Universidad Nacional Autónoma de México

Facultad de Ciencias


Criptografía y Seguridad

# Tarea 3

**Curvas elípticas y seguridad**

*Sebastián Alamina Ramírez* - 318685496

*Carlos Alberto Desiderio Castillo* - 312183839

*Camila Alexandra Cruz Miranda* - 316084707

Trabajo presentado como parte del curso de **Criptografía y Seguridad**, impartido por el profesor **Manuel Díaz Díaz** durante el semestre 2023-1 en la Facultad de Ciencias, UNAM.

Fecha de entrega: **23:59 martes 6 de diciembre del 2022**.

1. Dada la curva $y^2 = x^3 + x + 1 \bmod 103$ y el punto (6, 29) aplique el teorema de Hasse o el teorema con que se obtiene el orden del grupo, para obtener el orden del grupo de puntos de la curva y obtenga todos sus puntos.
Solución: Aplicando y desarrollando la desigualdad del teorema de Hasse, obtenemos lo siguiente:

$$|q + 1 - \#E(\mathbf{F}_q)| \leq 2\sqrt{q} \Rightarrow -2\sqrt{q} \leq q + 1 - \#E(\mathbf{F}_q) \leq 2\sqrt{q}$$

$$\Rightarrow q + 1 - 2\sqrt{q} \leq \#E(\mathbf{F}_q) \leq q + 1 + 2\sqrt{q} \qquad \therefore 104 - 2\sqrt{103} \leq \#E(\mathbf{F}_{103}) \leq 104 + 2\sqrt{103}$$

Por lo tanto el orden de los puntos en la curva está entre $83 \leq \#E(\mathbf{F}_{103}) \leq 125$, ahora con el punto (6, 29), buscamos su orden, ya que sabemos que el orden de $\#E(\mathbf{F}_{103})$ es un múltiplo del orden de algún punto $P$ de los puntos de la curva, es decir $\#E(\mathbf{F}_{103}) = n \cdot O(P)$ , con n $\in \mathbf{Z}$, por lo que buscamos el orden del punto (6, 29), calculando la suma de $P$ consigo mismo, hasta que resulte el punto al infinito. Con la suma definida como $P + Q = (x, y)$, donde $P = (P_x, P_y)$, $Q = (Q_x, Q_y)$, $x = \lambda^2 - P_x - Q_x \bmod 103$, $y = \lambda(P_x - x) - P_y \bmod 103$, $\lambda = \frac{Q_y - P_y}{Q_x - P_x} \bmod 103$ si $P \neq Q$ y $\lambda = \frac{3P_x^2 + a}{2P_y}$ si $P = Q$.
Así para $P$ =(6,29), usando la operación anterior calculamos sus potencias:

