

Criptografía II

A. Moreno

Contenido

1 El alfabeto de definición

2 Los conjuntos \mathbb{Z}_n

3 Criptografía

4 Sistema de desplazamiento con MatLab

Contenido

1 El alfabeto de definición

2 Los conjuntos \mathbb{Z}_n

3 Criptografía

4 Sistema de desplazamiento con MatLab

Contenido

1 El alfabeto de definición

2 Los conjuntos \mathbb{Z}_n

3 Criptografía

4 Sistema de desplazamiento con MatLab

Contenido

- 1 El alfabeto de definición**
- 2 Los conjuntos \mathbb{Z}_n**
- 3 Criptografía**
- 4 Sistema de desplazamiento con MatLab**

Digital Watermarking-Marcas de agua digitales



Congruencia

El concepto de relación de congruencia es uno de los más importantes en Criptografía.

El papel fundamental de una relación de congruencia definida en un conjunto es el de clasificar sus elementos. Frecuentemente, tal clasificación permite estudiar las propiedades de un conjunto de forma eficiente.

En Criptografía se usan principalmente relaciones de congruencia, definidas en el conjunto de los números enteros

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ y en el conjunto de los polinomios con coeficientes, en unas estructuras algebraicas especiales que denominamos anillos. De hecho \mathbb{Z} , con la suma y la multiplicación usuales constituye un anillo.

Congruencia

El concepto de relación de congruencia es uno de los más importantes en Criptografía.

El papel fundamental de una relación de congruencia definida en un conjunto es el de clasificar sus elementos. Frecuentemente, tal clasificación permite estudiar las propiedades de un conjunto de forma eficiente.

En Criptografía se usan principalmente relaciones de congruencia, definidas en el conjunto de los números enteros

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ y en el conjunto de los polinomios con coeficientes, en unas estructuras algebraicas especiales que denominamos anillos. De hecho \mathbb{Z} , con la suma y la multiplicación usuales constituye un anillo.

Congruencia

El concepto de relación de congruencia es uno de los más importantes en Criptografía.

El papel fundamental de una relación de congruencia definida en un conjunto es el de clasificar sus elementos. Frecuentemente, tal clasificación permite estudiar las propiedades de un conjunto de forma eficiente.

En Criptografía se usan principalmente relaciones de congruencia, definidas en el conjunto de los números enteros

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ y en el conjunto de los polinomios con coeficientes, en unas estructuras algebraicas especiales que denominamos anillos. De hecho \mathbb{Z} , con la suma y la multiplicación usuales constituye un anillo.

Congruencia

El concepto de relación de congruencia es uno de los más importantes en Criptografía.

El papel fundamental de una relación de congruencia definida en un conjunto es el de clasificar sus elementos. Frecuentemente, tal clasificación permite estudiar las propiedades de un conjunto de forma eficiente.

En Criptografía se usan principalmente relaciones de congruencia, definidas en el conjunto de los números enteros

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ y en el conjunto de los polinomios con coeficientes, en unas estructuras algebraicas especiales que denominamos anillos. De hecho \mathbb{Z} , con la suma y la multiplicación usuales constituye un anillo.

Congruencia

El concepto de relación de congruencia es uno de los más importantes en Criptografía.

El papel fundamental de una relación de congruencia definida en un conjunto es el de clasificar sus elementos. Frecuentemente, tal clasificación permite estudiar las propiedades de un conjunto de forma eficiente.

En Criptografía se usan principalmente relaciones de congruencia, definidas en el conjunto de los números enteros

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ y en el conjunto de los polinomios con coeficientes, en unas estructuras algebraicas especiales que denominamos anillos. De hecho \mathbb{Z} , con la suma y la multiplicación usuales constituye un anillo.

Ejemplo

Por ejemplo $p(x) = x^3 + \frac{1}{2}x + \frac{3}{4}$, es un polinomio con coeficientes en el conjunto de los números racionales que notamos \mathbb{Q} .

Definición

Si $a, b \in \mathbb{Z}$ entonces notamos $a | b$ si a divide b . En cuyo caso existe un $t \in \mathbb{Z}$, tal que $b = ta$.

Si notamos \mathbb{Z}^+ el conjunto de los enteros positivos y $p \in \mathbb{Z}^+$, es tal que p solo es divisible por si mismo o 1 entonces p es un número primo.

Definición

Si $a, b \in \mathbb{Z}$ entonces notamos $a | b$ si a divide b . En cuyo caso existe un $t \in \mathbb{Z}$, tal que $b = ta$.

Si notamos \mathbb{Z}^+ el conjunto de los enteros positivos y $p \in \mathbb{Z}^+$, es tal que p solo es divisible por si mismo o 1 entonces p es un número primo.

Definición

Si $a, b \in \mathbb{Z}$ entonces notamos $a | b$ si a divide b . En cuyo caso existe un $t \in \mathbb{Z}$, tal que $b = ta$.

Si notamos \mathbb{Z}^+ el conjunto de los enteros positivos y $p \in \mathbb{Z}^+$, es tal que p solo es divisible por si mismo o 1 entonces p es un número primo.

Ejemplo

2, 3, 5, 7, 17, 19, 61, 89 son números primos y sus correspondientes primos de Mersenne. Esto es, de la forma $2^n - 1$.

2305843009213693951, el último encontrado de este tipo (12/04/2009), tiene la forma $2^{43112609} - 1$, con 12837064, dígitos.

Ejemplo

2, 3, 5, 7, 17, 19, 61, 89 son números primos y sus correspondientes primos de Mersenne. Esto es, de la forma $2^n - 1$.

2305843009213693951, el último encontrado de este tipo (12/04/2009), tiene la forma $2^{43112609} - 1$, con 12837064, dígitos.

Ejemplo

2, 3, 5, 7, 17, 19, 61, 89 son números primos y sus correspondientes primos de Mersenne. Esto es, de la forma $2^n - 1$.

2305843009213693951, el último encontrado de este tipo (12/04/2009), tiene la forma $2^{43112609} - 1$, con 12837064, dígitos.

Ejemplo

2, 3, 5, 7, 17, 19, 61, 89 son números primos y sus correspondientes primos de Mersenne. Esto es, de la forma $2^n - 1$.

2305843009213693951, el último encontrado de este tipo (12/04/2009), tiene la forma $2^{43112609} - 1$, con 12837064, dígitos.

El algoritmo AKS

Determinar de forma eficiente, que números son primos es un problema de gran trascendencia en Matemáticas y Ciencias de la Computación.

Muchos de los algoritmos que realizan este tipo cálculo son de tipo probabilístico, como el de Solovay-Strassen.

Debemos anotar que la primera solución a este problema se la debemos a Agrawal, Saxena y Kayal (U. Kanpur-2002) quienes encontraron el algoritmo que ahora conocemos como el algoritmo AKS, el cual determina de manera eficiente la primalidad de un número n dado.

El algoritmo AKS

Determinar de forma eficiente, que números son primos es un problema de gran trascendencia en Matemáticas y Ciencias de la Computación.

Muchos de los algoritmos que realizan este tipo cálculo son de tipo probabilístico, como el de Solovay-Strassen.

Debemos anotar que la primera solución a este problema se la debemos a Agrawal, Saxena y Kayal (U. Kanpur-2002) quienes encontraron el algoritmo que ahora conocemos como el algoritmo AKS, el cual determina de manera eficiente la primalidad de un número n dado.

El algoritmo AKS

Determinar de forma eficiente, que números son primos es un problema de gran trascendencia en Matemáticas y Ciencias de la Computación.

Muchos de los algoritmos que realizan este tipo cálculo son de tipo probabilístico, como el de Solovay-Strassen.

Debemos anotar que la primera solución a este problema se la debemos a Agrawal, Saxena y Kayal (U. Kanpur-2002) quienes encontraron el algoritmo que ahora conocemos como el algoritmo AKS, el cual determina de manera eficiente la primalidad de un número n dado.

El algoritmo AKS

Determinar de forma eficiente, que números son primos es un problema de gran trascendencia en Matemáticas y Ciencias de la Computación.

Muchos de los algoritmos que realizan este tipo cálculo son de tipo probabilístico, como el de Solovay-Strassen.

Debemos anotar que la primera solución a este problema se la debemos a Agrawal, Saxena y Kayal (U. Kanpur-2002) quienes encontraron el algoritmo que ahora conocemos como el algoritmo AKS, el cual determina de manera eficiente la primalidad de un número n dado.

Definición

Si $a, b \in \mathbb{Z}$ entonces $a \equiv b \pmod{n}$, (se lee, a es congruente con b módulo n), si y solo si existe un entero t , tal que $a - b = tn$.

Partición de \mathbb{Z}

La relación de congruencia definida en \mathbb{Z} , podemos decir que parte o partitiona el conjunto de los enteros en n conjuntos los cuales denominamos clases.

Esto es, cada clase consta de números congruentes y el conjunto de todas las clases A lo notamos \mathbb{Z}_n .

Debemos anotar que $\mathbb{Z} = \bigcup_{[j] \in A} [j]$. Lo que significa que la unión de

todas las clases es el conjunto de los números enteros. Además, en este caso se tiene que

$$[i] \cap [j] = \emptyset \text{ si } i \neq j,$$

por lo que clases distintas no tienen elementos comunes.



Partición de \mathbb{Z}

La relación de congruencia definida en \mathbb{Z} , podemos decir que parte o partitiona el conjunto de los enteros en n conjuntos los cuales denominamos clases.

Esto es, cada clase consta de números congruentes y el conjunto de todas las clases A lo notamos \mathbb{Z}_n .

Debemos anotar que $\mathbb{Z} = \bigcup_{[j] \in A} [j]$. Lo que significa que la unión de

todas las clases es el conjunto de los números enteros. Además, en este caso se tiene que

$$[i] \cap [j] = \emptyset \text{ si } i \neq j,$$

por lo que clases distintas no tienen elementos comunes.



Partición de \mathbb{Z}

La relación de congruencia definida en \mathbb{Z} , podemos decir que parte o partitiona el conjunto de los enteros en n conjuntos los cuales denominamos clases.

Esto es, cada clase consta de números congruentes y el conjunto de todas las clases A lo notamos \mathbb{Z}_n .

Debemos anotar que $\mathbb{Z} = \bigcup_{[j] \in A} [j]$. Lo que significa que la unión de

todas las clases es el conjunto de los números enteros. Además, en este caso se tiene que

$$[i] \cap [j] = \emptyset \text{ si } i \neq j,$$

por lo que clases distintas no tienen elementos comunes.



Partición de \mathbb{Z}

La relación de congruencia definida en \mathbb{Z} , podemos decir que parte o partitiona el conjunto de los enteros en n conjuntos los cuales denominamos clases.

Esto es, cada clase consta de números congruentes y el conjunto de todas las clases A lo notamos \mathbb{Z}_n .

Debemos anotar que $\mathbb{Z} = \bigcup_{[j] \in A} [j]$. Lo que significa que la unión de

todas las clases es el conjunto de los números enteros. Además, en este caso se tiene que

$$[i] \cap [j] = \emptyset \text{ si } i \neq j,$$

por lo que clases distintas no tienen elementos comunes.



Partición de \mathbb{Z}

La relación de congruencia definida en \mathbb{Z} , podemos decir que parte o partitiona el conjunto de los enteros en n conjuntos los cuales denominamos clases.

Esto es, cada clase consta de números congruentes y el conjunto de todas las clases A lo notamos \mathbb{Z}_n .

Debemos anotar que $\mathbb{Z} = \bigcup_{[j] \in A} [j]$. Lo que significa que la unión de

todas las clases es el conjunto de los números enteros. Además, en este caso se tiene que

$$[i] \cap [j] = \emptyset \text{ si } i \neq j,$$

por lo que clases distintas no tienen elementos comunes.



Partición de \mathbb{Z}

La relación de congruencia definida en \mathbb{Z} , podemos decir que parte o partitiona el conjunto de los enteros en n conjuntos los cuales denominamos clases.

Esto es, cada clase consta de números congruentes y el conjunto de todas las clases A lo notamos \mathbb{Z}_n .

Debemos anotar que $\mathbb{Z} = \bigcup_{[j] \in A} [j]$. Lo que significa que la unión de todas las clases es el conjunto de los números enteros. Además, en este caso se tiene que

$$[i] \cap [j] = \emptyset \text{ si } i \neq j,$$

por lo que clases distintas no tienen elementos comunes.



Ejemplo

Si $n = 2$, entonces $\mathbb{Z}_2 = \{[0], [1]\}$ o simplemente escribimos $\mathbb{Z}_2 = \{0, 1\}$.

Note que módulo 2

$$[0] = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

$$[1] = \{\dots, -5, -3, -1, 1, 3, \dots\}.$$

$$\mathbb{Z}_3 = \{[0], [1], [2]\},$$

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$[2] = \{\dots, -4, -1, 2, 5, \dots\}.$$



Ejemplo

Si $n = 2$, entonces $\mathbb{Z}_2 = \{[0], [1]\}$ o simplemente escribimos $\mathbb{Z}_2 = \{0, 1\}$.

Note que módulo 2

$$[0] = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

$$[1] = \{\dots, -5, -3, -1, 1, 3, \dots\}.$$

$$\mathbb{Z}_3 = \{[0], [1], [2]\},$$

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$[2] = \{\dots, -4, -1, 2, 5, \dots\}.$$



Ejemplo

Si $n = 2$, entonces $\mathbb{Z}_2 = \{[0], [1]\}$ o simplemente escribimos $\mathbb{Z}_2 = \{0, 1\}$.

Note que módulo 2

$$[0] = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

$$[1] = \{\dots, -5, -3, -1, 1, 3, \dots\}.$$

$$\mathbb{Z}_3 = \{[0], [1], [2]\},$$

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$[2] = \{\dots, -4, -1, 2, 5, \dots\}.$$



Ejemplo

Si $n = 2$, entonces $\mathbb{Z}_2 = \{[0], [1]\}$ o simplemente escribimos $\mathbb{Z}_2 = \{0, 1\}$.

