Hệ mật Vigenere

m là số nguyên dương

P = C = K = (Z26)m

K = k1, k2, …km

eK(x1, x2, . . . , xm) = (x1 + k1, x2 + k2, . . . , xm + km)

dK(y1, y2, . . . , ym) = (y1 − k1, y2 − k2, . . . , ym − km)

Bài tập lớn

1. Sử dụng hệ mật Vigenere mã hoá file text

* Sử dụng hệ mật Vigenere truyền thống ta chỉ có thể mã hoá với các ngôn ngữ sử dụng chữ cái Latinh, với các ngôn ngữ không sử dụng chữ cái Latinh (tiếng Hàn, Nhật …) hoặc có sử dụng nhưng có các kí tự đặc biệt (tiếng Việt) hệ mật này không thể biểu diễn được các kí tự trong ngôn ngữ đó.
* Vì vậy em đề xuất phương pháp dựa trên bảng mã Unicode như sau:
* Unicode
  + Là bộ mã chuẩn quốc tế được xây dựng để sử dụng làm bộ mã duy nhất cho toàn bộ ngôn ngữ trên thế giới.
  + Không gia mã Unicode được chia thành 17 plane trong đó mỗi mặt có 216 code point.
  + 17 x 216 = 1,114,112
  + Hệ mật Vigenere dựa trên mã unicode với không gian:

P = C = K = (Z 1,114,112)m

* Ngoài ra em có bổ sung thêm lựa chọn để đưa chữ các chữ cái của bản mã về dạng base64 tức là chỉ bao gồm các kí tự Latinh, các số và 2 kí tự đặc biệt bởi mã Unicode biểu diễn rất nhiều ngôn ngữ do đó bản mã có thể sẽ chứa nhiều ngôn ngữ khác nhau làm khó cho người đọc.
* Base64
  + Là phương thức mã hoá 2 chiều từ binary sang string, các binary lúc này sẽ được biểu diễn bằng các ký tự mã ASCII
  + Các ký tự được sử dụng bao gồm A Z, a z, 0 9 , +, /
  + Tuy nhiên cách mã hoá này có nhược điểm khiến kích thước file lớn hơn

1. Sử dụng hệ mật Vigenere mã hoá các loại file khác

* Với phương pháp trên ta chỉ có thể mã hoá file txt hoặc các file python có thể mở và đọc được nội dung text bên trong. Vì vậy em đề xuất phương pháp khác để mã hoá các file còn lại như sau:
* Các file được lưu trong máy tính dưới dạng bytes, trong đó 1 byte = 8bits
* 8 bits được biểu diễn dưới dạng dãy 256 số từ (0,1, 2, 3,…255)
* Hệ mật Vigenere:

P = C = (Z 256)m

K = (Z 1,114,112)m