$P^2 = P + P = (6, 29) + (6, 29) =$ **(37,85)**, $P^3 = P^2 + P = (37, 85) + (6, 29) =$ **(25,43)**
$P^4 = P^3 + P = (25, 43) + (6, 29) =$ **(52,13)**, $P^5 = P^4 + P = (52, 13) + (6, 29) =$ **(79,77)**
$P^6 = P^5 + P = (79, 77) + (6, 29) =$ **(70,94)**, $P^7 = P^6 + P = (70, 94) + (6, 29) =$ **(87,3)**
$P^8 = P^7 + P = (87, 3) + (6, 29) =$ **(48,15)**, $P^9 = P^8 + P = (48, 15) + (6, 29) =$ **(72,96)**
$P^{10} = P^9 + P = (72, 96) + (6, 29) =$ **(27,48)**, $P^{11} = P^{10} + P = (27, 48) + (6, 29) =$ **(86,85)**
$P^{12} = P^{11} + P = (86, 85) + (6, 29) =$ **(29,27)**, $P^{13} = P^{12} + P = (29, 27) + (6, 29) =$ **(83,18)**
$P^{14} = P^{13} + P = (83, 18) + (6, 29) =$ **(96,28)**, $P^{15} = P^{14} + P = (96, 28) + (6, 29) =$ **(65,14)**
$P^{16} = P^{15} + P = (65, 14) + (6, 29) =$ **(36,31)**, $P^{17} = P^{16} + P = (36, 31) + (6, 29) =$ **(99,6)**
$P^{18} = P^{17} + P = (99, 6) + (6, 29) =$ **(62,7)**, $P^{19} = P^{18} + P = (62, 7) + (6, 29) =$ **(50,3)**
$P^{20} = P^{19} + P = (50, 3) + (6, 29) =$ **(5,50)**, $P^{21} = P^{20} + P = (5, 50) + (6, 29) =$ **(18,17)**
$P^{22} = P^{21} + P = (18, 17) + (6, 29) =$ **(80,45)**, $P^{23} = P^{22} + P = (80, 45) + (6, 29) =$ **(26,14)**
$P^{24} = P^{23} + P = (26, 14) + (6, 29) =$ **(78,25)**, $P^{25} = P^{24} + P = (78, 25) + (6, 29) =$ **(74,32)**
$P^{26} = P^{25} + P = (74, 32) + (6, 29) =$ **(69,100)**, $P^{27} = P^{26} + P = (69, 100) + (6, 29) =$ **(41,46)**
$P^{28} = P^{27} + P = (41, 46) + (6, 29) =$ **(11,101)**, $P^{29} = P^{28} + P = (11, 101) + (6, 29) =$ **(75,28)**
$P^{30} = P^{29} + P = (75, 28) + (6, 29) =$ **(31,46)**, $P^{31} = P^{30} + P = (31, 46) + (6, 29) =$ **(19,94)**
$P^{32} = P^{31} + P = (19, 94) + (6, 29) =$ **(0,1)**, $P^{33} = P^{32} + P = (0, 1) + (6, 29) =$ **(73,36)**
$P^{34} = P^{33} + P = (73, 36) + (6, 29) =$ **(54,49)**, $P^{35} = P^{34} + P = (54, 49) + (6, 29) =$ **(21,42)**
$P^{36} = P^{35} + P = (21, 42) + (6, 29) =$ **(9,92)**, $P^{37} = P^{36} + P = (9, 92) + (6, 29) =$ **(14,9)**
$P^{38} = P^{37} + P = (14, 9) + (6, 29) =$ **(12,89)**, $P^{39} = P^{38} + P = (12, 89) + (6, 29) =$ **(82,35)**
$P^{40} = P^{39} + P = (82, 35) + (6, 29) =$ **(71,77)**, $P^{41} = P^{40} + P = (71, 77) + (6, 29) =$ **(45,4)**
$P^{42} = P^{41} + P = (45, 4) + (6, 29) =$ **(56,77)**, $P^{43} = P^{42} + P = (56, 77) + (6, 29) =$ **(35,75)**
$P^{44} = P^{43} + P = (35, 75) + (6, 29) =$ **(35,28)**, $P^{45} = P^{44} + P = (35, 28) + (6, 29) =$ **(56,26)**
$P^{46} = P^{45} + P = (56, 26) + (6, 29) =$ **(45,99)**, $P^{47} = P^{46} + P = (45, 99) + (6, 29) =$ **(71,26)**
$P^{48} = P^{47} + P = (71, 26) + (6, 29) =$ **(82,68)**, $P^{49} = P^{48} + P = (82, 68) + (6, 29) =$ **(12,14)**
$P^{50} = P^{49} + P = (12, 14) + (6, 29) =$ **(14,94)**, $P^{51} = P^{50} + P = (14, 94) + (6, 29) =$ **(9,11)**
$P^{52} = P^{51} + P = (9, 11) + (6, 29) =$ **(21,61)**, $P^{53} = P^{52} + P = (21, 61) + (6, 29) =$ **(54,54)**
$P^{54} = P^{53} + P = (54, 54) + (6, 29) =$ **(73,67)**, $P^{55} = P^{54} + P = (73, 67) + (6, 29) =$ **(0,102)**
$P^{56} = P^{55} + P = (0, 102) + (6, 29) =$ **(19,9)**, $P^{57} = P^{56} + P = (19, 9) + (6, 29) =$ **(31,57)**
$P^{58} = P^{57} + P = (31, 57) + (6, 29) =$ **(75,75)**, $P^{59} = P^{58} + P = (75, 75) + (6, 29) =$ **(11,2)**
$P^{60} = P^{59} + P = (11, 2) + (6, 29) =$ **(41,57)**, $P^{61} = P^{60} + P = (41, 57) + (6, 29) =$ **(69,3)**
$P^{62} = P^{61} + P = (69, 3) + (6, 29) =$ **(74,71)**, $P^{63} = P^{62} + P = (74, 71) + (6, 29) =$ **(78,78)**
$P^{64} = P^{63} + P = (78, 78) + (6, 29) =$ **(26,89)**, $P^{65} = P^{64} + P = (26, 89) + (6, 29) =$ **(80,58)**
$P^{66} = P^{65} + P = (80, 58) + (6, 29) =$ **(18,86)**, $P^{67} = P^{66} + P = (18, 86) + (6, 29) =$ **(5,53)**
$P^{68} = P^{67} + P = (5, 53) + (6, 29) =$ **(50,100)**, $P^{69} = P^{68} + P = (50, 100) + (6, 29) =$ **(62,96)**
$P^{70} = P^{69} + P = (62, 96) + (6, 29) =$ **(99,97)**, $P^{71} = P^{70} + P = (99, 97) + (6, 29) =$ **(36,72)**
$P^{72} = P^{71} + P = (36, 72) + (6, 29) =$ **(65,89)**, $P^{73} = P^{72} + P = (65, 89) + (6, 29) =$ **(96,75)**

