## Phân tích HTTP

* Cho một mẫu .pcap bao gồm các gói tin HTTP trao đổi giữa client và server <https://www.cloudshark.org/captures/26c43039ccd6>
* Dựa trên các thông tin các gói tin, sinh viên trả lời các câu hỏi sau:
  + Cho biết IP của client và IP của Webserver

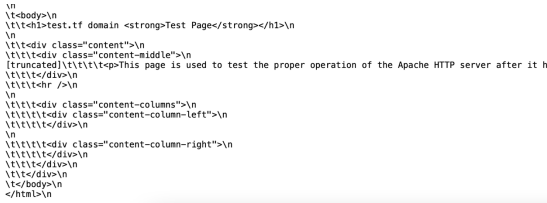
IP client: 192.168.88.189

IP webserver: 176.31.61.170

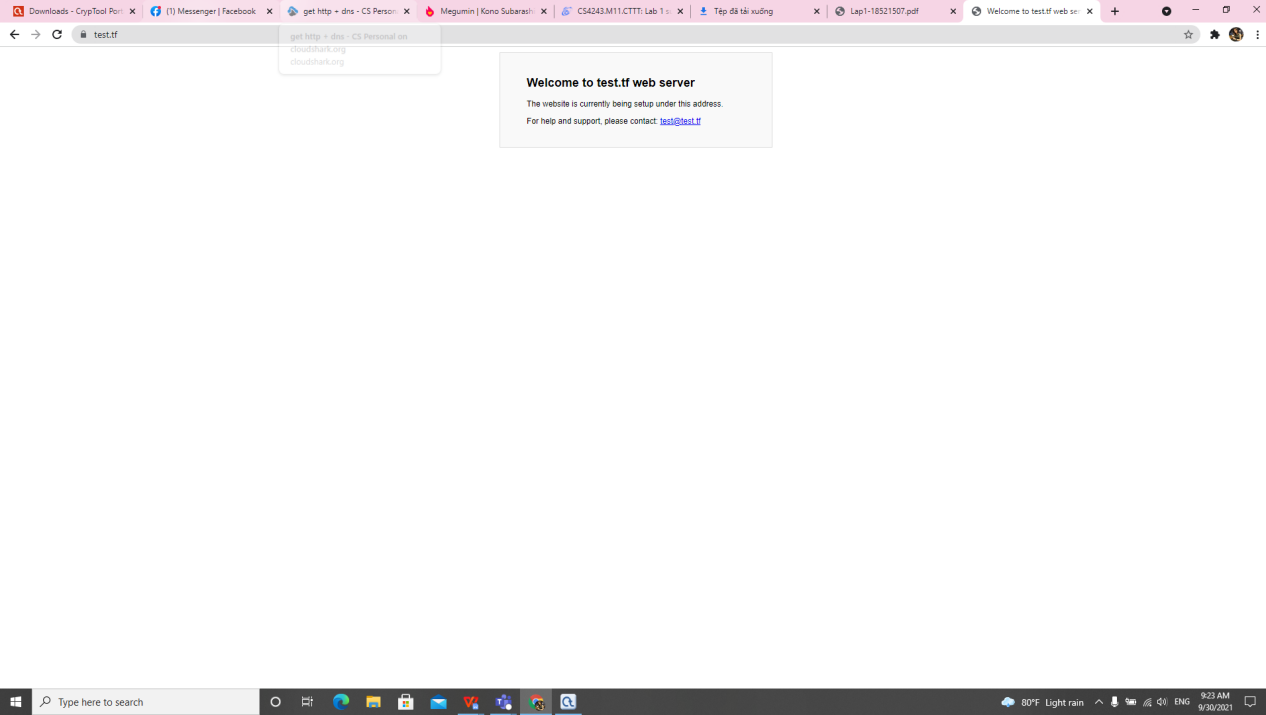
* + Tên miền của Webserver

www.test.tf

* + Cho biết nội dung của trang web trả về bởi Webserver



