**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)

b. (15, 30)

c. (13,17)

d. (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
2. 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
3. Cho bản rõ “**qt**” khóa k là:

|  |  |
| --- | --- |
| 3 | 2 |
| 8 | 7 |

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

Kết quả: SJ

1. cho bản rõ “**ka**” khóa k là:

|  |  |
| --- | --- |
| 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?

Kết quả: MS

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
   4. KSQE
4. 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?
   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
6. 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

1. 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
2. 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

1. 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 ?

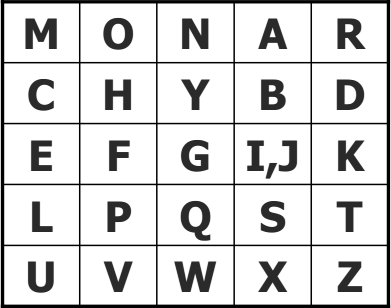
* 1. Reabs
  2. Earbs
  3. Bears
  4. Bsear

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 ?

* 1. Shoes
  2. Eoshs
  3. Sheos
  4. 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

c. 26!

d. 26\*26 = 676

<https://123docz.net/document/4278351-de-cuong-mon-an-toan-vs-bao-mat-thong-tin.htm?fbclid=IwAR0KTd-N1vi0Jn4n1_tlgxWGITfusE6KcvV2Vb4hMI3clJmj8yYP5UUqSYU>

<https://123docz.net/document/1244641-de-cuong-an-toan-bao-mat-van-dung-ma-hoan-vi.htm?fbclid=IwAR3Kr7V7Jiyvv1GG4UiepZ5HPqVQBXWkiN6LS9lOovbpd8tj1x29b6eyAds>

<https://123docz.net/document/1244642-de-cuong-an-toan-bao-mat-van-dung-ma-affine.htm?fbclid=IwAR3lPRqqijrgGz_ZAT0q22Do0faQMkOMc5OaS2kZPbZA51jYGdy8X4k-pCQ>