

Ficha y Control de Resultados de las Prácticas

Datos de Identificación

Apellido, Nombre	Cédula de Identidad	Nro. de Práctica	Fecha
Diego Bastardo	27948046	14	25/11/2022
Gabriel Manrique	26921248		
Nombre de la Práctica		Criptografía	
Grupo (últimos 2 dígitos del NRC)	1489	Mesa	

Direccionamiento IP/Máscara:

Equipo origen/fuente:	172.30.114.4	Equipo Objetivo/Destino:	172.30.114.5
Otros Equipos involucrados:			

Ejecución de la práctica:

Por cada actividad desarrollada durante la ejecución de la práctica debe narrar la(s) actividad(es) llevadas a cabo y colocar las evidencias resultantes, a saber: evidencia de comandos, aplicaciones, programas ejecutados, así como los resultados obtenidos de la ejecución de los mismos:

Para esta práctica nos adentramos en el mundo de la criptografía la cual busca cifrar la información delicada y confidencial de una organización con el fin de protegerla. Esta práctica a diferencia de las anteriores la realizaremos en un sistema operativo Windows. El computador utilizado en los laboratorios de práctica tiene instalado la aplicación Cryptool, herramienta crucial para la realización de esta práctica. El objetivo de la ejecución de este laboratorio es cifrar un mensaje, con diferentes algoritmos, y compartirlo a nuestro compañero de equipo para ser descifrado posteriormente.

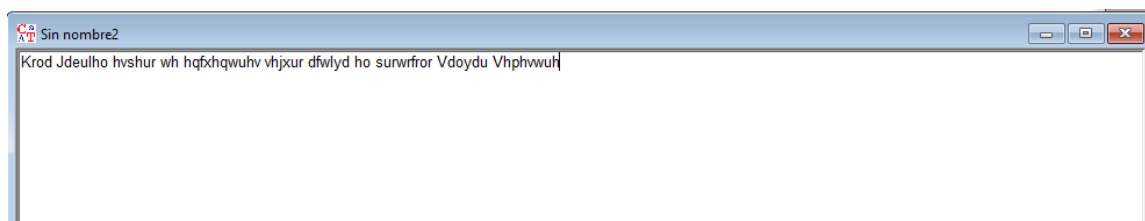
Algunos conceptos importantes para el mayor conocimiento de esta práctica #7, el cifrado de datos es una forma de convertir los datos de texto sin formato (sin cifrar) en texto cifrado. Los usuarios pueden acceder a los datos cifrados con una clave de cifrado y a los datos descifrados con una clave de descifrado. Hay diferentes tipos de cifrado, como son el cifrado simétrico y asimétrico, el cifrado de clave secreta o simétrico, usa una clave única para cifrar y descifrar datos. Es necesario compartir esta clave con el destinatario.

Criptografía asimétrica o de clave pública, se utiliza para proteger archivos, carpetas y unidades completas contra el acceso no autorizado e intercambiar mensajes confidenciales. Para este propósito, se emplean unas claves que sirven para cifrar y descifrar los datos.

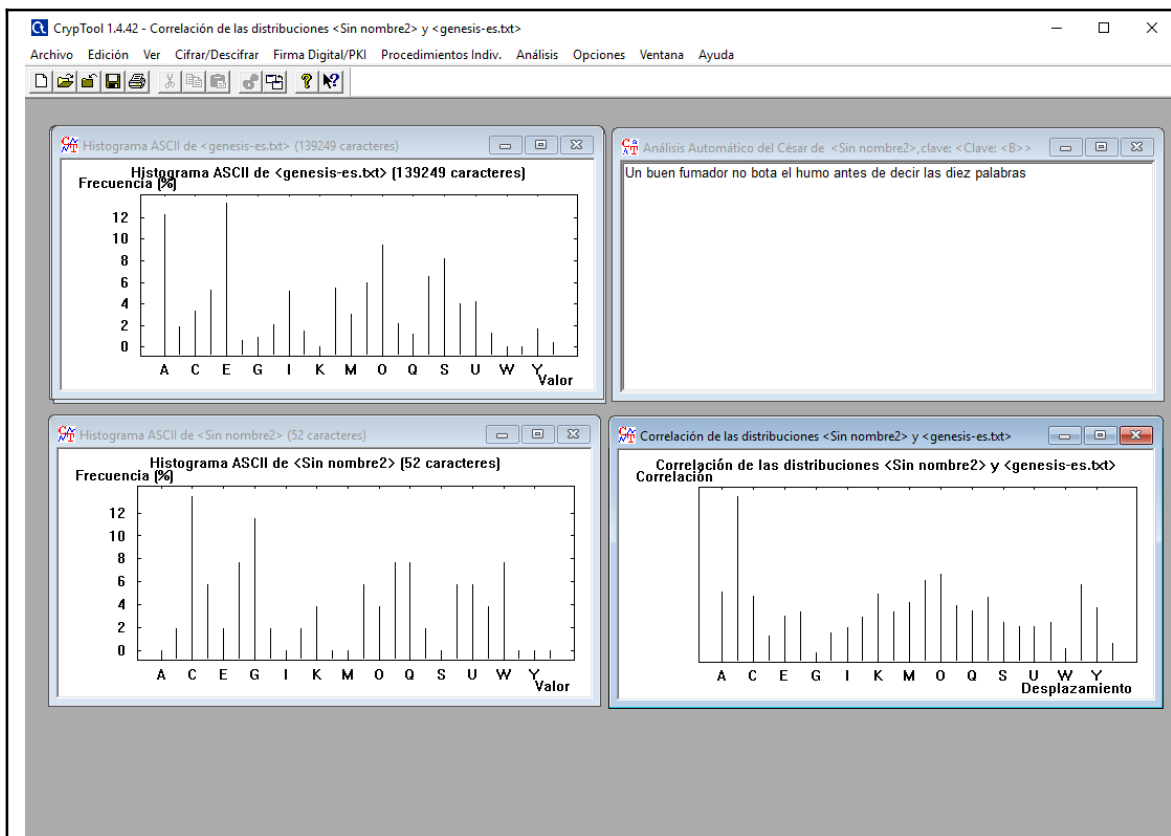
Los métodos utilizados en encriptación de esta práctica fue, el cifrado César este es un cifrado simétrico basado en una sustitución. Esto significa que cada letra usada en el mensaje es reemplazada por una nueva letra. La letra de sustitución resulta de un desfase de letras dentro del alfabeto que se determina de antemano. El otro método utilizado es el algoritmo de Vigenère una forma de sustitución polialfabética para encriptar texto alfabético usando una palabra clave. El cifrado Vigenère es fácil de entender e implementar. Consiste en varios cifrados César en secuencia con diferentes valores de desplazamiento.