$P^{74} = P^{73} + P = (96, 75) + (6, 29) =$ **(83,85)**, $P^{75} = P^{74} + P = (83, 85) + (6, 29) =$ **(29,76)**
$P^{76} = P^{75} + P = (29, 76) + (6, 29) =$ **(86,18)**, $P^{77} = P^{76} + P = (86, 18) + (6, 29) =$ **(27,55)**
$P^{78} = P^{77} + P = (27, 55) + (6, 29) =$ **(72,7)**, $P^{79} = P^{78} + P = (72, 7) + (6, 29) =$ **(48,88)**
$P^{80} = P^{79} + P = (48, 88) + (6, 29) =$ **(87,100)**, $P^{81} = P^{80} + P = (87, 100) + (6, 29) =$ **(70,9)**
$P^{82} = P^{81} + P = (70, 9) + (6, 29) =$ **(79,26)**, $P^{83} = P^{82} + P = (79, 26) + (6, 29) =$ **(52,90)**
$P^{84} = P^{83} + P = (52, 90) + (6, 29) =$ **(25,60)**, $P^{85} = P^{84} + P = (25, 60) + (6, 29) =$ **(37,18)**
$P^{86} = P^{85} + P = (37, 18) + (6, 29) =$ **(6,74)**, $P^{87} = P^{86} + P = (6, 74) + (6, 29) =$ **(inf,inf)**

Por lo tanto el orden de $P$ =(6, 29) es 87, ya que es el menor entero positivo tal que $P^{87}$ resulta ser el punto al infinito, y además por el teorema de Hasse, recordemos que $83 \leq \#E(\mathbf{F}_{103}) = n \cdot O(P) = n \cdot 87 \leq 125$, donde $n = 1$, ya que si $2 \leq n$, entonces $125 \leq n \cdot 87$, por lo tanto $\#E(\mathbf{F}_{103}) = O(P) = 87 \Rightarrow < (6, 29) >= E(\mathbf{F}_{103})$, es decir el punto $P$ genera a todos los puntos de la curva, y al calcular todas sus potencias hasta su neutro aditivo, encontramos todos los puntos de la curva sobre el campo $\mathbf{Z}_{103}$.

2. Dada la curva $y^2 = x^3 + x + 1 mod(10403)$, encuentre un factor de 10403.

   **Solución:**

   Tenemos el punto $P = (0,1) \in \mathbf{Z}_{10403}$, entonces usando el algoritmo ECM podemos calcular los múltiplos enteros de $P \dots P_{20}$ con la operación suma y hasta $P^{21}$ resulta que:

$$21P = 20P + P = (4242, 403) + (0,1)$$

$$\lambda = \frac{(403-1)}{4242} = \frac{402}{4242} mod(10403)$$

   Pero el máximo común divisor entre 4242 y 10403 es 101, por lo tanto 101 es un factor de 10403. Entonces $P^{21}$ es indeterminado porque 4242 no tiene inverso multiplicativo en $\mathbf{Z}_{10403}$.

3. Dada la Curva $y^2 = x^3 + x + 4 \bmod 53$ y la curva $y^2 = x^3 + 16x + 11 \bmod 53$ muestre que son isomorfas y de el isomorfismo.
   Por el teorema visto en una ayudantía, sabemos que dos curvas son isomorfas si y solo si sus **J-invariantes** son los mismos, por lo que si ambas curvas son isomorfas sus J-invariantes debe ser el mismo para ambas. Entonces primero veamos si los J-invariante de ambas es igual, y de ser cierto buscaremos el isomorfismo.
   Recordemos que el j-invariante de una curva $y^2 = x^3 + Ax + B$ se define como $j = 1728 \cdot \frac{4A^3}{4A^3+27B^2}$, entonces para la curva $y^2 = x^3 + x + 4$ su j-invariante es el siguiente:

$$j_1 = 1728 \cdot \frac{4(1)^3}{4(1)^3 + 27(4)^2} \bmod 53 = 32\frac{4}{4 + 27(16)} \bmod 53 = 32\frac{4}{436} \bmod 53 = 32(4)(31) \bmod 53 = 46$$

