mất hoặc bị đánh cắp? A. Kích hoạt mã hóa. B. Thực hiện xóa dữ liệu từ xa. C. Kích hoạt khóa màn hình. D. Vô hiệu hóa phát hiện Bluetooth.?	B
11.	Một người dùng báo cáo sự cố bàn phím USB. Bạn kiểm tra mặt sau của máy tính để đảm bảo bàn phím được kết nối đúng cách và nhận thấy một đầu nối nhỏ giữa bàn phím và cổng USB của máy tính. Sau khi điều tra, bạn biết rằng phần cứng này nắm bắt mọi thứ mà người dùng nhập vào. Đây là loại phần cứng nào? A. Smartcard B. Trojan C. Keylogger D. Bộ chuyển đổi PS/2	C
12.	Loại phần mềm nào giúp lọc bỏ các email rác không mong muốn? A. Anti-spam B. Antivirus C. Antispyware D. Anti-adware	A
13.	Khi lập kế hoạch thiết kế hạ tầng mạng, bạn quyết định sử dụng tường	B

	lửa phân tách giữa mạng Internet và mạng nội bộ. Bạn nên sử dụng tường lửa như thế nào? A. Quy tắc ACL cuối cùng sẽ cho phép tất cả. B. Sử dụng các thiết bị tường lửa từ các nhà cung cấp khác nhau. C. Quy tắc ACL đầu tiên nên từ chối tất cả. D. Sử dụng các thiết bị tường lửa từ cùng một nhà cung cấp	
14.	Những kỹ thuật kiểm thử ứng dụng nào giúp tìm kiếm những xử lý đầu vào không đúng? A. Fuzzing B. Overloading C. Kiểm thử xâm nhập D. Quét lỗ hổng	A
15.	Một đoạn mã độc sử dụng các cuộc tấn công từ điển vào máy tính để có quyền truy cập vào tài khoản quản trị. Đoạn mã này sau đó liên kết các máy tính bị xâm nhập với nhau nhằm mục đích nhận các lệnh từ xa. Thuật ngữ nào mô tả ĐÚNG NHẤT loại mã độc này? A. Exploit B. Botnet C. Logic bomb D. Backdoor	B
16.	Bạn kiện toàn máy tính sử dụng Linux và đã vô hiệu hóa SSH và thay bằng Telnet. Bạn đảm bảo rằng mật khẩu được yêu cầu để truy cập Telnet. Bạn đã mắc phải lỗi nào trong trường hợp trên. A. Telnet bảo mật phải được bật xác thực khóa công khai. B. Chỉ nên sử dụng mật khẩu mạnh với Telnet. C. SSH nên được sử dụng thay vì Telnet. D. Cổng Telnet nên được thay đổi từ 23 thành 8080	C
17.	Sự khác biệt giữa rootkit và tấn công leo thang đặc quyền? A. Rootkit tự nhân bản. B. Sự leo thang đặc quyền là kết quả của một rootkit. C. Rootkit là kết quả của sự leo thang đặc quyền. D. Mỗi kiểu sử dụng một cổng TCP khác nhau.	B
18.	Chức năng User Account Control (UAC) trong Windows 8 cho phép người dùng có thể thay đổi các cài đặt của Windows nhưng trước khi thay đổi sẽ hiển thị lời nhắc để xác nhận lại sự thay đổi này cho người dùng. Điều này giúp chống lại tấn công nào? A. Leo thang đặc quyền B. Adware C. Spyware D. Worms	A
19.	Ai là người xác định cách gán nhãn dữ liệu? A. Người giám sát B. Chủ sở hữu C. Nhân viên bảo mật D. Quản trị viên hệ thống	B
20.	Bạn đã được yêu cầu triển khai một giải pháp dựa trên bộ định tuyến cho phép lưu lượng SSH đến từ một	b

