Actividad 4: Herramientas para criptografía y criptoanálisis

Seguridad Informática

16/10/2014

Brais López Yáñez

ÍNDICE

1. ATAQUE AL CIFRADO DE SUSTITUCIÓN MONOALFABÉTICO

Usando las herramientas para el análisis de frecuencias (por ejemplo, las proporcionadas en Cracking the Substitution Cipher), la primera parte de la práctica consiste en intentar descifrar un texto cifrado procedente de un cifrado monoalfabético aleatorio (conservando los espacios entre las palabras para hacerlo más fácil, o sin espacios para probar nuestra habilidad).

Alternativamente, se puede utilizar el enlace "Crack a substitution cipher" en la web del CryptoClub.

En cualquiera de los dos casos, debéis incluir en el informe de la sesión una descripción de la técnica empleada para romper este tipo de cifrado, y detallar el ejemplo analizado, mostrando los pasos necesarios en el análisis: qué herramientas habéis utilizado, qué valores de frecuencia (letras individuales, pares de letras, etc.), cuántos intentos han sido necesarios. Debéis también incluir ambos textos: el texto cifrado, y el texto plano una vez recuperado, así como la clave si la habéis averiguado.

Para realización de la descifración del texto se han necesitado 2 intentos. En el primer intento no estaban claros que patrones y que estrategias utilizar. Una vez, comprobamos la solución del primer intento, intentamos crear una estrategia que funcionó para el segundo intento:

CIFRADO MONOALFABÉTICO

Texto Cifrado: LTKHNMEVKG KE CVH VRTMHEC CVKNB KN CVH WXTFM CX HAGFRKN KCE NXC EXQHCVKNB YXP FHRTN KN EZVXXF OPC KL YXP VRIHNC FHRTNHM CVH QHRNKNB XL LTKHNMEVKG YXP THRFFY VRIHNC FHRTNHM RNYCVKNB QPVRQQRM RFK

DESCUBRIR EL IDIOMA

Para proceder a discifrar un texto lo primero que podemos hacer es pensar en el idioma que hemos elegido. Una vez sabemos de qué idioma se trata, en este caso será el inglés. Nuestro objetivo será el de ver las letras que más se repiten.

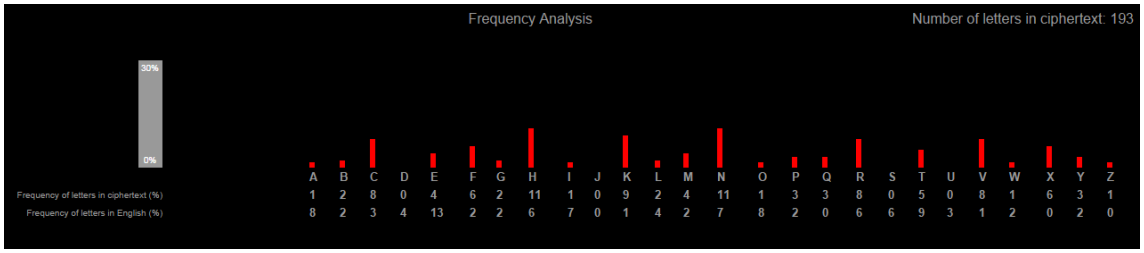
ANALIZAR LOS GRUPOS DE LETRAS

Tras esto, podemos ir analizando las cadenas de letras del texto cifrado. Un elemento clave a la hora de seguridad va a ser interpretar de forma correcta los resultados. Si nos ponemos en un lugar de un nativo inglés, podemos darnos cuenta de algunas de las preposiciones más usadas son: “the”, “to”, “a”, “an”, etc.