Note que módulo 2

$$[0] = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

$$[1] = \{\dots, -5, -3, -1, 1, 3, \dots\}.$$

$$\mathbb{Z}_3 = \{[0], [1], [2]\},$$

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$[2] = \{\dots, -4, -1, 2, 5, \dots\}.$$



Ejemplo

Si $n = 2$, entonces $\mathbb{Z}_2 = \{[0], [1]\}$ o simplemente escribimos $\mathbb{Z}_2 = \{0, 1\}$.

Note que módulo 2

$$[0] = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

$$[1] = \{\dots, -5, -3, -1, 1, 3, \dots\}.$$

$$\mathbb{Z}_3 = \{[0], [1], [2]\},$$

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$[2] = \{\dots, -4, -1, 2, 5, \dots\}.$$



Ejemplo

Si $n = 2$, entonces $\mathbb{Z}_2 = \{[0], [1]\}$ o simplemente escribimos $\mathbb{Z}_2 = \{0, 1\}$.

Note que módulo 2

$$[0] = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

$$[1] = \{\dots, -5, -3, -1, 1, 3, \dots\}.$$

$$\mathbb{Z}_3 = \{[0], [1], [2]\},$$

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$[2] = \{\dots, -4, -1, 2, 5, \dots\}.$$



\mathbb{Z}_{12} 

El abecedario en inglés puede ser asociado con \mathbb{Z}_{26} . de forma tal que :

$$A \rightarrow 0, B \rightarrow 1, C \rightarrow 2, \dots, Z \rightarrow 25.$$

El abecedario en inglés puede ser asociado con \mathbb{Z}_{26} . de forma tal que :

$$A \rightarrow 0, B \rightarrow 1, C \rightarrow 2, \dots, Z \rightarrow 25.$$

Definición

Para n fijo podemos definir la suma y multiplicación en \mathbb{Z}_n , de forma tal que

$$[i] + [j] = [i + j].$$

$$[i] \cdot [j] = [i \cdot j].$$

Definición

Para n fijo podemos definir la suma y multiplicación en \mathbb{Z}_n , de forma tal que

$$[i] + [j] = [i + j].$$

$$[i] \cdot [j] = [i \cdot j].$$

Definición

Para n fijo podemos definir la suma y multiplicación en \mathbb{Z}_n , de forma tal que

$$[i] + [j] = [i + j].$$

$$[i] \cdot [j] = [i \cdot j].$$

Definición

Para n fijo podemos definir la suma y multiplicación en \mathbb{Z}_n , de forma tal que

$$[i] + [j] = [i + j].$$

$$[i] \cdot [j] = [i \cdot j].$$

Ejemplo

En \mathbb{Z}_2 y \mathbb{Z}_3 , se tiene que :

+	0	1
0	0	1
1	1	0

+	0	1	2
0	0	1	2
1	1	2	0

Ejemplo

En \mathbb{Z}_3 y \mathbb{Z}_4 , se tiene que :

.	1	2
1	1	2
2	2	1

.	1	2	3
1	1	2	3
2	2	0	2
3	1	2	1

Ejemplo

En \mathbb{Z}_6 :

.	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Propiedades de las operaciones $+$, \cdot en \mathbb{Z}_n

Para n fijo

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a + b \in \mathbb{Z}_n$,
- ② $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a + 0 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a + (-a) = 0$, en donde $[-a] = -[a] = [n - a]$, para todo $a \in \mathbb{Z}_n$,
- ⑤ $a + b = b + a$, para todo $a, b \in \mathbb{Z}_n$.

Propiedades de las operaciones $+$, \cdot en \mathbb{Z}_n

Para n fijo

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a + b \in \mathbb{Z}_n$,
- ② $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a + 0 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a + (-a) = 0$, en donde $[-a] = -[a] = [n - a]$, para todo $a \in \mathbb{Z}_n$,
- ⑤ $a + b = b + a$, para todo $a, b \in \mathbb{Z}_n$.

Propiedades de las operaciones $+$, \cdot en \mathbb{Z}_n

Para n fijo

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a + b \in \mathbb{Z}_n$,
- ② $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a + 0 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a + (-a) = 0$, en donde $[-a] = -[a] = [n - a]$, para todo $a \in \mathbb{Z}_n$,
- ⑤ $a + b = b + a$, para todo $a, b \in \mathbb{Z}_n$.

Propiedades de las operaciones $+$, \cdot en \mathbb{Z}_n

Para n fijo

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a + b \in \mathbb{Z}_n$,
- ② $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a + 0 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a + (-a) = 0$, en donde $[-a] = -[a] = [n - a]$, para todo $a \in \mathbb{Z}_n$,
- ⑤ $a + b = b + a$, para todo $a, b \in \mathbb{Z}_n$.

Propiedades de las operaciones $+$, \cdot en \mathbb{Z}_n

Para n fijo

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a + b \in \mathbb{Z}_n$,
- ② $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a + 0 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a + (-a) = 0$, en donde $[-a] = -[a] = [n - a]$, para todo $a \in \mathbb{Z}_n$,
- ⑤ $a + b = b + a$, para todo $a, b \in \mathbb{Z}_n$.

Propiedades de las operaciones $+$, \cdot en \mathbb{Z}_n

Para n fijo

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a + b \in \mathbb{Z}_n$,
- ② $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a + 0 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a + (-a) = 0$, en donde $[-a] = -[a] = [n - a]$, para todo $a \in \mathbb{Z}_n$,
- ⑤ $a + b = b + a$, para todo $a, b \in \mathbb{Z}_n$.

Propiedades de las operaciones $+$, \cdot en \mathbb{Z}_n

Para n fijo

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a + b \in \mathbb{Z}_n$,
- ② $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a + 0 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a + (-a) = 0$, en donde $[-a] = -[a] = [n - a]$, para todo $a \in \mathbb{Z}_n$,
- ⑤ $a + b = b + a$, para todo $a, b \in \mathbb{Z}_n$.

Propiedades de las operaciones $+$, \cdot en \mathbb{Z}_n

Para n fijo

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a + b \in \mathbb{Z}_n$,
- ② $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a + 0 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a + (-a) = 0$, en donde $[-a] = -[a] = [n - a]$, para todo $a \in \mathbb{Z}_n$,
- ⑤ $a + b = b + a$, para todo $a, b \in \mathbb{Z}_n$.

Propiedades de las operaciones $+$, \cdot en \mathbb{Z}_n

Para n fijo

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a + b \in \mathbb{Z}_n$,
- ② $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a + 0 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a + (-a) = 0$, en donde $[-a] = -[a] = [n - a]$, para todo $a \in \mathbb{Z}_n$,
- ⑤ $a + b = b + a$, para todo $a, b \in \mathbb{Z}_n$.

Propiedades de las operaciones $+$, \cdot en \mathbb{Z}_n

Para n fijo

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a + b \in \mathbb{Z}_n$,
- ② $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a + 0 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a + (-a) = 0$, en donde $[-a] = -[a] = [n - a]$, para todo $a \in \mathbb{Z}_n$,
- ⑤ $a + b = b + a$, para todo $a, b \in \mathbb{Z}_n$.

Propiedades de las operaciones $+$, \cdot en \mathbb{Z}_n

Para n fijo

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a + b \in \mathbb{Z}_n$,
- ② $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a + 0 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a + (-a) = 0$, en donde $[-a] = -[a] = [n - a]$, para todo $a \in \mathbb{Z}_n$,
- ⑤ $a + b = b + a$, para todo $a, b \in \mathbb{Z}_n$.

Estructura algebraica de \mathbb{Z}_n

Las 5 propiedades anteriores, permiten que \mathbb{Z}_n , con esta operación constituya un grupo abeliano.

Propiedades de la multiplicación

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a \cdot b \in \mathbb{Z}_n$,
- ② $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a \cdot 1 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a \cdot b = b \cdot a$, para todo $a, b \in \mathbb{Z}_n$,
- ⑤ $a \cdot (b + c) = a \cdot b + a \cdot c$.

Estas propiedades junto con aquellas de la suma logran que \mathbb{Z}_n , sea un anillo conmutativo con unidad.

Propiedades de la multiplicación

① Si $a, b \in \mathbb{Z}_n$ entonces $a \cdot b \in \mathbb{Z}_n$,

② $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in \mathbb{Z}_n$,

③ $a \cdot 1 = a$, para todo $a \in \mathbb{Z}_n$,

④ $a \cdot b = b \cdot a$, para todo $a, b \in \mathbb{Z}_n$,

⑤ $a \cdot (b + c) = a \cdot b + a \cdot c$.

Estas propiedades junto con aquellas de la suma logran que \mathbb{Z}_n , sea un anillo conmutativo con unidad.

Propiedades de la multiplicación

① Si $a, b \in \mathbb{Z}_n$ entonces $a \cdot b \in \mathbb{Z}_n$,

② $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in \mathbb{Z}_n$,

③ $a \cdot 1 = a$, para todo $a \in \mathbb{Z}_n$,

④ $a \cdot b = b \cdot a$, para todo $a, b \in \mathbb{Z}_n$,

⑤ $a \cdot (b + c) = a \cdot b + a \cdot c$.

Estas propiedades junto con aquellas de la suma logran que \mathbb{Z}_n , sea un anillo conmutativo con unidad.

Propiedades de la multiplicación

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a \cdot b \in \mathbb{Z}_n$,
- ② $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a \cdot 1 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a \cdot b = b \cdot a$, para todo $a, b \in \mathbb{Z}_n$,
- ⑤ $a \cdot (b + c) = a \cdot b + a \cdot c$.

Estas propiedades junto con aquellas de la suma logran que \mathbb{Z}_n , sea un anillo conmutativo con unidad.

Propiedades de la multiplicación

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a \cdot b \in \mathbb{Z}_n$,
- ② $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a \cdot 1 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a \cdot b = b \cdot a$, para todo $a, b \in \mathbb{Z}_n$,
- ⑤ $a \cdot (b + c) = a \cdot b + a \cdot c$.

Estas propiedades junto con aquellas de la suma logran que \mathbb{Z}_n , sea un anillo conmutativo con unidad.

Propiedades de la multiplicación

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a \cdot b \in \mathbb{Z}_n$,
- ② $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a \cdot 1 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a \cdot b = b \cdot a$, para todo $a, b \in \mathbb{Z}_n$,
- ⑤ $a \cdot (b + c) = a \cdot b + a \cdot c$.

Estas propiedades junto con aquellas de la suma logran que \mathbb{Z}_n , sea un anillo conmutativo con unidad.

Propiedades de la multiplicación

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a \cdot b \in \mathbb{Z}_n$,
- ② $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a \cdot 1 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a \cdot b = b \cdot a$, para todo $a, b \in \mathbb{Z}_n$,
- ⑤ $a \cdot (b + c) = a \cdot b + a \cdot c$.

Estas propiedades junto con aquellas de la suma logran que \mathbb{Z}_n , sea un anillo conmutativo con unidad.

Propiedades de la multiplicación

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a \cdot b \in \mathbb{Z}_n$,
- ② $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a \cdot 1 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a \cdot b = b \cdot a$, para todo $a, b \in \mathbb{Z}_n$,
- ⑤ $a \cdot (b + c) = a \cdot b + a \cdot c$.

Estas propiedades junto con aquellas de la suma logran que \mathbb{Z}_n , sea un anillo conmutativo con unidad.

Propiedades de la multiplicación

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a \cdot b \in \mathbb{Z}_n$,
- ② $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a \cdot 1 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a \cdot b = b \cdot a$, para todo $a, b \in \mathbb{Z}_n$,
- ⑤ $a \cdot (b + c) = a \cdot b + a \cdot c$.

Estas propiedades junto con aquellas de la suma logran que \mathbb{Z}_n , sea un anillo conmutativo con unidad.

Propiedades de la multiplicación

- ① Si $a, b \in \mathbb{Z}_n$ entonces $a \cdot b \in \mathbb{Z}_n$,
- ② $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in \mathbb{Z}_n$,
- ③ $a \cdot 1 = a$, para todo $a \in \mathbb{Z}_n$,
- ④ $a \cdot b = b \cdot a$, para todo $a, b \in \mathbb{Z}_n$,
- ⑤ $a \cdot (b + c) = a \cdot b + a \cdot c$.

Estas propiedades junto con aquellas de la suma logran que \mathbb{Z}_n , sea un anillo conmutativo con unidad.

Inversibilidad

En general para n fijo no todo elemento $a \in \mathbb{Z}_n$, tiene un inverso multiplicativo. Esto es, un elemento $b \in \mathbb{Z}_n$, tal que $[a \cdot b] = [1]$ o $a \cdot b \equiv 1 \pmod{n}$ (observe \mathbb{Z}_4 y \mathbb{Z}_6).

Por lo que tenemos la siguiente proposición :

Para n fijo, $a \in \mathbb{Z}_n$ es inversible si y solo si $(a, n) = 1$, esto es a y n son primos relativos lo que significa que estos dos números, no poseen divisores comunes distintos de 1.

Inversibilidad

En general para n fijo no todo elemento $a \in \mathbb{Z}_n$, tiene un inverso multiplicativo. Esto es, un elemento $b \in \mathbb{Z}_n$, tal que $[a \cdot b] = [1]$ o $a \cdot b \equiv 1 \pmod{n}$ (observe \mathbb{Z}_4 y \mathbb{Z}_6).

Por lo que tenemos la siguiente proposición :

Para n fijo, $a \in \mathbb{Z}_n$ es inversible si y solo si $(a, n) = 1$, esto es a y n son primos relativos lo que significa que estos dos números, no poseen divisores comunes distintos de 1.

Inversibilidad

En general para n fijo no todo elemento $a \in \mathbb{Z}_n$, tiene un inverso multiplicativo. Esto es, un elemento $b \in \mathbb{Z}_n$, tal que $[a \cdot b] = [1]$ o $a \cdot b \equiv 1 \pmod{n}$ (observe \mathbb{Z}_4 y \mathbb{Z}_6).

Por lo que tenemos la siguiente proposición :

Para n fijo, $a \in \mathbb{Z}_n$ es inversible si y solo si $(a, n) = 1$, esto es a y n son primos relativos lo que significa que estos dos números, no poseen divisores comunes distintos de 1.