	mạng con cụ thể. Bạn nên cấu hình cái gì? A. NIC B. ACL C. Proxy D. PSK	
21.	Một người dùng trên mạng của bạn nhận được e-mail từ ngân hàng nói rằng đã có sự cố bảo mật tại ngân hàng. Email tiếp tục bằng cách yêu cầu người dùng đăng nhập vào tài khoản ngân hàng của mình bằng cách theo liên kết được cung cấp và xác minh rằng tài khoản của cô ấy không bị giả mạo. Đây là loại tấn công nào? A. Phishing B. Spam C. Dictionary attack D. Spim	A
22.	Giao thức nào sử dụng cổng TCP 443? A. FTPS B. HTTP C. HTTPS D. SSH	C
23.	Hưng đang thực hiện việc theo dõi lưu lượng mạng Wi-Fi bằng cách sử dụng bộ phân tích gói tin và có thể đọc được các nội dung truyền qua mạng. Biện pháp nào sau đây có thể giữ cho các kết nối qua mạng được riêng tư? A. Cài đặt chứng chỉ số trên mỗi thiết bị truyền. B. Đặt mật khẩu quản trị viên mạnh cho bộ định tuyến Wi-Fi. C. Sử dụng xác thực thẻ thông minh. D. Mã hóa lưu lượng Wi-Fi.?	D
24.	Những thiết bị nào trong doanh nghiệp của bạn nên được cập nhật bản vá thường xuyên? (Chọn tất cả các đáp án đúng.) A. Mainframes B. Máy trạm C. Các máy ảo ảo hóa trên đám mây công cộng D. IP addresses	A,B
25.	Một trang web không đáp ứng được một lượng lớn yêu cầu truy vấn HTTP đến máy chủ web. Giải pháp nào giúp tăng hiệu năng và giải quyết tình trạng này cho máy chủ web? A. Nâng cấp dung lượng RAM cho máy chủ web. B. Cài đặt hai máy chủ web lưu trữ cùng một nội dung. Cấu hình bộ cân bằng tải để phân phối kết nối HTTP đến giữa hai máy chủ web. C. Đặt bộ định tuyến giữa máy chủ web và Internet để điều tiết các kết nối HTTP đến. D. Kích hoạt SSL trên máy chủ web.	b
26.	Người dùng ở trụ sở Đà Nẵng không thể kết nối với máy chủ web của công ty được đặt tại Hà Nội, nhưng họ có thể kết nối với các trang web khác trên Internet. Các kỹ thuật viên ở Hà Nội khẳng định máy chủ web đang chạy vì người dùng ở Hà Nội không gặp vấn đề gì khi kết nối với máy chủ web này. Bạn sử dụng công cụ ping đến máy chủ web ở	A

	Hà Nội nhưng không nhận được phản hồi. Bạn nên sử dụng công cụ nào tiếp theo? A. tracert B. ipconfig C. Telnet D. HTTP	
27.	Các nhà phát triển web tại công ty của bạn đang thử nghiệm mã trang web mới nhất của họ trước khi đi vào hoạt động để đảm bảo rằng nó hoạt động hiệu quả và an toàn. Trong quá trình thử nghiệm, họ cung cấp các URL không đúng định dạng với các tham số bất thường bổ sung cũng như sự phong phú của dữ liệu ngẫu nhiên. Thuật ngữ nào mô tả hành động của họ? A. Cross-site scripting B. Fuzzing C. Vá D. Debugging	B
28.	Là quản trị viên Windows, bạn cấu hình dịch vụ mạng Windows để chạy với tài khoản được tạo đặc biệt với các quyền hạn chế. Tại sao bạn cần làm điều này? A. Để ngăn chặn sâu máy tính xâm nhập vào mạng. B. Để ngăn chặn tin tặc nhận được các đặc quyền nâng cao do dịch vụ mạng bị xâm nhập. C. Dịch vụ mạng Windows sẽ không chạy với quyền quản trị. D. Các dịch vụ mạng Windows phải chạy với quyền truy cập hạn chế.	B
29.	Điều nào sau đây thể hiện TỐT NHẤT nguyên tắc đặc quyền tối thiểu? A. Phát hiện sử dụng Internet không phù hợp B. Phát hiện phần mềm độc hại đang chạy mà không có đặc quyền nâng cao C. Gán cho người dùng toàn quyền kiểm soát tài nguyên mạng D. Gán các quyền cần thiết để cho phép người dùng hoàn thành nhiệm vụ?	D
30.	Loại lỗ hổng nào dẫn đến việc ghi dữ liệu vượt ra ngoài ranh giới bộ nhớ dự kiến? A. Pointer dereference B. Integer overflow C. Buffer overflow D. Rò rỉ bộ nhớ	C
31.	Tùy chọn nào sẽ bảo vệ máy tính xách tay của nhân viên khi họ đi du lịch và kết nối với mạng không dây? A. Phần mềm tường lửa cá nhân B. Lọc địa chỉ MAC C. Ảo hóa D. Thẻ không dây tương thích 802.11n	A
32.	Được phát hiện vào năm 1991, virus Michelangelo được cho là đã được kích hoạt để ghi đè lên 100 sector đĩa cứng đầu tiên với dữ liệu null mỗi năm vào ngày 6 tháng 3, đúng vào ngày sinh nhật của nghệ sĩ người Ý. Michelangelo thuộc loại virus nào?	D

