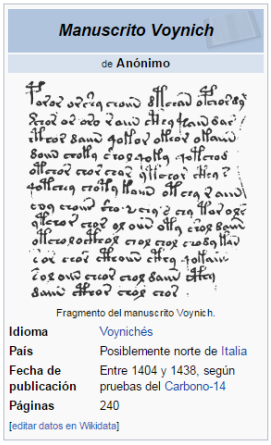
Manuscrito Voynich

El **manuscrito Voynich** es un libro ilustrado, de contenidos desconocidos, escrito hace unos 500 años por un autor anónimo en un alfabeto no identificado y un idioma incomprensible, el denominado *voynichés*.

A lo largo de su existencia comprobada el manuscrito ha sido objeto de intensos estudios por numerosos criptógrafos profesionales y aficionados, incluyendo destacados especialistas estadounidenses y británicos en descifrados de la Segunda Guerra Mundial. Hasta febrero de 2014 ninguno había conseguido descifrar una sola palabra. Esta sucesión de fracasos ha convertido al manuscrito en el Santo Grial de la criptografía histórica, pero a la vez ha alimentado la teoría de que el libro no es más que un elaborado engaño, una secuencia de símbolos al azar sin sentido alguno.

En febrero de 2014, Stephen Bax, profesor de la Universidad de Bedfordshire (Reino Unido), anunció haber descifrado el manuscrito en forma parcial.[1]



Manuscrito Voynich

de **Anónimo**

Fragmento del manuscrito Voynich.

Idioma	Voynichés
País	Posiblemente norte de Italia
Fecha de publicación	Entre 1404 y 1438, según pruebas del Carbono-14
Páginas	240

[editar datos en Wikidata]

Para la realización de esta práctica, puedes utilizar para las comprobaciones la herramienta safeDES que puedes descargar desde la red temática Criptored y el archivo que se indica.

safeDES: http://www.criptored.upm.es/software/sw_m001j.htm

Pregunta 1. Se sabe que el siguiente texto en hexadecimal

C=“A0F74AB368AB79FC61B855C66816E07948F0500665C1F4CA08A344E320020CF9040026F24EE0D018D8F06B9ED9F6
399E099146F670F1A92067687E03DB4C35282F06758E29E65D07DDAF55CC2526D71E5AC57E4F9429303078B9399588B7
8F4174CB54705260B8D0475A09B92E26B61A17A86FD3ED2E781793E7DF8E2742CD4D73AAD354B428C858CEC52F7DE
A168E243EBF0C300E5D1B88B74808FFAE350C240B05281F0138BA6F0481A22A4AC7DAC19DC4599B4683B54E9A8AB0
E2534CBD5A7DA7095FFF2B7608B43FF68EFFAB844196DBA9189B62F93DC1D9699E25400AB05CCB4652294C78D09E5
55960679A34E7B78D14CC8F0384C155C55189AF73AA08B08EE9A2D0DDDE038CCAA5C2F4AC782EC53FA717DF2C84
AA6685E304B00E93FFAEDFF3E1DCA64B72B66BC94108ED1A54BF795A90B31EF75C73564F8FAE7E47D867126BA085F
8BCCB” ha sido obtenido al cifrar un mensaje M con la clave en hexadecimal K= 544f4d414e4f5441.

¿Cómo es posible que además de descifrarse con dicha clave, pueda descifrarse con esta otra K = 554e4c414e4f5440?

El mensaje M es: “Las actualizaciones de software son necesarias: Pocas cosas son mas fastidiosas que las ventanas emergentes recordándonos realizar alguna actualización a los cientos de programas que tenemos instalados, pero muchas veces esto es lo que te protege entre ser dueño de tu información o que otra persona tenga acceso.”

Pregunta 2. Indica otra clave distinta de las anteriores que permita descifrar el criptograma C y obtener el mismo mensaje M.