Ejemplo

En \mathbb{Z}_{26} , los elementos inversibles para la multiplicación son :

$$1^{-1} = 1, 3^{-1} = 9, 5^{-1} = 21, 7^{-1} = 15, 11^{-1} = 19, 17^{-1} = 23 \text{ y} \\ 25^{-1} = 25.$$

Ejemplo

En \mathbb{Z}_{26} , los elementos inversibles para la multiplicación son :

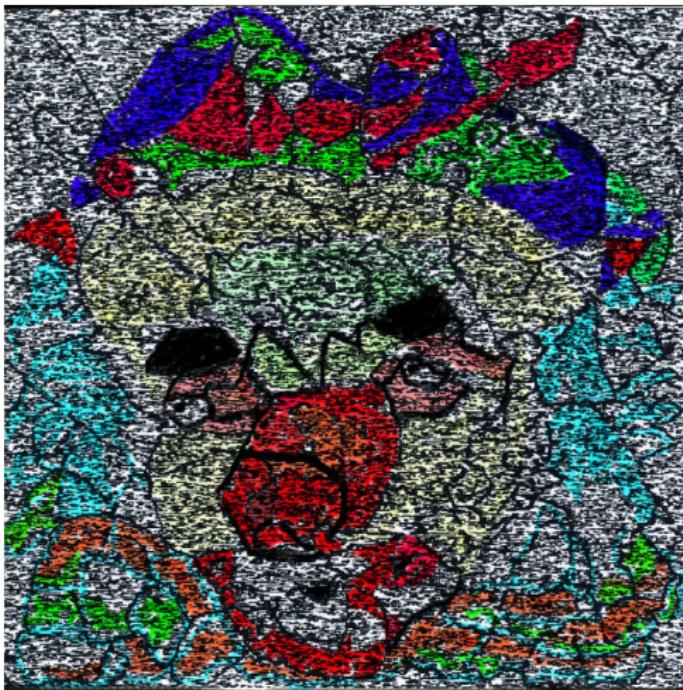
$$1^{-1} = 1, 3^{-1} = 9, 5^{-1} = 21, 7^{-1} = 15, 11^{-1} = 19, 17^{-1} = 23 \text{ y} \\ 25^{-1} = 25.$$

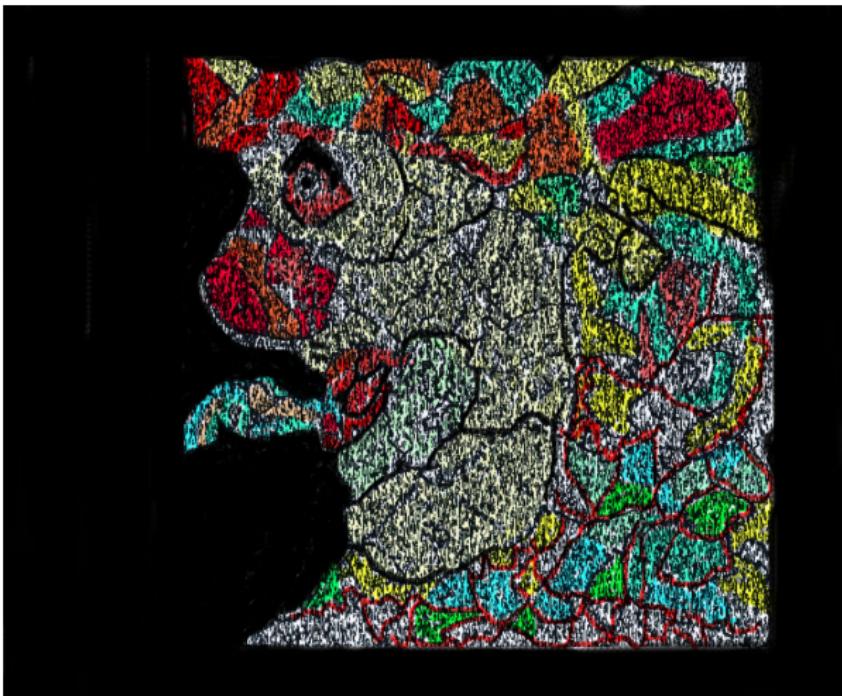
Ejemplo

En \mathbb{Z}_{26} , los elementos inversibles para la multiplicación son :

$1^{-1} = 1, 3^{-1} = 9, 5^{-1} = 21, 7^{-1} = 15, 11^{-1} = 19, 17^{-1} = 23$ y
 $25^{-1} = 25$.

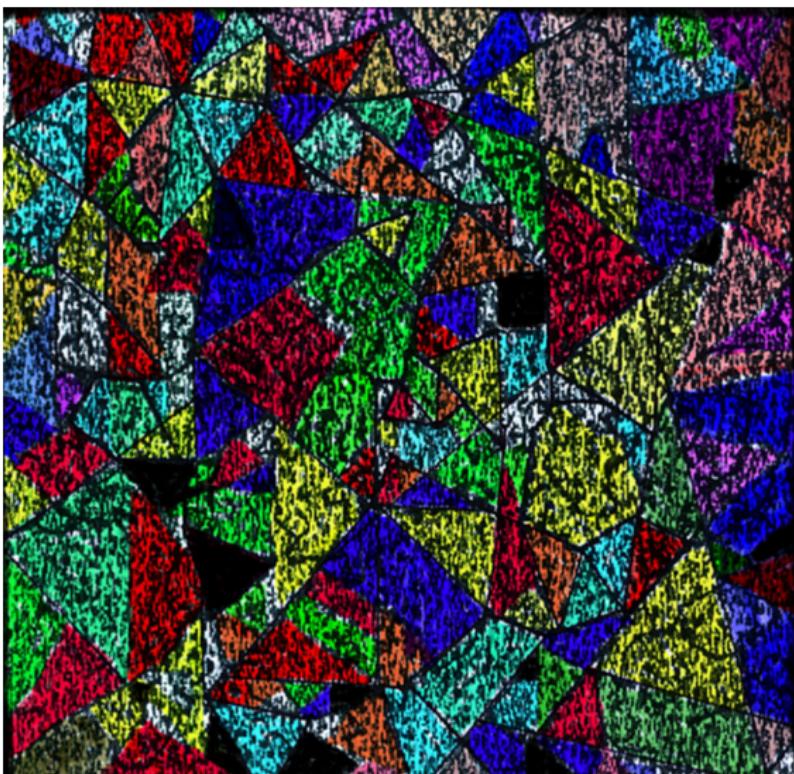
<http://www.mersenne.org/primes/perfect/perfect1398269.txt>

