Comenzado el	jueves, 5 de marzo de 2020, 19:54
Estado	Finalizado
Finalizado en	jueves, 5 de marzo de 2020, 21:04
Tiempo empleado	1 hora 9 minutos
Calificación	**9,00** de 10,00 (**90**%)

Pregunta 1

Correcta

Puntúa 1,00 sobre 1,00

Eve ha interceptado una comunicación entre Alice y Bob y ha podido recuperar el mensaje en claro correspondiente a un texto cifrado que se habían enviado previamente. Ahora está trabajando en descubrir la clave que utilizaron, ya que de esta manera podrá descifrar todas las comunicaciones futuras entre Alice y Bob (siempre y cuando no decidan cambiar la clave). Eve ha conseguido descubrir que el texto estaba cifrado con el criptosistema de sustitución de César con un valor de clave arbitrario, pero no es capaz de adivinar cual es este valor. ¿La puedes ayudar? ¿Cuál es el valor de clave utilizado por Alice y Bob?

Texto en claro = ITHINKSHEKNOWSEVERYTHING
Texto cifrado = SDRSXUCROUXYGCOFOBIDRSXQ

Nota 1: El texto en claro es un texto en inglés codificado con un alfabeto de 26 caracteres.
Nota 2: Para descubrir porqué Eve quiere interceptar los mensajes entre Alice y Bob, puedes visitar: Alice & Bob

Seleccione una:

- a. 21
- b. 10 ✓
- c. 20
- d. 11
- e. 9

La respuesta correcta es: 10

Pregunta 2

Correcta

Puntúa 1,00 sobre 1,00

Dado el texto en claro FRIEDMAN, seleccionad todos los posibles textos cifrados que pueden ser resultado de cifrar este texto en claro con un criptosistema de transposición.

Seleccione una o más de una:

- a. NFEDRAMI ✓
- b. IRMFNIDI
- c. NAMDFIRF
- d. FFFFFFFF

La respuesta correcta es: NFEDRAMI

Pregunta 3

Correcta

Puntúa 1,00 sobre 1,00

Relaciona cada uno de los siguientes criptosistemas históricos con el concepto o característica que mejor los defina.

Vigenère	Tabula Recta ✓
Beale	Declaración de Independencia de los Estados Unidos de América ✓
César	Clave = 3 ✓
Vernam	Segunda Guerra Mundial ✓

La respuesta correcta es: Vigenère → Tabula Recta, Beale → Declaración de Independencia de los Estados Unidos de América, César → Clave = 3, Vernam → Segunda Guerra Mundial

Pregunta 4

Correcta

Puntúa 1,00 sobre 1,00

¿Un criptosistema de Vernam es vulnerable a ataques con solo texto cifrado?

Seleccione una:

- a. No, nunca. ✓
- b. Sí, siempre.
- c. Sí, si el criptoanalista dispone de una capacidad de cómputo ilimitada.
- d. Sí, si el criptoanalista dispone de un texto lo suficientemente largo.

La respuesta correcta es: No, nunca.

Pregunta 5

Correcta

Puntúa 1,00 sobre 1,00

¿Son los criptosistemas de substitución simple susceptibles a ataques con texto en claro conocido?

Seleccione una:

- a. Sí, si el criptoanalista dispone de un texto lo suficientemente largo.
- b. No, nunca.
- c. Sí, siempre. ✓
- d. Sí, si el criptoanalista dispone de una capacidad de cómputo ilimitada.

La respuesta correcta es: Sí, siempre.

Pregunta 6

Correcta

Puntúa 1,00 sobre 1,00

Si el conjunto de textos en claro que acepta un criptosistema E está formado por todas las palabras de 13 caracteres que se pueden crear utilizando las letras del alfabeto inglés (tanto en mayúsculas como minúsculas), ¿cuál es el tamaño del conjunto de textos en claro que acepta E?

Respuesta:

2032560433728501003

El alfabeto inglés tiene 26 caracteres. Si consideramos tanto mayúsculas como minúsculas, entonces cada posición del texto puede tener 52 posibles letras.

El número de textos disponibles de un solo carácter es pues 52. Si consideramos textos de dos letras, entonces tenemos 52 posibles letras en la primera posición y 52 más en la segunda. Por lo tanto, hay 52x52 = 2.704 posibles textos en claro. En general, para un texto de tamaño n, tendremos pues 52^n posibles textos diferentes.

La respuesta correcta es: 20325604337285010030592

Pregunta 7

Correcta

Puntúa 1,00 sobre 1,00

Los siguientes textos cifrados corresponden a cifrar el mensaje m = "IHAVEBEENREUSINGMYKEYS" utilizando una cifra homofónica con una misma clave k. Hay un texto, sin embargo, que ha sido cifrado usando una clave diferente. Identificad el texto que ha sido cifrado usando una clave diferente que el resto.

Seleccione una:

- a. ucJMojQoWdPAaqWTktHotb
- b. qeBMPjQPWOgrbVpTktHQtb
- c. VSjMoJQPWFuaxupTDtHPtA ✓
- d. VeJMQjgPIOPrbuITDtHgtx

La teva resposta és correcta.

La respuesta correcta es: VSjMoJQPWFuaxupTDtHPtA

Pregunta 8

Correcta

Puntúa 1,00 sobre 1,00

Descifrad el mensaje c = VYQHBGCJMRKSVDMHLOIV sabiendo que ha sido cifrado con Vigenère utilizando la clave k = CRIPTO.

Nota: los caracteres válidos corresponden al alfabeto inglés en mayúsculas.

Respuesta:

THISISASECRETMESS

Para descifrar el mensaje, hay que restar, a cada carácter, la clave correspondiente a su posición. Así, utilizaremos la primera letra de la clave para descifrar el primer carácter, la segunda letra para el segundo carácter, etc., hasta llegar al final de clave, momento en el que volveremos a empezar a utilizar el primer carácter de esta para seguir descifrando el texto.

La respuesta correcta es: THISISASECRETMESSAGE

Pregunta 9

Correcta

Puntúa 1,00 sobre 1,00

Resolved el siguiente sistema de ecuaciones modulares

4x+9=0 mod(15)

1x+11=0 mod(16)

Dad el resultado como [s, m] que correspondría a la solución x = s mod(m)

Respuesta: [69, 240]

La respuesta correcta es: [69, 240]

Pregunta 10

Sin contestar

Puntúa como 1,00

Calculad el inverso del polinomio (4*x + 1) módulo el polinomio (x^3 + 4*x^2 + 1) teniendo en cuenta que los coeficientes de los polinomios son del cuerpo de los enteros módulo 7.

Proporcionad la solución en el mismo formato que se os muestran los polinomios, respectando símbolos y espacios, sin paréntesis).

Respuesta:

La respuesta correcta es: 6 x^2 + 5 x + 4

◄ Avisos Ir a... PEC2 ►