Un sistema de cifrado de sustitución simple es polialfabético cuando cada carácter no se sustituye siempre por el mismo carácter. Es decir, en el sistema hay implicados varios alfabetos y dependiendo de la circunstancias se aplicará uno u otro.

Comenzamos la primera parte de la práctica con el cifrado de dos frases secretas pertenecientes a cada uno de los miembros del equipo. La primera “Wp dwgp hwocfqt pq dqvc gn jwoq cpvgu fg fgekt ncu fkgb rcncdtcu” y la segunda “Krod Jdeulho hvshur wh hqfxhqwuhv vhjxur dfwlyd ho surwrfror Vdoydu Vhphvwuh”. Para cifrar estas frases se usó el algoritmo simétrico clásico Cesar, al ser simétrico quiere decir que tiene una única llave privada.

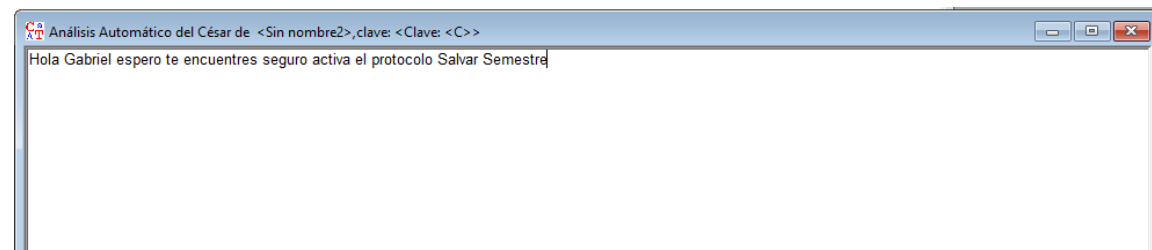


Luego de recibir la frase encriptada correspondientemente se analizó y descifrar usando el mismo algoritmo. Cryptool nos generó la letra clave que requerimos para descifrar el mensaje.



La clave utilizada por Gabriel fue C, la clave utilizada o desfasada por cryptools es B.

