

## CÂU HỎI ÔN TẬP GIỮA KỲ AN TOÀN THÔNG TIN

- Cho hệ mật mã Affine.  $K=(a,b)$  là khóa của hệ mật mã này. Hãy chọn khóa  $K$ 
  - (27,15)
  - (15, 30)
  - (13,17)
  - (17,20)
- cho bản rõ “**cato**” khóa  $k=(11, 7)$ . Khi mã hóa bản rõ với khóa  $k$  theo hệ mã **affine** ta sẽ thu được bản mã nào sau đây?
  - DHIF
  - HIFG
  - NOMS
  - HFJK
- cho bản rõ “**clok**” khóa  $k=(19, 7)$ . Khi mã hóa bản rõ với khóa  $k$  theo hệ mã **affine** ta sẽ thu được bản mã nào sau đây?
  - IMPT
  - TINK
  - YUOI
  - TINP
- Cho bản rõ “**qt**” khóa  $k$  là:  
$$\begin{matrix} 3 & 2 \\ 8 & 7 \end{matrix}$$

Khi mã hóa bản rõ với khóa  $k$  theo hệ mã **hill** ta sẽ thu được bản mã nào sau đây?
- cho bản rõ “**ka**” khóa  $k$  là:  
$$\begin{matrix} 9 & 7 \\ 3 & 4 \end{matrix}$$

Khi mã hóa bản rõ với khóa  $k$  theo hệ mã **hill** ta sẽ thu được bản mã nào sau đây?
- Cho hoán vị  
$$\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{matrix}$$

Khi mã hóa bản rõ “**justs**” theo mã hoán vị ta sẽ thu được bản mã nào sau đây ?

  - GJHJH
  - SJTUS
  - GSHDG
  - GTHDD
- Cho hoán vị  
$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 2 & 6 & 3 \end{matrix}$$

Khi mã hóa bản rõ “**kimson**” theo mã hoán vị ta sẽ thu được bản mã nào sau đây ?

  - KOUFHK
  - MISONK
  - ONSMIK
  - KOSINM
- cho bản rõ “pin” khóa  $k=(15,7)$ . Khi mã hóa bản rõ với khóa  $k$  theo hệ mã affine ta sẽ thu được bản mã nào sau đây?
  - YXU

- b. YXD
  - c. YXC
  - d. YUI
9. cho bản rõ “**small**” khóa  $k = (11, 3)$ . Khi mã hóa bản rõ với khóa  $k$  theo hệ mã **affine** ta sẽ thu được bản mã nào sau đây?
- a. UUDFT
  - b. TFDUU
  - c. TFUDU
  - d. FPUHJ
10. Cho bản rõ “just” khóa  $k = 24$ . Khi mã hóa bản rõ với khóa  $k$  theo hệ mã Ceasar ta sẽ thu được bản mã nào sau đây?
- a. HSJK
  - b. HSQP
  - c. HSQR
  - d. KSQE
11. Cho bản rõ “wen” khóa  $k = 14$ . Khi mã hóa bản rõ với khóa  $k$  theo hệ mã Ceasar ta sẽ thu được bản mã nào sau đây?
- a. KSJ
  - b. KIO
  - c. KIL
  - d. KSB
12. cho bản mã “OMSTV” khóa  $k$  là “HI”. Khi giải mã bản mã với khóa  $k$  theo hệ mã **Vigenere** ta sẽ thu được bản rõ nào sau đây?
- a. Hands
  - b. Shape
  - c. Pages
  - d. Hello
13. cho bản mã “JECK” khóa  $k$  là “READ”. Khi giải mã bản mã với khóa  $k$  theo hệ mã **Vigenere** ta sẽ thu được bản rõ nào sau đây?
- a. SGJF
  - b. SACH
  - c. SUCEE
  - d. SACK
14. cho bản mã “HVT” khóa  $k = (11, 3)$ . Khi giải mã bản mã với khóa  $k$  theo hệ mã affine ta sẽ thu được bản rõ nào sau đây?
- a. Yes
  - b. Vit
  - c. Sit
  - d. Sec
15. cho bản mã “GVHOU” khóa  $k = (7, 17)$ . Khi giải mã bản mã với khóa  $k$  theo hệ mã **affine** ta sẽ thu được bản rõ nào sau đây?
- a. Right
  - b. Might
  - c. Light
  - d. Sight

16. Cho hoán vị

1 2 3 4 5  
3 4 5 2 1

Khi giải mã bản mã “ARSEB” theo mã hoán vị ta sẽ thu được bản rõ nào sau đây ?

- a. Reabs
- b. Earbs
- c. Bears
- d. Bsear

17. Cho hoán vị

1 2 3 4 5  
5 2 3 4 1

Khi giải mã bản mã “SHOES” theo mã hoán vị ta sẽ thu được bản rõ nào sau đây ?

- a. Shoes
- b. Eoshs
- c. Sheos
- d. Seosh

18. Cho ma trận khóa của hệ mã Playfair như sau:

<b>M</b>	<b>O</b>	<b>N</b>	<b>A</b>	<b>R</b>
<b>C</b>	<b>H</b>	<b>Y</b>	<b>B</b>	<b>D</b>
<b>E</b>	<b>F</b>	<b>G</b>	<b>I,J</b>	<b>K</b>
<b>L</b>	<b>P</b>	<b>Q</b>	<b>S</b>	<b>T</b>
<b>U</b>	<b>V</b>	<b>W</b>	<b>X</b>	<b>Z</b>

Giải mã cặp bản mã **QS** thu được bản mã nào sau đây?

- a. PQ
- b. ST
- c. WX
- d. ZW

19. Thế nào là tính bí mật của hệ thống thông tin?

- a. Là đặc tính của hệ thống trong đó chỉ có những người dùng được cho phép mới có thể truy xuất được thông tin
- b. Là đặc tính của hệ thống trong đó thông tin được giữ bí mật không cho ai truy xuất.
- c. Là đặc tính của hệ thống trong đó tất cả thông tin được lưu trữ dưới dạng mật mã.
- d. Là đặc tính của hệ thống trong đó chỉ có người quản trị cao nhất (Administrator) mới có thể truy xuất được thông tin

20. Worms – sâu máy tính được hiểu là phần mềm gì?

- a. Là phần mềm làm cho máy tính bị chậm hoặc treo, chiếm băng thông của hệ thống mạng, có thể lây lan quan mạng một cách tự động
- b. Là bộ phần mềm sử dụng cho mục đích che dấu sự tồn tại và hoạt động của những tiến trình mà Hacker mong muốn.
- c. Là phần mềm bí mật ghi lại các thao tác bàn phím, chuột, màn hình rồi gửi tới Hacker
- d. Phần mềm gián điệp ăn trộm thông tin

Câu 21: Hệ mã hóa Vigenère trong không gian bảng chữ cái tiếng anh  $Z_{26}$  có tối đa bao nhiêu khóa có thể ?

- a.  $26^m$
- b. 26
- c.  $26!$
- d.  $26*26 = 676$