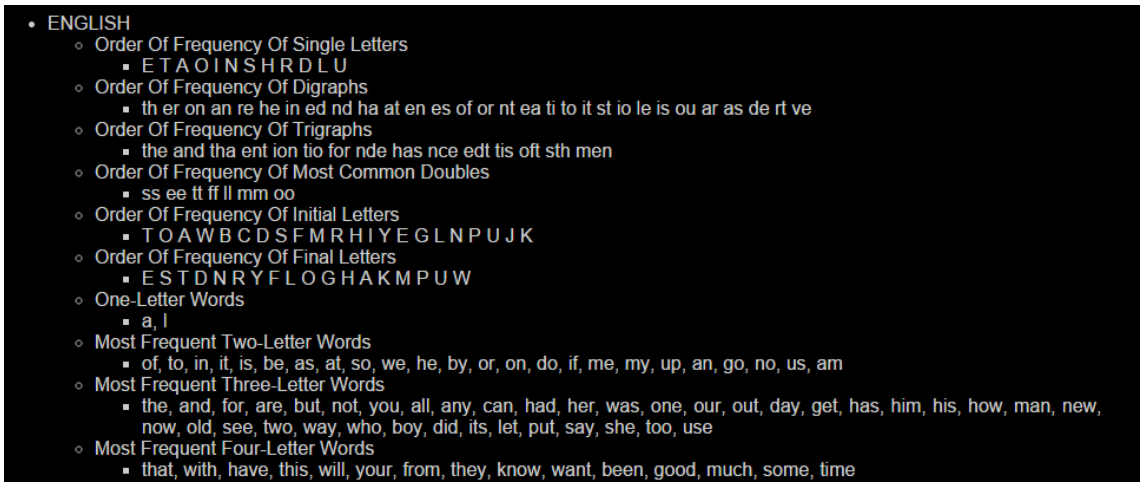
Una vez buscamos el grupo de preposiciones más usadas en inglés, buscaremos si las letras más repetidas en el texto cifrado pueden ser las más repetidas en inglés.

CARACTERES MÁS REPETIDOS

Según el idioma con el que estés trabajando, unas letras se repiten más que otros. Esta es la razón que nos hará capaces de descifrar los grupos de preposiciones. Analizaremos detenidamente los resultados de las letras más repetidas en el texto cifrado.



Tras ver la frecuencia en la que se usan determinadas letras en el texto cifrado, las intentaremos sustituir por las letras más usadas en el idioma escogido, el inglés.



Una vez comparadas las letras, en el texto cifrado con las más usadas en inglés. Procedemos a una **clasificación inicial con las posibles relaciones**.

LETRAS

11 LETRAS:

- Letra cifrada H= E;
- Letra cifrada N = A

9 LETRAS :

- Letra cifrada K= ¿A?

8 LETRAS: ¿O I N?

- Letra cifrada V=
- Letra cifrada R=
- Letra cifrada C=

6 LETRAS: ¿S H?

- Letra cifrada X=
- Letra cifrada F=

CONCLUSIÓN Y OBTENCIÓN

Tras observar nuestra posible clasificación ideal, procedemos a probar por intuición y lógica los grupos de letras por las letras que más se pueden repetir. Probamos a sustituir las preposiciones the por el el grupo cifrado CVH. Tras esto y pensando en inglés, procedemos a aplicar la misma estrategia para el resto de letras que no identificamos. Si fallamos y el texto no tiene lógica probamos, asegurándonos de que tenga sentido.

Texto Descifrado: FRIENDSHIP IS THE HARDEST THING IN THE WORLD TO EXPLAIN ITS NOT SOMETHING YOU LEARN IN SCHOOL BUT IF YOU HAVENT LEARNED THE MEANING OF FRIENDSHIP YOU REALLY HAVENT LEARNED ANYTHING MUHAMMAD ALI

2. ATAQUE AL CIFRADO DE SUSTITUCIÓN POLIALFABÉTICO (VIGENÈRE)

La web "The Black Chamber" proporciona también algunos ejemplos y herramientas para intentar romper el cifrado de Vigenère. Esta es una tarea más compleja, pero siguiendo el ejemplo (Cracking the Vigenère Cipher) puede realizarse sin mucha dificultad.

Alternativamente, podéis usar en el "CryptoClub" el enlace "Crack Vigenère": http://www.cryptoclub.org/tools/crack_vigenerecipher.php.

Debéis incluir en el informe una descripción de la técnica empleada para romper el cifrado de Vigenère, y los detalles de ejemplo analizado: texto cifrado a atacar, etapas seguidas en el análisis, número de intentos para averiguar la longitud de la clave, número de pruebas para determinar cada una de las letras de la clave, herramientas de ayuda utilizadas, y el texto plano una vez recuperado.

Para realizar esta parte de la actividad nos centramos en entender que es el cifrado de Vigenere, en el cifrado monoalfabético lo que se hacía es cambiar la cadena de letras por otras letras. Estaríanos usando otro alfabeto para codificar cualquier texto. Las frecuencias más representativas de este serían equivalentes a las letras más empleadas en ese idioma. Con el cifrado de Vigenere esto cambia:

Definición: es un cifrado basado en diferentes series de caracteres o letras del cifrado César formando estos caracteres una tabla, llamada tabla de Vigenère, que se usa como clave. El cifrado de Vigenère es un cifrado de sustitución simple polialfabético.