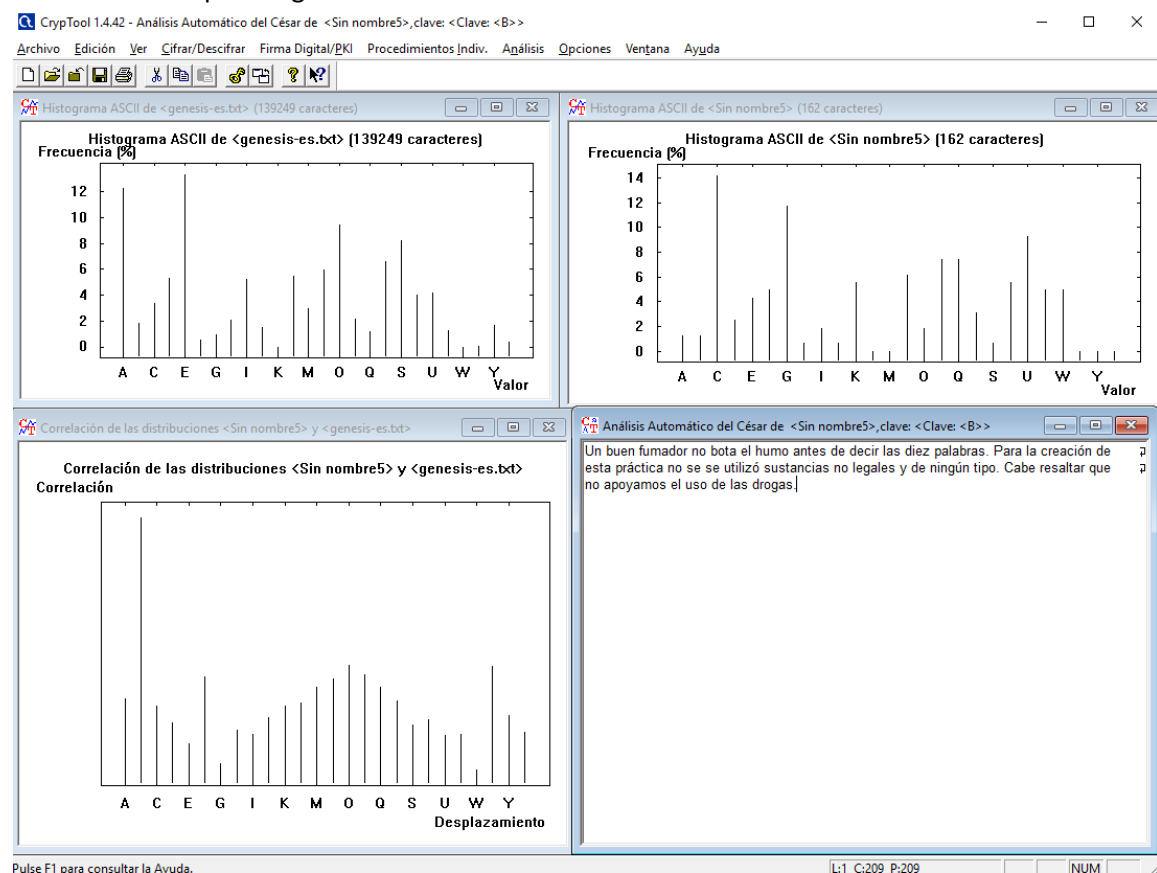
La clave utilizada por Diego fue D, la clave utilizada por cryptools es C.



Para la segunda parte de esta práctica ciframos nuevamente una frase pero esta vez con una longitud mayor a 10 palabras. Utilizamos el algoritmo simétrico (clásico) Vigenére.

Frase Encriptada Gabriel: Wp dwgp hwocfqt pq dqvc gn jwoq cpvgu fg fgekt ncu fkgb rcncdtcu.
Rctc nc etgcekóp fg guvc rtáevkec pq ug ug wvknkbó uwuvcpcku pq ngicngu a fg pkpiúp vkrq.
Ecdg tgucnvct swg pq crqacoqu gn wuq fg ncu ftqicu.

frase descifrada por Diego

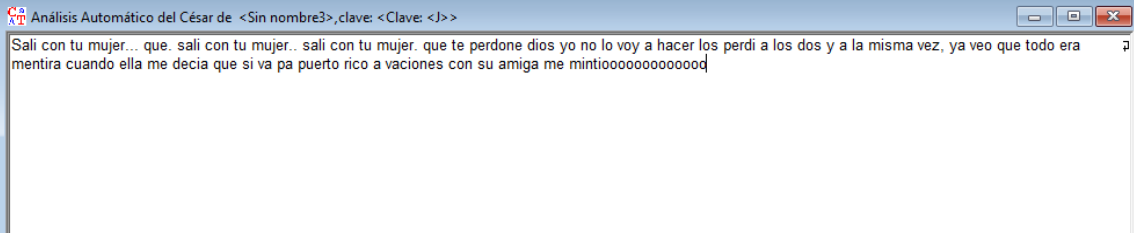


Frase Encriptada Diego: Ckvs myx de wetob... aeo. ckvs myx de wetob.. ckvs myx de wetob. aeo do zobnyxo nsyc iy xy vy fyi k rkmob vyc zobns k vyc nyc i k vk wscwk foj, ik foy aeo dyny obk woxdsbk meknxy ovvk wo nomsk aeo cs fk zk zeobdy bsmy k fkmsyxoc myx ce kwsqk wo wsxdsyyyyyyyyyyyyyy

Sin nombre3

Ckvs myx de wetob... aeo. ckvs myx de wetob.. ckvs myx de wetob. aeo do zobnyxo nsyc iy xy vy fyi k rkmob vyc zobns k vyc nyc i k vk wscwk foj, ik foy aeo dyny obk woxdsbk meknxy ovvk wo nomsk aeo cs fk zk zeobdy bsmy k fkmsyxoc myx ce kwsqk wo wsxdsyyyyyyyyyyyyyy

