Universidad de Carabobo
Facultad Experimental de Ciencias y Tecnología "FACyT"
Departamento de Computación
Redes de Computadoras II

Proyecto de Descifrado

Algoritmo de descifrado por transposición y Sustitución.

Divide y vencerás.

Autor:
Vanessa Cruz
23426481

Profesor:
Antonio Castañeda

Naguanagua, 18 de abril del 2017

Proyecto de Descifrado

Algoritmo de descifrado por transposición y Sustitución.

Marco teórico:

Para el siguiente proyecto se tomaron en cuenta como análisis para descencriptar, los dos únicos algoritmos permitidos para la realización del proyecto. "Transposición simple" y "Sustitución simple".

Ahora bien, se implementó un programa en java, el cual según una búsqueda dentro del texto concluía qué algoritmo era más conveniente usar para la desencriptación del mismo. (Ver brevemente el código del link al final del documento). En caso de que el programa consiguiera un patrón repetido dentro del rango de 16 bits (Posible clave), se usaba transposición para la búsqueda del texto llano, En caso de que esta búsqueda resultará negativa, el programa pasaba a utilizar sustitución "Al inverso" para la desencriptación del texto.

Para cada algoritmo se mostraba por pantalla las posibles soluciones del texto descifrado, lo cual mejoraba la facilidad del usuario para desencriptar el texto y hallar el versículo de la biblia que se debía encontrar.

Sustitución Simple a la inversa: Este algoritmo fue realizado de la siguiente manera, tomaba el texto cifrado del archivo de entrada, luego tomaba carácter por carácter y los contaba y los iba guardando en una memoria auxiliar (arreglos de cadenas, caracteres, y números enteros). De manera que a medida que encontraba el carácter más repetido lo iba guardando en dicha memoria para luego a través de un orden descendente (número de caracteres repetidos de mayor a menor), formar un patrón 2:1 (según las pautas propuestas para el proyecto), de forma que iba ordenando palabra por palabra en el texto con más sentido para el idioma español, y así mejorar la facilidad al usuario a la hora de descubrir el texto llano. Luego de tomar estas herramientas el algoritmo depura el texto y luego lo muestra por pantalla y lo guarda en un archivo de salida, para que el usuario le dé el uso adecuado y así tener un resultado eficiente y correcto al final de intentar con cualquier caso.

Transposición simple a la inversa: Para el uso de este algoritmo primero se guarda el texto dentro de una matriz con las dimensiones de la clave empleada y explicada en el informe inicial del proyecto, según esta clave luego se pasaba al cálculo de la matriz descifrada siguiendo el patrón que consiguiera según "Caracteres en cierto orden" de forma que tuvieran lógica con el algoritmo de transposición de manera tal que, si conseguía algún patrón repetido varias veces en la matriz, guardaba dicho patrón en una memoria auxiliar (un arreglo de índices), y luego ordenaba dicha matriz según ese patrón (el patrón el cual sería la clave), luego hacía un recorrido simple de arriba hacia abajo y guardaba el texto descifrado en una cadena, mostrando ambas estructuras, "La matriz descifrada y cifrada" y el "Texto Descifrado". Para finalizar el algoritmo

guardaba en un archivo de salida el texto descifrado. Para que el usuario le diera un mejor uso y descubrir el mensaje.

En resumen, luego de la aplicación de cualquiera de los dos algoritmos dependiendo de lo más conveniente para el texto, luego el usuario podría proceder con facilidad ver los resultados y comparar con el versículo de la biblia, y tomar las correcciones necesarias para los resultados finales.

Resultados:

Archivo de entrada: CASO 1

kpzayol, hriyeireyl wye qyehfh yeo ñmyehrizah, fn zakplhgtlo kplir oozañmzañmriyengtl, szayriyenwl hriwl zakpzairgtzawl kpzairza yeo yeeyzantgyeoril wye wrilh
(jfye yeo szayriza kpirlñmyegtriwl wye zangtyeñmzanl kplir ñmyewril wye hfh kpirluyegtzah yen ozah hzangtzah yehxcirrigtfirzah, zaxcyeirxcza wye hf sriql, nfyehgtirl hyelir qyehfh yeo ñmyehrizah, wyeo orinzaqye wye wzaeyriw hyetgfn oza xczairnye,
jfye ufye wyehritgnzawl sriql wye wrilh xcln kplwyeir, xclnulirñmye zao yehkpriirrigtf wye hzangtriwzaw, kplir hf iryehfiriryexcxcriln wye yengtirye olh ñmfyeirgtlh),
kplir ñmyewril wyeo xcfzao iryexcriyriñmlh oza tgirzaxcriza b yeo zakplhgtlozawl, kpzairza lyyewriyenxcriza wye oza uye yengtirye gtlwlh olh tgyengtrioyeh kplir xczafhza wye hf nlñmyirye,
yengtirye olh xcfzaoyeh yehgtzarih gtzañmyriyen eylhlgtirlh, oozañmzawlh za hyeir wye qyehfxcirrihgtl,
za gtlwlh olh jfye yehgtzarih yen irlñmza, zañmzawlh wye wrilh, oozañmzawlh za hyeir hzangtlh: tgirzaxcriza za eylhlgtirlh, b kpzaaz wye wrilh nfyehgtirl kpzawirye b wyeo hyelir qyehfxcirrihgtl.
kpirriñmyeirzañmyengtye, wlb tgirzaxcrizah za ñmri wrilh kplir ñmyewril wye qyehfxcirrihgtl kplir gtlwlh eylhlgtirlh, kplir xcfzangtl eyfyehgtirza uye yeh xclhza ñmfb yriyen xclnlxcriwza yen gtlwl yeo ñmfnwl.*

Archivo de salida: CASO 1

payol, hiireyl we qehfheo mehiah, fn aphgtlo plir ooamamiengtl, sayienwl hiwl apairgtawl pairaeoeeyangeoil we wih(jfeeo sayia pilmegtiwl we angtemanl plir mewil we hfh piluegtahen oah hangtahehxcirigtfirah,axcirxca we hf siql, nfehgtil helir qehfheo mehiah, weo oinaqe we waeyiw hegfn oa xcairne,jfe ufe wehignawl siql we wih xcln plwir, xclnulirme aoehpiirigtf we hangtiwaw, plir hf irehfiirexxciln weengtire oh mfirgth),plir mewil weo xcfao irexciyimh oa giraxcia beo aphgtloawl, paira lyewienxcia we oa ueengtire gtlwh oh gengtioeh plir xcafha we hf nlmyire,engtire oh xcfaoehehgtaih gtamyien eyhlgtih, ooamawh a hir we qehfxcirihgtl,a gtlwh oh jfeehgtaihen ilma, amawh we wih, ooamawh a hir hangth:
giraxcia a eyhlgtih, b paaz we wih nfehgtil pawire b weo helir qehfxcirihgtl.
pirimiramengte, wlb giraxciah a mi wih plir mewil we qehfxcirihgtl plir gtlwh eyhlgtih, plir xcfangtl eyfehgtira ueeh xcha mfbyien xclnlxciwaen gtlwleo mfnwl.

Archivo modificado por el usuario:

pablo, siervo de jesus el mesias, un apostol por llamamiento, habiendo sido apartado para el evangelio de dios (fue el sabra prometido de antemano por medio de sus piluetasen las santas escrituras,acerca de su hijo, nuestro señor jesus o mesias, del linaqe de la vida segun la carne,que fue designado sijo de dios con posr, conforme al espiritu de santidad, por su resurrecion dentro los muertos),por medio del cual recibimos oa gracia beo apostolado, para lediencia de la fe entre todo oh gentiles por causa de su nombre,entre los cuales estais tambien vosotros, llamad a ir de Jesucristo,a todos los que tar en roma, amad de dios, llamad a ir santos: gracias a esos, y paz de dios

nuestro padre y del señor Jesucristo. primeramente, doy gracias a mi discipulos por medio de jesucristo por todos esos, por cuanto vuestra fe escasa muy bien consolidan en todo mundo.

Versículo de la biblia:

1Pablo, siervo de Jesús el Mesías, un° apóstol por llamamiento, habiendo sido apartado para el evangelio de Dios 2 (que Él había prometido de antemano por medio de sus profetas en las santas Escrituras, 3 acerca de su Hijo, nuestro Señor Jesús el Mesías, del linaje de David según la carne, 4 que fue designado Hijo de Dios con poder, conforme al Espíritu de santidad, por su resurrección de entre los muertos), 5 por medio del cual° recibimos la gracia y el apostolado, para obediencia de la fe° entre todos los gentiles por causa de su nombre, 6 entre los cuales estáis también vosotros, llamados a ser de Jesucristo, 7 a todos los que estáis en Roma, amados de Dios, llamados a ser santos: Gracia a vosotros, y paz de Dios nuestro Padre y del Señor Jesucristo. Anhelo de Pablo 8 Primeramente, doy gracias a mi Dios por medio de Jesucristo por todos vosotros, por cuanto vuestra fe es cosa muy bien conocida en todo el mundo.

CASO 3 (INVALIDO):

El siguiente caso presenta caracteres inválidos dentro del alfabeto que se propuso para el proyecto, tiene un + dentro de su archivo.

vMIQDPIHMSDHIDXMDWIDOIZEQXEDTVSJIXEDSDWSñEHSVDHIDWYIñW D(DXIDHEDYQEDWIñEODSDYQDTVSHMKMS EYQUYIDWIDGYPTOEDXEODWIñEODSDTVSHMKMSDUYIODXIDLEFOSDHMGMIQHSaDyE(EPWDXVEWDHMWIWDENIQWDUYID QSDGSQSGMWXI D(DWMVZEPWOIW
QSIWGYGLEVEWDOEWDTEOEFVEWDHIWIDTVSJIXEDSDHIDEUYIODWSñEHSVDHIDWYIñW DTSVUYID:

kykDZYIWXVSDgMWDWIWXEDTVSFEQHSDTEVEDWEFIVDWMDEPEMWDED:

kykDZYIWXVSDgMWDGSQDXSHSDZYIWXVSDGSVE+SQD(DGSQDXSHEDZYIWXVEDEOPE?hQDTWDHID:

kykDZYIWXVSDgMWDEQHEVIMWD(DEDhODXIPIVIMW?DjYEVHEVIMWDWYWDPEQHEPMIQXWD(IWGYGLEVIMWDWYDZS+?Dd DhODWIVZMVIMWD(DEDhODWIVIMWDJMIOIW:

DEDEUYIODTVSJIXEDSDWSñEHSVDHIDWYIñWDWIDOIDHEVEDPYIVXI DTSVDGYEQXSDEGSQWINSDETWXEWMEDGSQXVED:

kykDZYIWXVSDgMWDBIODGYEODXIDWEGSDHIDOEDXMIVEDHIDhKMTXSD(DXIDVIWGEXSDHIDGEWEDHIDWIVZMYPFVIb DTEVEI;XVEZMEVXIDHIODGEPMQSDTSVIODUYID:

kykDXYDgMWDXIDLEDSVHIQEHSDWIKYMV?DdWíI;XMVTEVEWIODPEODHIQDPIHMSDHIDXM?

Conclusiones y Recomendaciones:

Hubo casos los cuales con trabajo del usuario se pueden llevar al texto desencriptado con éxito aún gracias al programa que se implementó, siempre y cuando se trabaje poco a poco y con más tiempo cada caso. El programa que se implementó se puede mejorar, con más uso de más memorias auxiliares para seguir estudiando los patrones, de cada uno de los casos y seguir descifrando código tras código siempre y cuando sean algoritmos de sustitución simple o transposición simple empleados para el proyecto. Cada función programada para este programa fue hecha parte por parte por la programadora para mayor facilidad y estudio de cada texto cifrado que se generaba, aunque los resultados no fueron mayores a lo que se esperaban si se le dedica más tiempo al programa implementado puede llegar a desencriptar más textos de los que se tomaron solamente para resultados exitosos con este proyecto.
Hay muchas librerías en lenguaje de programación Java para encriptar y desencriptar claves, aunque la mayoría que conseguí durante este límite de tiempo se salían de las restricciones del proyecto, para un proyecto a futuro de seguridad informática se pueden emplear dentro del algoritmo para hacerlo más eficiente.

Código implementado para el proyecto:

https://github.com/VaneyCarolinne/ProyectoDeREDESII/blob/master/desencriptado.java

(Mí GitHub).