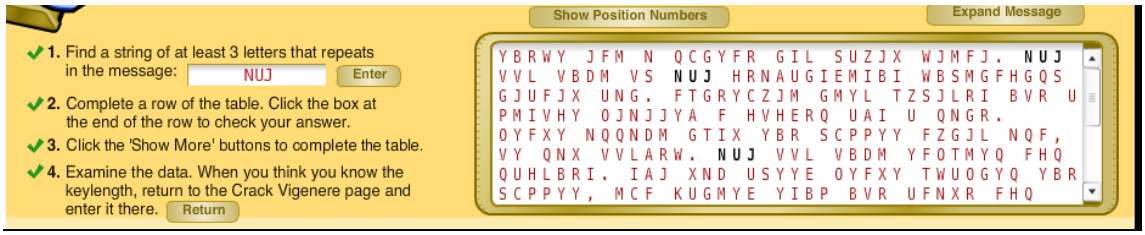
Al ser un cifrado polialfabético todo va a depender de la longitud de la clave, que serían los grupos empleados para cifrar el texto. Si sabemos las letras más representativas de cada grupo habremos descifrado el texto.

Para esta parte del ejercicio usaremos: http://www.cryptoclub.org/tools/crack_vigenerecipher.php, ver la imagen.

Seguiremos los pasos indicados.

Texto cifrado: YBRWY JFM N QCGYFR GIL SUZJX WJMFJ. NUJ VVL VBDM VS NUJ HRNAUGIEMIBI WBSMGFHGQS GJUFJX UNG. FTGRYCZJM GMYL TZSJLRI BVR U PMIVHY OJNJJYA F HVHERQ UAI U QNGR. OYFXY NQQNDM GTIX YBR SCPPYY-FZGJL NQF, VY QNX VVLARW. NUJ VVL VBDM YFOTMYQ FHQ QUHLBRI. IAJ XND USYYE OYFXY TWUOGYQ YBR SCPPYY, MCF KUGMYE YIBP BVR UFNXR FHQ XUVI, "DRXMR, YBBXY OTSF FLR RUXNHTKOA TZ LTO. GMYL YBVSE LTO QTH'G PHBB NUJ XVRY VX QBWNU RIEJ NUFH GMY ANWXJF." WJMFJ AENHAJX NSX FFCQ, "IIA'Y QBWLL IUQ. N EATQ JMCPM CF BIEYB ZTLR. GOG NZ V YIBP NUJ XVRY, GMYL BIHQX FYIC IIVSA VY. MB KUE N'PR HIYQYPYYQ $10 IIYQUEX."