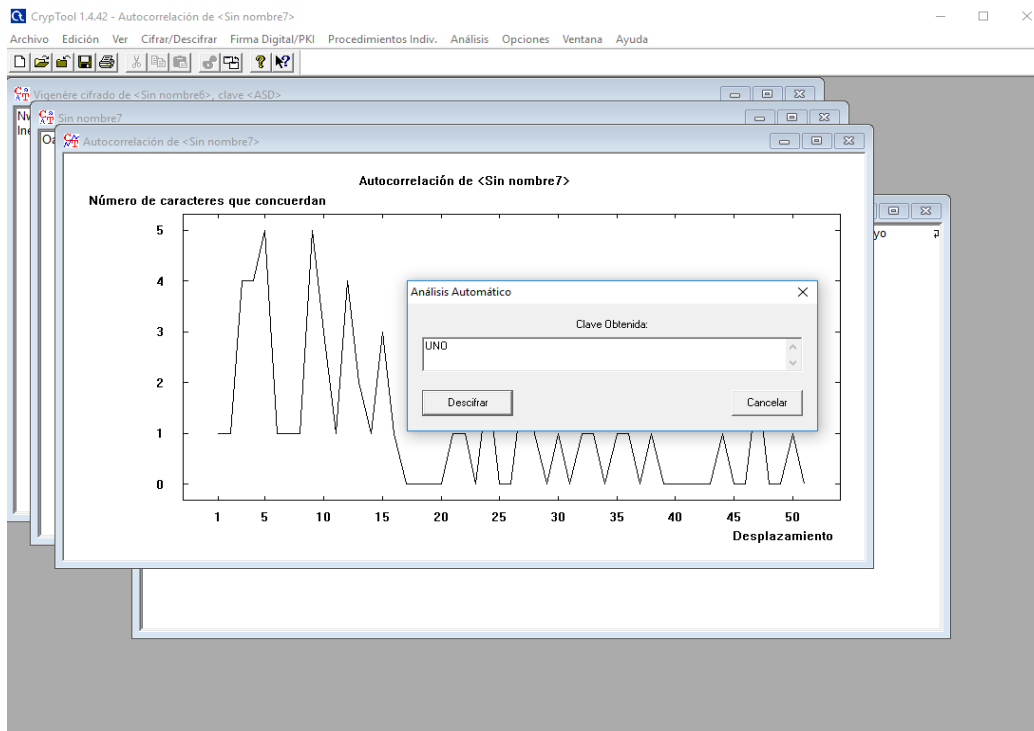
Frase Clave descryptada por Gabriel



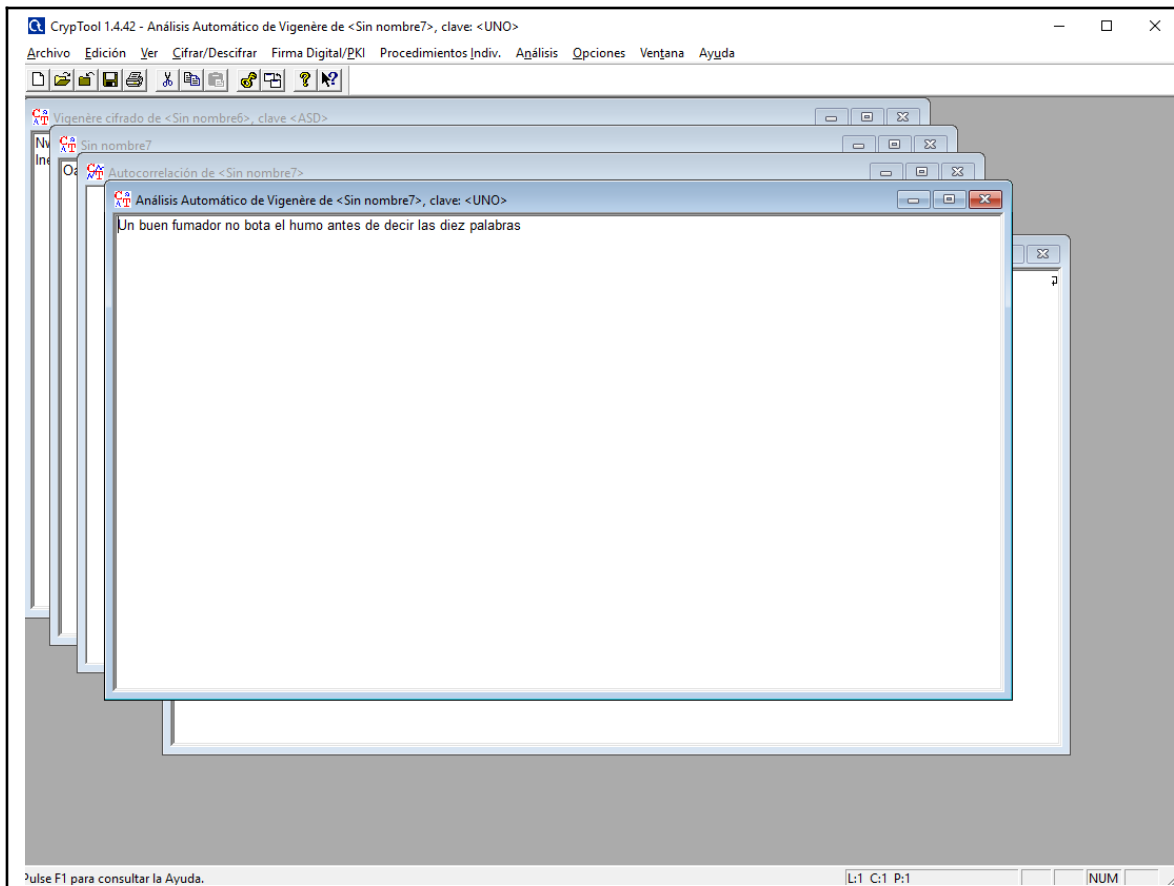
Para la tercera parte de la práctica nos centramos en colocar una clave de 3 caracteres, en el ejemplo la clave es **UNO**