	A. Zero day B. Worm C. Trojan D. Logic bomb	
33.	Biện pháp đối phó nào sau đây được thiết kế để bảo vệ chống lại cuộc tấn công vét cạn vào mật khẩu? A. Vá B. Khóa tài khoản C. Độ phức tạp của mật khẩu D. Mật khẩu mạnh	B
34.	Người quản lý của bạn đã đọc về các cuộc tấn công SQL Injecttion và đang tự hỏi có thể làm gì để bảo vệ chống lại chúng đối với các ứng dụng được phát triển nội bộ. Bạn muốn giới thiệu điều gì cho quản lý của mình? A. Vá B. Antivirus C. Xác thực đầu vào D. Tường lửa	C
35.	Bạn đang cấu hình một nhóm máy tính xách tay Windows cho nhân viên đi du lịch, một số người thích sử dụng chuột USB. Điều quan trọng là các máy móc càng an toàn càng tốt. Bạn nên cấu hình cái gì? (Chọn ba đáp án hợp lý nhất.) A. Tắt các cổng USB. B. Yêu cầu mã hóa thiết bị USB. C. Kích hoạt và cấu hình tường lửa Windows. D. Cài đặt và cấu hình phần mềm chống vi-rút. E. Kích hoạt chế độ lên lịch quản lý điện năng	B,C,D
36.	Mã hóa và ký điện tử lên e-mail bằng khóa công khai và khóa riêng có thể được thực hiện với công nghệ nào? A. 3DES B. DES C. Blowfish D. PGP	D
37.	Đâu là các hệ mật mã khối? (Chọn tất cả các đáp án đúng.) A. DES B. RSA C. RC4 D. AES	A,D
38.	Một nhân viên thu được lưu lượng truy cập mạng trên mạng LAN trong khoảng thời gian 24 giờ được biểu diễn như hình dưới. Nếu muốn xem lưu lượng truy cập mạng liên quan đến người dùng kết nối với các trang web thì anh ta cần lọc cột Giao thức nào trong cột giao thức trong hình?	A

	 A. HTTP B. DNS C. TCP D. SSDP	
39.	Để dễ dàng cấp quyền truy cập vào tài nguyên mạng cho nhân viên, bạn quyết định phải có một cách dễ dàng hơn là cấp cho người dùng quyền truy cập cá nhân vào tệp, máy in, máy tính và ứng dụng. Mô hình bảo mật nào bạn nên xem xét sử dụng? A. Kiểm soát truy cập bắt buộc B. Kiểm soát truy cập tùy ý C. Kiểm soát truy cập dựa trên vai trò D. Kiểm soát truy cập thời gian trong ngày	C
40.	Giao thức TCP / IP nào được thiết kế để đồng bộ hóa thời gian giữa các máy tính? A. SNMP B. Windows Time Service C. NTP D. SMTP	C
41.	Chính sách bảo mật của công ty nhấn mạnh tính bảo mật dữ liệu và bạn phải cấu hình các thiết bị máy tính một cách phù hợp. Bạn nên làm những gì? (Chọn hai.) A. Cài đặt trình đọc thẻ thông minh để người dùng có thể nhận dạng chính họ trước khi gửi các tin nhắn e-mail quan trọng. B. Thực thi mã hóa thẻ SD trên điện thoại thông minh cấp cho nhân viên. C. Cấu hình một cụm chuyển đổi dự phòng máy chủ để đảm bảo rằng các tài liệu nhạy cảm luôn có sẵn. D. Đặt quyền truy cập tệp và thư mục để kiểm soát quyền truy cập tệp của người dùng.	B,D
42.	Bạn lưu trữ tài liệu cá nhân và bảng tính trên một dịch dụ lưu trữ đám mây. Bạn muốn dữ liệu của mình chỉ khả dụng cho những người có khóa được chia sẻ đặc biệt. Bạn nên áp dụng điều gì cho các tài liệu và bảng tính của bạn? A. Quyền truy cập tệp B. Băm tập tin	D

	C. Sao lưu tệp D. Mã hóa tập tin	
43.	Dữ liệu quan trọng về mạng nội bộ của công ty bạn đã bị rò rỉ trực tuyến. Kẻ tấn công đã không tấn công mạng của bạn. Đây là vấn đề có thể xảy ra do nguyên nhân nào? A. Kiểm tra tính toàn vẹn của tệp B. Tường lửa dựa trên máy chủ C. Phương tiện truyền thông xã hội D. Lỗi DLP cho người dùng độc hại	C
44.	Mô hình bảo mật nào sử dụng phân loại dữ liệu và phân quyền người dùng dựa trên phân loại dữ liệu A. RBAC B. DAC C. PKI D. MAC	D
45.	Là quản trị viên máy chủ, bạn cấu hình cài đặt bảo mật sao cho mật khẩu phức tạp dài ít nhất tám ký tự phải được sử dụng cho tất cả tài khoản người dùng. Điều này là ứng dụng của nguyên tắc quản lý nào? A. Hết hạn B. Phục hồi C. Thông tin xác thực D. Vô hiệu hóa	C
46.	Phát biểu nào sau đây đúng? (Chọn tất cả các đáp án đúng.) A. Worms ghi lại tất cả các ký tự đã gõ vào một tệp văn bản. B. Worms tự phát tán sang các hệ thống khác. C. Worms có thể mang virus. D. Worms lây nhiễm vào đĩa cứng MBR.	B,C
47.	Bạn đang kiểm tra cấu hình bộ định tuyến của mình và phát hiện ra lỗ hổng bảo mật. Sau khi tìm kiếm trên Internet, bạn nhận ra rằng lỗ hổng này chưa được biết. Loại tấn công nào gây ảnh hưởng lớn nhất bộ định tuyến của bạn trong trường hợp này? A. Từ chối dịch vụ B. Phishing attack C. Zero-day exploit D. Ping of death	C
48.	Giải pháp nào sau đây đảm bảo an toàn cho việc truy cập một máy UNIX từ xa? A. SSH B. SSL C. SSO D. SHA	A
49.	Kiểu tấn công nào liên quan đến việc hacker gửi quá nhiều dữ liệu đến một dịch vụ hoặc ứng dụng thường dẫn đến việc hacker có quyền truy cập quản trị vào hệ thống? A. Tấn công ngày sinh nhật B. Typo squatting/URL hijacking C. Eavesdrop	D

	D. Buffer overflow	
50.	Phát biểu nào sau đây đúng với backdoors? (Chọn tất cả các đáp án đúng.) A. Chúng là mã độc. B. Chúng cho phép điều khiển quyền truy cập của người dùng thông qua cổng 26. C. Chúng được truy cập thông qua rootkit. D. Chúng cung cấp quyền truy cập vào tài khoản root Windows.	A,C
51.	Bạn đang kiểm tra một hệ thống của một người dùng sau khi cô ấy phàn nàn về tốc độ sử dụng Internet chậm hơn thường ngày. Sau khi phân tích hệ thống, bạn nhận thấy rằng địa chỉ MAC của cổng mặc định trong bộ đệm ARP đang tham chiếu sai địa chỉ MAC. Kiểu tấn công nào đã xảy ra? A. Brute force B. DNS poisoning C. Buffer overflow D. ARP poisoning	D
52.	Công nghệ nào sau đây đảm bảo tính toàn vẹn cho dữ liệu? A. 3DES B. RC4 C. AES D. MD5	D
53.	Bạn là nhân viên an toàn thông tin trong một cơ quan chính phủ. Bạn đang sửa đổi chính sách bảo mật USB. Những mục nào áp dụng cho bảo mật USB? (Chọn hai.) A. Không cho phép các ổ USB ngoài lớn hơn 1TB. B. Vô hiệu hóa cổng USB. C. Ngăn chặn dữ liệu của công ty bị sao chép vào thiết bị USB trừ khi mã hóa thiết bị USB được bật. D. Ngăn chặn dữ liệu công ty bị sao chép vào thiết bị USB trừ khi mã hóa cổng USB được bật.	B,C
54.	Quản trị viên mạng phải cấp quyền truy cập mạng phù hợp cho nhân viên mới. Điều nào sau đây là chiến lược tốt nhất? A. Cung cấp cho nhân viên mới tài khoản người dùng và các quyền cần thiết. B. Thêm tài khoản người dùng của nhân viên mới vào một nhóm. Đảm bảo rằng nhóm có các quyền cần thiết. C. Cung cấp cho nhân viên mới quyền quản trị mạng. D. Hỏi nhân viên mới những quyền mà cô ấy muốn.	B
55.	Trong khi thiết lập các cơ chế an toàn cho mạng, bạn triển khai một chính sách mật khẩu người dùng phức tạp. Mọi người dùng thường xuyên bày tỏ than phiền về việc quên mật khẩu. Những gì bạn nên cấu hình để làm giảm bớt những than phiền này? A. Hết hạn mật khẩu B. Thay đổi mật khẩu định kỳ C. Gợi ý mật khẩu D. Độ dài mật khẩu tối đa	C

56.	Bạn đang định cấu hình thiết bị mã hóa mạng và phải tính đến các thiết bị khác có thể không hỗ trợ các thuật toán mới hơn và mạnh hơn. Phát biểu nào sau đây liệt kê các tiêu chuẩn mã hóa từ yếu nhất đến mạnh nhất? A. DES, 3DES, RSA B. 3DES, DES, AES C. RSA, DES, Blowfish D. RSA, 3DES, DES	A
57.	Bạn quyết định rằng các máy tính LAN của bạn sẽ sử dụng mã hóa bất đối xứng với IPSec để bảo mật lưu lượng LAN. Trong khi đánh giá làm thế nào điều này có thể được thực hiện, bạn được trình bày với một loạt các lựa chọn các phương pháp và thuật toán mã hóa. Chọn phân loại chính xác của tiêu các thuật toán mật mã. A. Không đối xứng: RSA, AES Đối xứng: DES, 3DES B. Đối xứng: 3DES, DES Không đối xứng: Blowfish, RSA C. Đối xứng: 3DES, DES Không đối xứng: RC4, RSA D. Đối xứng: AES, 3DES Không đối xứng: RSA	D
58.	Thuật ngữ nào mô tả quá trình che dấu dữ liệu trong một tệp tin? A. Trojan B. Steganography C. Mã hóa D. Chữ ký số	B
59.	Khi chuyên gia an ninh cấp quyền cho các thư mục trên máy chủ tệp để cho phép các tài liệu của một phòng ban chỉ được phép truy cập và sửa đổi bởi các thành viên trong phòng ban đó thì mục tiêu an toàn thông tin nào đã được thỏa mãn? A. Bí mật B. Tính toàn vẹn C. Sẵn có D. An toàn	A
60.	Phương pháp tiếp cận mật mã nào sử dụng các điểm trên một đường cong để xác định các cặp khóa công khai và bí mật? A. RSA B. DES C. ECC D. PKI	C

Sinh viên KHÔNG được sử dụng mọi tài liệu, nộp bài làm kèm theo đề thi

Giáo viên ra đề
(Ký, ghi rõ họ tên)

Chủ nhiệm bộ môn
(Ký, ghi rõ họ tên)