IDENTIFICAR GRUPO DE STRING

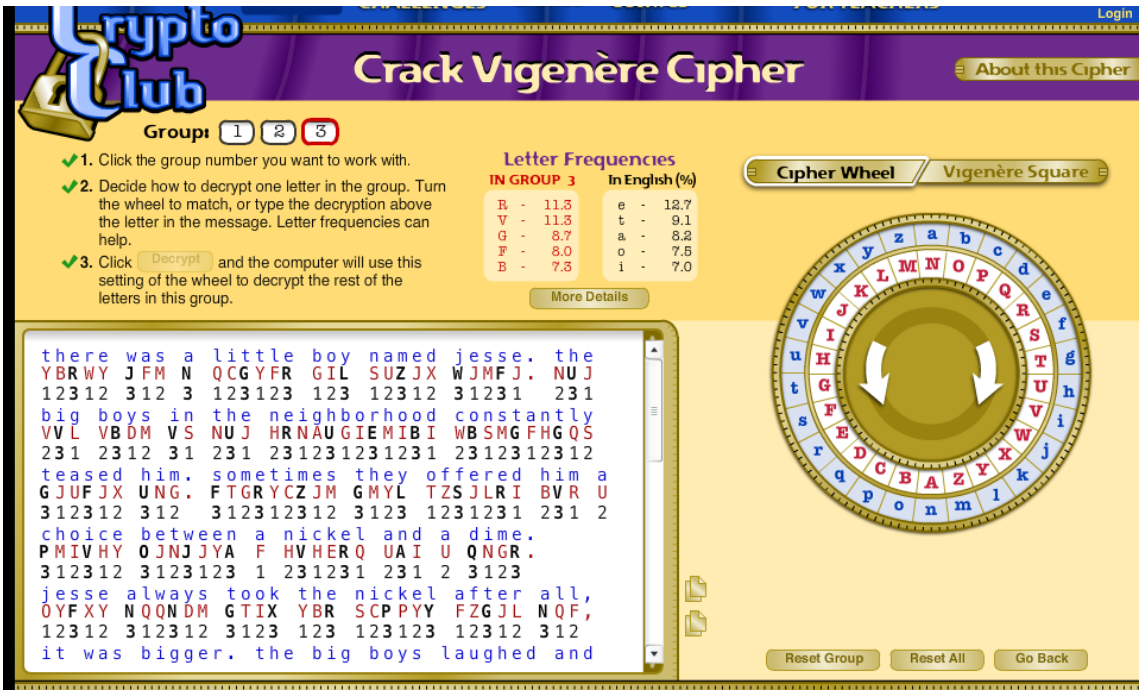


Lo primero que nos aconsejan desde la página empleada es encontrar un string de 3 letras que se repitan en el mensaje. Nuestra elección ha sido NUJ (posible the). Tras esto seguimos los pasos recomendados y podemos ver los factores de distancia, que son los múltiplos del valor más repetido (clave).

POSIBLE KEYLENGTHS

Siguiendo lo anterior, tras ver los posibles múltiplos del valor más repetido, obtendremos la posible keygenlenths. Para hallarla seleccionaremos los múltiplos más repetidos, y su miramos de qué son múltiplo. En este caso 3. Con este número probaremos para ver si es posible obtener el texto descifrado (si hemos elegido la correcta lo haremos).

DESCIFRANDO LOS GRUPOS



Una vez tenemos la supuesta clave, conseguimos diferenciar los grupos de alfabetos utilizados. Lo siguiente que tendremos que hacer, es adivinar la letra más repetida de cada grupo. Al igual

que en la parte uno, iremos probando por un método de ensayo/error pensando en el idioma del que queremos obtener el texto.

CONCLUSIÓN Y OBTENCIÓN

Para los tres grupos, probaremos hasta que nos quede un texto con sentido. En el caso de la imagen, el grupo 3 tiene R=E, que es la letra que se repite con más frecuencia en inglés. Con esto obtendremos el texto descifrado.

Texto descifrado: there was a little boy named jesse. the big boys in the neighborhood constantly teased him. Sometimes they offered him a choice between a nickel and a dime. Jesse always took the nickel after all, it was bigger. The big boys laughed and laughed. One day after jesse grabbed the nickel, his father took him aside and said, "jesse, those boys are makingfun of you. The think you don't know the dime is worth more than the nickel." Jesse grinned and said, "don't worry dad. I know which is worth more. But if I took the dime, they would stop doing it. So far i've collected $10 dollars."

3. MÁQUINA DE CIFRADO ENIGMA

Para la última parte de la sesión es recomendable instalar un simulador de la máquina Enigma. A mayores, podéis encontrar información sobre su uso enhttp://www.enigmaworldcodegroup.com/

En la web http://www.cryptomuseum.com/crypto/enigma/ se describe también el principio de funcionamiento de la máquina Enigma, así como una breve explicación de cómo este método de cifrado fue roto por los aliados durante la Segunda Guerra Mundial, usando la "Bombe".

Para esta parte de la práctica, debéis incluir en el informe una breve explicación de cómo los distintos elementos (rotores, conexiones, etc.) que intervienen en el cifrado contribuyen a que el cifrado sea más robusto que un cifrado polialfabético convencional como el de Vigenère; y una explicación de cómo se establecía y se compartía entre ambos lados del canal de comunicación la clave de cifrado.

¿QUÉ ES ENIGMA?

Enigma era el nombre de una máquina que disponía de un mecanismo de cifrado rotatorio, que permitía usarla tanto para cifrar como para descifrar mensajes. Varios de sus modelos fueron muy utilizados en Europa desde inicios de los años 1920.

Su fama se debe a haber sido adoptada por las fuerzas militares de Alemania desde 1930. Su facilidad de manejo y supuesta inviolabilidad fueron las principales razones para su amplio uso.

Para descifrar Enigma los aliados establecieron su centro de operaciones numéricas en Bletchley Park, dónde estaban reunidos Alan Turing y sus colaboradores.

Turing tuvo una de las ideas más geniales. Imaginó una nueva máquina formada por tres máquinas Enigma con las posiciones de los rotores desplazadas según el rizo interconectadas de manera que se anulara el efecto del clavijero. Bletchley Park consiguió presupuesto para convertir la idea de Turing en una máquina que llamaron *bomba* como las primeras réplicas de Enigma de Rejewski. El 14 de marzo de 1940 llegaba la primera bomba prototipo a la que llamaron *Victory*. Y el 8 de agosto la nueva bomba llamada *Agnes*. Si bien las bombas

representaron un gran avance, no siempre conseguían descifrar los mensajes. Había que probar con distintos puntales y una vez hallado el correcto había que encontrar la posición adecuada en el mensaje donde ubicarlo, para entonces iniciar la desencriptación con una bomba.