Frase encriptada Gabriel: Oa porb zhauqcl ac vbhu rz bhai nbng xr rypwl yom qwym duyoveom

clave descifrada:



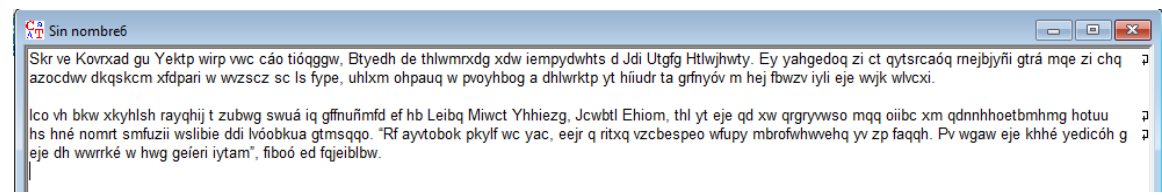
Mensaje descifrado utilizando la clave UNO



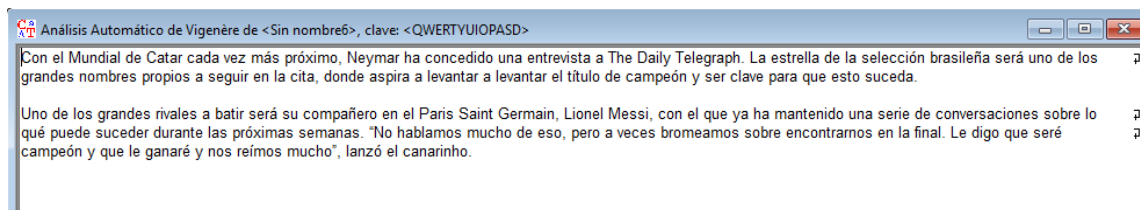
Para probar la existencia de desplazamiento a la hora de descifrar un mensaje cifrado con el algoritmo simétrico (clásico) Vigenère ingresamos un clave de más de 10 caracteres para cifrar un párrafo con muchas palabras.

FRASE ENCRIPTADA CON 10 CARACTERES DE CLAVE DIEGO: Skr ve Kovrxad gu Yektp wirp vwc cáo tíoqggw, Btyedh de thlwmxrdg xdw iempydwhts d Jdi Utgfg Htlwjhwty. Ey yahgedoq zi ct qytsrcaóq rnejbjyñi gtrá mqe zi chq azocdwv dkqskcm xfdpari w wvzscz sc ls fype, uhlxm ohpauq w pvoyhbog a dhlwrkt p yt híiudr ta grfnyóv m hej fbwzv iyli eje wvjw wlvxci.

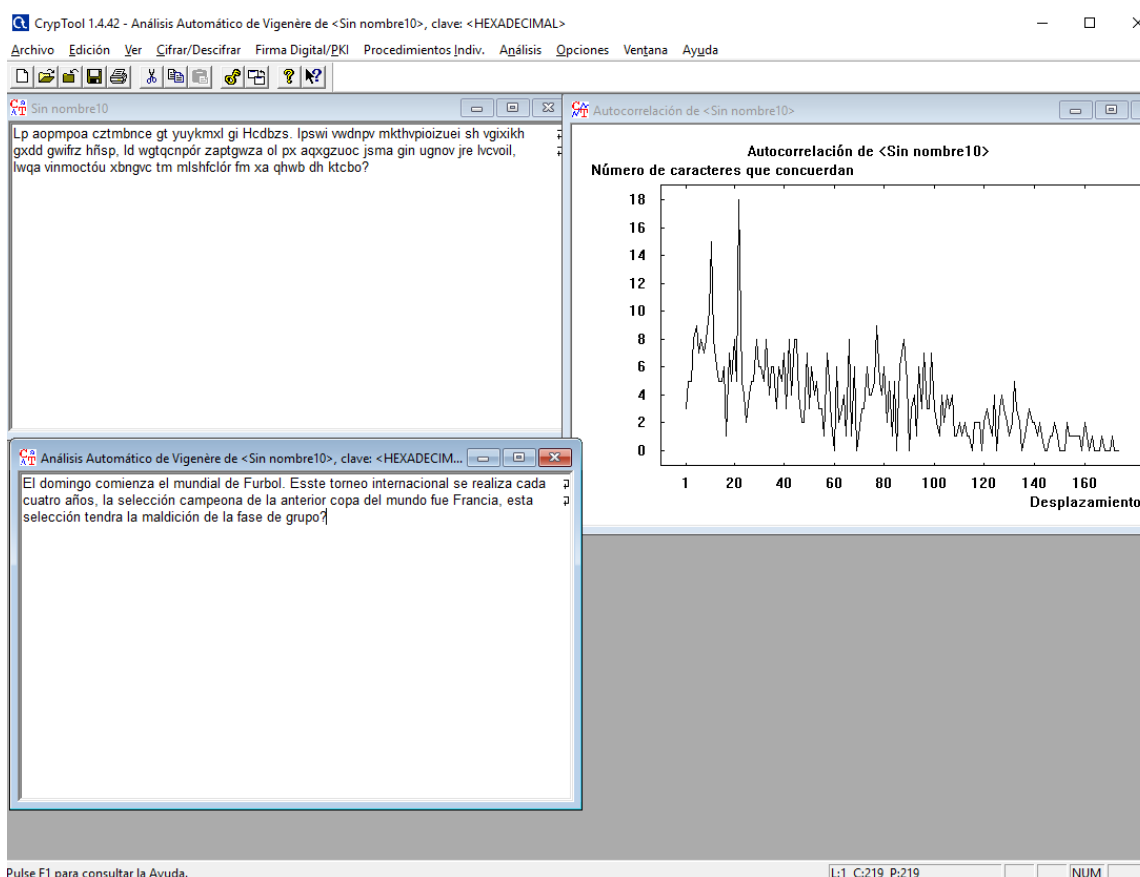
Ico vh bkw xkyhlsh rayqhij t zubwg swuá iq gffnuñmfd ef hb Leibq Miwct Yhhiezg, Jcwbt Ehiom, thl yt eje qd xw qrgryvso mqq oiibc xm qdnnhhoetbmhmng hotuu hs hné nomrt smfuzii wsliebie ddi lvóobkua gtmsqqo. "Rf ayvtobok pkylf wc yac, eejr q ritxq vzcbespeo wfupy mbrofwhwvehq yv zp faqqh. Pv wgaw eje khhé yedicóh g eje dh wwrké w hwg geieri iytam", fiboó ed fajeiblbw.