* + Truy cập thử tên miền đã xác định ở trên



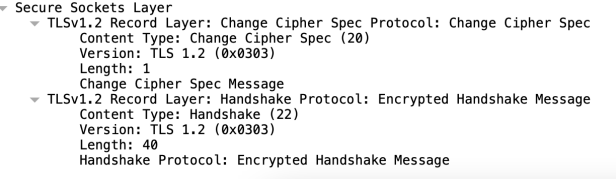
## Phân tích HTTPS

* Cho một mẫu .pcap bao gồm các gói tin HTTPS trao đổi giữa client và server <https://www.cloudshark.org/captures/832753499470>
* Dựa trên các thông tin các gói tin, sinh viên trả lời các câu hỏi tương tự như mục 1.1.
  1. IP client: 10.26.3.163

IP Webserver: 10.197.193.121

Tên miền : Encrypted

Nội dung trả về :

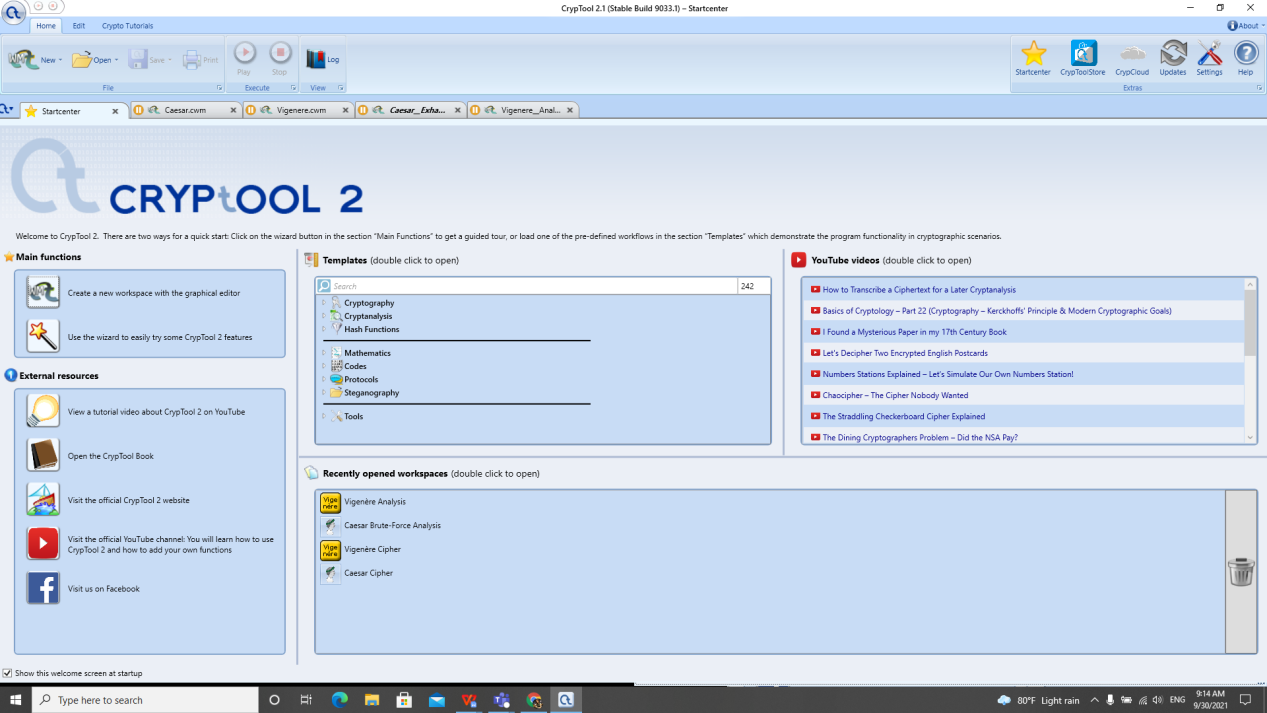


* So sánh các thông tin giữa HTTP và HTTPS

HTTPs có tính bảo mật cao hơn HTTP.