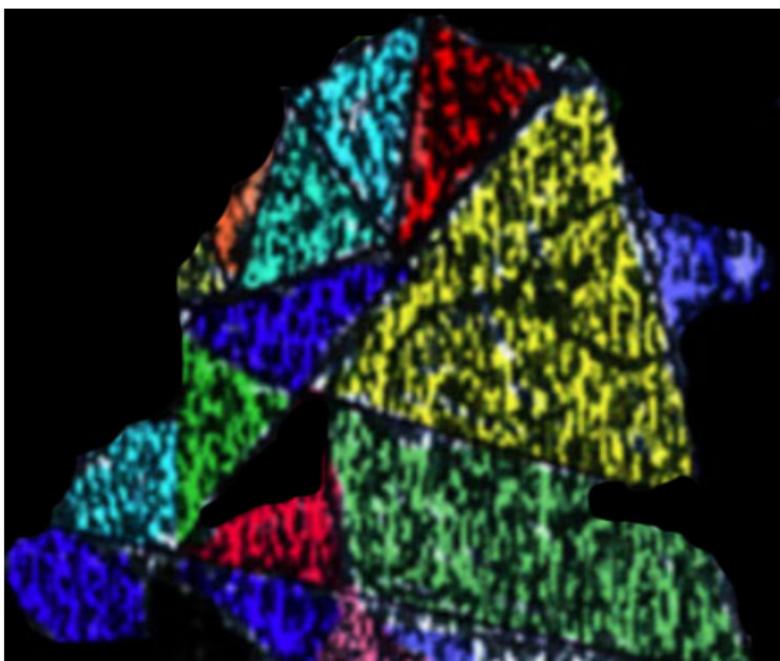


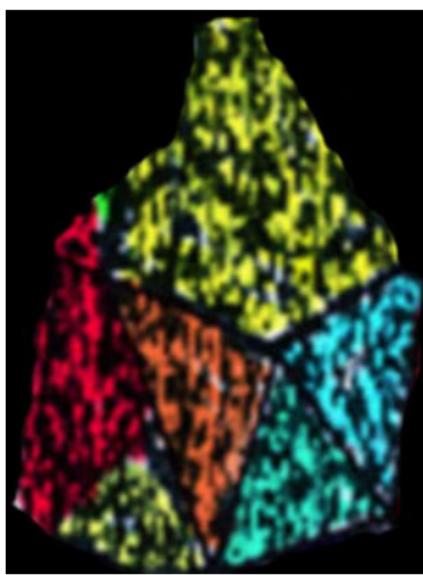


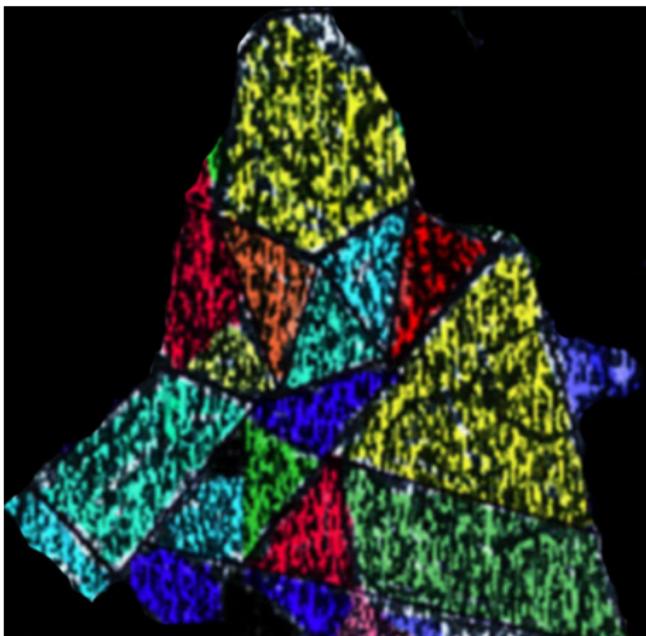




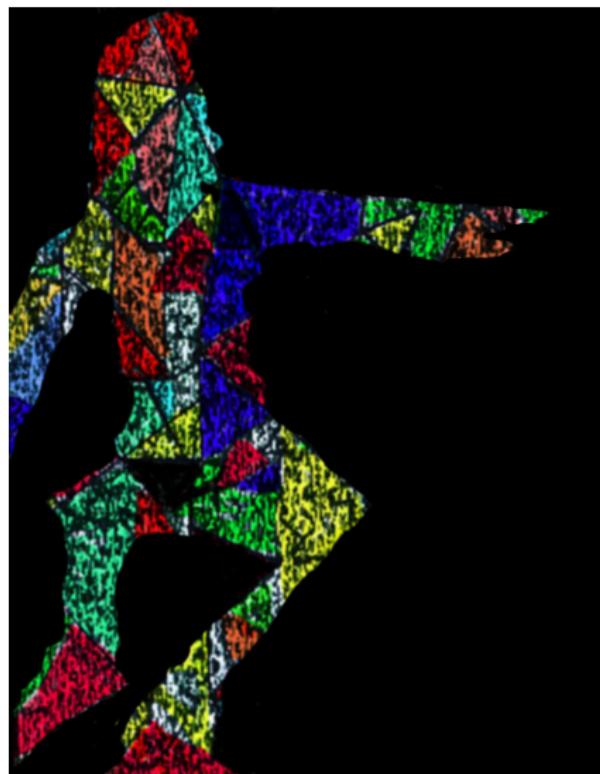


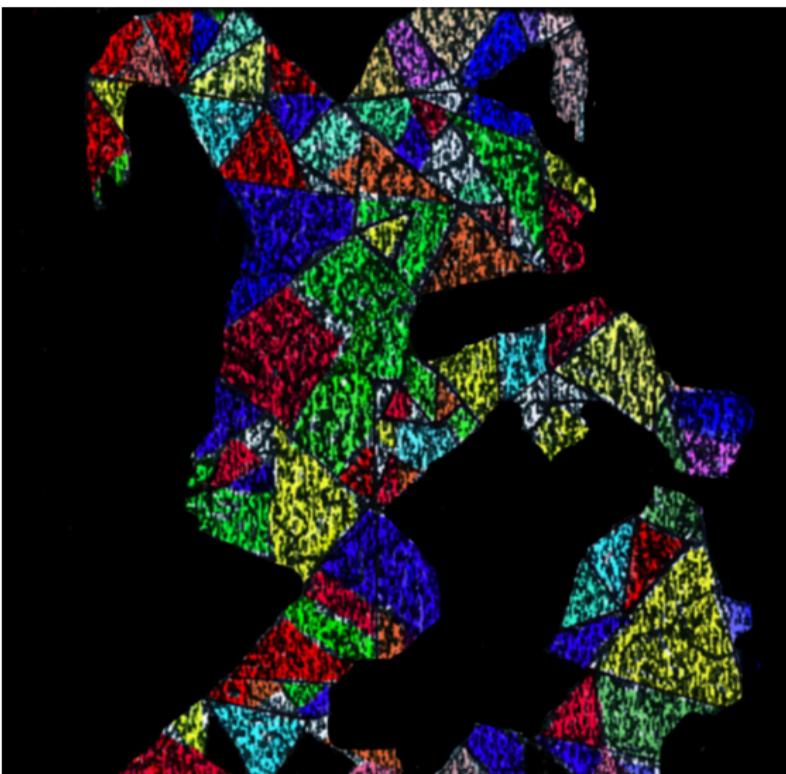


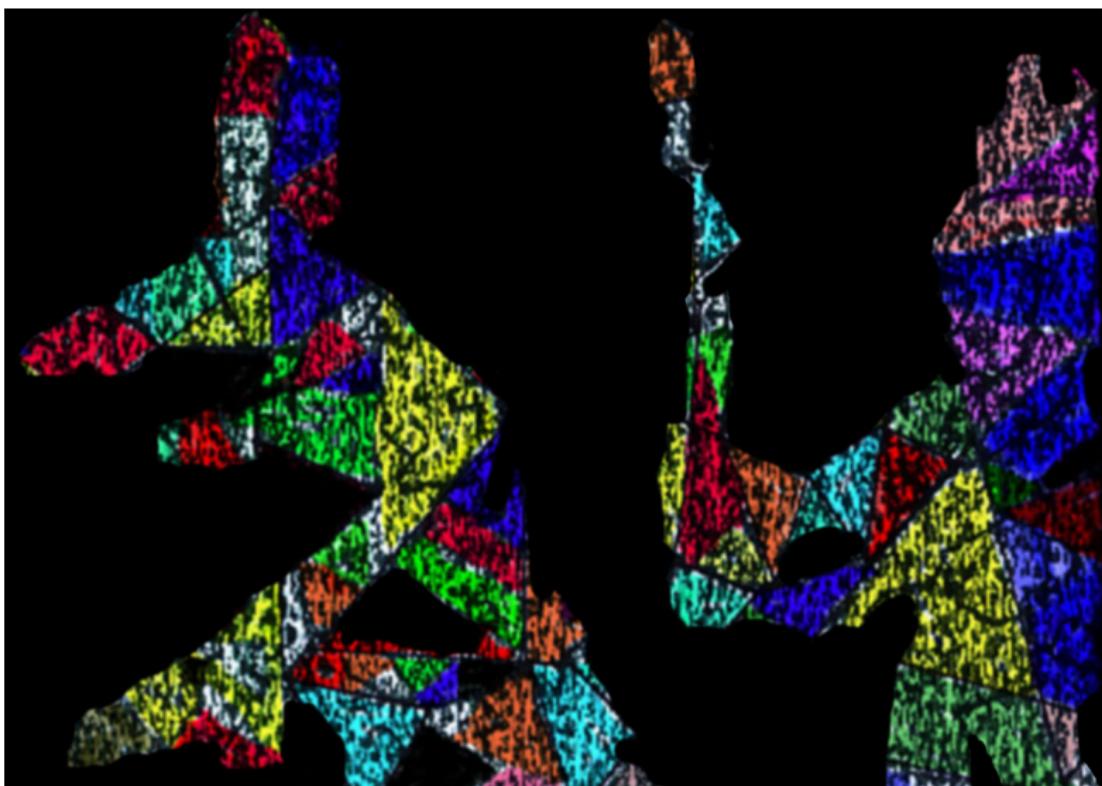


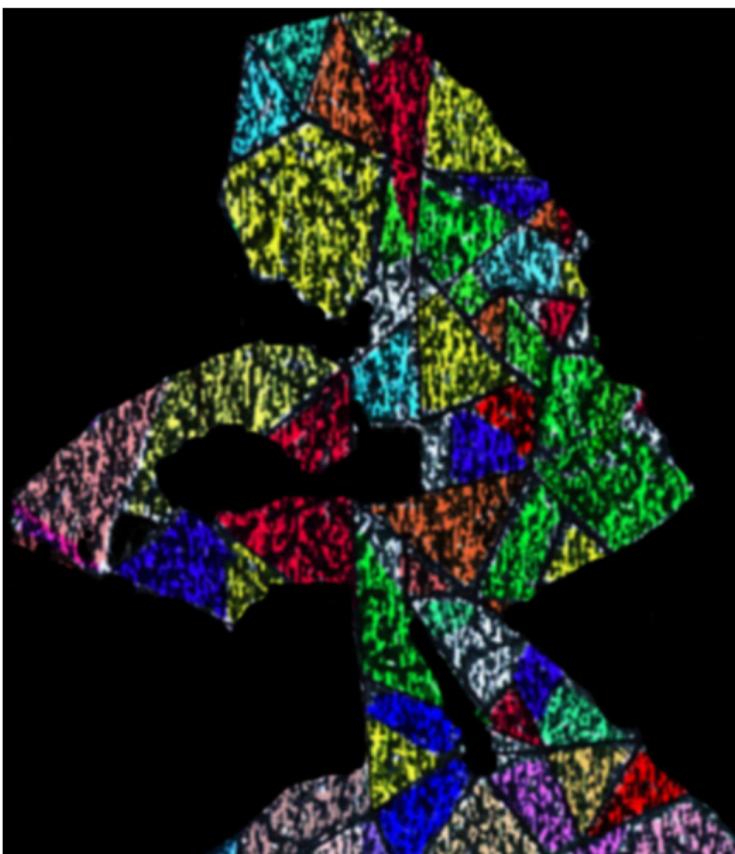


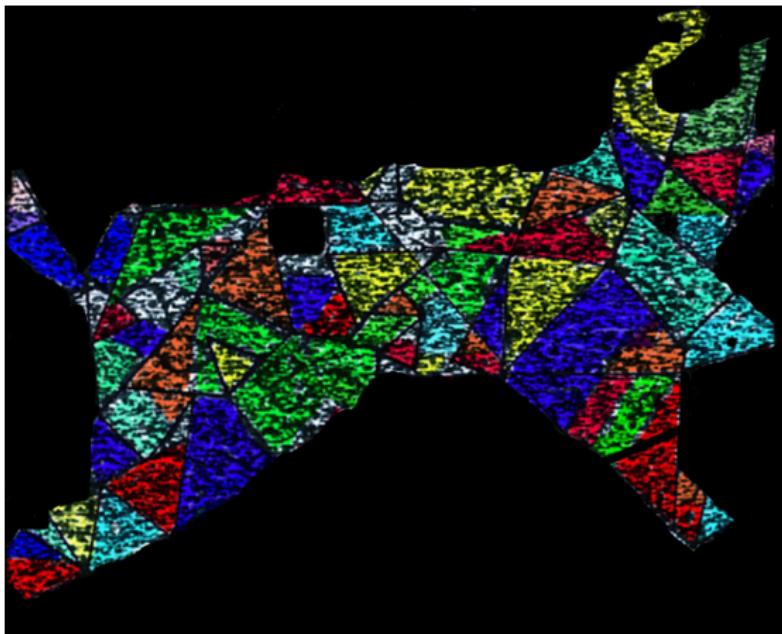


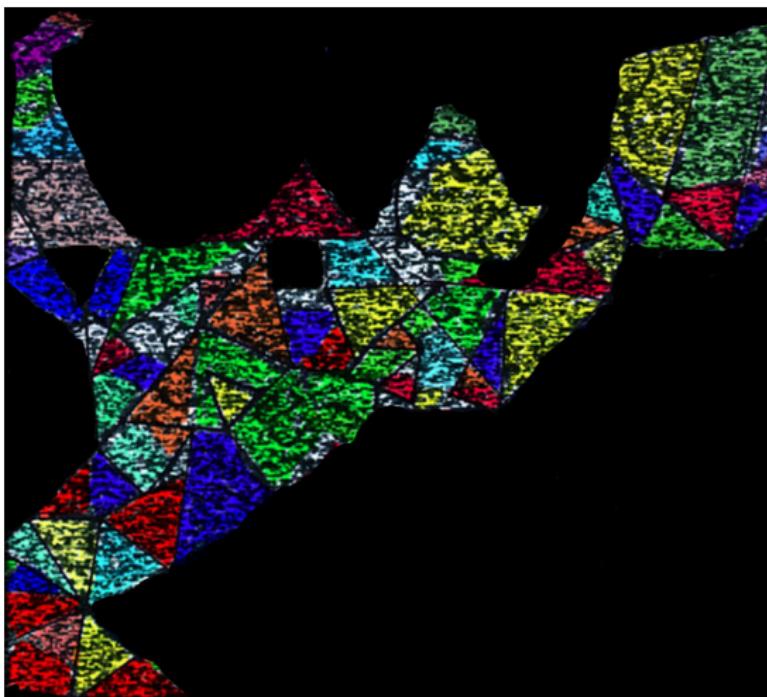


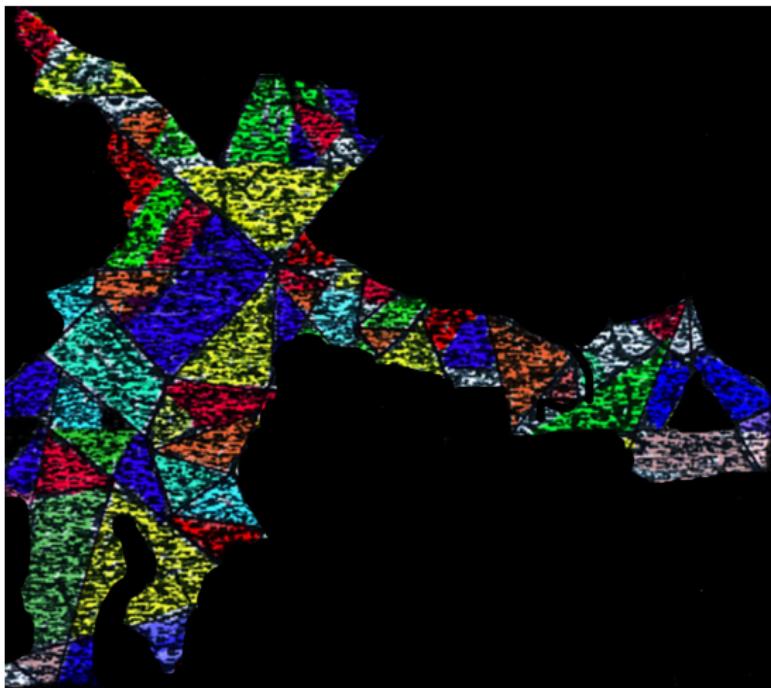


