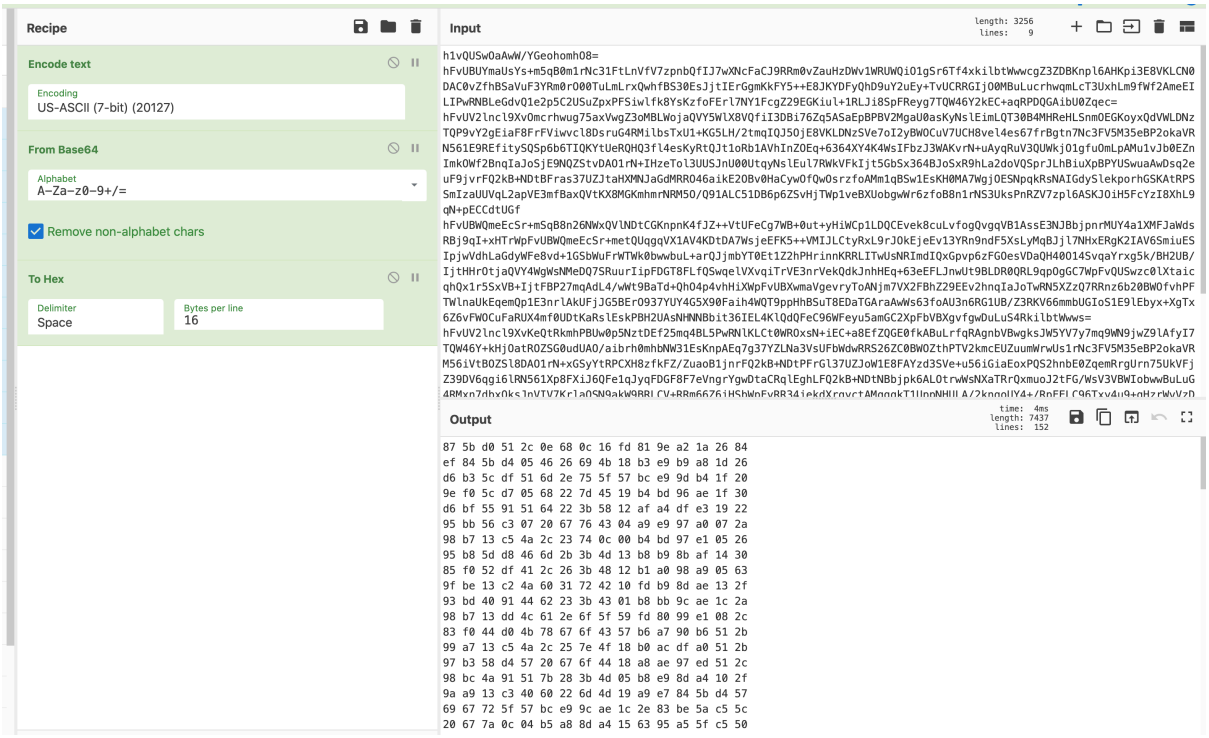
jeudi 8 octobre 2020

TP - Cryptanalyse / Cryptographie

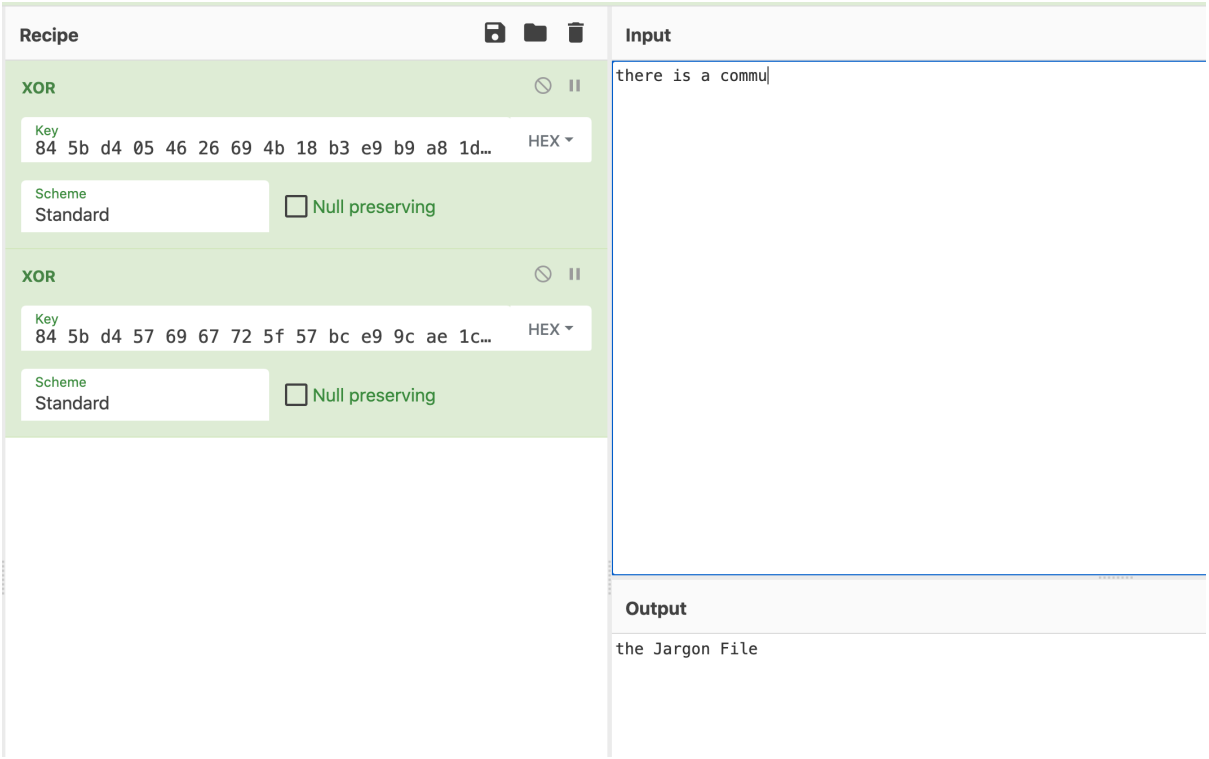
Sécu info exercice 1

Pour trouver la solution à ce problème, voici les étapes que nous avons réalisées :

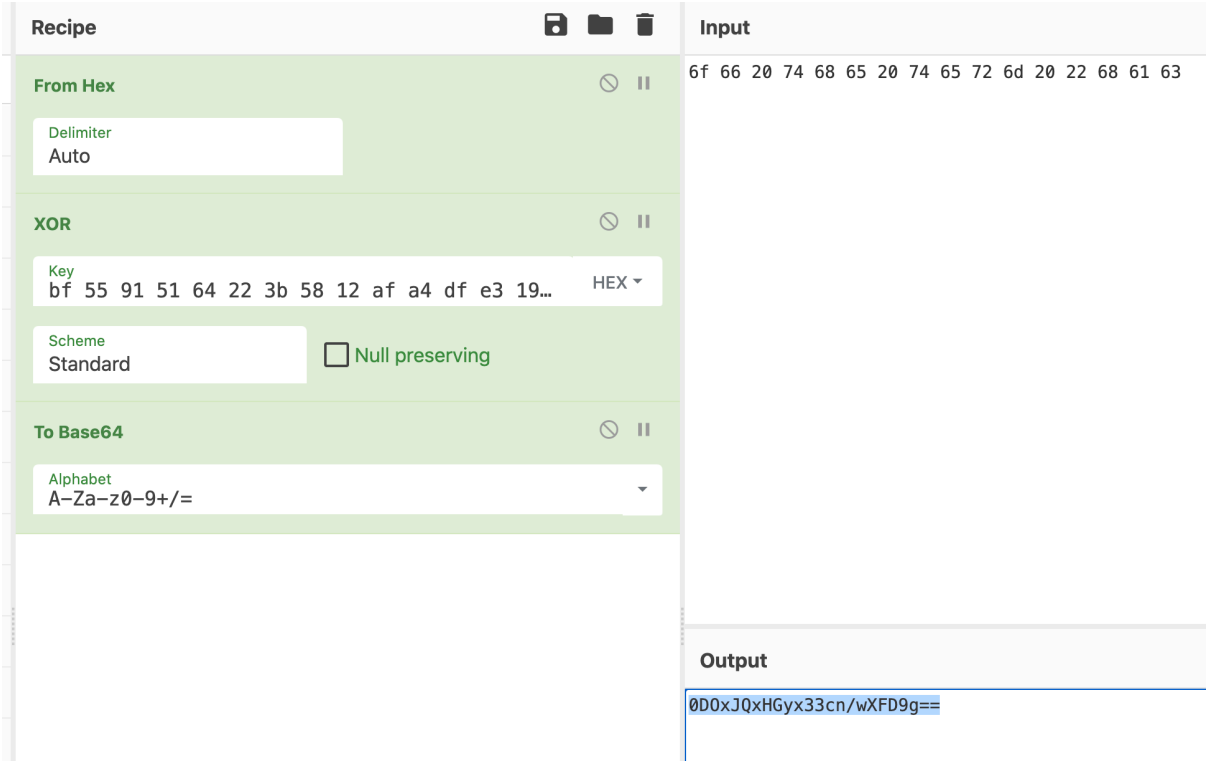
- Nous utilisons le site « CyberChef » (https://gchq.github.io/CyberChef/) pour tester nos premières hypothèses en évitant les limitations techniques liées au Python.
- Nous prenons le ciphertext, l'encodons en ASCII (pour éviter les soucis d'encodage), le décodons en Base64 et le convertissons en hexadécimal en limitant la taille des blocs à 16 octets.



