**Report Week 3**

1. **Code chaotic-based stream cipher**

* Sử dụng [**dyadic transformation**](https://en.wikipedia.org/wiki/Dyadic_transformation)làm logistic map.
* Code: [code](https://github.com/miscitaofvh/Cryptography/blob/main/Assignment/Assignment3/chaotic.py)
* Thực hiện kiểm thử encrypt:

**A screenshot of a computer

AI-generated content may be incorrect.**

* Mở file sau khi encrypted ra thì nhận thấy rằng file không còn đọc được nữa:

**A screenshot of a video player

AI-generated content may be incorrect.**

* Tiếp tục thử giải mã xem có thể khôi phục về file ban đầu hay không:

**A screenshot of a computer

AI-generated content may be incorrect.**

* Mở file sau khi decrypt ra thì thấy rằng file đã được khôi phục:

**A screenshot of a video game

AI-generated content may be incorrect.**

1. **Cryptanalysis Stream Cipher**

* Stream Cipher sẽ không an toàn nếu sử dụng một key để mã hóa nhiều file vì khi chúng ta mã hóa 2 file M1 và M2 bằng một key thì có được hai file E1, E2. Chỉ cần lấy E1 xor E2 thì chúng ta đã có được giá trị của M1 xor M2.
  + Nếu attacker có được M1 hoặc M2 thì có thể dễ dàng biết được file còn lại.
  + Tương tự, nếu có nhiều cặp M1 và M2 thì attacker cũng có thể dựa vào chúng để tăng độ chính xác và giảm được nhiều thời gian trong việc tìm ra key.