****Simulador de una Máquina Enigma*

¿COMO FUNCIONA ENIGMA Y POR QUÉ ES MÁS ROBUSTA QUE UN CIFRADO POLIALFABÉTICO?

La máquina Enigma era un dispositivo electromecánico, es decir, tenía una parte eléctrica y otra mecánica. El mecanismo consistía en una serie de teclas, con las letras del alfabeto, al igual que una máquina de escribir, que en realidad eran interruptores que accionaban los dispositivos eléctricos y hacían mover unos cilindros rotatorios. El funcionamiento, cara al usuario, era bastante sencillo. El operador tenía que teclear las letras de su mensaje y anotar las letras que devolvía la máquina (a través de un alfabeto que se iba iluminando). El código a usar se fijaba con las posiciones de los cilindros que constaban, cada uno, de 26 cables que se conectaban al teclado pero, con la particularidad, que el primer cilindro giraba un veintiseisavo de vuelta después de cada pulsación, de tal manera que la posición de las conexiones iba cambiando con cada entrada del teclado, obteniendo un cifrado polialfabético. Además, para dar mayor robustez (que el cifrado polialfabético), el segundo cilindro sólo daba un giro cuando el primero había completado 26 giros y el tercero cuando el segundo había dado sus correspondientes 26 y añadió la posibilidad de que los rodillos pudiesen ser intercambiados de posición, de manera que el número de posibilidades aumentase hasta tener 105.456 alfabetos.

Además, el sistema contaba con 6 cables de conexión que también permitían introducir modificaciones dado que podrían conectarse a 26 lugares (representando a las 16 letras del alfabeto de Enigma) lo que producía 100.391.791.500 maneras distintas de conectar los cables.

¿CÓMO SE ESTABLECÍA Y SE COMPARTÍA ENTRE AMBOS LADOS DEL CANAL DE COMUNICACIÓN LA CLAVE DE CIFRADO?

Al principio de cada mes, se daba a los operadores de la Enigma un nuevo libro que contenía las configuraciones iniciales para la máquina. Por ejemplo, en un día particular las configuraciones podrían ser poner el rotor n.° 1 en la hendidura 7, el n.° 2 en la 4 y el n.° 3 en la 6. Están entonces rotados, para que la hendidura 1 esté en la letra X, la hendidura 2 en la letra J y la hendidura 3 en la A. Como los rotores podían permutarse en la máquina, con tres rotores en tres hendiduras se obtienen otras 3 x 2 x 1 = 6 combinaciones para considerar, para dar un total de 105.456 posibles alfabetos.

A estas alturas, el operador seleccionaría algunas otras configuraciones para los rotores, esta vez definiendo sólo las posiciones o "giros" de los rotores. Un operador en particular podría seleccionar ABC, y éstos se convierten en la configuración del 'mensaje para esa sesión de cifrado'. Entonces teclearon la configuración del mensaje en la máquina que aún está con la configuración inicial. Los alemanes, creyendo que le otorgaban más seguridad al proceso, lo tecleaban dos veces, pero esto se desveló como una de las brechas de seguridad con la que "romper" el secreto de Enigma. Los resultados serían codificados para que la secuencia ABC tecleada dos veces podría convertirse en XHTLOA. El operador entonces gira los rotores a la configuración del mensaje, ABC. Entonces se teclea el resto del mensaje y lo envía por la radio.

En el extremo receptor, el funcionamiento se invierte. El operador pone la máquina en la configuración inicial e introduce las primeras seis letras del mensaje. Al hacer esto él verá ABCABC en la máquina. Entonces gira los rotores a ABC e introduce el resto del mensaje cifrado, descifrándolo.

Aunque se enviaran muchos mensajes en cualquier día con seis letras a partir de la configuración inicial, se asumía que esas letras eran al azar. Mientras que un ataque en el propio cifrado era posible, en cada mensaje se usó un cifrado diferente, lo que hace que el análisis de frecuencia sea inútil en la práctica.

4.FUENTES:

- http://www.simonsingh.net/The_Black_Chamber/chamberguide.html
- http://www.cryptoclub.org/tools/crack_vigenerecipher.php
- http://www.u-historia.com/uhistoria/tecnico/articulos/enigma/enigma.htm
- http://es.wikipedia.org/wiki/Enigma_(m%C3%A1quina), verificada
- http://blogs.elpais.com/turing/2013/06/alan-turing-el-descifrado-de-la-maquina-enigma.html
- http://alt1040.com/2011/07/la-maquina-enigma-el-sistema-de-cifrado-que-puso-en-jaque-a-europa