**Môn Học : Nhập Môn Mã Hóa – Mật Mã**

**Họ tên: Nguyễn Đức Thắng**

**MSSV: 19120654**

**Câu 1**: Từ điển thuật ngữ

* **Plaintext:** là thông điệp nguyên gốc chưa được mã hóa.
* **Ciphertext**: là thông điệp đã được mã hóa bằng thuật toán mã hóa
* **CryptoSystem**: là hệ mật mã dùng để mã hóa dữ liệu, thường gồm các thuật toán để mã hóa và các key để giải mã dữ liệu
* **Active attacks**: tấn công tích cực, kẻ tấn công cố gắng xâm nhập vào hệ thống và thay đổi dữ liệu lưu trữ
* **Man in middle:** là kẻ tấn công đứng giữa cuộc trao đổi thông tin giữa bên gửi và bên nhận nhằm đánh cắp dữ liệu và tìm cách giải mã
* **Encrypt**: mã hóa – biến đổi dữ liệu gốc thành dữ liệu đã được mã hóa
* **Decrypt**: giải mã – biến đổi dữ liệu đã được mã hóa thành dữ liệu ban đầu
* **Birthday attack:** sử dụng sự đụng độ của hàm băm để tìm cách giải mã dữ liệu tìm ra K
* **Asymmetric cryptosystem:** hệ mã bất đối xứng có khóa mã hóa nhưng không suy ra được khóa để giải, và công khai khóa mã hóa
* **Symmetric cryptosystem** : hệ mã đối xứng dùng 1 khóa private để mã hóa cũng như là giải mã

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

**Câu 2:** Minh họa cách mã hóa dữ liệu

* **Docs:** Mat ma hoc la mot linh vuc lien quan den cac ky thuat ngon ngu va thuat toan de dam bao an toan thong tin cu the la trong thong tin lien lac, cong nghe thong tin
* Thêm nhiễu để các từ có chiều dài bằng nhau bằng cách thêm kí tự **z** vào cuối sao cho mỗi từ đủ 6 kí tự, ta được: Matzzz mazzzz hoczzz lazzzz motzzz linhzz vuczzz lienzz quanzz denzzz caczzz kyzzzz thuatz ngonzz nguzzz vazzzz thuatz toanzz dezzzz damzzz baozzz anzzzz toanzz thongz tinzzz cuzzzz thezzz lazzzz thongz thongz tinzzz lienzz laczzz, congzz nghezz thongz tinzzz
* **Plaintext :**

130120262626 130126262626 081503262626 120126262626 131520262626 120914082626 222103262626 120905142626 172101142626 040514262626 030103262626 112526262626 200821012026 140715142626 140722262626 220126262626 200821012026 261501142626 040526262626 040113262626

011426262626 020115262626 011426262626 201501142626

200815140726 200914262626 032126262626 200805262626

120126262626 201815140726 200815140726 200914262626

120905142626 120103262626 031514072626 140708052626 200815140726 200914262626

* Mã hóa

Chọn k=6598327401

Ta được:

586596979797 586597979797 605268979797 596597979797 585296979797 596153609797 999568979797 596162539797 549565539797 636253979797 686568979797 559297979797 966095659697 536452539797 536499979797 996597979797 966095659697 975265539797 636297979797 636558979797 655397979797 696552979797 655397979797 965265539797

966052536497 966153979797 689597979797 966062979797

596597979797 965052536497 966052536497 966153979797

596162539797 596568979797 685253649797 536460629797 966052536497 966153979797

**Câu 3** Tấn công hệ mã ở trên

* Ta nhận thấy ở cuối mỗi từ đều có số 97 suy ra 97 là kí tự gây nhiễu, có thể là z,f,j,w
* 5364 xuất hiện ở cả cuối từ lẫn đầu từ với 8 lần suy đoán là “ng”
* 53 xuất hiên cuối từ 6 lần suy đoán có thể là chữ “n”
* 96 xuất hiên đầu từ nhiều nhất là 12 lần suy đoán thường là chữ t
* 9660 xuât hiên đầu từ 4 lần có thể là chứ “tr” hoặc “th”
* 65 xuất hiện bất kì bất kì nhiều nhất với 18 lần có thể đoán là “o” hoặc “a”
* 52 xuất hiện bất kì trong từ khá nhiều với 12 lần cũng có thể đoán là “o” hoặc “a”
* **96605**2**5364**97 **96**6153979797 xuất hiên lại 3 lần (5 chữ và 3 chữ ), kết hợp lại những thông tin ở trên có thể đoán được đó là chữ **thong tin**

Tìm ra được k=6598327401