   Ahora para la curva $y^2 = x^3 + 16x + 11$, su j-invariante es:

$$j_2 = 1728 \cdot \frac{4(16)^3}{4(16)^3 + 27(11)^2} \bmod 53 = 32\frac{16384}{16384 + 3284} \bmod 53 = 32\frac{7}{41} \bmod 53 = 32(7)(22) \bmod 53 = 52$$

   Por lo tanto $j_1 \neq j_2$, lo que implica que las curvas no son isomorfas por el teorema antes mencionado.

4. Sea la curva $y^2 = x^3 + x + 1 \bmod 71$ y el punto $P = (18, 61)$. Encuentre $m$ tal que $mP = (59, 6)$.

**Solución**: Tenemos que $m = 1 \implies mP = P \neq (59, 6)$, por lo que ahora intentamos con $m = 2$...

$$m = 2 \implies mP = 2P = P + P = (18, 61) + (18, 61) = P + Q$$

$$\text{Como } P = Q \implies \lambda = \frac{3x^2+a}{2y} \; mod \; 71 = \frac{3(18)^2+1}{2(61)} \; mod \; 71 = \frac{50}{51} \; mod \; 71 = 50 \times 39 \; mod \; 71 = 33$$

Así:

$$2P_x = \lambda^2 - x_1 - x_2 \; mod \; 71 = 1089 - 18 - 18 \; mod \; 71 = 1053 \; mod \; 71 = 59$$

$$2P_y = \lambda(x_1 - 2P_x) - y_1 \; mod \; 71 = 33(18 - 59) - 61 \; mod \; 71 = -1414 \; mod \; 71 = 6$$

Por lo que $2P = (59, 6)$ implica que $m$ es 2. □

Dado el cifrado en ECIES con parámetros $E(y^2 = x^3 + x + 1, (18, 61), m, (59, 6), 71)$, descifre el siguiente mensaje. Los caracteres son tomados módulo 26, es decir $a = 0 = 26, b = 1, ..., z = 25$.

$$((23, 0), 21), ((13, 1), 47), ((9, 1), 57), ((44, 0), 25), ((39, 1), 11), ((64, 1), 53), ((5, 1), 26)$$

**Solución**: Considerando que cada caracter viene cifrado de la forma $y = (y_1, y_2)$, donde $y_1 \in \mathbb{Z}_p \times \mathbb{Z}_2$ y $y_2 \in \mathbb{Z}_p^*$, tenemos:

$$\underline{\text{Para } y = ((23, 0), 21)}:$$

Primero calculamos el punto de descompresión de $y_1 = (23, 0)$...

$$z = x^3 + ax + b \; mod \; p = 12191 \; mod \; 71 = 50$$

Como $p \equiv 3 \; mod \; 4$ y $z$ es residuo cuadrático módulo 71, tenemos que:

$$\sqrt{z} = z^{\frac{p+1}{4}} \; mod \; p = 50^{18} \; mod \; 71 = 60 = y$$

$$\text{Como } y \equiv i \; mod \; 2 \text{ pues } 60 \equiv 0 \; mod \; 2 \implies punto\_de\_descompresión(y_1) = (x, y) = (23, 60).$$

Luego, calculamos $m(23, 60) = 2(23, 60) = (23, 60) + (23, 60)$...

$$\text{Como } \lambda = \frac{3x^2+a}{2y} \; mod \; 71 = \frac{3(23)^2+1}{2(60)} \; mod \; 71 = \frac{26}{49} \; mod \; 71 = 26 \times 29 \; mod \; 71 = 44.$$

$$2P_x = \lambda^2 - x_1 - x_2 \; mod \; 71 = 1936 - 23 - 23 \; mod \; 71 = -2 \; mod \; 71 = 44$$

$$2P_y = \lambda(x_1 - 2P_x) - y_1 \; mod \; 71 = 44(23 - 44) - 60 \; mod \; 71 = -984 \; mod \; 71 = 10$$

$$\text{Por lo que } m \times punto\_de\_descompresión(y_1) = (x_0, y_0) = (44, 10).$$

$$\text{Finalmente, } d_k(y) = y_2(x_0)^{-1} \; mod \; p = 21(44)^{-1} \; mod \; 71 = 21 \times 21 \; mod \; 71 = 441 \; mod \; 71 = 15.$$

