INF808 – LAB1

**Robert Byrka (byrr2101)**

Question 1 :

*Au vu du code du listing 1 expliquer comment la représentation numérique d’un caractère permet d’implémenter une translation de caractère ?*

Un caractère est encodé sur un octet de 8 bits. Un charactère est d’abord un nombre binaire, qui peut être ensuite translaté en nombre décimale/hexadécimale. La table ASCII est un standard de représentation des charactères. Les caractères alphabétiques de [a-z] sont définit à partir du nombre 97 en décimale, 67 en hexadécimale jusqu’à 122 en décimale, 7A en hexadécimale. Grâce à ce standard, la représentation des caractères est universelle.

Question 4 :

*Expliquer et trouver deux clés différentes k et k 0 qui donnent un même chiffré. En déduire le nombre (minimal) de clés qui, pour un texte claire donné, fournissent des chiffrés différents*

Prenons k = 1, k’ = 27. Si on utilise la fonction encrypt(‘abc’,k) et encrypt(‘abc’,k’). On retombe sur le même chiffré. Cela s’explique car il y a 26 caractères différents dans l’alphabet et donc le chiffrement est lié à ce modulo 26. On en déduit donc qu’il y a 25 clés différentes car k > 0.

*Expliquer pourquoi le code de Cæsar se prête à une attaque de force brute et décrire comment vous procèderiez à une attaque de type brute force pour décoder un chiffré dont vous n’avez pas la clé k.*

Avec un peu d’analyse, on déduit que l’attaque par force brute prendra un temps en complexité O(n). Pour procéder à une attaque de force brute, vu qu’il n’y a que 25 permutations possibles on va chercher parmi les 25 possibilités après décalage de +1 à chaque tour de boucle le message qui nous parait le plus probable à être déchiffré.

Question 6 :

*Au vue du code exécute dans le listing 2 et des tables 1 et 2, expliquer pour le caractère ’é’ ayant un code de 233 qui est inférieure à 255 est codée sur deux octets et non 1 octet. Donner la valeur du code ASCII étendu associée au caractère ’é’*

La table 1 indique que é est U+00E9 ce qui fait parti de la représentation du code UTF-8 avec 2 octets. Le tableau 2 nous montre que 00E9 se trouve dans la tranche avec 2 octets.

La valeur de é dans la table ascii étendue est donc de 130.  
ref : <https://theasciicode.com.ar/extended-ascii-code/letter-e-acute-accent-e-acute-lowercase-ascii-code-130.html>

Question 7 :

Le nombre de clés possibles est :

216 est le nombre de possibilités qu’un caractère peut être encodé sur 16 bits. Le -1 représente la prochaine lettre qui peut être codé sur 16 bits sans la précédente etc. Le tout donne la somme de i = 0 jusqu’à n de 216-i

Si on applique un algorithme brute force pour tenter de trouver la clé, on remarque que l’algorithme va tester i2 possibilités. Donc de l’ordre de O(i2)

Question 10 :

*\*\*\* question 8*

*freq\_hugo: [(' ', 285), ('e', 232), ('s', 119), ('a', 114), ('l', 102), ('r', 99), ('u', 95), ('t', 95), ('i', 84), ('n', 81), ('d', 66), ('o', 62), ('m', 49), ('Ã', 40), ('c', 37), ('©', 27), ('p', 24), ('v', 20), ('€', 19), ('g', 19), ('q', 19), ('b', 19), ('â', 18), ('™', 18), (',', 18), ('f', 18), ('h', 15), ('.', 11), ('y', 9), ('x', 6), ('-', 5), ('¨', 5), ('j', 5), ('\n', 3), ('S', 2), ('A', 2), ('\xa0', 2), ('L', 2), ('»', 2), ('T', 1), ('C', 1), ('¢', 1), ('§', 1), ('Å', 1), ('“', 1), ('I', 1), ('E', 1), ('B', 1), ('ª', 1), ('N', 1), ('D', 1)]*

