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

1. Cho hệ mật mã Affine. *K=(a,b)* là khóa của hệ mật mã này. Hãy chọn khóa *K*

a. (27,15)

* 1. (15, 30)
  2. (13,17)
  3. **(17,20)**

1. 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?
   1. **DHIF**
   2. HIFG
   3. NOMS
   4. HFJK

***Giải:***

* “c” = 2: ⬄ (11 \* 2 + 7) Mod 26 = 3 : “D”
* “a” = 0 ⬄ (11\*0 + 7) Mod 26 = 7 : “H”
* “t” = 19 ⬄ (11 \* 19 + 7 ) Mod 26 = 8 : “I”
* “o” = 14 ⬄ (11\*14 + 7) Mod 26 = 5 : “F”

1. 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?
   1. IMPT
   2. TINK
   3. YUOI
   4. **TINP**
2. Cho bản rõ “**qt**” khóa k là: **SJ**

3 2

8 7

***Giải:***

* “q” = 16 , “t” = 19
* 16 19 ( 3 2

8 7 )

* +) (16 \* 3 + 19 \* 8) Mod 26 = 18 : “S”

+) (16 \* 2 + 19 \* 7) Mod 26 = 9 : “J”

Khi mã hóa bản rõ với khóa k theo hệ mã **hill** ta sẽ thu được bản mã nào sau đây?

1. cho bản rõ “**ka**” khóa k là: **MS**

9 7

3 4

Khi mã hóa bản rõ với khóa k theo hệ mã **hill** ta sẽ thu được bản mã nào sau đây?

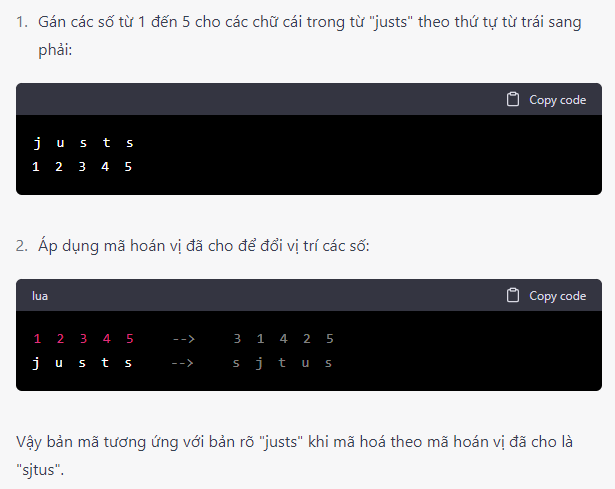
1. Cho hoán vị

1 2 3 4 5

3 1 4 2 5

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

* 1. GJHJH
  2. **SJTUS**
  3. GSHDG
  4. GTHDD



1. Cho hoán vị

1 2 3 4 5 6

1 5 4 2 6 3

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

* 1. KOUFHK
  2. MISONK
  3. ONSMIK
  4. **KOSINM**

1. 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?
   1. **YXU**
   2. YXD
   3. YXC
   4. YUI
2. 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?
   1. UUDFT
   2. **TFDUU**
   3. TFUDU
   4. FPUHJ
3. 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?
   1. HSJK
   2. HSQP
   3. **HSQR ( Lấy 26 – khóa k = bao nhiêu thì lùi vị trí chữ cái = nấy đó . Trong bài này 26 – 24 = 2 . thì ta lùi các chữ cái về 2 đơn vị . J = 9 -> lùi 2 đơn vị = 7 : h )**
   4. KSQE
4. Cho bản rõ “**wen**” khóa k= 14. Khi mã hóa bản rõ với khóa k theo hệ mãCeasar ta sẽ thu được bản mã nào sau đây?
   1. KSJ
   2. KIO
   3. KIL
   4. **KSB**
5. 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?
   1. Hands
   2. Shape
   3. Pages
   4. **Hello**

**( - Ta có “HI” = 7 8 . Mà Bản mã có 5 kí tự “OSMTV” thì ta phải lặp Khóa lên 5 kí tự . => Khóa k = 7 8 7 8 7 .   
Lấy BẢN MÃ – KHÓA K :**

* + **Nếu Dương : Chuyển sang Kí tự tương ứng với số luôn**
  + **Nếu Âm : Lấy 26 + ( Phần âm )**