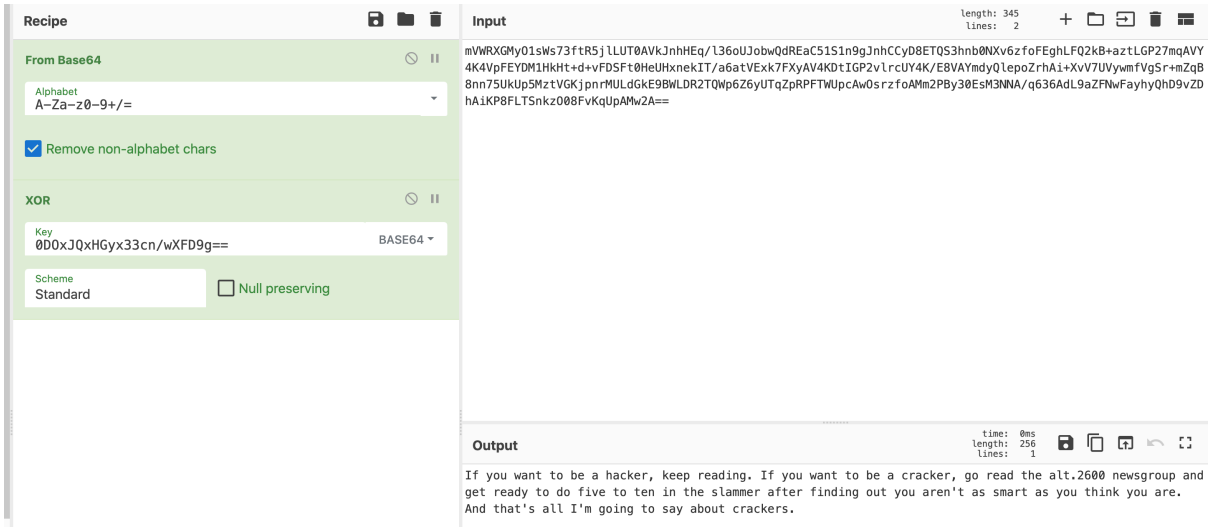
- Puis nous prenons deux blocs (c.à.d. deux lignes de 128 bits) par exemple :
  - 84 5b d4 05 46 26 69 4b 18 b3 e9 b9 a8 1d 26 d6
  - 84 5b d4 57 69 67 72 5f 57 bc e9 9c ae 1c 2e 83
- Nous utilisons l'opérateur 'XOR' pour 'xorer' nos deux blocs ensembles et également avec un mot en anglais, par exemple « the » et au fur et à mesure, nous sommes arrivé à un début de piste :



- Nous pouvons voir que nous obtenons un output qui vaut « The Jargon File ». Nous avons inversé l'input et l'output puis nous avons continué et nous avons obtenu : « The Jargon File contains a bunch of ».
- Cet extrait fait donc partie du ciphertext. Partant de là nous avons pu déduire la suite du texte mais également la clé de chiffrement.
- Pour obtenir la clé nous avons « xoré » l'hexadécimal de notre cipher avec l'hexadécimale notre plain text puis nous l'avons encodé en base 64. Nous obtenons la clé suivante : 0DOxJQxHGyx33cn/wXFD9g==



- Si nous xorons chaque ligne du chiphertext avec la clé, nous déchiffrons le texte :



What Is a Hacker?

The Jargon File contains a bunch of definitions of the term "hacker", most having to do with technical adeptness and a delight in solving problems and overcoming limits. If you want to know how to become a hacker, though, only two are really relevant.

