**Hướng dẫn sử dụng tool thi GK ATTT - tháng 1 2022**

**<Đây là nội dung soạn thảo của Hedspi Nichibu K65**

**Yêu cầu không leak ra ngoài !!!>**

1. Tải file theo link dưới đây

[Link tải OneD9rive Tool](https://husteduvn-my.sharepoint.com/:f:/g/personal/chien_nd205059_sis_hust_edu_vn/EmQrWsg-XTVNiqQIriL-J_gBeXohOC6YMjmy290ZY5s6Dw?e=Rq6Bjx) : yêu cầu máy đã cài python, C/C++

Tải hết các file source code, để chung 1 folder và chạy file .\main.exe là được nhóe ;)

1. Giai diện và cách dùng:

Text

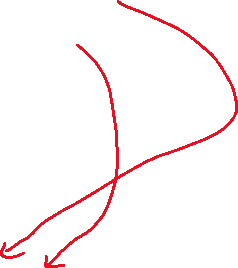
Description automatically generated

1. Mã hóa OTP :

Dùng cho câu này:

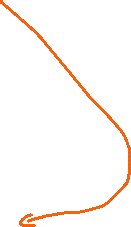
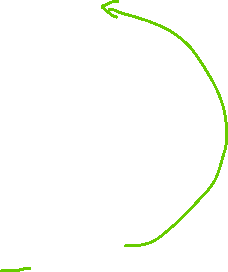
Graphical user interface, text, application

Description automatically generated



Text

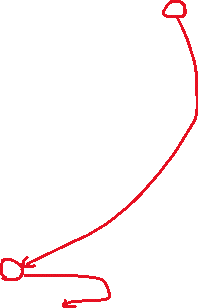
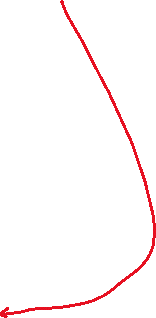
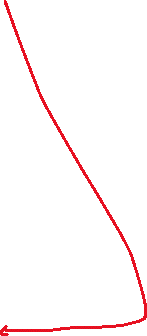
Description automatically generated



1. Logarit Rời Rạc tính:

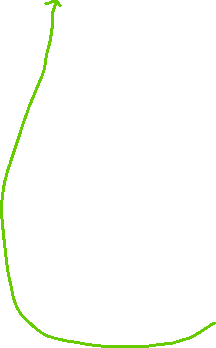
Graphical user interface, application

Description automatically generated



Text

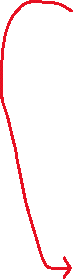
Description automatically generated



1. Diffel Hellman:

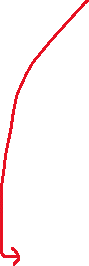
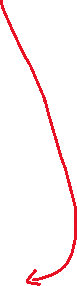
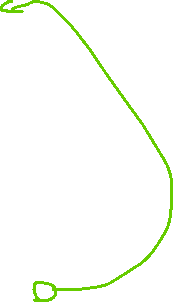
A picture containing graphical user interface

Description automatically generated



Text

Description automatically generated



1. Tính số dư lũy thừa <cái này dễ nên tự làm nha>

Graphical user interface, text, application, Word

Description automatically generated

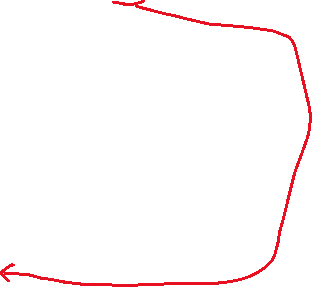
Text

Description automatically generated

1. Kiểm tra phần tử sinh của Module

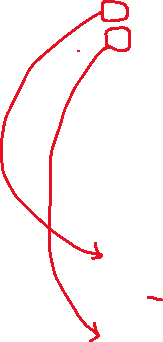
Text

Description automatically generated



Text

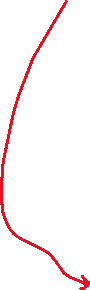
Description automatically generated



1. RSA không kết hợp hàm băm

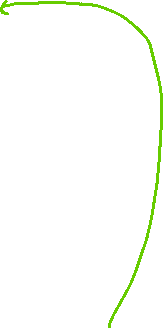
Graphical user interface, text, application

Description automatically generated



Text

Description automatically generated

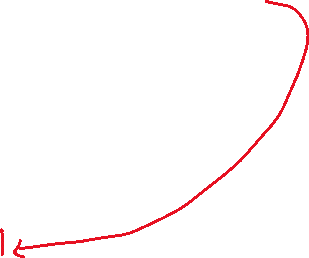
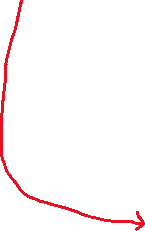
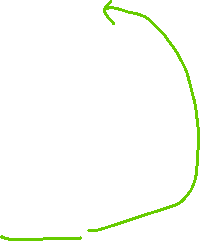


1. RSA

Text, application

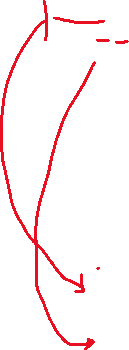
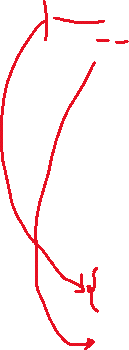
Description automatically generatedText

Description automatically generated



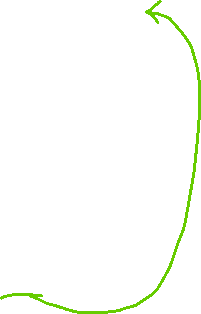
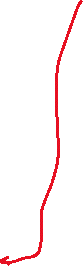
1. ElGamal tìm chu kỳGraphical user interface, text, application

   Description automatically generated



Text

Description automatically generated



1. Tính a^-1 của a trong Module Zp

Graphical user interface, application

Description automatically generated with medium confidence



Text

Description automatically generated



Table

Description automatically generated

Ta có phần tử sinh G(5,1)6

Số K bằng 19

Ta có - P(13,10) = 11.G

- a.P = ( 6,14) = 17.G

=> a.11.G = 17.G

a.11 = 17 (1)

nhưng trong bảng k =19 , nên phương trình (1) dùng trong mod 19

=> a = 5 vì 5.11 % 19 = 17

- b.P = (16,13) = 6.G1

=> b = 4

a.b.P = 5.4.11.G = 220.G = 11.G (mod19)

=> 11.G = (13.11)

Graphical user interface, application

Description automatically generated