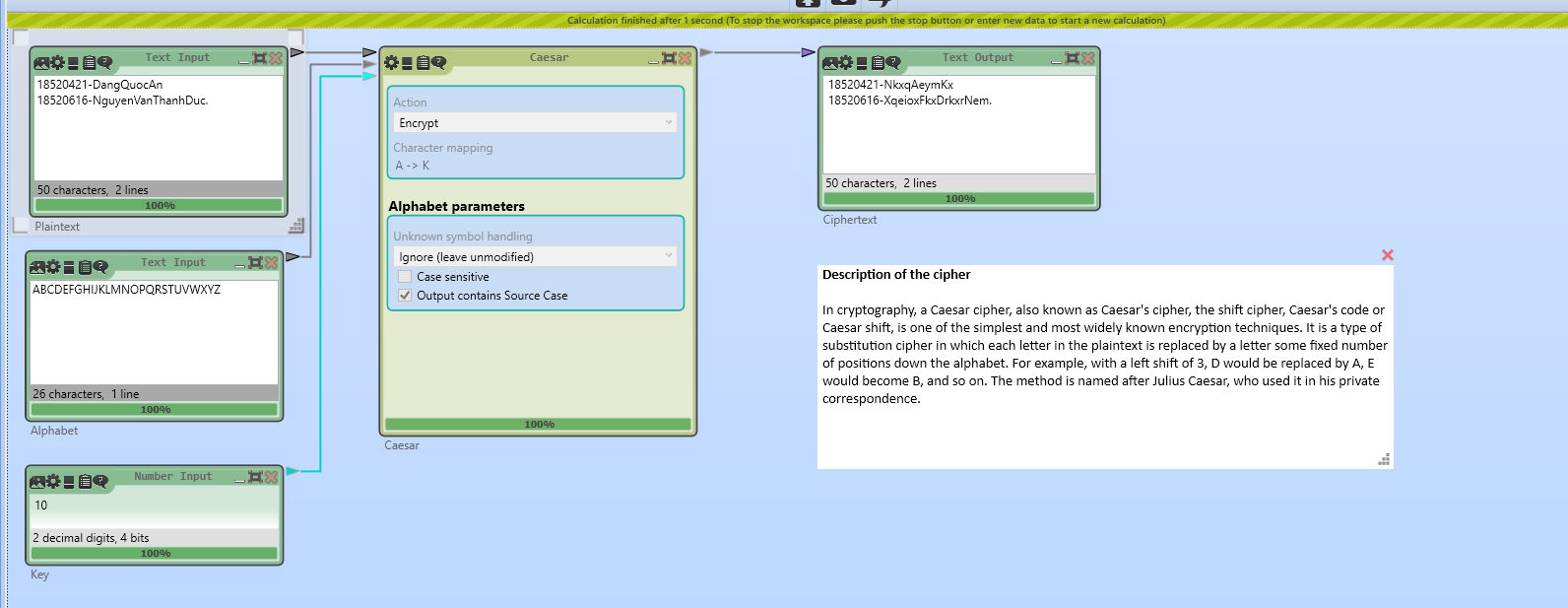
# Mã hóa cơ bản

## Cài công cụ Cryptool

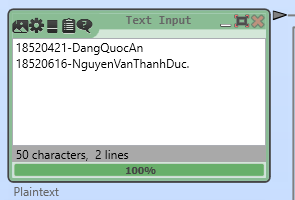
* Tải công cụ Cryptool2 (đối với Windows) hoặc JCrypTool (đối với Linux/MacOS) từ trang website <https://www.cryptool.org/en/>
* Cài đặt công cụ (với bản .exe) hoặc giải nén để sử dụng trực tiếp (bản .zip
* 

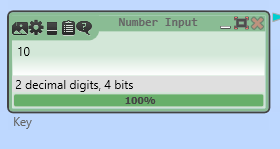
## Mã hóa và giải mã với thuật toán Caesar