**)**

1. 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?
   1. SGJF
   2. **SACH**
   3. SUCEE
   4. SACK
2. 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?
   1. **Yes**
   2. Vit
   3. Sit
   4. Sec
3. 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?
   1. **Right**
   2. Might
   3. Light
   4. Sight
4. 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

* + - 1. Earbs
      2. **Bears**
      3. Bsear

1. Cho hoán vị

1 2 3 4 5

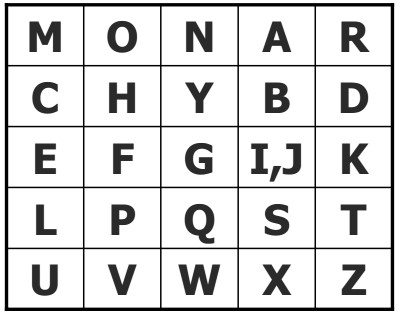
5 2 3 4 1

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

**a. Shoes**

* + - 1. Eoshs
      2. Sheos
      3. Seosh

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



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

* + 1. PQ
    2. **ST**
    3. WX
    4. ZW

1. Thế nào là tính bí mật của hệ thống thông tin?
   1. Là đặc tính của hệ thống trong đó chỉ có những người dùng được cho phép mới có thể truy xuất được thông tin
   2. **Là đặc tính của hệ thống trong đó thông tin được giữ bí mật không cho ai truy xuất.**
   3. Là đặc tính của hệ thống trong đó tất cả thông tin được lưu trữ dưới dạng mật mã.
   4. Là đặc tính của hệ thống trong đó chỉ có người quản trị cao nhất (Adminstrator) mới có thể truy xuất được thông tin
2. Worms – sâu máy tính được hiểu là phần mềm gì?
   1. **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**
   2. 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.
   3. Là phần mềm bí mật ghi lại các thao tác bàn phím, chuột, màn hình rồi gửi tới Hacker
   4. Phần mềm gián điệp ăn trộm thông tin

Câu 21: Hệ mã hóa Vegenère trong không gian bảng chữ cái tiếng anh Z26 có tối đa bao nhiêu khóa có thể ?

1. **26m**
2. 26
3. 26!
4. 26\*26 = 676

**Lý thuyết**

1. **Nguy cơ mất ATTT**
   * Lỗi ng dùng or lỗi hệ thống
   * Vi phạm sở hữu trí tuệ
   * Nguy cơ phần mềm
   * Lỗi phần mềm
   * Nguy cơ phá hoại
2. **Không gian mạng ( Cyber space ):**

* Là 1 k.gian ảo có tính động, kết hợp các thành phần điện tử nhằm mục đích tạo lập, lưu trữ, xử lý, sửa đổi, trao đổi, chia sẻ, sử dụng thông tin và tài nguyên vật lý.
* *Bao gồm:*
  + Tài nguyên vật lý
  + Các hệ thống mt và p.mềm
  + Mạng lưới kết nối
  + Các thiết bị truy nhập đầu cuối
  + Dữ liệu và ứng dụng