Pregunta 3. Al cifrar cualquier mensaje M con la clave $K_{1\ hex}$ = fee0fee0fef1fef1 y volver a cifrar el resultado con la clave $K_{2\ hex}$ = e0fee0fef1fef1fe, obtenemos nuevamente el mensaje M. ¿Qué puedes decir de estas claves? ¿Es posible en los cifradores simétricos obtener el mensaje en claro realizando una operación de cifrado sobre el criptograma? Justifica tu repuesta.

Pregunta 4. Supongamos que un atacante intercepta dos mensajes cifrados con DES con modo de cifra ECB, cuyo destino es una entidad bancaria:

$C1_{HEX}$ = A06770378D0B58049B8A00C4B2F31767E403F2382E69BC0E

$C2_{HEX}$ = A06770378D0B5804978D1322521A8348CF3AA5B388035F8D

Además, el atacante sabe que dichos criptogramas se corresponden con las siguientes dos transacciones bancarias:

M_1 = INGRESAR ALBERTO 100

M_2 = INGRESAR ALFONSO 10000

El atacante desconoce la clave de cifrado utilizada, aunque sabe que es la misma en ambos mensajes. Por otra parte, es capaz de eliminar $C1_{HEX}$, evitando que llegue al banco; y se propone enviar un mensaje fraudulento en su lugar. Para lo cual, a partir de los dos criptogramas interceptados, es capaz de construir un nuevo criptograma que se corresponde con el mensaje

M_3 = INGRESAR ALBERTO 10000

Escribe el criptograma que tendría que enviar, explicando cómo lo has obtenido

Pregunta 5. ¿Podría haber realizado el fraude de la pregunta anterior si los criptograma se hubieran obtenido con el algoritmo DES y el modo de cifra CBC? Justifica tu repuesta

Solución:

Pregunta 6. En una vuelta del DES se tiene como entrada a las cajas el texto hexadecimal **fabadafabada**. Se pide encontrar la salida de las cajas y mostrar toda la cadena de bits resultantes de la operación de las cajas S en esa vuelta, separados por octetos. Si quieres puedes utilizar la tabla siguiente:

Caja		S_1		S_2		S_3		S_4		S_5		S_6		S_7		S_8	
Entrada en binario																	
Fila binario	Columna binario																
Fila decimal	Columna decimal																
Celda en decimal																	
Salida en binario																	

Pregunta 7. Fijándote en el resultado de la pregunta 6.

a) ¿Cuántas operaciones habría que realizar como máximo para romper la caja S7 en esa vuelta? Justifica la respuesta.
b) ¿Cuántas operaciones habría que realizar como máximo para romper las 8 cajas S de esa vuelta? Justifica la respuesta.
c) ¿Y cuántas operaciones habría que realizar como máximo para romper las cajas S de un bloque de cifra del DES? Justifica la respuesta.

Pregunta 8. Al atacar al DES por fuerza bruta dentro de un espacio de claves de unos 15 millones de valores en el que sabemos se encuentra la clave K que se ha usado para cifrar, conociendo el texto en claro y el texto cifrado, la clave inicial y clave final del ataque, el texto en claro y el criptograma son los siguientes:

$K_{inicial}$ = AABBCCDD0CCCCCCC

K_{final} = AABBCCDD1AAAAAAA

Texto en claro = A1427261766F212C206C6F20686173206C6F677261646F2E

Criptograma = F6BAE1143E072505EC45C074CB798B7A0BD4B096DE8B491B

Se han obtenido los siguientes resultados:

Número de Claves válidas: 256 claves y entre ellas está la clave utilizada.

El tiempo que ha tardado en encontrarla es de 30 segundos.

El tiempo que necesitaría para probar todas las claves entre $K_{inicial}$ y la K_{final} sería de 154 segundos.

Número de claves que debería probar: 14.399.344.

Número de claves probadas 2.791.741.

Claves por segundo probadas: 93.058.

a) ¿Por qué hay tantas claves válidas y qué tienen en particular? Justifícalo.
b) ¿En qué zona del espacio de clave usado en el ataque se encontraba la clave K?
c) Indica qué tiempo en años tardarías en encontrar la clave en todo el espacio de claves del algoritmo DES.