Explicar pensamiento y búsqueda de la solución

Solución

Explicación de pensamiento a grandes rasgos.

1. Encontrar la llave.
2. Decodificar el mensaje.
3. Imprimir respuesta.

Explicación de pensamiento mejor abordado.

1. Encontrar la llave.
   1.1. Se identificó que la llave tenía una longitud de 4 caracteres alfabéticos en ASCII, que cumplía con la siguiente regex: [a-z].

   1.2. Se realizó un análisis de frecuencia de caracteres del abecedario en el mensaje encriptado para determinar la posible llave. Los caracteres del mensaje encriptado cumple la siguiente regex: [a-zA-Z0-9\s.,@\-_\/].
   1.3. Se estableció la relación entre la posición de la llave y las posiciones correspondientes en el mensaje encriptado, considerando un desplazamiento de 4 caracteres. Obteniendo así que en la posición 0, le corresponde los caracteres en las siguientes posiciones: 0,4,8,12...
   A la posición 1: 1,5,9,13...
   A la posición 2: 2,6,10,14...
   A la posición 3: 3,7,11,15...
   1.4. Finalmente, obtenido la letra que cumple la mayor frecuencia se toma como posible llave su código ASCII.
2. Decodificar el mensaje.
   2.1. Una vez obtenido la llave, debemos volver a recorrer el mensaje encriptado, pero con su correspondiente llave aplicando XOR y así obtener el mensaje desencriptado en formato ASCII.
3. Imprimir respuesta.
   3.1. Una vez obtenido el mensaje desencriptado en formato ASCII debemos volver a recorrer una ultima vez para decodificar cada uno de sus caracteres y ver cuales son las siguientes instrucciones.

Búsqueda de la solución

1. Entender que el mensaje como la clave su representación está dada en ASCII
2. Comprender que la manera en cómo se encripta y desencripta este dado por XOR.
3. Se seleccionó Java como el lenguaje de programación para implementar la solución.
4. Se realizó una investigación sobre cómo utilizar la operación XOR en Java.

5. Se encontró que Java proporcionaba un operador XOR fácil de usar para aplicar la operación sobre el mensaje y la llave.
6. Se entendió que la clave tenia una longitud de 4.
7. Se estableció que era necesario realizar al menos 4 búsquedas por cada uno de los dígitos de la llave.
8. Lo que me ayudo a comprender que se tenia que mirar la frecuencia fue que cuando estaba en la universidad viendo la materia de Seguridad informática, nos pusieron un ejemplo similar. El cual tocaba encontrar la Frecuencia de aparición de letras en el mensaje encriptado por medio del cifrado de cesar. Por lo cual entendí inmediatamente que debíamos ver la frecuencia del abecedario.
9. Se realizó una primera iteración utilizando una secuencia predefinida de caracteres como una aproximación inicial para la llave.
   Secuencia usada: 'a','b','c','d','e','f','g','h','i','j','k','l','m','n'
   Lo cual me dio resultado de:
   Con secuencia 'a','b','c','d','e','f','g','h','i','j','k','l','m','n'
   Llave: [100, 100, 109, 98]
   Mensaje Desencriptado: [70, 114, 108, 121, 99, 126, 100, 113, 100, 114, 115, 48, 68, 114, 105, 102, 105, 115, 32, 67, 101, 117, 97, 99, 116, 126, 97, 126, 32, 90, 101, 116, 105, 121, 97, 48, 82, 118, 116, 121, 118, 118, 44, 48, 104, 118, 115, 48, 108, 120, 103, 98, 97, 115, 111, 48, 100, 114, 115, 115, 105, 113, 114, 113, 114, 55, 101, 124, 32, 122, 101, 126, 115, 118, 106, 117, 46, 55, 32, 81, 104, 120, 114, 113, 44, 55, 112, 113, 114, 118, 32, 97, 117, 114, 32, 89, 110, 100, 105, 102, 101, 55, 114, 117, 99, 120, 110, 127, 122, 116, 97, 48, 116, 98, 32, 124, 111, 112, 114, 127, 44, 55, 115, 101, 98, 114, 32, 117, 108, 55, 99, 127, 100, 114, 32, 115, 111, 121, 32, 117, 108, 55, 113, 101, 101, 55, 114, 117, 115, 120, 108, 102, 105, 100, 116, 117, 32, 114, 115, 100, 101, 55, 101, 122, 101, 101, 99, 121, 99, 126, 111, 48, 101, 121, 32, 87, 105, 99, 72, 101, 98, 56, 71, 121, 116, 91, 97, 114, 32, 110, 32, 115, 111, 122, 112, 113, 114, 99, 101, 48, 101, 123, 32, 117, 110, 123, 97, 115, 101, 55, 97, 48, 115, 120, 112, 127, 114, 99, 101, 80, 105, 121, 115, 121, 118, 114, 46, 115, 108, 57]
   Mensaje decodificado:
   Frlyc~dqdrs0Drifis Ceuact~a~ Zetiya0Rvtyvv,0hvs0lxgbaso0drssiqrqr7e| ze~svju.7 Qhxrq,7pqrv aur Yndife7rucxn□zta0tb |opr□,7sebr ul7c□dr soy ul7qee7rusxlfidtu rsde7ezeecyc~o0ey WicHeb8Gyt[ar n sozpqrce0e{ un{ase7a0sxp□rcePiysyvr.sl9
10. Se observó que el mensaje tenía una longitud de 230 caracteres, lo que llevó a la suposición inicial de que los primeros 57 caracteres correspondían a la primera posición de la llave. Fijándome que no era así cuando se solucionó.
11. Se corrigió la estrategia de búsqueda de la llave al comprender que la llave se repetía cada 4 caracteres del mensaje encriptado.
12. Finalmente, cuando decido observar nuevamente las instrucciones del problema me percato del siguiente comentario. El proceso de cifrado se realizó utilizando una llave de longitud 4 con caracteres incluidos por la siguiente regex: [a-z]
13. Por lo cual entendí que el patrón debía ser de a – z. Permitiendo así finalmente validar si el resultado de aplicar XOR cumplía con el patrón de pertenecer a un número o letra

o símbolo de acorde a las reglas: Los caracteres del mensaje encriptado cumple la siguiente regex: [a-zA-Z0-9\s.,@\-_\/]

14. Finalmente, obtenido la llave correcta pudimos obtener el mensaje desencriptado, pero hacía falta decodificar ASCII para obtener un texto legible.