

Comenzado el lunes, 7 de octubre de 2019, 20:07

Estado Finalizado

Finalizado en lunes, 7 de octubre de 2019, 21:37

Tiempo empleado 1 hora 29 minutos

Calificación 8,00 de 10,00 (80%)

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 = THISMESSAGEISSECRET

Texto cifrado = KYZJDVJJRXVZJJVTIVK

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. 16
- ☐ b. 2
- ☐ c. 18
- ☒ d. 17 ✓
- ☐ e. 1

La respuesta correcta es: 17

Pregunta 2

Correcta

Puntúa 1,00 sobre
1,00

Dado el texto en claro CSHANNON, 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. CCCCCCCC
- ☒ b. ONCHANNS ✓
- ☐ c. NONNCHSC
- ☐ d. HSNCNHNH

La respuesta correcta es: ONCHANNS

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.

Beale	Resistente a análisis de frecuencias	✓
César	Sustitución simple	✓
Vigenère	Kasiski	✓
Vernam	Secreto perfecto	✓

La respuesta correcta es: Beale → Resistente a análisis de frecuencias, César → Sustitución simple, Vigenère → Kasiski, Vernam → Secreto perfecto

Pregunta 4

Correcta

Puntúa 1,00 sobre 1,00

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

Seleccione una:

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

La respuesta correcta es: Sí, si el criptoanalista dispone de un texto lo suficientemente largo.

Pregunta 5

Correcta

Puntúa 1,00 sobre 1,00

¿Son los criptosistemas de sustitución 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, si el criptoanalista dispone de una capacidad de cómputo ilimitada.
- ☒ d. Sí, siempre. ✓

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:

20325604337285010030592

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 $52 \times 52 = 2.704$ 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. uSjMoJQPIdgaxqlTDtHgtA ✓
- ☐ b. ucNMojoQpFQrbVITDtHPtb
- ☐ c. ucJMoJQoWOPAaulTktHgth
- ☐ d. VcNMoJQoWFoAaqWTDtHgtx

La teva resposta és correcta.

La respuesta correcta es: uSjMoJQPIdgaxqlTDtHgtA

Puntuá 1,00 sobre
1,00

SECRETS DO EXIST

La respuesta correcta es: **SECRETSDOEXIST**

Puntuá 0,00 sobre 1,00

La respuesta correcta es: [223, 368]

Puntuá como 1,00

La respuesta correcta es: 5 x