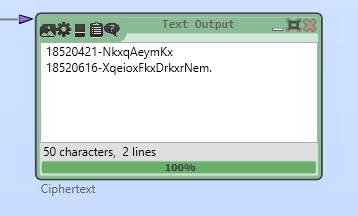
* Mở công cụ Cryptool2
* Mã hóa một đoạn văn bất kỳ (khoảng 50 từ) nhưng có MSSV-Họ tên SV với thuật toán Caesar. Sử dụng template có sẵn của Cryptool (Open -> C:\Program Files (x86)\CrypTool 2\Templates\Cryptography\Classic -> Ceasar)



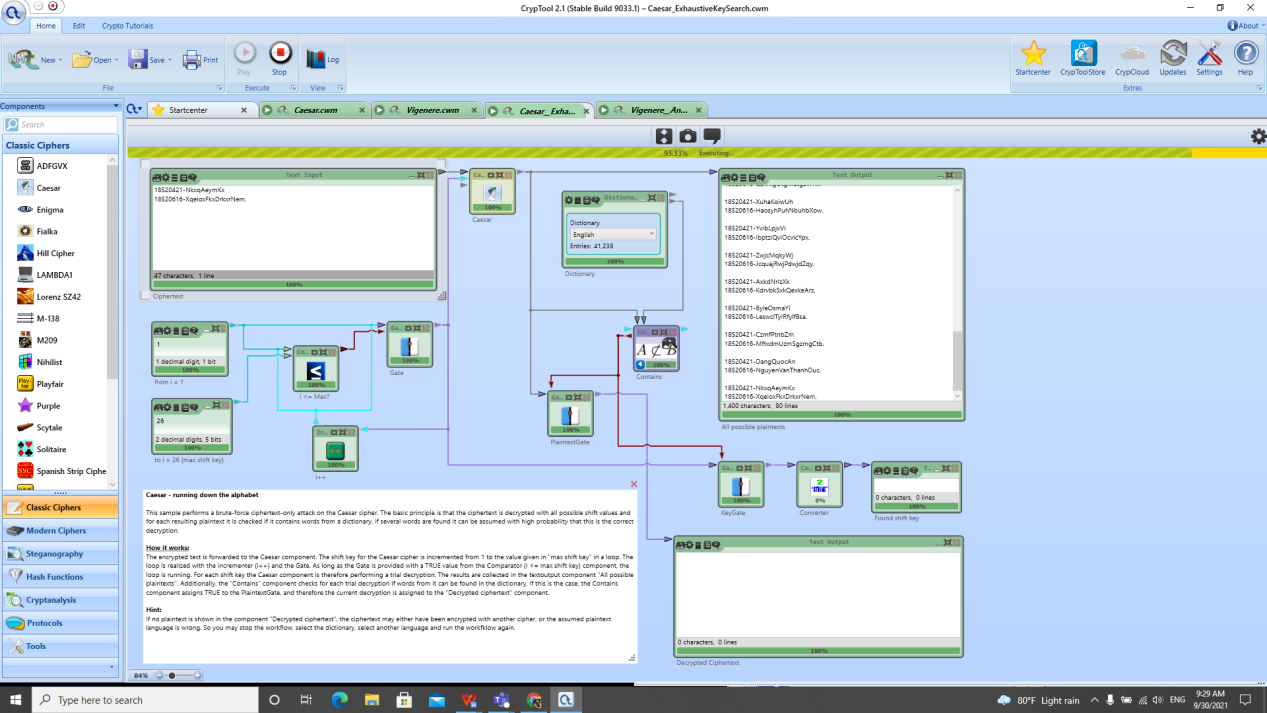
* Sinh viên chụp hình quá trình mã hóa vào báo cáo: plaintext, key, ciphertext.