frase descriptada



frase encriptada Gabriel con clave 10 caracteres: Lp aopmpoa cztmnbce gt yuykxnl gi Hcdbzs. Ipswi vwdnpv mkthvpioizuei sh vgixikh gxdd gwifrz hñsp, ld wgtqcnpór zaptgwza ol px aqxgzuoç jsma gin ugnov jre lvcvoil, lwqa vinmoctóu xbngrvc tm mlshfclór fm xa qhwb dh ktcbo?



Por último analizaremos cómo funciona la creación de firmas digitales utilizadas para la autenticación de documentos, archivos entre otros. Primero generamos un par de claves con el cifrado de clave asimétrica RSA.

Generación de Pares de Claves Asimétricas

Algoritmo

☒ RSA
Longitud del módulo RSA (en)

☐ DSA
Longitud del primo DSA (en bits):

☐ Curvas Elípticas
Identificador (longitud en bits y parámetros):

Datos de Usuario

El par de claves se añadirá a un PSE cifrado con la información siguiente. El par de claves será protegido por tu código PIN.

Apellido:

Nombre:

Identificador de Clave (opcional):


El parámetro del dominio de la curva

Parámetros	Valor de los Parámetros

Formato de Representación de los números

☐ Octal ☒ Decimal ☐ Hexadecimal

CrypTool

 Los parámetros elegidos y el nuevo par de claves se han guardado correctamente. El identificador de clave asignado es '[Bastardo][Diego][RSA-1024][1668697645]'.

Tiempo invertido en la creación del par de claves: 9.041 segundos.

Firmar un Documento

Elija la función Hash

Algoritmo:	Longitud
<input type="radio"/> MD2	128 bits
<input type="radio"/> MD5	128 bits
<input type="radio"/> RIPEMD-160	160 bits
<input type="radio"/> SHA	160 bits
<input checked="" type="radio"/> SHA-1	160 bits

Elija el algoritmo de firma

Algoritmos basados en la Factorización

☒ RSA

Logaritmos basados en el Logaritmo Discreto

☐ DSA

Algoritmos basados en Curvas Elípticas

☐ ECSP-DSA
☐ ECSP-NR

Formato de Presentación

☐ Coordenadas Afines
☒ Coordenadas Projectivas

Elija una clave /PSE para utilizarla en el proceso de firma

Apellido	Nombre	Tipo de Clave	Identificador de ...	Creado	ID interno
Bastardo	Diego	RSA-1024		17.11.2022 11:07:25	1668697645
HybridEncrypti...	Bob	EC-prime239v1	PIN=1234	09.05.2007 05:21:14	1178702474
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 05:51:34	1152179494

Tipos de Claves:

