



## An toàn thông tin\_ Nhóm 10

Nhà của tôi / Các khoá học của tôi / INSE330380\_22\_1\_10 / Test 2\_ Begin 19h, 4/12/2022 / Test 2\_Review\_all

### Câu hỏi 41

Chưa trả lời

Đạt điểm 1,00

Trong mã hóa bất đối xứng (còn gọi là mã hóa hóa công khai). Alice cần **giải mã** văn bản mà Bob gửi cho thì Alice cần dùng khóa gì?

- ☒ a. Khóa Private của Alice
- ☐ b. Khóa Public của Bob
- ☐ c. Khóa Private của Bob
- ☐ d. Khóa Public của Alice

[Clear my choice](#)

### Câu hỏi 42

Chưa trả lời

Đạt điểm 1,00

Tệp nào lưu trữ thông tin mật khẩu đã được mã hóa của hệ thống Unix?

Select one:

- ☐ a. /etc/security.
- ☒ b. /etc/passwd.
- ☐ c. /etc/shadow.
- ☐ d. /etc/pwlog

[Clear my choice](#)

**Câu hỏi 43**

Chưa trả lời

Đạt điểm 1,00

Việc gỡ bỏ những dịch vụ và giao thức không cần thiết gọi là?

- ☒ a. Hardening
- ☐ b. Auditing
- ☐ c. Nonrepudiation
- ☐ d. Hashing

**Clear my choice****Câu hỏi 44**

Chưa trả lời

Đạt điểm 1,00

Phần nào trong kiến trúc bộ nhớ lưu trữ biến cục bộ trong chương trình, các dữ liệu liên quan đến lời gọi hàm?

- ☐ a. Data Segment
- ☒ b. Stack
- ☐ c. BSS segment
- ☐ d. Text
- ☐ e. Heap

**Clear my choice****Câu hỏi 45**

Chưa trả lời

Đạt điểm 1,00

Cho hai số nguyên tố  $p=13$ ,  $q=19$ , giá trị  $e$  nào sẽ được chọn trong thuật toán mã hóa RSA từ số các giá trị sau:

- ☐ a. 27
- ☐ b. 21
- ☐ c. 39
- ☒ d. 35

**Clear my choice**
$$\begin{aligned}n &= p \cdot q = 13 \cdot 19 = 247 \\N &= (p-1)(q-1) = 216 \\GCD(e, 216) &= 1 \\ \Rightarrow e &= 35 \text{ (public key)} \\e \cdot d \bmod N &= 1 \\ \Rightarrow e \cdot d &= 1 \bmod N \\ \Rightarrow 35 \cdot d &= 1 \bmod 216 \\ \Rightarrow d &= 1 \text{ (private key)}\end{aligned}$$

**Câu hỏi 46**

Chưa trả lời

Đạt điểm 1,00

What is missing from a half-open scan?

Select one:

- ☐ a. RST
- ☐ b. FIN
- ☒ c. ACK
- ☐ d. SYN, ACK

**Clear my choice****Câu hỏi 47**

Chưa trả lời

Đạt điểm 1,00

Assume RSA has the public key (7,187) and private key (23,187). The ciphertext C= 3 will be decrypted to .....

- ☐ a. 171
- ☐ b. 133
- ☒ c. 181
- ☐ d. 121

$$m = c^d \bmod n = 3^{23} \bmod 187 = 181$$

**Clear my choice****Câu hỏi 48**

Chưa trả lời

Đạt điểm 1,00

Các giải pháp mã hóa KHÔNG đảm bảo được tính chất nào sau đây

- ☐ a. Tính bí mật
- ☐ b. Tính xác thực
- ☐ c. Tính toàn vẹn
- ☒ d. Tính sẵn sàng

**Clear my choice**

**Câu hỏi 49**

Chưa trả lời

Đạt điểm 1,00

During an FIN scan, what indicates that a port is closed?

Select one:

- ☐ a. No return response
- ☐ b. SYN
- ☒ c. RST
- ☐ d. ACK

**Clear my choice****Câu hỏi 50**

Chưa trả lời

Đạt điểm 1,00

Given below table for encryption and decryption. Which is the plaintext of cypher = 010?

3 bits  
↓

	00	01	10	11
0	011	101	111	100
1	000	010	001	110

↓  
3 bits

Table used for encryption

3 bits  
↓

	00	01	10	11
0	100	110	101	000
1	011	001	111	010

↓  
3 bits

Table used for decryption

- ☐ a. 011
- ☒ b. 101
- ☐ c. 110
- ☐ d. 001

$$010 = 01 \text{ (ct)} + 0 \text{ (hàng)} = 110$$

**Clear my choice****◀ Chapter 12 - Hash - MAC - HMAC - Digital Signature**

Chuyển tới...

**Review - Chapter 1,3,4,5,6 ▶**