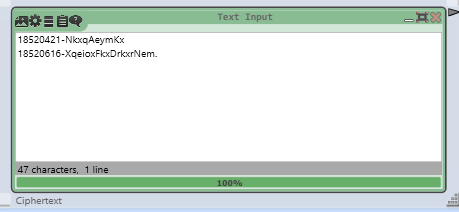


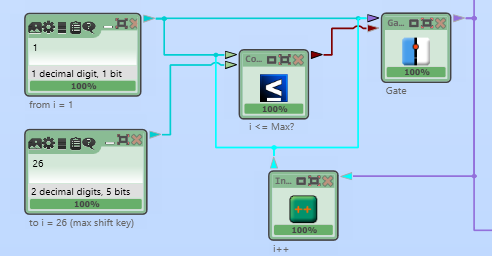


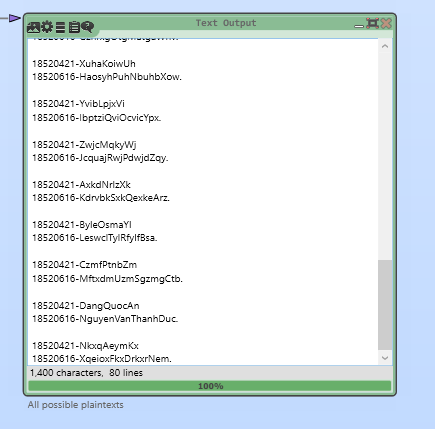
* Đưa đoạn text đã được mã hóa cho nhóm khác (không gửi key).
* Giải mã đoạn text vừa nhận được từ nhóm khác, sử dụng template thích hợp để giải mã CrypTool (Open -> C:\Program Files (x86)\CrypTool 2\Templates\Cryptanalysis\Classic)