☒ Claves RSA
☒ Claves DSA
☒ Claves EC

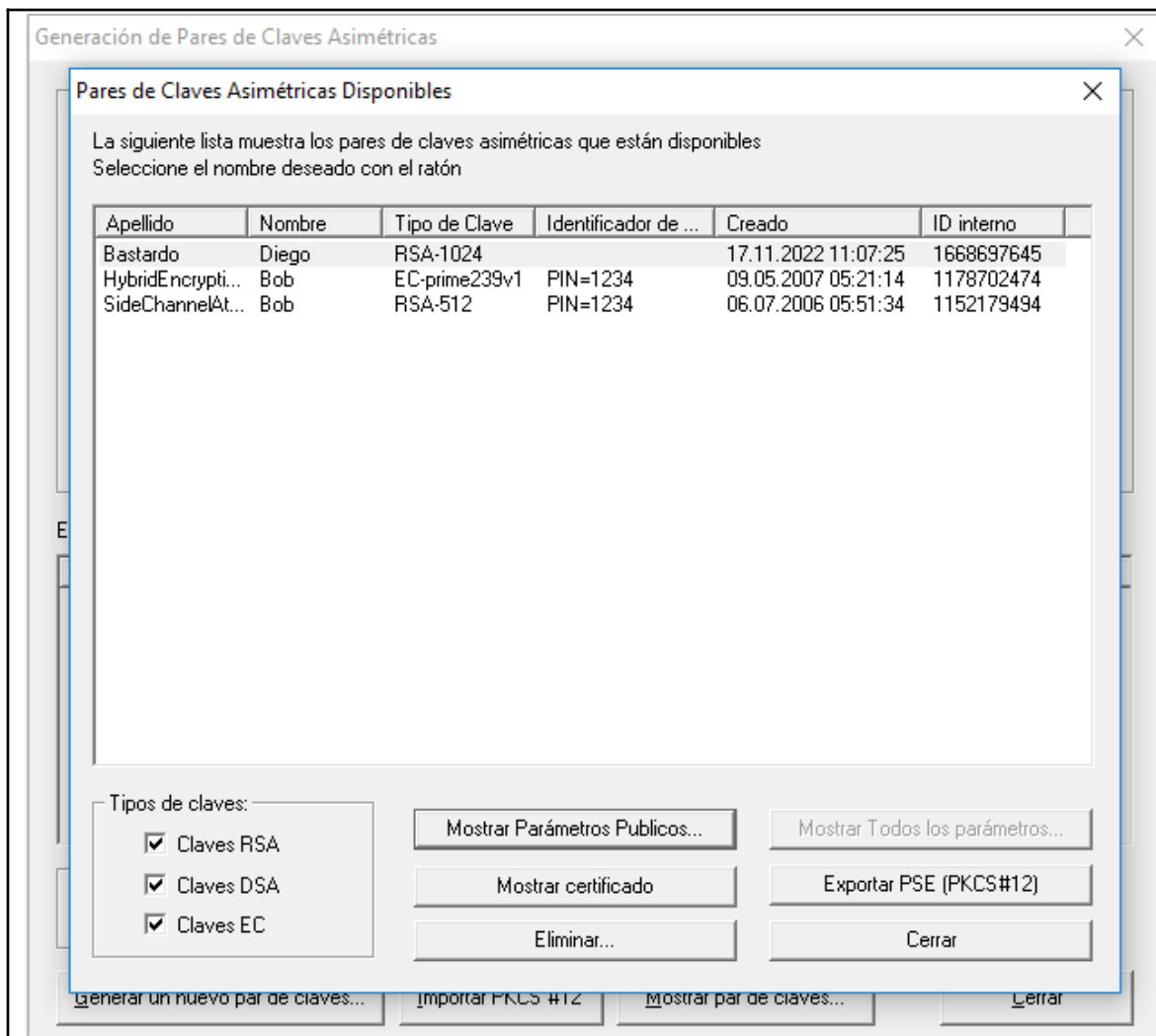
Código PIN para el PSE elegido:

