

Comenzado el	jueves, 29 de febrero de 2024, 19:17
Estado	Finalizado
Finalizado en	viernes, 8 de marzo de 2024, 11:52
Tiempo empleado	7 días 16 horas
Calificación	10,00 de 10,00 (100%)

Pregunta 1

Correcta
Se puntúa 3,00 sobre 3,00

El cifrado Tripos es un cifrado de bloques que opera sobre bloques de 4 bits, escritos como dígitos hexadecimales tal que para una clave particular K, la salida es:

m	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$E_K(m)$	1	b	5	c	7	e	2	a	4	9	f	d	0	3	6	8

Usando esta clave K, descifra el siguiente texto cifrado en el modo ECB: 188b06

Respuesta: ✓

La respuesta correcta es: 0ff1ce

Pregunta 2

Correcta
Se puntúa 4,00 sobre 4,00

El cifrado Tripos es un cifrado de bloques que opera sobre bloques de 4 bits, escritos como dígitos hexadecimales tal que para una clave particular K, la salida es:

m	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$E_K(m)$	1	b	5	c	7	e	2	a	4	9	f	d	0	3	6	8

Usando esta clave K y vector de inicialización IV=0, descifra el siguiente texto cifrado en el modo CFB: 10f6d

Respuesta: ✓

La respuesta correcta es: 0beef

Pregunta 3

Correcta

Se puntúa 3,00 sobre 3,00

El cifrado Tripos es un cifrado de bloques que opera sobre bloques de 4 bits, escritos como dígitos hexadecimales tal que para una clave particular K, la salida es:

<i>m</i>	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
<i>E_K(m)</i>	1	b	5	c	7	e	2	a	4	9	f	d	0	3	6	8

Usando esta clave K y vector de inicialización IV=0, descifra el siguiente texto cifrado en el modo CBC: 301b2

Respuesta: 

La respuesta correcta es: df00d