The hacker mind-set is not confined to this software-hacker culture. There are people who apply the hacker attitude to other things, like electronics or music actually, you can find it at the highest levels of any science or art. Software hackers recognize these kindred spirits elsewhere and may call them "hackers" too and some claim that the hacker nature is really independent of the particular medium the hacker works in. But in the rest of this document we will focus on the skills and attitudes of software hackers, and the traditions of the shared culture that originated the term hacker.

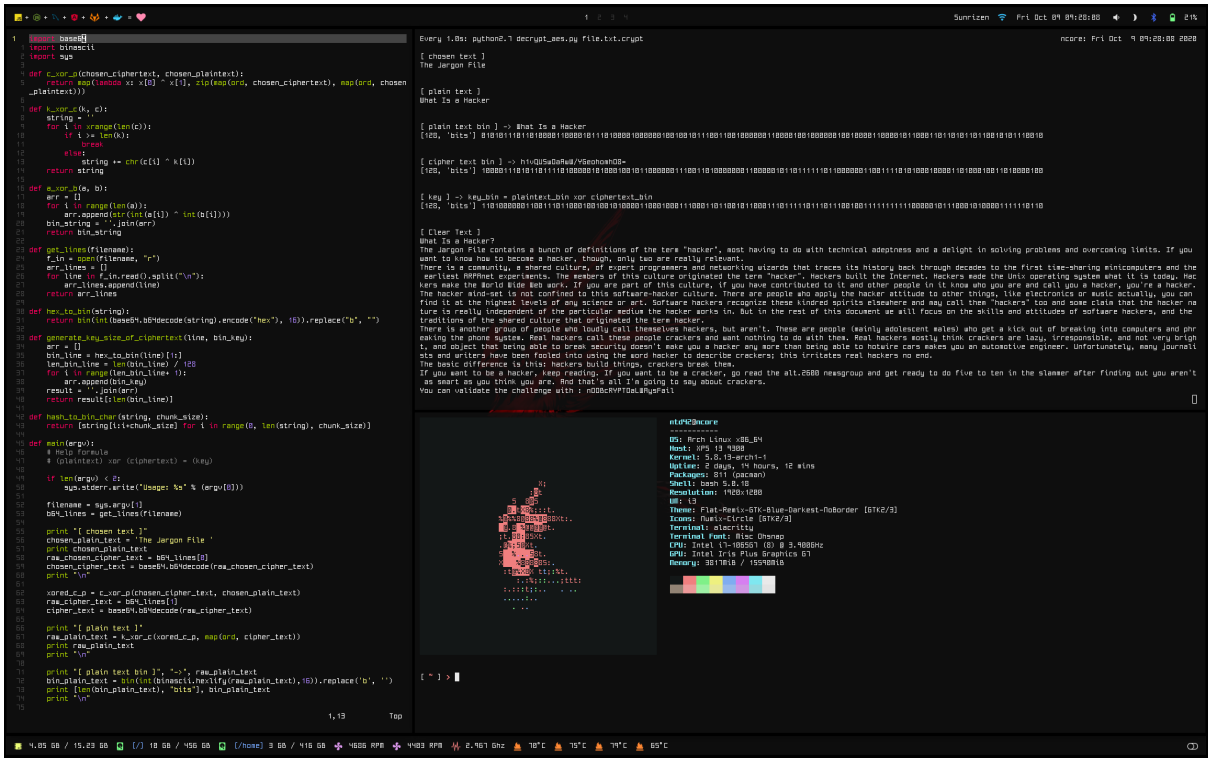
There is another group of people who loudly call themselves hackers, but aren't. These are people (mainly adolescent males) who get a kick out of breaking into computers and phreaking the phone system. Real hackers call these people crackers and want nothing to do with them. Real hackers mostly think crackers are lazy, irresponsible, and not very bright, and object that being able to break security doesn't make you a hacker any more than being able to hotwire cars makes you an automotive engineer. Unfortunately, many journalists and writers have been fooled into using the word hacker to describe crackers; this irritates real hackers no end.

The basic difference is this: hackers build things, crackers break them.

If you want to be a hacker, keep reading. If you want to be a cracker, go read the alt.2600 newsgroup and get ready to do five to ten in the slammer after finding out you aren't as smart as you think you are. And that's all I'm going to say about crackers.

You can validate the challenge with : nOOBcRYPTOaLWAysFail

- Nous avons par la suite traduit ce principe dans un script python nous permettant d'obtenir la clé (Script joint avec ce dossier).



Participant : LAERA Jérémie, DORVILLE Mathieu, BOUMANS Jimmy