*\*\*\* question 9*

*[(b'\x96\x97', 285), (b'\x1e\x0e', 232), (b'\x06,', 119), (b'\xf0\xab', 114), (b')5', 102), (b'\x85$', 99), (b'\x86\xdd', 95), (b'5\x92', 95), (b'\x13\x99', 84), (b'\xad\xdb', 81), (b'!\xb0', 66), (b'\xb6\xe6', 62), (b'\x95\xcc', 49), (b'\x81\xf5', 37), (b'@l', 27), (b'\xab\x9a', 24), (b'\x9f\xde', 20), (b'\t\x8e', 19), (b'\\\x07', 19), (b'\xaa\xb6', 19), (b'\x1b\xfd', 18), (b'\xd6\xc6', 18), (b'\x8bu', 18), (b'i\x19', 15), (b'\xa06', 11), (b'\xbf\xec', 9), (b'\x925', 6), (b'F\xf2', 5), (b'\x1c\x8b', 5), (b't\x8c', 5), (b'z\*', 3), (b'\xda\xb4', 2), (b'\x01\xa5', 2), (b'\xcda', 2), (b'y\xbe', 2), (b'\xdfR', 2), (b'\xcc@', 1), (b'[\x0e', 1), (b'\xf6m', 1), (b'\x9d\r', 1), (b'C\xcd', 1), (b'\xa5\xd8', 1), (b'\x83+', 1), (b'|\xc5', 1), (b'8\x9f', 1), (b'\xc8l', 1), (b'\xb9\xa6', 1), (b'\x93&', 1)]*

On remarque que la fréquence des tuples dans notre liste est dans la même à la question 8 et 9. On peut donc conjecturer que le texte en claire va correspondre à cipher\_text\_1

Question 12 :

*Csuts Dt;i sÃennaL♦eau del mtn☺an)↔ ii eiir☺e)↔ ts ▬eV ☺en♣reau ☺asrau L♦asPu)↔ ii dtrlle rs dntWtsm ltrdano lÃellau mesl lts iauo lÃeddr;esu lrn lts dtitc0ts)↔ ii dnau rs nt☺eso ai iÃtrL♦nauo ai iru ☺eal ai sÃ; lealalleau ♣rÃrs a☺←ntPiat ctsWrlo ai ←rueau utru asluesu lrn rs ☺tu mtsu ai aPstneau ie laPsaWaceuats)↔ii e←esmtsse lts nt☺es lrn lts iau)↔ ii eiie lts ieL♦e←t ai ☺traiie rs Pesu ♣rÃai delle lrn lts Wntsuo lrn lts ctr)↔ts dtril ←euueau untd Wtnu)↔ ii eL♦eau c0erm)↔ ii trL♦nau lts L♦elaluelo lcnrue ie srau)↔ ii Wealeau mtrU)↔ 8s ←nrau asmaluascu ☺tsueau mr Wer←trnP)↔ 8s cenaiitso dirl itrnm ♣rÃrs Pielo dirl ltrnm ♣rÃrs utclaso dirl dntWtsm ♣rÃrs ←trnmtso sts itaso ltsse untal ctrdl)↔ [renuaso rs ciedtual dieasuaW laPseieau rs c0eiesm ♣ra delleau)↔rn iÃe←euuesu mr L♦elaluelo rs esa☺ei er u0tneU asmaPto iÃeaPraiits leWneso sa rs ceWenmo sa rs c0enes8tso ☺eal dirupu rs enualtso lÃeL♦es8eauo une#4sesu rs ←nas mÃeiWe)↔ ii lÃeddntc0eo L♦triesu iÃedieuan mÃrs ctrd L♦aWo ☺eal iÃesa☺ei dnau lts L♦tio maldeneallesu mesl ie srau eL♦esu ♣rÃai eau dr iÃelleaiian)↔*

On ne peut pas lire des mots.