☐ Mostrar tiempo empleado
☐ Mostrar resultados intermedios

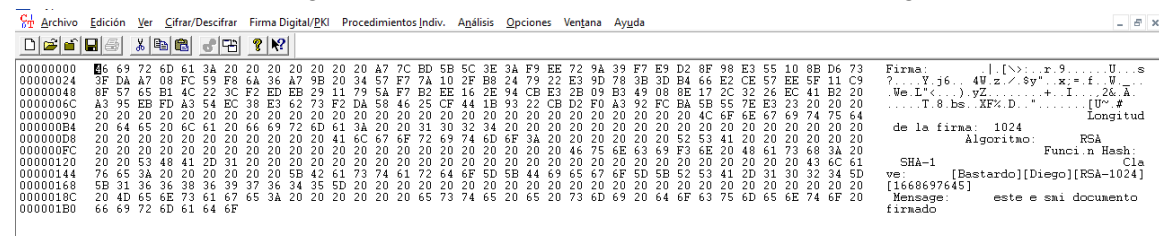
Firmar

Cancelar

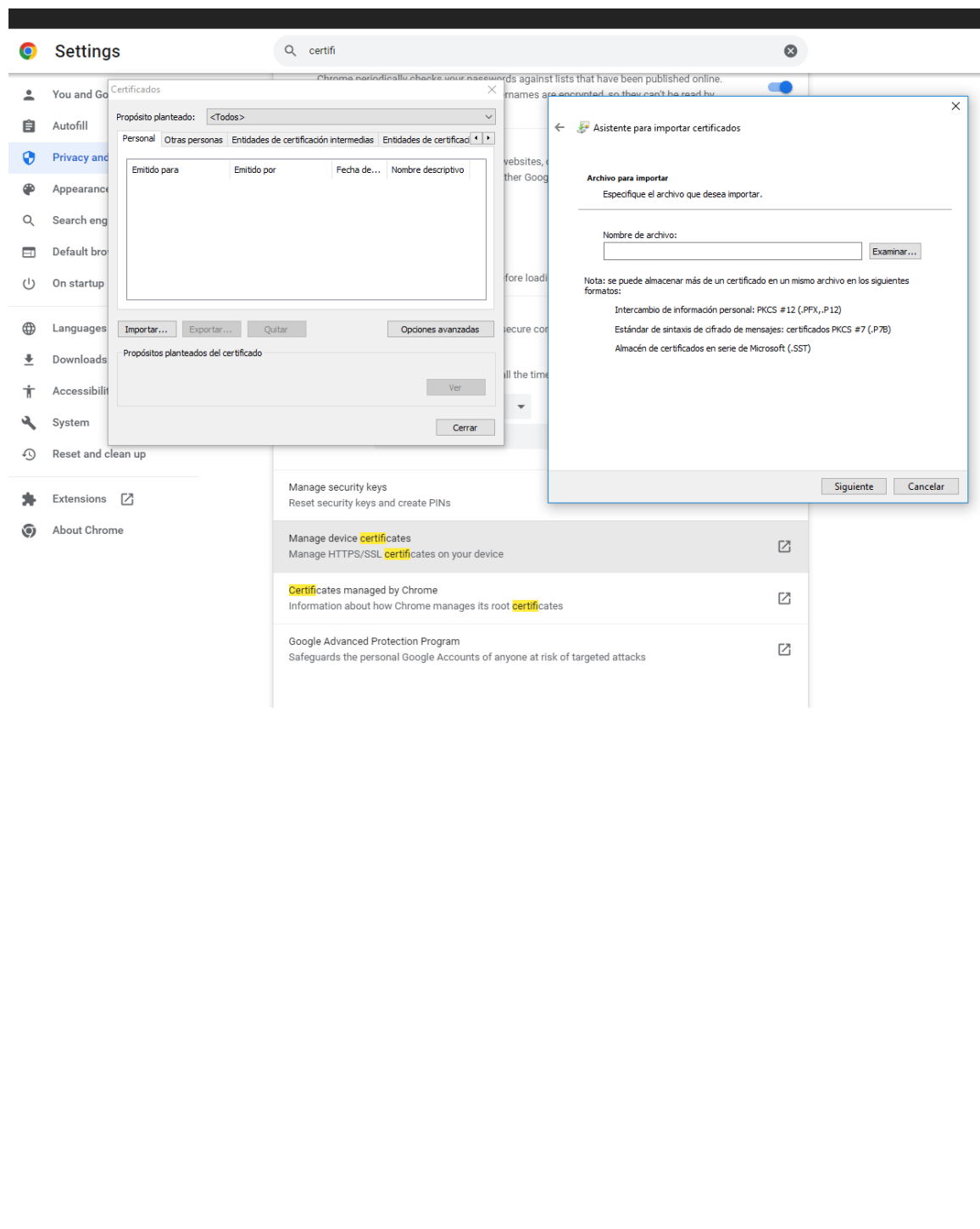
Luego de esto procedimos a exportar la clave al formato PKCS#12.



Y por último nos encargamos de firmar un documento con la firma digital creada.



Como actividad final, adicional a la ejecución de la práctica aprendimos a configurar nuestra firma digital para que esté validada por el proxy de nuestro navegador de manera tal que nos permite firmar documentos de word.



Referencias Bibliográficas

<https://www.ibm.com/es-es/topics/encryption>
<https://www.hornetsecurity.com/es/knowledge-base/criptografia/>
<https://blog.mailfence.com/es/cifrado-simetrico-vs-asimetrico/>
<https://www.techiedelight.com/es/vigenere-cipher-implementation/>

Hallazgos y/o conclusiones de la actividad desarrollada (Explique su experiencia y el análisis de los resultados):

En medio de una sociedad cada vez más y más dependiente de la tecnología, resulta de vital importancia para las organizaciones, y usuarios en general, aprender a dominar disciplinas como la criptografía: una herramienta que destaca dentro del mundo de la seguridad informática como una de los mejores métodos para cifrar información confidencial y delicada, la cual puede llegar a ser víctima de amenazas tecnológicas externas.

Durante esta práctica pudimos aprender a profundidad los distintos métodos de cifrado que existen en la actualidad, enfocándonos específicamente en el Algoritmo de Vigenère y el Cifrado César. Asimismo, comprendimos cuáles utilizar frente a distintos escenarios dependiendo del tipo de información a proteger, así como la longitud de la misma.

Al enfocarnos en cifrar y descifrar los distintos mensajes o claves utilizados durante esta práctica con el apoyo de la aplicación Cryptool, también pudimos obtener una visión mucho más global y gráfica de cómo funciona realmente el proceso de encriptación digital en el mundo real; y su importancia para proteger conversaciones o códigos confidenciales en el día a día.

Otro factor importante dentro de la práctica dedicada a la criptografía fue la creación de firmas digitales: herramientas que en la actualidad resultan sumamente útiles para salvaguardar la integridad y la fidelidad de aquellos documentos que viajan en la red; permitiendo que los procesos de autenticación de información sean mucho más fidedignos y útiles.

Contribución de esta actividad en su Proyecto: