Đề kiểm tra giữa kỳ (Học kỳ I) (2009)
Môn: **Mật Mã & An Ninh Mạng**
Thời gian: 30 phút
(Không được dùng tài liệu)

Câu 1: DDOS thuộc loại tấn công nào:
=> Active Attack

Câu 2: Việc tránh sử dụng trái phép tài nguyên:
=> Access Control

Câu 3: Việc bảo vệ nhằm chống lại sự từ chối của một trong các bên của 1 giao tiếp
=> Non-Repudiation

Câu 4: Khóa trong mã hóa đối xứng phải được biết bởi ai?
=> Bên nhận và gửi (a và b đúng)

Câu 5: Cesar thuộc vào mã hóa đối xứng truyền thống nào:
=> Substitution Cipher (mã thay thế)

Câu 6: Trong 3 loại MH đối xứng (Trans, Subs, Product), mã hóa nào dẫn xuất của 2 loại kia:
=> Product Cipher (mã nhân)

Câu 7: Hãy dùng mã hóa Playfair để mã hóa chuỗi ……
=> ……

Câu 8: Dùng mã hóa Vigenère với key là chuỗi sau ……
=> ……

Câu 9: Dùng định lý Fermat: 3^(……) mod 11
=> ……

Câu 10: Giá trị hàm Euler Totient: O(70) là: (phi của 70)
=> 24

Câu 11: Đối với phương pháp MH công khai, khóa nào được sử dụng khi cần MH data trước gửi
=> Khóa công khai của người nhận

Câu 12: Đối với phương pháp MH công khai, khóa nào tạo chữ ký số trên 1 message
=> Khóa riêng của người gửi

Câu 13: Đối với lược đồ MH công khai RSA, khóa công khai được diễn tả là:
=> (e, n)

Câu 14: Đối với lược đồ MH công khai RSA, cho biết khóa d quan hệ với e như thế nào
=> $e.d \equiv 1 \bmod o(n)$ và $0 < d < n$

Câu 15: Đối với lược đồ MH công khai RSA, cho n = 187, e = 3. Chọn d
=> 107

Câu 16: Đối với lược đồ MH công khai RSA, cho n = 187, e = 7, d = 23. Cho biết MH của M = 88
=> 11

Câu 17: Sun Java hỗ trợ JCA bao gồm
=> Provider, Service

Câu 18: Trong JCA, method getInstance() dùng để
=> Xác định dẫn xuất liên quan đến 1 phương pháp mã hóa

Câu 19: Trong JCA, giả sử có 2 provider cùng hỗ trợ 1 phương pháp mã hóa. Khi người dùng gọi MH, provider nào được chọn?
=> Tùy thuộc vào giá trị "preference order" của 1 provider
=> Người dùng chọn provider nào thì dùng provider đó

Câu 20: Chọn SAI khi lập trình mã hóa RSA sử dụng service Cipher trong JCA
=> Lớp SecretKey dùng để sinh khóa cho RSA

Chép lại đề và đáp án: HLND (email: hoanglenghiaduc@gmail.com)

cuu duong than cong . com