1. **Dữ liệu ( Data** ): Các giá trị đại lượng vật lý, ký tự, ký hiệu, âm thanh, hình ảnh được biểu thị dưới dạng thuận tiện cho việc truyền tải, xử lý
2. **Thông tin :** Là DL tổ chức, biểu diễn, kết hợp, chuyển đổi thành dạng có nghĩa theo ngữ cảnh cụ thể
3. **Dữ liệu là nguyên liệu thô của thông tin.**
4. **Hệ thống thông tin** là 1 hệ thống gồm con người, dữ liệu và những hoạt động xử lý dữ liệu và thông tin trong 1 tổ chức
5. **Tài sản của HTTT**
   * Phần cứng
   * Phần mềm
   * Dữ liệu
   * Truyền thông giữa các mt của hệ thống
   * Môi trường làm việc
   * Con người
6. **ATTT là** đảm bảo cho tính bí mật ( **confidence** ), tính toàn vẹn ( **Intergrity** ), tính khả dụng ( **Availability** ), tính xác thực ( **Authenticity** ), tính chống chối bỏ của thông tin và HTTT. Chống bị truy nhập sử dụng sửa đổi trái phép, chống tiết lộ, cản trở, phá hoại.
7. **Đảm bảo ATTT** là đảm bảo an toàn kỹ thuật cho hoạt động của các cơ sở HTTT, trong đố gồm cả phần cứng và phần mềm.
8. **Các nguyên tắc nền tảng của ATTT**
   * *Tính bí mật* - **Confidentiality** ( Bảo vệ dữ liệu không bị lộ ra ngoài 1 cách trái phép )
   * *Tính toàn vẹn -* **Integrity** ( Chỉ những người dùng đc ủy quyền mới đc phép edit Data )
   * *Tính sẵn sàng -* **Availability** ( Đảm bảo dữ liệu luôn SS khi ng dùng hoặc ứng dụng đc ủy quyền yêu cầu
   * *Tính chống thoái thác*
9. **Các nguy cơ mất ATTT**
   * Cơ sở hạ tầng mạng
   * Thông tin
   * Công nghệ
   * Con người
   * Quy trình, quản lý
10. **Các pp đảm bảo an toàn tt**
    * Các biện pháp công nghệ
    * Các biện pháp về chính sách và tổ chức
    * Các biện pháp về đảo tạo, tập huấn, nâng cao nhận thức
    * Biện pháp hợp tác quốc tế
11. **Các thành phần cần bảo vệ trong HTTT**
    * Phần cứng
    * Mạng
    * CSDL
    * Hệ quản trị CSDL
    * NGười dùng
    * Người lập trình hệ thống
    * Người quản trị CSDL

**CHƯƠNG 2:**

1. **Mục tiêu AN HTTT** là giảm các rủi ro đến 1 mức chấp nhận được
2. **Có 3 mối đe dọa ( Threat ) chính :**
   * Các mối đe dọa tự nhiên
   * Các mối đe dọa không chủ ý
   * Các mối đe dọa có chủ ý
3. **Lỗ hổng - Vulnerability**
4. **Risk – Rủi ro**

* **Risk = Threat + Vulnerability**

1. **3 hình thức chủ yếu đe dọa đối với hệ thống:**

* Phá hoại
* Sửa đổi
* Can thiệp

1. **Các mối đe dọa thường gặp**

* Lỗi và thiếu sót của người dùng
* Gian lận và đánh cắp thông tin
* Kẻ tấn công nguy hiểm
* Mã độc
* Tấn công từ chối dịch vụ
* Socail Engineering

1. **Tấn công HTTT là** Các tác động hoặc trình tự liên kết giữa các tác động để phá hủy, dẫn đến việc hiện thực hóa các nguy cơ.
2. **Các loại hình tấn công**

* Tấn công ngăn chặn thông tin
* Tấn công chặn bắt thông tin
* Tấn công sửa đổi thông tin
* Chèn thông tin giả mạo

1. **Các kỹ thuật tấn công**

* Tấn công thăm dò
* Tấn công sử dụng mã độc
* Tấn công xâm nhập
* Tấn công từ chối dịch vụ
* Tấn công sử dụng kỹ nghệ xã hội

1. **Tấn công thăm dò**

* Sniffing ( nghe lén )
* Ping Sweep : Hđ trên các thiết bị chuyển mạch Switch
* Port Scanning: Các cổng kết nối …

1. **Xu hướng tấn công HTTT**

* Sử dụng các Tool tấn công tự động
* Sử dụng các tool tấn công khó phát hiện’
* Phát hiện nhanh các lỗ hổng bảo mật
* Tấn công bất đối xứng và tấn công diện rộng
* Thay đổi mục đích tấn công

1. **Mã độc là MALWARE (** Malicious Software )
2. **1 số loại mã độc:**

* Virus
* Worms – Sâu máy tính
* Zoombie
* Trojan Horses
* BackDoor
* Keylogger
* Rootkit
* Adware
* Spyware
* Ransomware
* Attacker Tool

1. **1 số biện pháp phòng chống mã độc**

* Cài đặt các phần mềm diệt Virus chính hãng
* Xây dựng chính sách vs các thiết bị PnP
* Thiết lập quy tập tắc với các file
* Truy cập web an toàn
* Cập nhật máy tính, phần mềm
* Nhờ các chuyên gia

1. **Mục tiêu của bảo mật**

* Ngăn chặn
* Phát hiện
* Phục hồi

1. **4 cơ chế bảo mật**

* Điều khiển truy cập
* Điều khiển suy luận
* Điều khiển dòng thông tin
* Mã hóa