Tareas de SPSI

curso 2020/2021

fco. m. garcía olmedo

7 de noviembre de 2020

Tarea 1.) El algoritmo de exponenciación rápida ha sido explicado como la codificación de la función $e(a, b)$ definida por:

$$e(a,b) = \begin{cases} 1 & \text{, si } b = 0 \\ e(a^2, \frac{b}{2}) & \text{, si } b > 0 \text{ y } b \equiv 0 \text{ mód } 2 \\ e(a^2, \frac{b-1}{2})a & \text{, si } b > 0 \text{ y } b \equiv 1 \text{ mód } 2 \end{cases}$$

Es fácil demostrar que para cualesquiera números naturales a y b se cumple que $e(a, b) = a^b$. Haga lo siguiente en Python (en formato `.ipynb` al menos):

a) Implemente $e(a, b)$ suponiendo que tanto a como b son números naturales.

b) Modifique la implementación anterior para dar un sentido coherente a $e(a, b)$ permitiendo que b sea un número entero cualquiera.

c) Modifique esta última implementación para hacer el cálculo módulo un número natural n distinto de 0 y de 1.

Tarea 2.) Implemente en Python el criptosistema de Vigenère.

Tarea 3.) Implemente en Python un "laboratorio" con lo sucinto para poder atacar cualquier criptograma cifrado mediante un criptosistema de Vigenère. Para ello básese en lo contenido en el libro [7] de la bibliografía que figura en el fichero `spsi_lectures.pdf` (puede ser descargado legalmente desde el dominio de la UGR) y en el contenido de ese mismo fichero pdf.

Tarea 4.) Lo siguiente:

```
UECWKDVLOTTVACKTPVGEZQMDAMRNPDDUXLBUICAMRHOECBHSPQLVIWO
FFEAILPNTESMLDRUURIFAEQTTPXADWIAWLACCRPBHSRZIVQWOFROGTT
NNXEVIVIBPDTTGAHVIACLAYKGJIEQHGECMESNNOCTHSGGNVWTQHKBPR
HMVUOYWLIAFIRIGDBOEBQLIGWARQHNLOISQKEPEIDVXXNETPAXNZGDX
WWEYQCTIGONNGJVHSQGEATHSYGSDVVOAQCXLHSPQMDMETRTMDUXTEQQ
JMFAEEAAIMEZREGIMUECICBXRVQRSMENNWTXTNSRNBPZHMRVRDYNECG
SPMEAVTENXKEQKCTTHSPCMQQHSQGTXMFPBGLWQZRBOEIZHQHGRTOBSG
TATTZRNFOSMLEDWESIWDRNAPBFOFHEGIXLFVOGUZLNUSRCRAZGZRTTA
YFEHKHMCQNTZLENPUCKBAYCICUBNRPCXIWEYCSIMFPRUTPLXSYCBGCC
UYCQJMWIEKGTUBRHVATTLEKVACBXQHGPDZEANNTJZTDRNSDTFEVPDXK
TMVNAIQMUQNOHKKOAQMTBKOFSUTUXPRTMXBXNPCLRCEAEOIAWGGVVUS
GIOEWLIQFOZKSPVMEBLOHLXDVCYSMGOPJEFCXMRUIGDXNCCRPMLCEWT
PZMOQQSAWLPHPTDAWEYJOGQSOAVERCTNQQEAVTUGKLJAXMRTGTIEAFW
PTZYIPKESMEAFCGJILSBPLDABNFVRJUXNGQSWIUIGWAAMLDRNNPDXGN
PTTGLUHUOBMXSPQNDKBDBTEECLECGRDPTYBVRDATQHKQJMKEFROCLXN
FKNSCWANNAHXTRGKCJTTRRUEMQZEAEIPAWEYPAJBBLHUEHMVUNFRPVM
EDWEKMHRREOGZBDBROGCGANIUYIBNZQVXTGORUUCUTNBOEIZHEFWNBI
GOZGTGWXNRHERBHPHGSIWXNPQMJVBCNEIDVVOAGLPONAPWYPXKEFKOC
MQTRTIDZBNQKCPLTTNOBXMGLNRRDNNNQKDPLTLNSUTAXMNPTXMGEZKA
EIKAGQ
```

es el resultado de cifrar determinado texto mediante un criptosistema de Vigenère. Basándose en lo implementado en el apartado anterior, descubra: la longitud de la clave utilizada, la clave misma y el contenido del mensaje que resulto cifrado en el texto anterior.