Por lo que el primer caracter es $15 \; mod \; 26 = 15 = P$. □

$$\underline{\text{Para } y = ((13, 1), 47)}:$$

$$punto\_de\_descompresión(y_1) = punto\_de\_descompresión((13, 1)) = ...$$

$$z = x^3 + ax + b \; mod \; p = 2211 \; mod \; 71 = 10$$

$$\text{Como } z \text{ es residuo cuadrático módulo } 71 \wedge p \equiv 3 \; mod \; 4 \implies \sqrt{z} = z^{\frac{p+1}{4}} \; mod \; p = 10^{18} \; mod \; 71 = 9 = y$$

$$\text{Así, } y \equiv i \; mod \; 2 \text{ pues } 9 \equiv 1 \; mod \; 2 \implies punto\_de\_descompresión(y_1) = (x, y) = (13, 9).$$

$$\text{Luego, } m \times punto\_de\_descompresión(y_1) = 2(13, 9) = (64, 19) = (x_0, y_0).$$

$$\text{Finalmente, } d_k(y) = y_2(x_0)^{-1} \; mod \; p = 47(64)^{-1} \; mod \; 71 = 44.$$

Por lo que el caracter correspondiente es $44 \; mod \; 26 = 18 = S$. □

Para $y = ((9,1),57)$:

$$punto\_de\_descompresión(y_1) = punto\_de\_descompresión((9,1)) = ...$$

$$z = x^3 + ax + b \ mod \ p = 739 \ mod \ 71 = 29$$

Como $z$ es residuo cuadrático módulo 71 $\wedge$ $p \equiv 3 \ mod \ 4 \implies \sqrt{z} = z^{\frac{p+1}{4}} \ mod \ p = 29^{18} \ mod \ 71 = 10 = y$

Así, $y \equiv i \ mod \ 2$ pues $10 \equiv 1 \ mod \ 2 \implies punto\_de\_descompresión(y_1) = (x,y) = (9,10)$.

Luego, $m \times punto\_de\_descompresión(y_1) = 2(9,10) = (57,56) = (x_0,y_0)$.

Finalmente, $d_k(y) = y_2(x_0)^{-1} \ mod \ p = 57(57)^{-1} \ mod \ 71 = 1$.

Por lo que el caracter correspondiente es $1 \ mod \ 26 = 1 = B$. □

Para $y = ((44,0),25)$:

$$punto\_de\_descompresión(y_1) = punto\_de\_descompresión((44,0)) = ...$$

$$z = x^3 + ax + b \ mod \ p = 85229 \ mod \ 71 = 29$$

Como $z$ es residuo cuadrático módulo 71 $\wedge$ $p \equiv 3 \ mod \ 4 \implies \sqrt{z} = z^{\frac{p+1}{4}} \ mod \ p = 29^{18} \ mod \ 71 = 10 = y$

Así, $y \equiv i \ mod \ 2$ pues $10 \equiv 0 \ mod \ 2 \implies punto\_de\_descompresión(y_1) = (x,y) = (44,10)$.

Luego, $m \times punto\_de\_descompresión(y_1) = 2(44,10) = (12,26) = (x_0,y_0)$.

Finalmente, $d_k(y) = y_2(x_0)^{-1} \ mod \ p = 25(12)^{-1} \ mod \ 71 = 8$.

Por lo que el caracter correspondiente es $8 \ mod \ 26 = 8 = I$. □

Para $y = ((39,1),11)$:

$$punto\_de\_descompresión(y_1) = punto\_de\_descompresión((39,1)) = ...$$

$$z = x^3 + ax + b \ mod \ p = 59359 \ mod \ 71 = 3$$

Como $z$ es residuo cuadrático módulo 71 $\wedge$ $p \equiv 3 \ mod \ 4 \implies \sqrt{z} = z^{\frac{p+1}{4}} \ mod \ p = 3^{18} \ mod \ 71 = 43 = y$

Así, $y \equiv i \ mod \ 2$ pues $43 \equiv 1 \ mod \ 2 \implies punto\_de\_descompresión(y_1) = (x,y) = (39,43)$.

Luego, $m \times punto\_de\_descompresión(y_1) = 2(39,43) = (50,37) = (x_0,y_0)$.

Finalmente, $d_k(y) = y_2(x_0)^{-1} \ mod \ p = 11(50)^{-1} \ mod \ 71 = 13$.