* Sinh viên chụp hình quá trình giải mã: ciphertext, key, plaintext

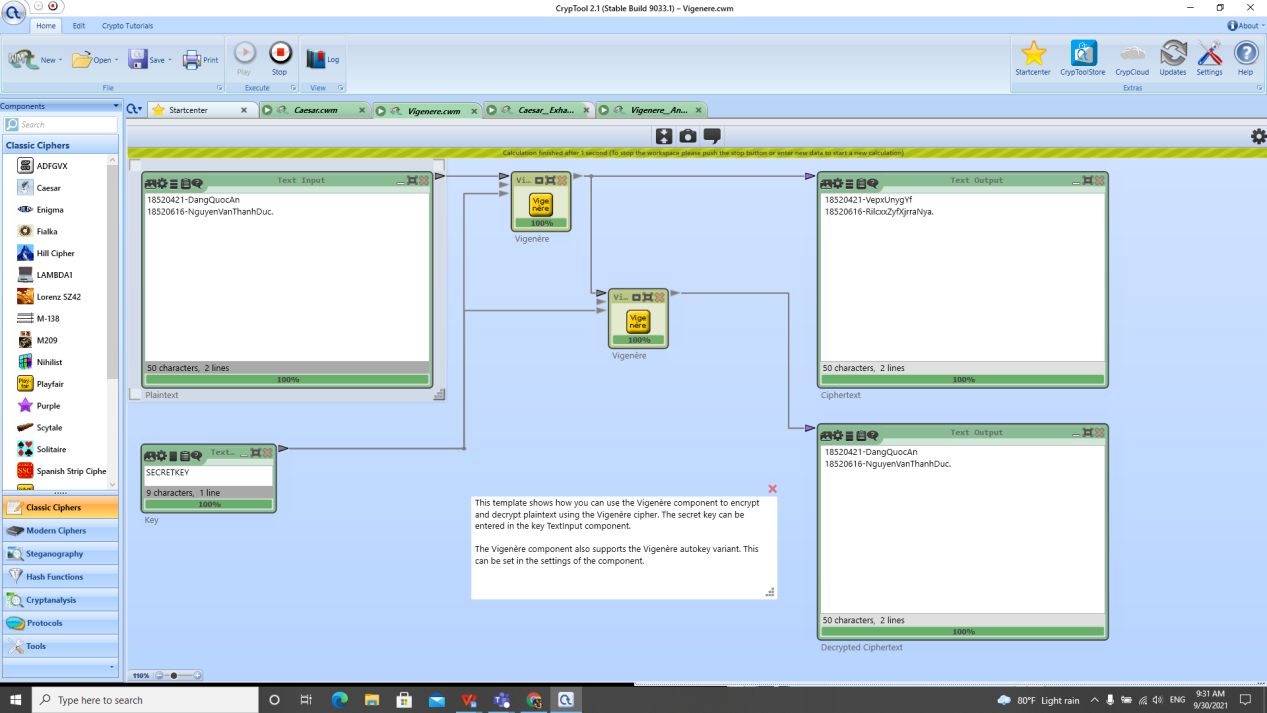




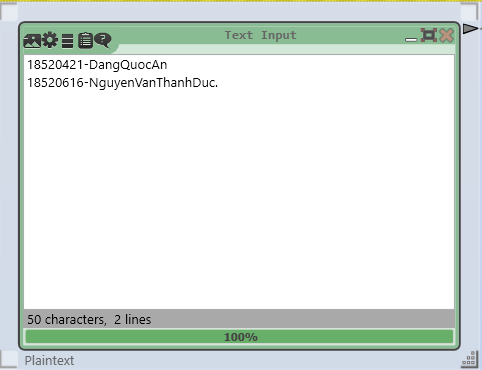


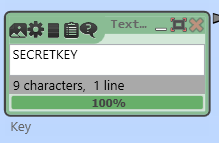
## Mã hóa và giải mã với thuật toán Vigenere

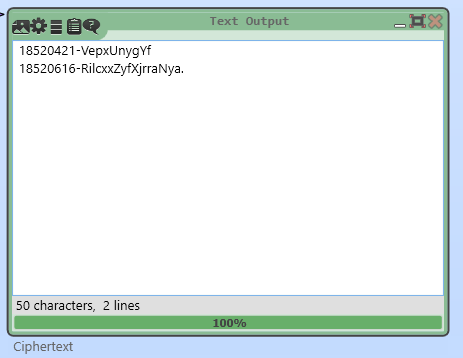
* Mở công cụ Cryptool2
* Mã hóa một đoạn text bất kỳ (khoảng 50 từ) nhưng có MSSV-Họ tên SV với thuật toán Vigenere, sử dụng template.



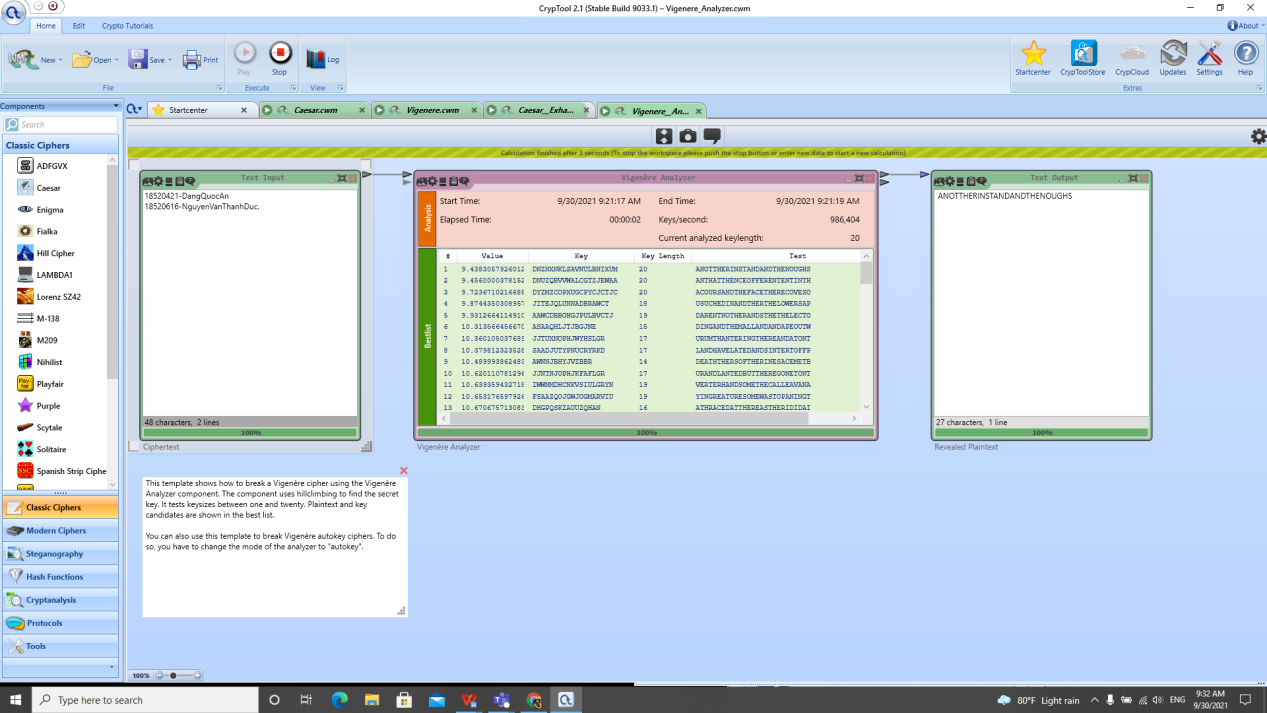
* Sinh viên chụp hình quá trình mã hóa vào báo cáo: plaintext, key, ciphertext.



