Tercer tarea

Manuel Díaz, José Canek García, Jesús Jara y Gerardo López

January 22, 2021

1) Sea la curva $y^2 = x^3 + 2x + 7$ en $\mathbb{Z}_{11}$

   a) Mostrar que el punto $p = (6, 2)$ pertenece a la curva $y^2 = x^3 + 2x + 7$.

   b) Dar el orden del punto p.

   c) Usar el orden del punto $p = (6, 2)$ y el teorema de Hasse par determinar el orden del conjunto de puntos que satisfacen $y^2 = x^3 + 2x + 7$.

2) Sea la curva elíptica E dada por $y^2 - x^3 - x - 8 = 0$ en $\mathbb{Z}_{17}$

   a) Muestre que $\alpha = (0, 5)$ es una raíz primitiva. Sugerencia utilize el teorema de Hasse y el orden de α.

   b) Alicia desea enviar el siguiente mensaje cifrado en Gammal elíptico $c = ((5, 6), (6, 3))$ a Bob los párametros públicos son $\alpha = (0, 5)$ y $\beta = (4, 5)$ donde $\beta = s\alpha$ y s es la llave privada. Encontrar s y descifrar el mensaje.

3) Sea E la curva elíptica dada por los puntos que satisfacen la ecuación $y^2 + 30x^3 = x + 14$ en $\mathbb{Z}_{31}$ y $p = (8, 21)$ de orden 39 el cual es un generador del grupo cíclico. El texto cifrado en ECIES simplificado definido sobre $\mathbb{Z}_{31}$ como espacio de texto plano con $A = 1, B = 2, \ldots, Z = 26$ y sea la clave privada $m = 8$.

   a) calcula $Q = mp$.

   b) Descifra el siguiente mensaje $((9, 1), 2)$, $((19, 0), 10)$,$((29, 1), 24)$,$((12, 1), 24)$,$((0, 1), 19)$, $((24, 1), 13)$, $((9, 1), 15)$,$((19, 0), 1)$,$((29, 1), 17)$,$((24, 1), 20)$,$((0, 1), 16)$,$((27, 0), 4)$,$((0, 1), 29)$.

4) En el sitio web http://redtiger.labs.overthewire.org/level1.php utilizar la herramienta sqlmap para obtener el usuario y contraseña para el sitio, como se hizo en clase con José Canek.

   Poner fotos donde se muestre el proceso usado con sqlmap para obtener el usuario y contraseña.

5) Resuma las diez recomendaciones de OWASP de seguridad (no copie y pegue) si lo hace a mano con caligrafía legible.

6) ¿En que capa de red según el esquema OSI se realiza el cifrado?

7) Informática Forense

   a) ¿ Cuáles son los tres objetivos de la informática forense dados en clase?

   b) ¿Qué se entiende por evidencía digital?

   c) De cuatro comandos utilizados en servidores Microsoft que se dieron en clase y explique para que sirven.

d) ¿Cuáles son la tres prioridades en la recolección de la información en análisis forense que se dieron en clase?

e) Dar las cuatro tecnicas más usadas para evadir un análisis forense.

f) Resuma el cápitulo II Acceso ilicito a sistemas y equipos de informática.