Por lo que el caracter correspondiente es $13 \ mod \ 26 = 13 = N$. □

Para $y = ((64,1),53)$:

$$punto\_de\_descompresión(y_1) = punto\_de\_descompresión((64,1)) = ...$$

$$z = x^3 + ax + b \ mod \ p = 262209 \ mod \ 71 = 6$$

Como $z$ es residuo cuadrático módulo 71 $\wedge$ $p \equiv 3 \ mod \ 4 \implies \sqrt{z} = z^{\frac{p+1}{4}} \ mod \ p = 6^{18} \ mod \ 71 = 19 = y$

Así, $y \equiv i \ mod \ 2$ pues $19 \equiv 1 \ mod \ 2 \implies punto\_de\_descompresión(y_1) = (x,y) = (64,19)$.

Luego, $m \times punto\_de\_descompresión(y_1) = 2(64,19) = (51,69) = (x_0,y_0)$.

Finalmente, $d_k(y) = y_2(x_0)^{-1} \ mod \ p = 53(51)^{-1} \ mod \ 71 = 8$.

Por lo que el caracter correspondiente es $8 \ mod \ 26 = 8 = I$. □

Para $y = ((5,1),26)$:

$$punto\_de\_descompresión(y_1) = punto\_de\_descompresión((5,1)) = ...$$

$$z = x^3 + ax + b \ mod \ p = 131 \ mod \ 71 = 60$$

Como $z$ es residuo cuadrático módulo 71 $\wedge$ $p \equiv 3 \ mod \ 4 \implies \sqrt{z} = z^{\frac{p+1}{4}} \ mod \ p = 60^{18} \ mod \ 71 = 29 = y$

Así, $y \equiv i \ mod \ 2$ pues $29 \equiv 1 \ mod \ 2 \implies punto\_de\_descompresión(y_1) = (x,y) = (5,29)$.

Luego, $m \times punto\_de\_descompresión(y_1) = 2(5,29) = (33,20) = (x_0,y_0)$.

Finalmente, $d_k(y) = y_2(x_0)^{-1} \ mod \ p = 26(33)^{-1} \ mod \ 71 = 18$.

Por lo que el caracter correspondiente es $18 \ mod \ 26 = 18 = S$. □

Por lo tanto, el mensaje descifrado es PSBINIS. ■

5. Describa tres ataques cibernéticos y en que consiste el computo forense.

   (a) **Análisis de tráfico o *sniffers*:** Son ataques con el objetivo de observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando herramientas como los sniffers.

   (b) **Detección de vulnerabilidades en el sistema:** Ataques que tratan de detectar y documentar las posibles vulnerabilidades de un sistema, para a continuación desarrollar una herramienta que permita explotarlas fácilmente o *exploits*.

   (c) **Ataques de suplantación de la identidad:** Estos ataques tienen muchas variantes, siendo una de las más conocidas la denominada *IP spoofing*, mediante la cual un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado.

   **Cómputo forense:** El cómputo forense no tiene como objetivo prevenir delitos ya que de eso se encarga la seguridad informática; sin embargo como objetivos tiene:

   - La compensación de los daños causados por los criminales o intrusos.
   - La persecución y procesamiento judicial de los criminales.
   - La creación y aplicación de medidas para prevenir casos similares.

   La principal forma de hacerlo es la recolección de evidencia.

   El cómputo forense puede analizar el disco duro de una computadora o de un servidor, dispositivos móviles, memorias USB, BIOS, archivos, carpetas, información electrónica MAC address, logs de seguridad, IP, redes, software, credenciales de autenticación, agendas electrónicas, dispositivos GPS, impresoras, etc. Hoy en día existe gran variedad de herramientas que nos facilitan el trabajo sobre sobre el análisis forense, según el uso que tienen.

   Una de las herramientas más utilizadas en la actualidad es conocida como Autopsy, que permite analizar de manera eficiente los discos duros y los teléfonos inteligentes además de poder recuperar archivos del mismo, es una plataforma de análisis forense digital y la interfaz gráfica para el Sleuth Kit (conjunto de herramientas de línea de instrucciones y una librería de C). Tiene una arquitectura plug-in que permite encontrar módulos adicionales o desarrollar módulos personalizados en Java o Python.[1]

[1] González. (2016, April 12). Cómputo forense — Seguridad en Cómputo. http://blogs.acatlan.unam.mx/lasc/2016/04/12/computo-forense/