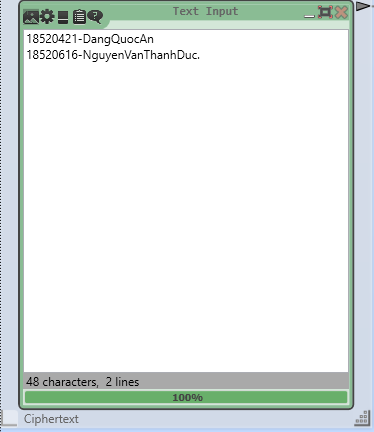


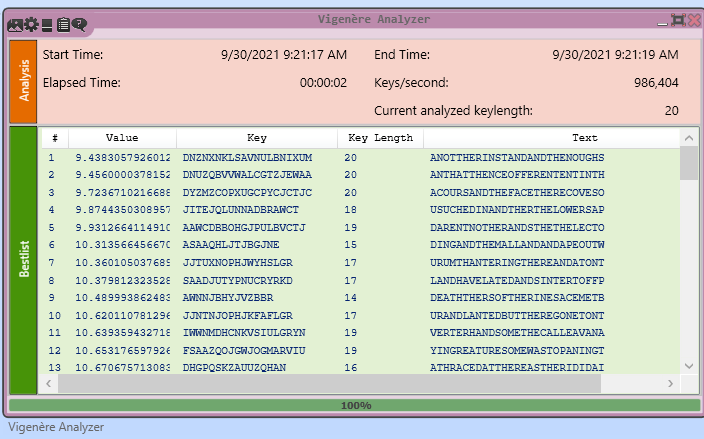


* Đưa đoạn text đã được mã hóa cho nhóm khác (không gửi key).
* Giải mã đoạn text vừa nhận được từ nhóm khác, sử dụng template thích hợp để giải mã.

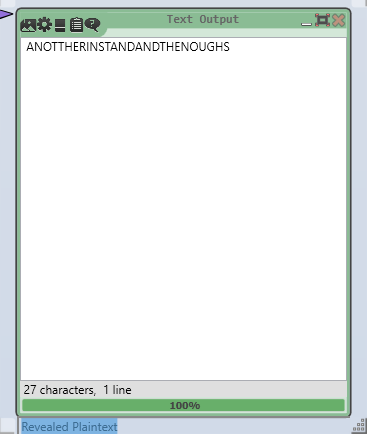


* Sinh viên chụp hình quá trình giải mã: ciphertext, key, plaintext. Cho biết key nào là key đúng cho việc giải mã).





key true for decode:



## Giải thích/So sánh 2 thuật toán

The Vigenere algorithm is more secure because Caesar with a key number from 0-9 will be easy to guess. Vigenere has the key will self-made, so it is difficult for others to attack to steal information