

|                 |                                     |
|-----------------|-------------------------------------|
| Comenzado el    | miércoles, 1 de mayo de 2024, 12:28 |
| Estado          | Finalizado                          |
| Finalizado en   | miércoles, 1 de mayo de 2024, 12:36 |
| Tiempo empleado | 7 minutos 24 segundos               |
| Calificación    | 10,00 de 10,00 (100%)               |

Pregunta 1

Correcta

Se puntúa 5,00 sobre 5,00

Aplica protocolo de **Feige-Fiat-Shamir** con parámetros:  $p=5$ ,  $q=13$  e identificación secreta de A formada por  $s_1=4$ , compromiso secreto de A formado por  $r=11$  y signo  $s=+1$ , y reto de B formado por  $a_1=1$ .

y

44

✓

v1

16

✓

x

56

✓

n

65

✓

La respuesta correcta es:  $y \rightarrow 44$ ,  $v1 \rightarrow 16$ ,  $x \rightarrow 56$ ,  $n \rightarrow 65$

Pregunta 2

Correcta

Se puntúa 1,00 sobre 1,00

Los protocolos interactivos de reto-respuesta para identificación fuerte pueden estar basados en: clave secreta, clave pública o

Respuesta:

conocimiento nulo

✓

La respuesta correcta es: conocimiento nulo

**Pregunta 3**

Correcta

Se puntúa 1,00 sobre 1,00

Entre las propiedades que deben tener los retos usados en identificación fuerte están:

Seleccione una o más de una:

- ☒ a. caducidad ✓
- ☐ b. conmutatividad
- ☐ c. asociatividad
- ☒ d. unicidad ✓
- ☒ e. impredecibilidad ✓
- ☐ f. identidad

Respuesta correcta

Las respuestas correctas son: unicidad, caducidad, impredecibilidad

**Pregunta 4**

Correcta

Se puntúa 1,00 sobre 1,00

Problemas de esquemas de identificación fuerte

Basados en Clave Secreta Predistribución de claves ✓

Basados en Clave Pública Certificación de claves ✓

Respuesta correcta

La respuesta correcta es: Basados en Clave Secreta → Predistribución de claves, Basados en Clave Pública → Certificación de claves

**Pregunta 5**

Correcta

Se puntúa 1,00 sobre 1,00

La tarjeta soporte del DNI electrónico contiene los datos de filiación del ciudadano, los datos biométricos (modelo dactilar, foto y firma manuscrita) y ¿cuántos pares de claves? (escribe el número)

Respuesta:  ✓

La respuesta correcta es: 2

**Pregunta 6**

Correcta

Se puntúa 1,00 sobre 1,00

¿En qué año tuvo la Dirección General de la Policía que suspender el certificado electrónico de muchos DNIs por un fallo de seguridad?

Respuesta:



La respuesta correcta es: 2017