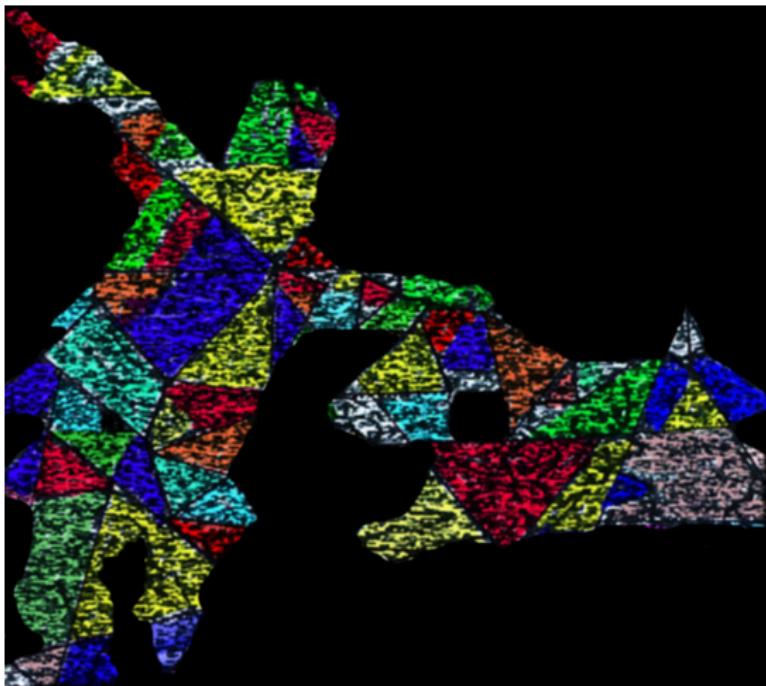






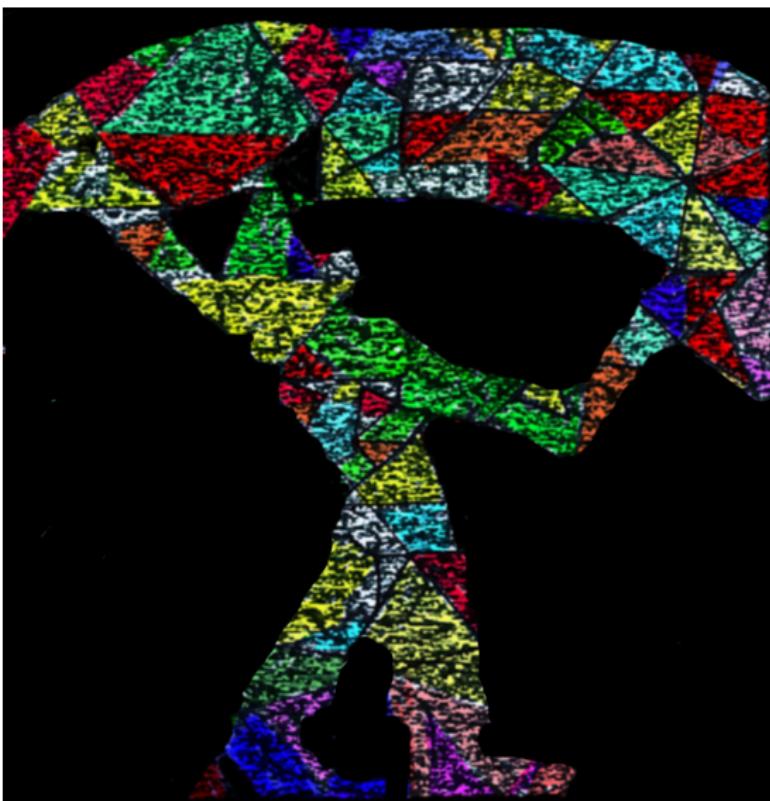


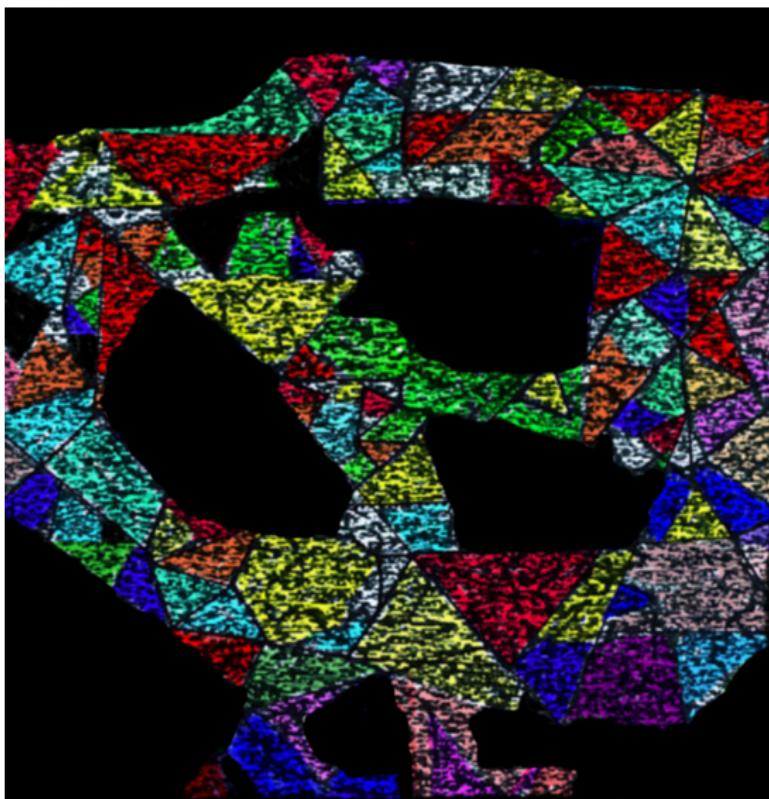


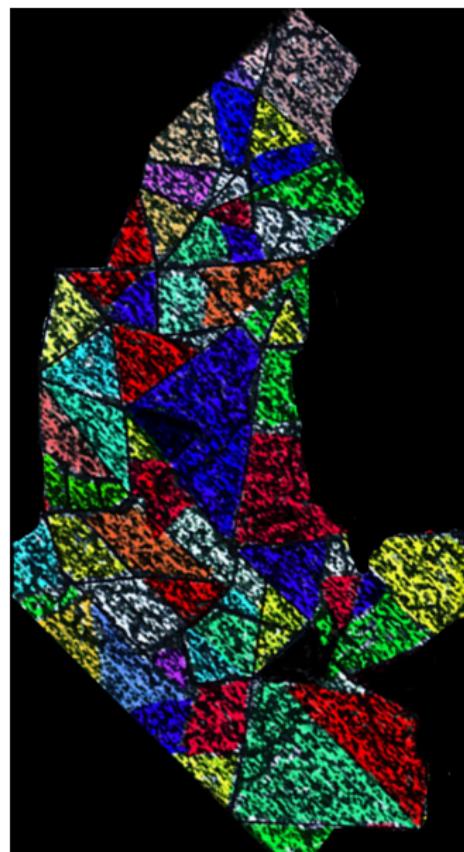


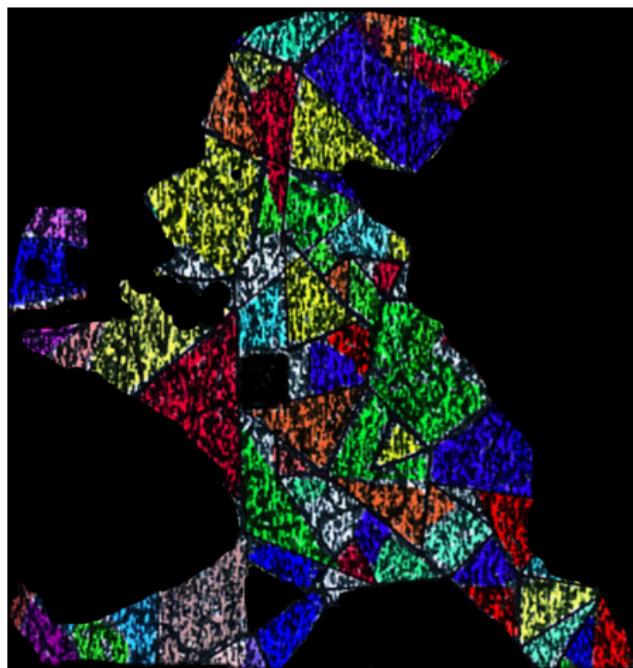


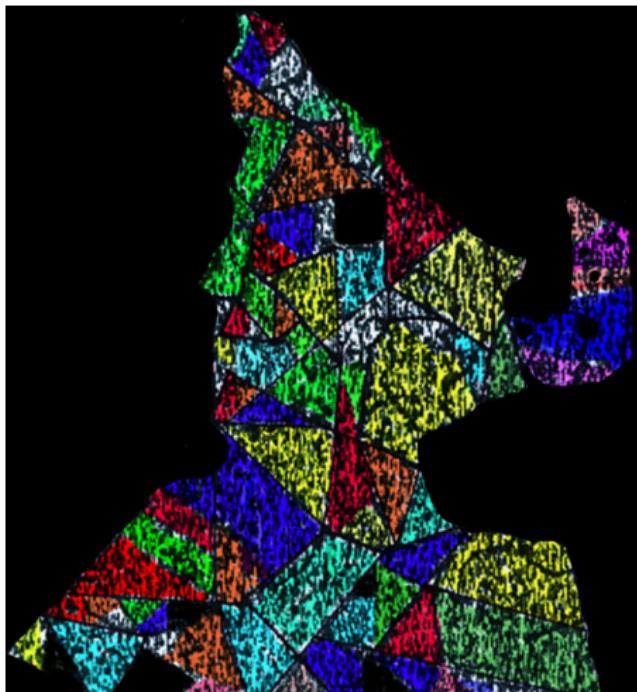


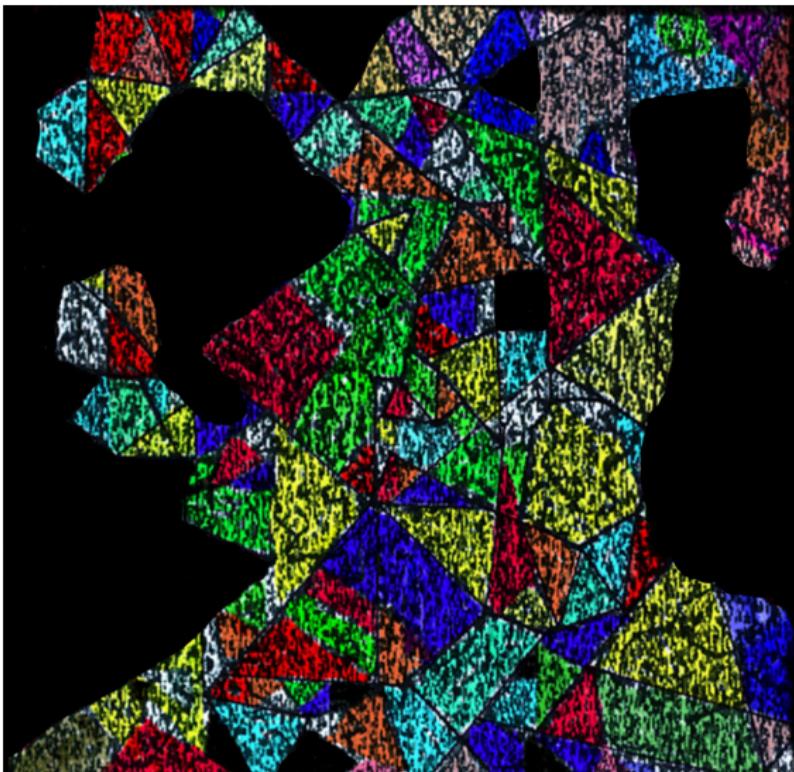


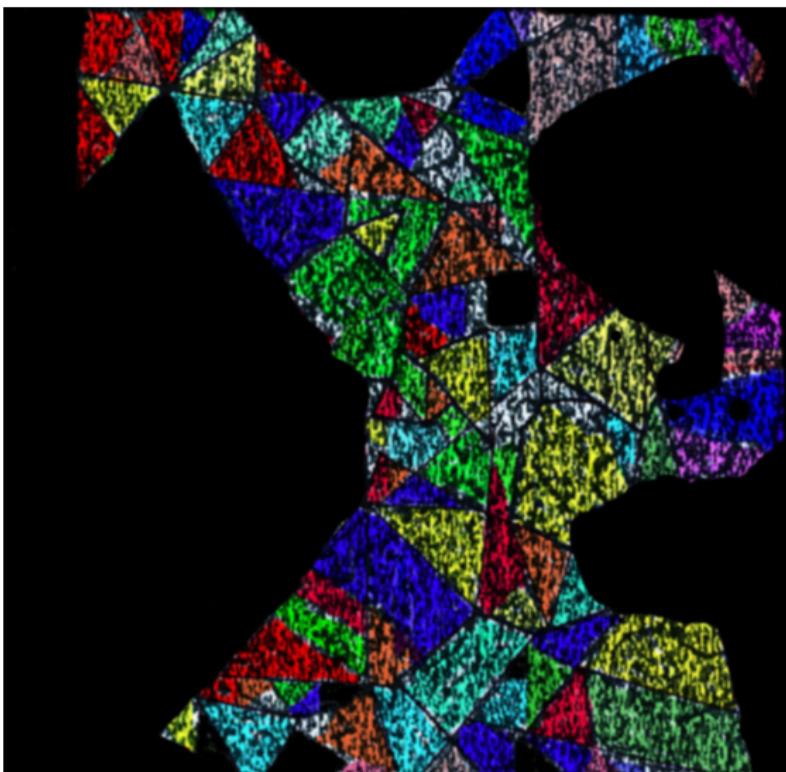


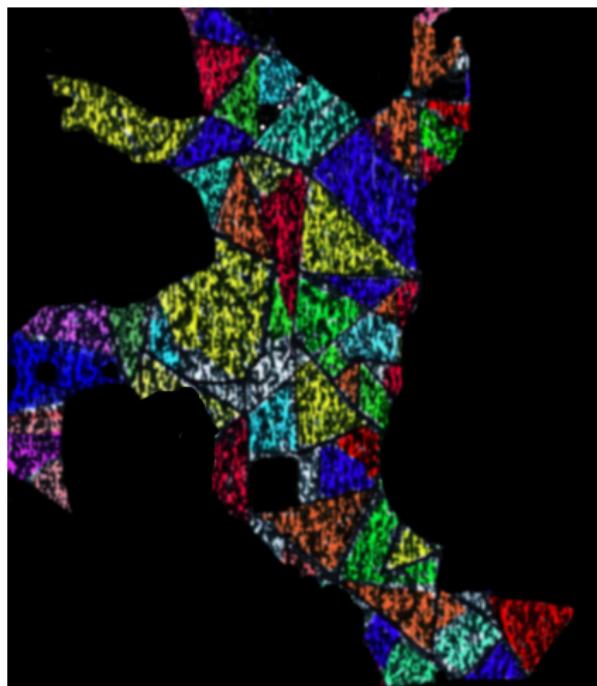


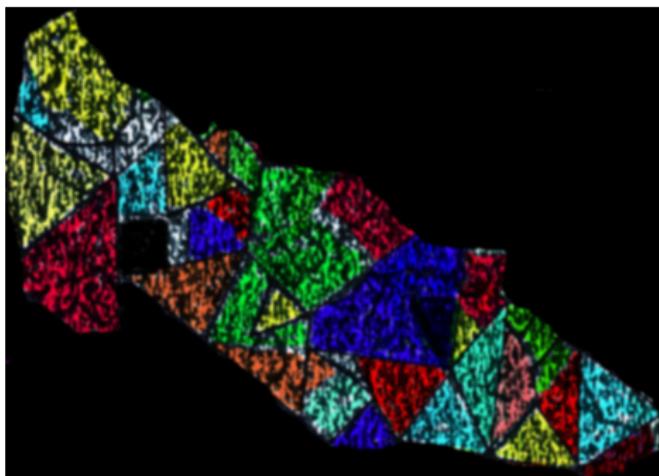


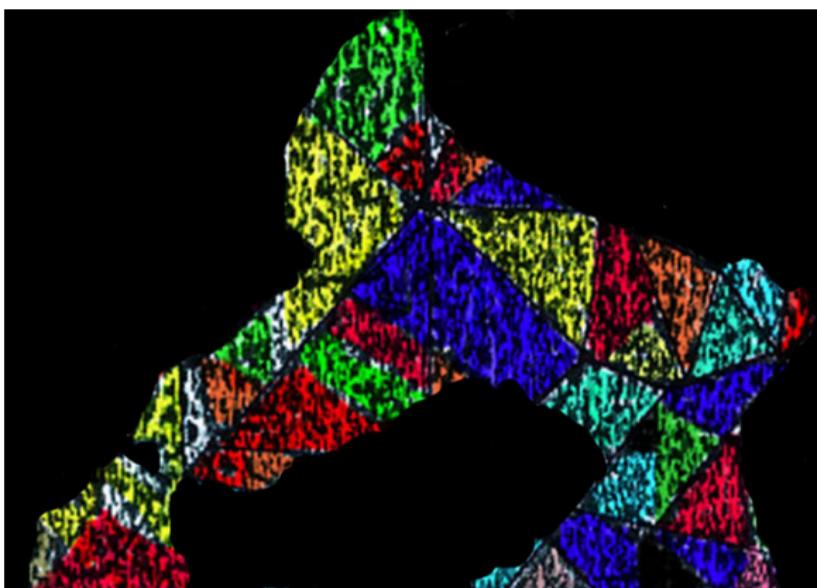


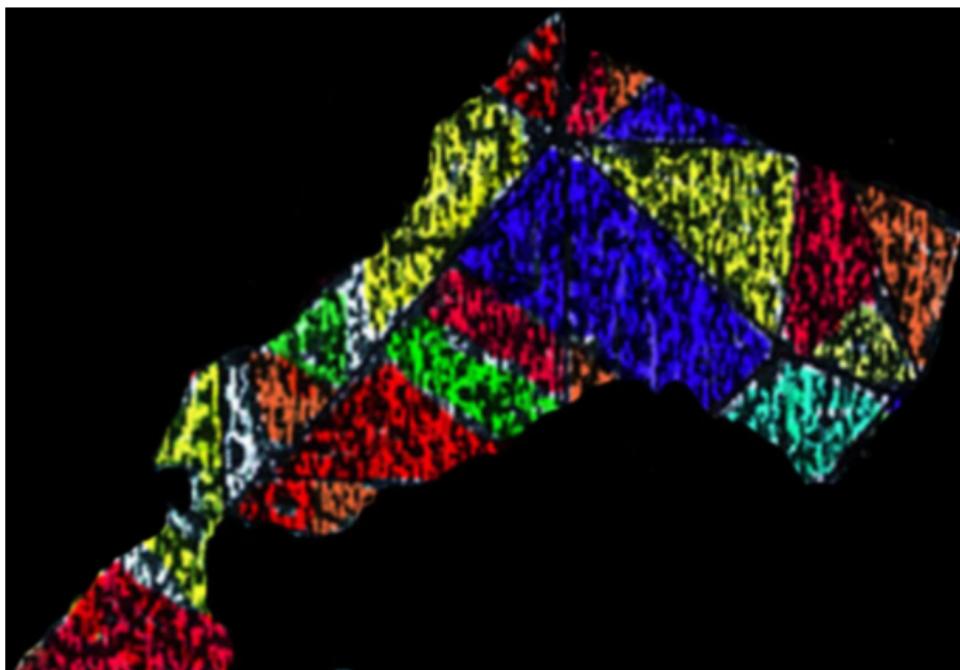




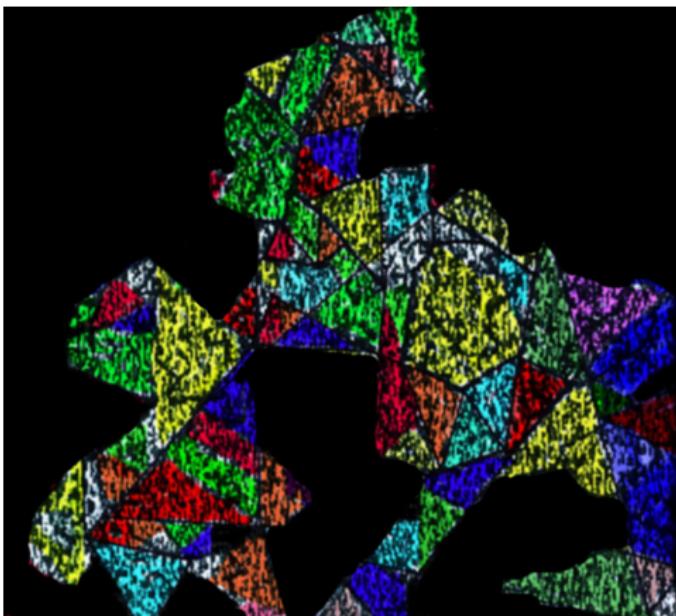


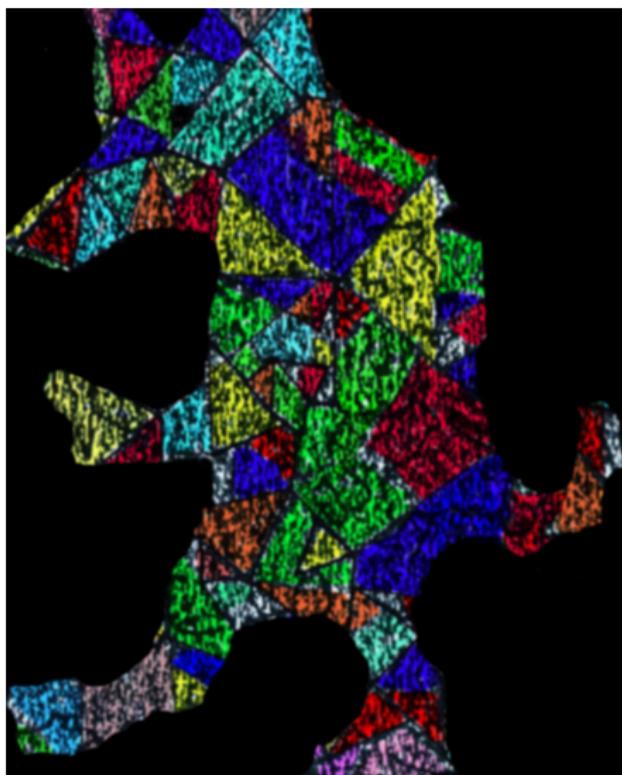


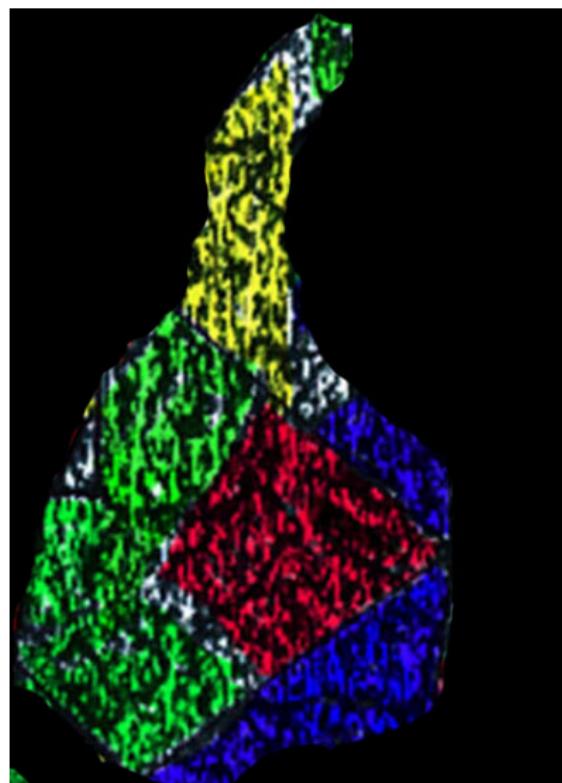


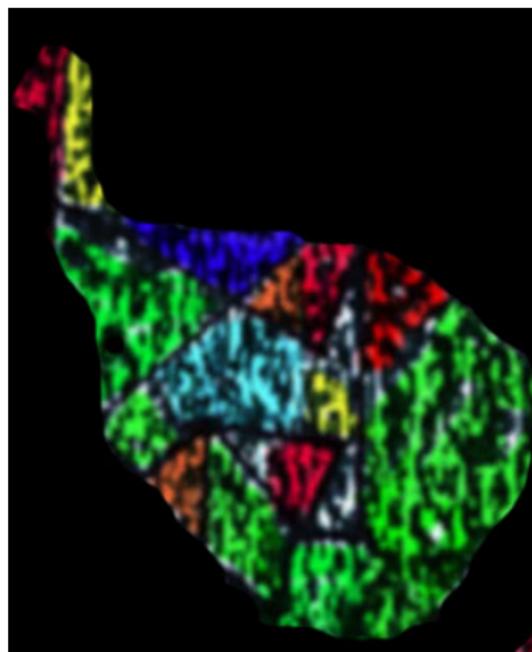




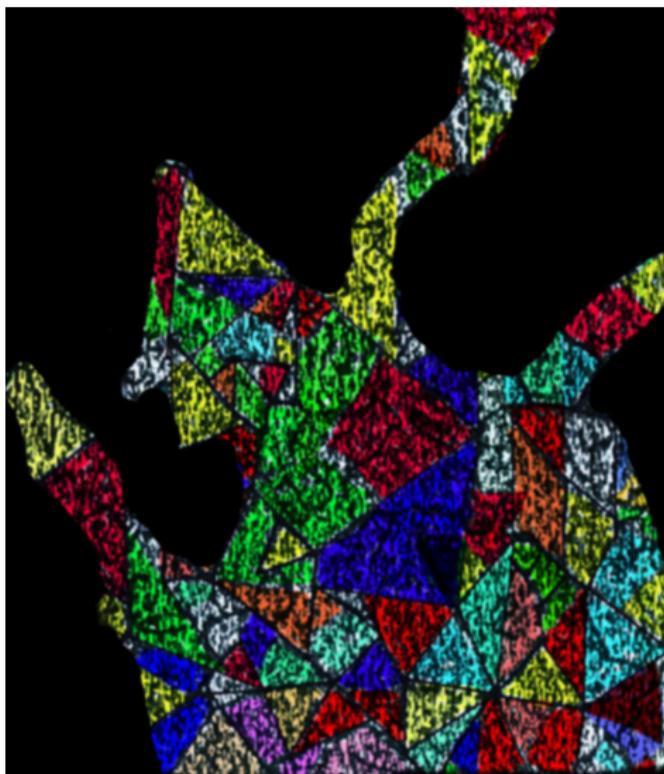


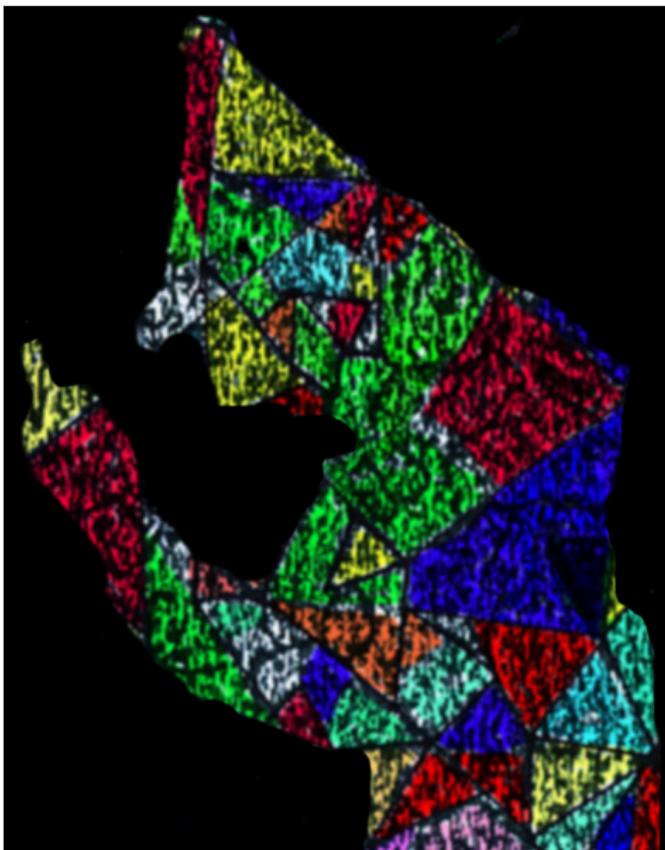


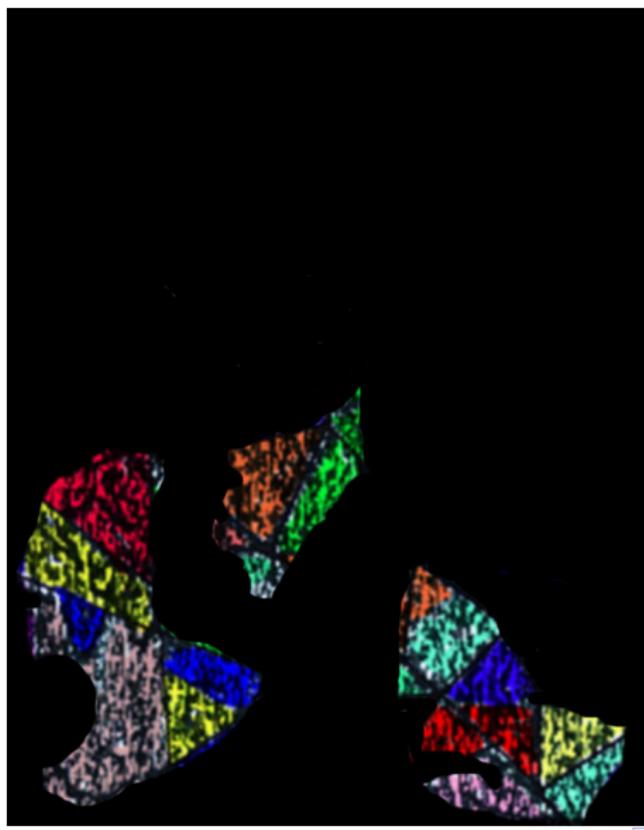


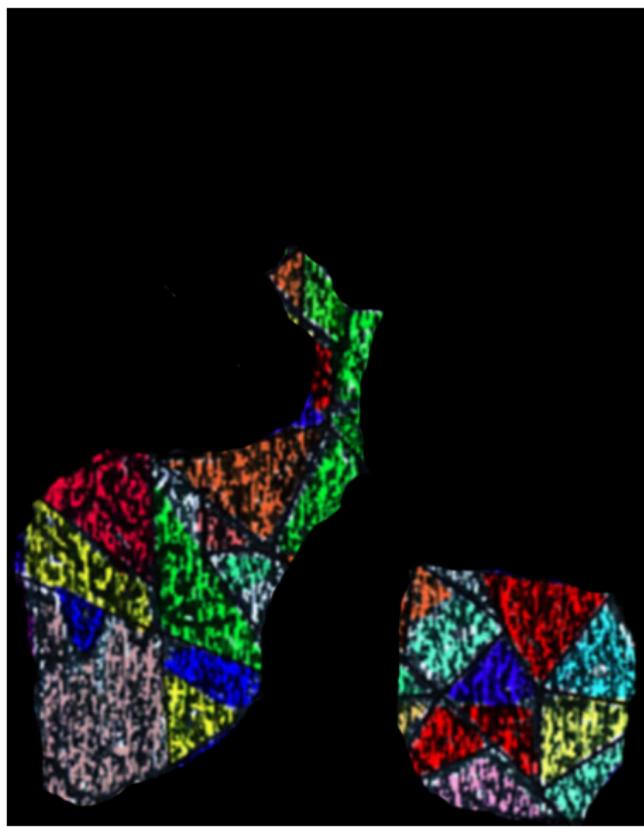


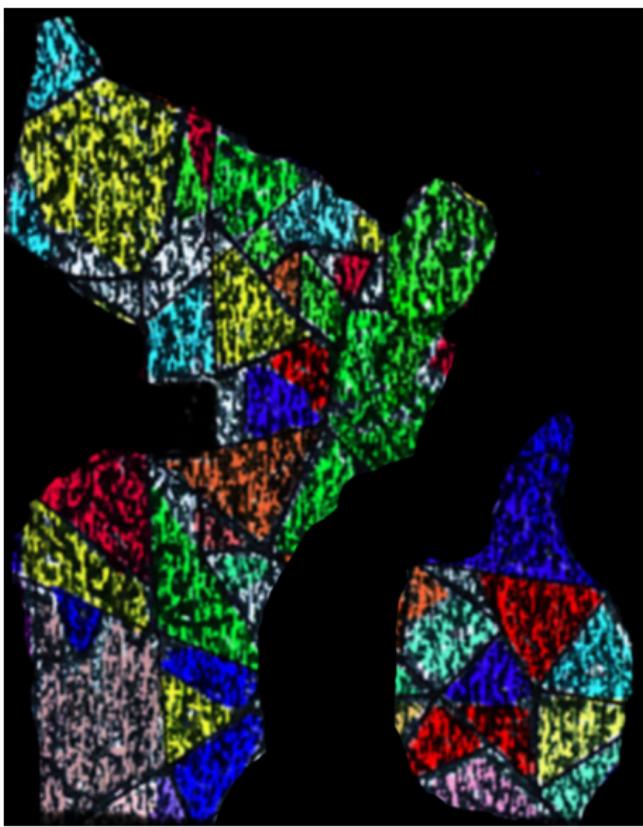


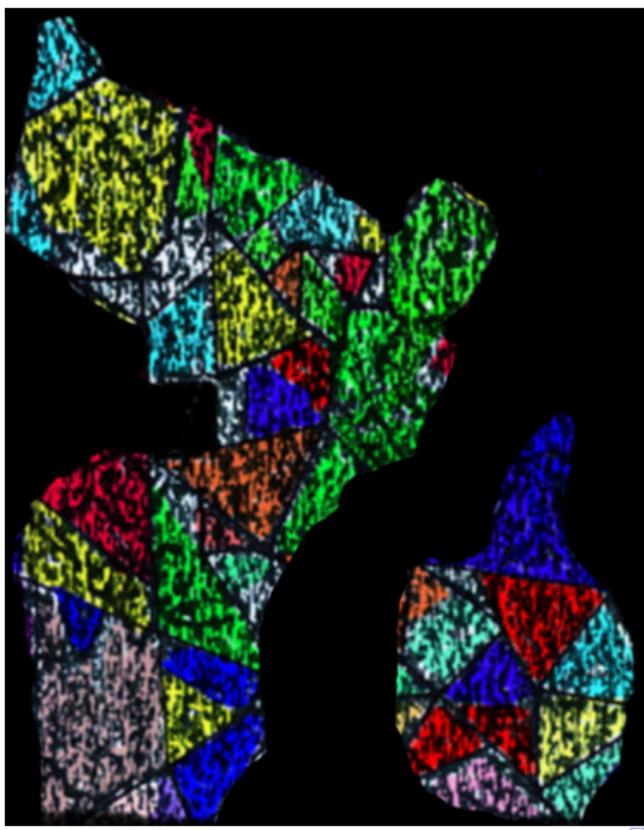


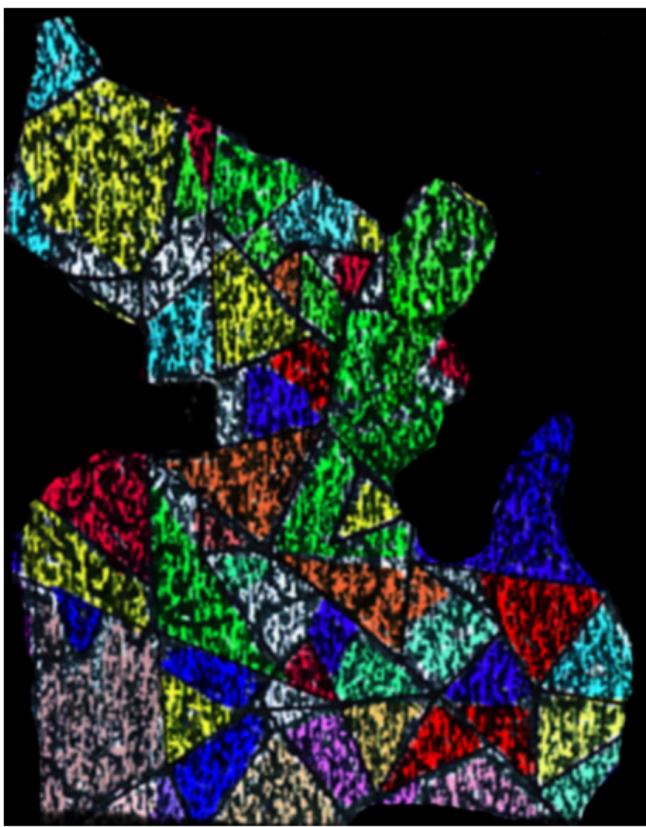


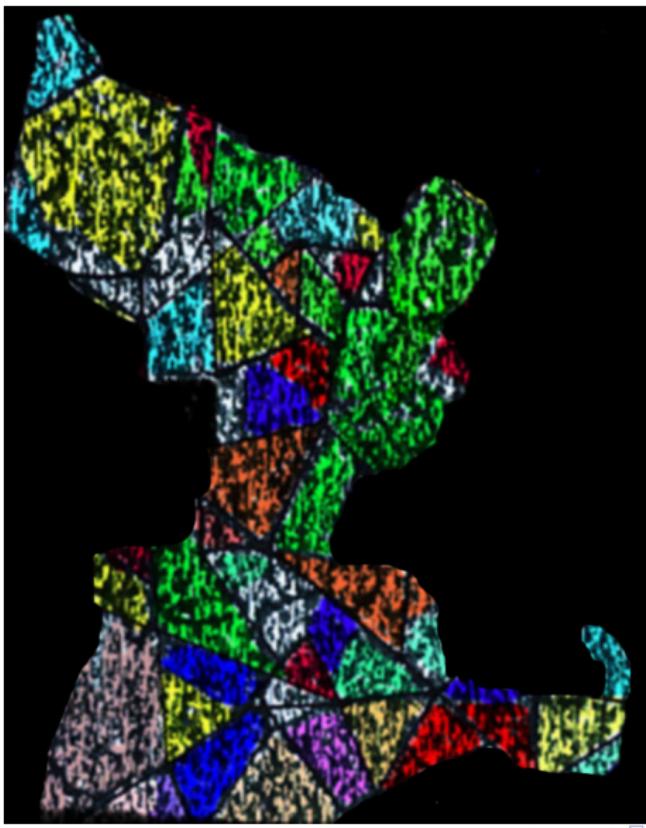


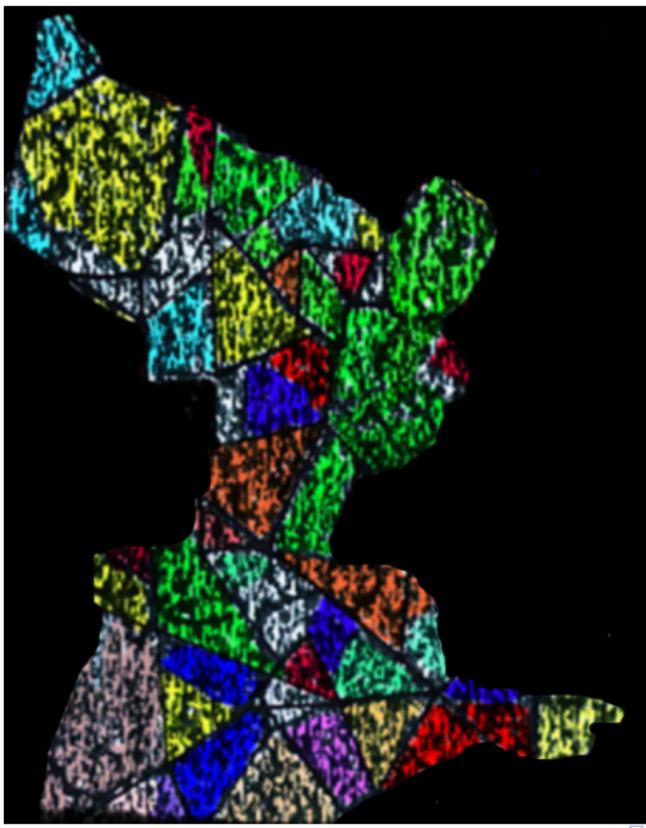


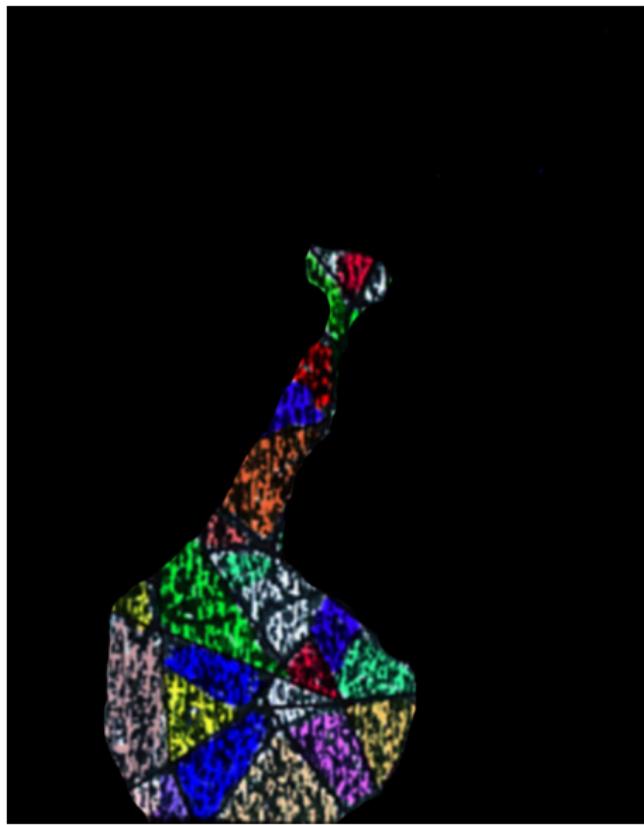


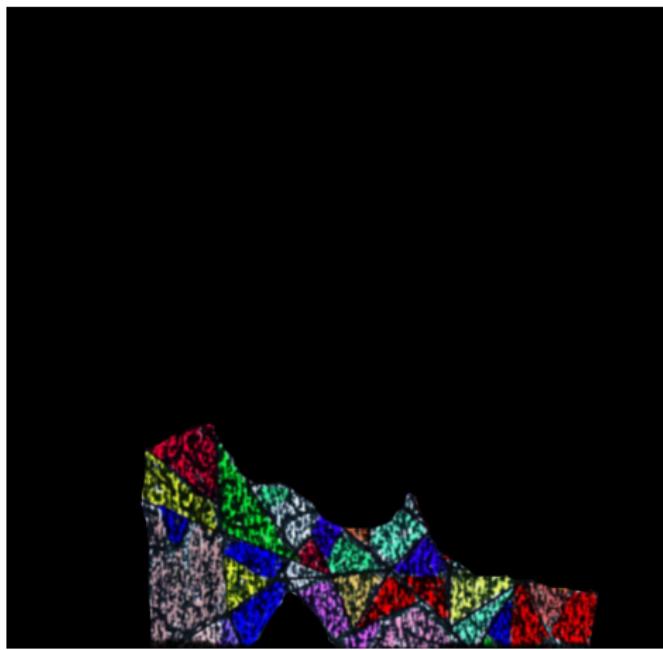


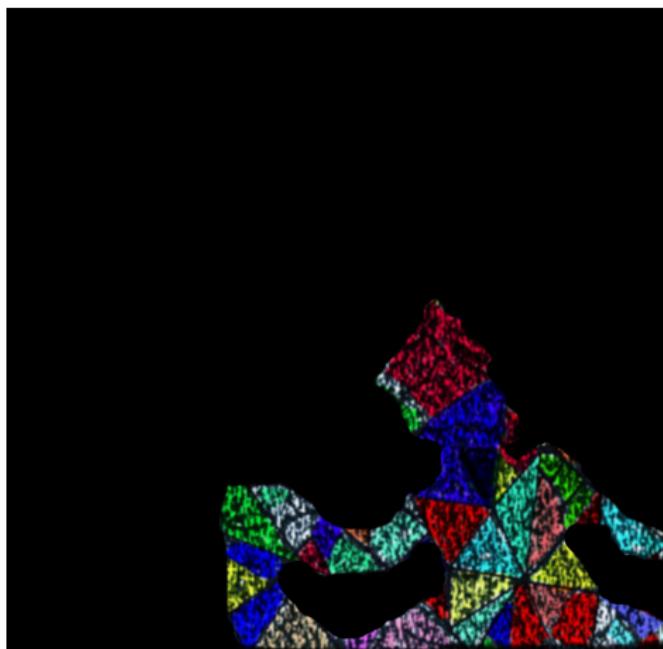


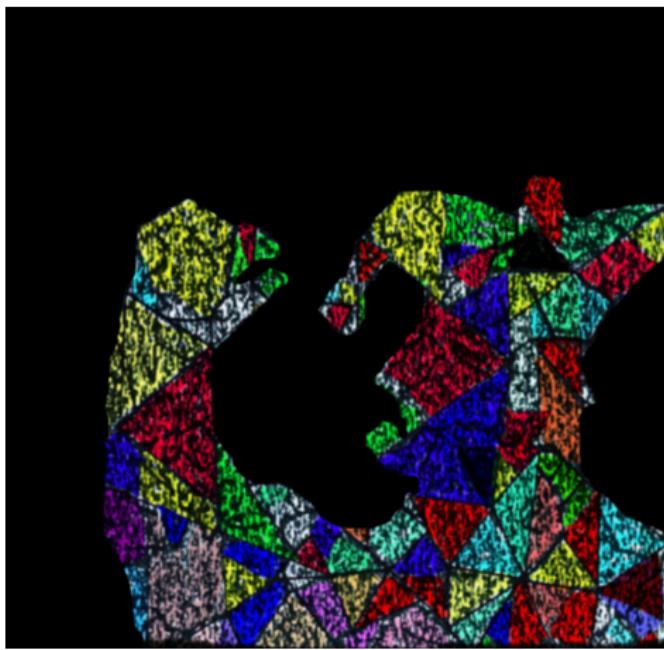


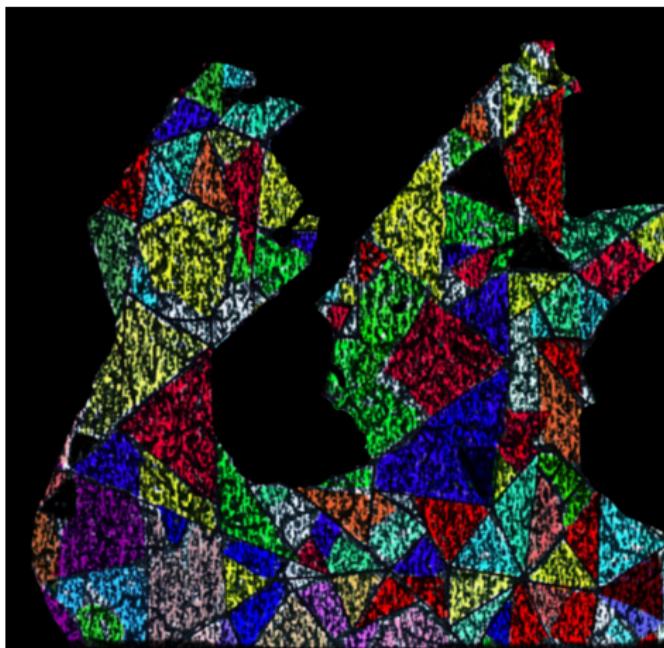


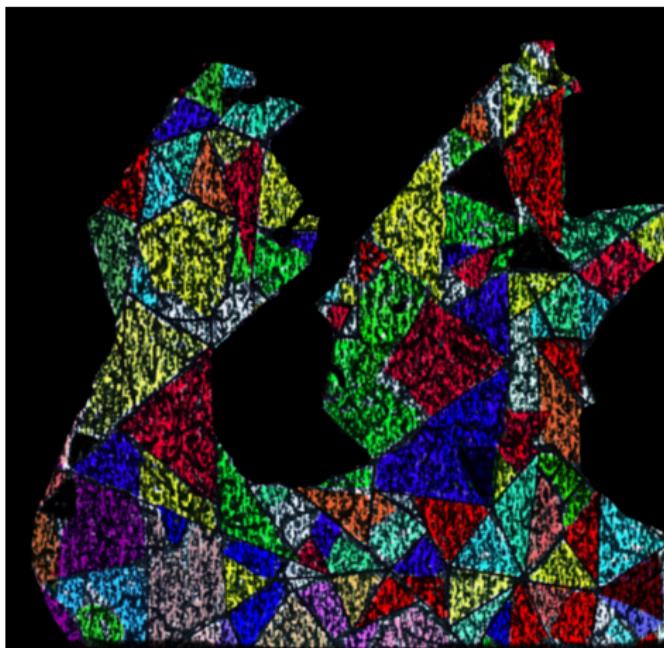


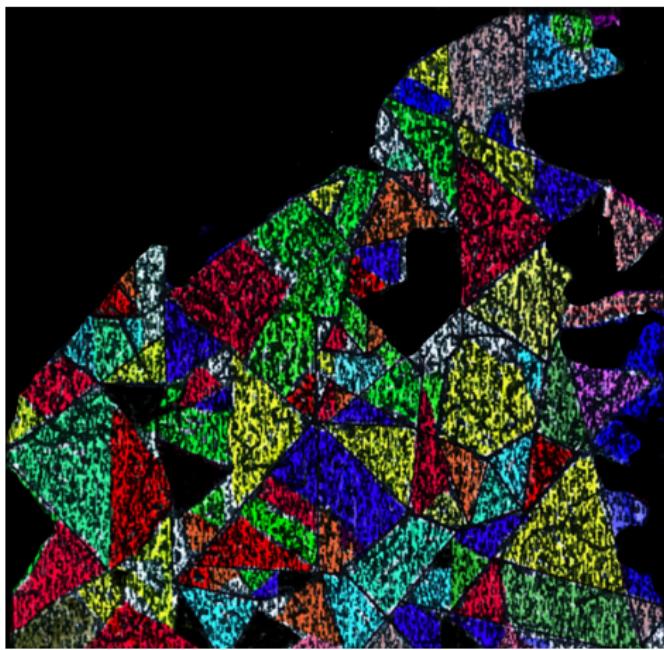


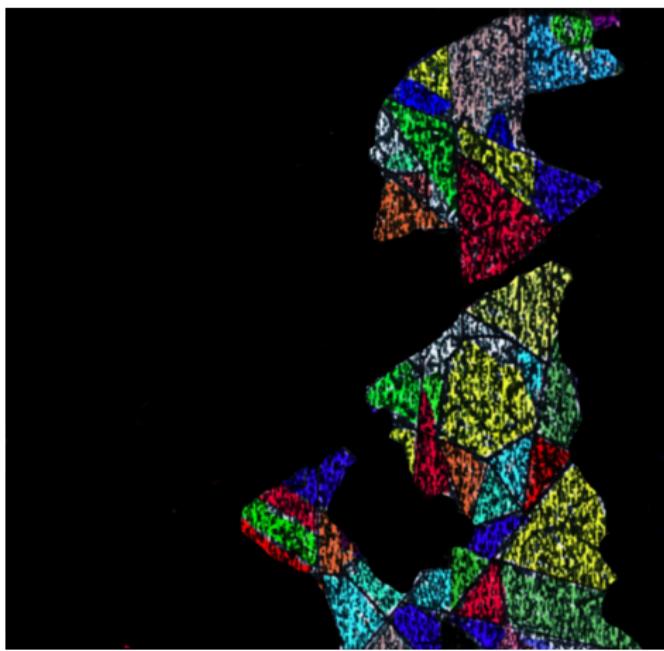


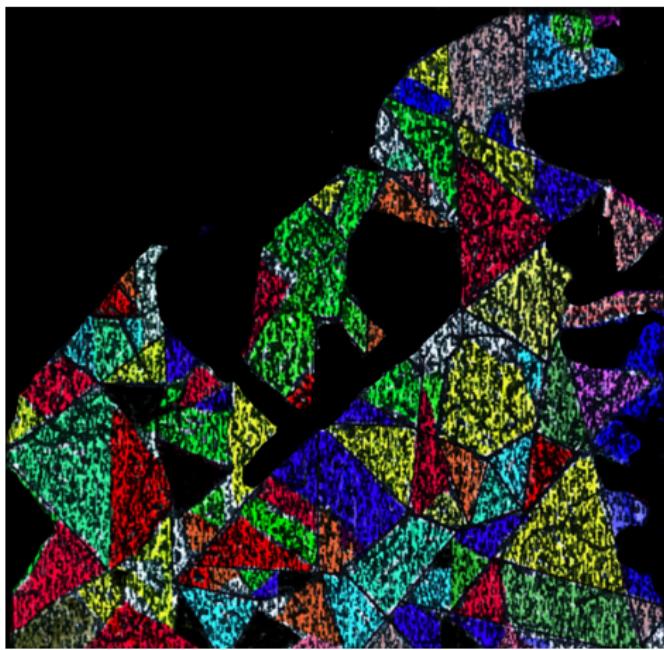


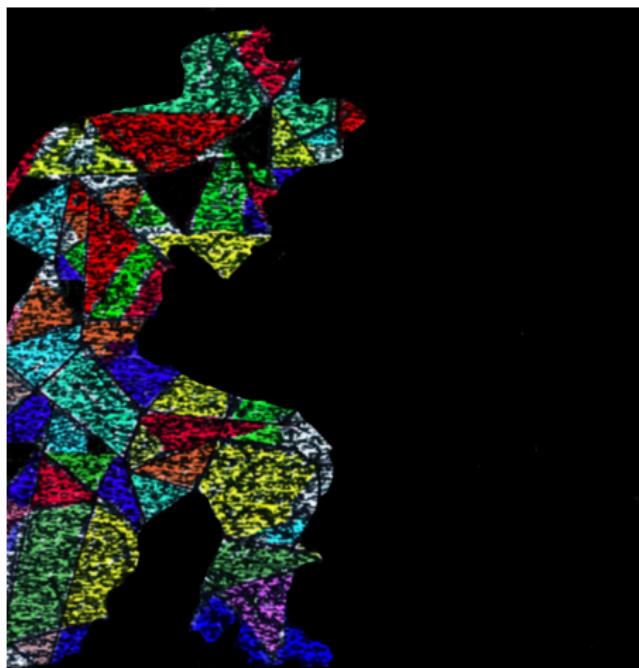


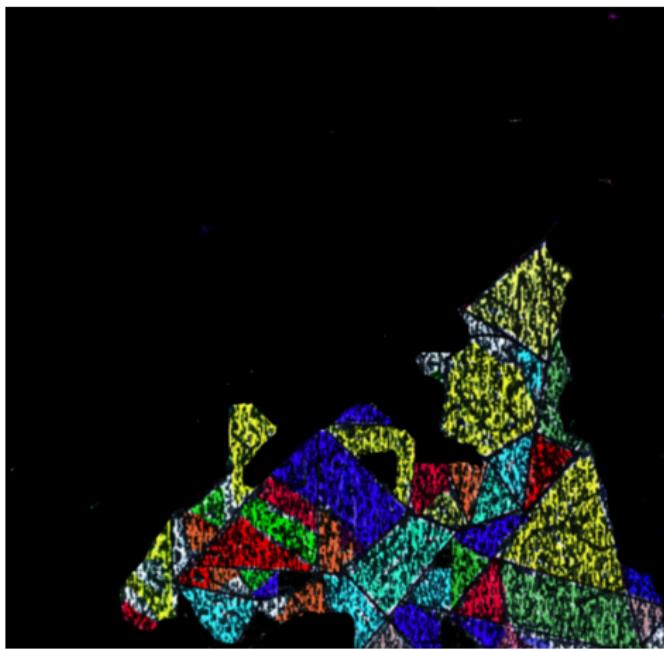


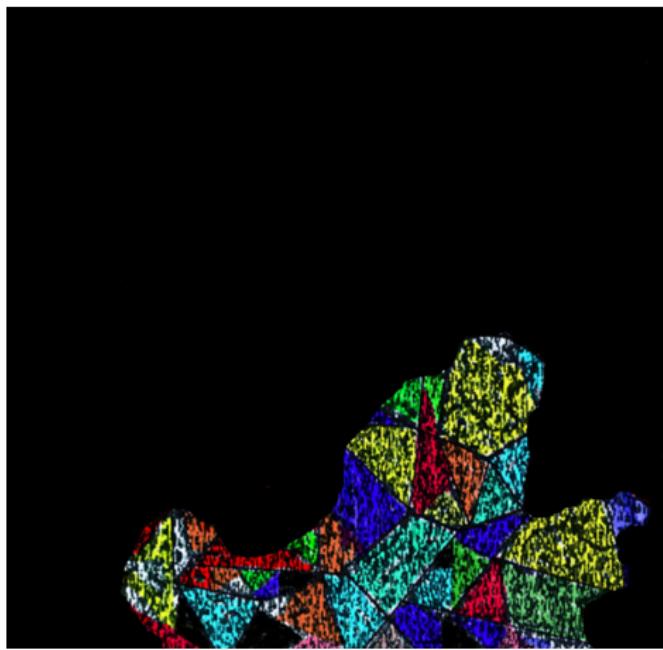


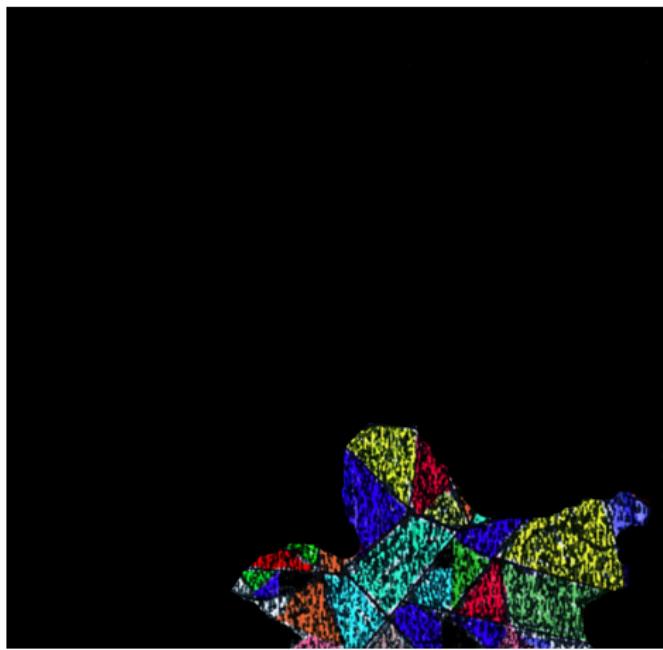


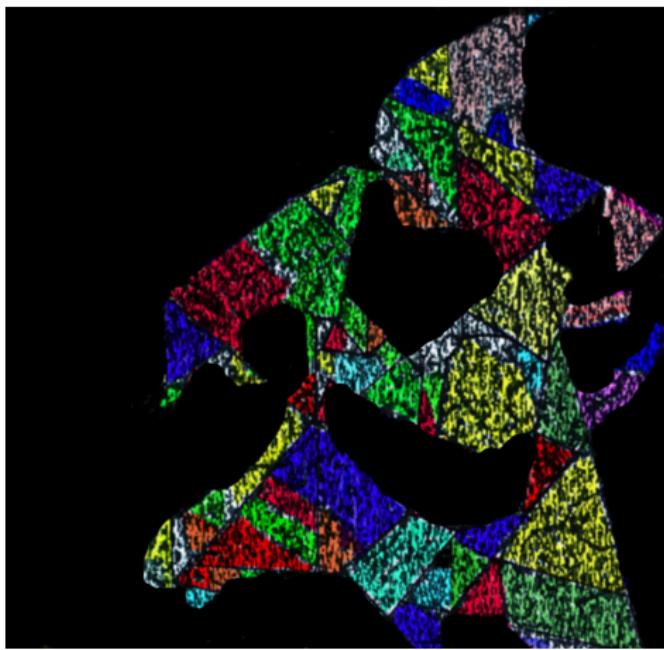


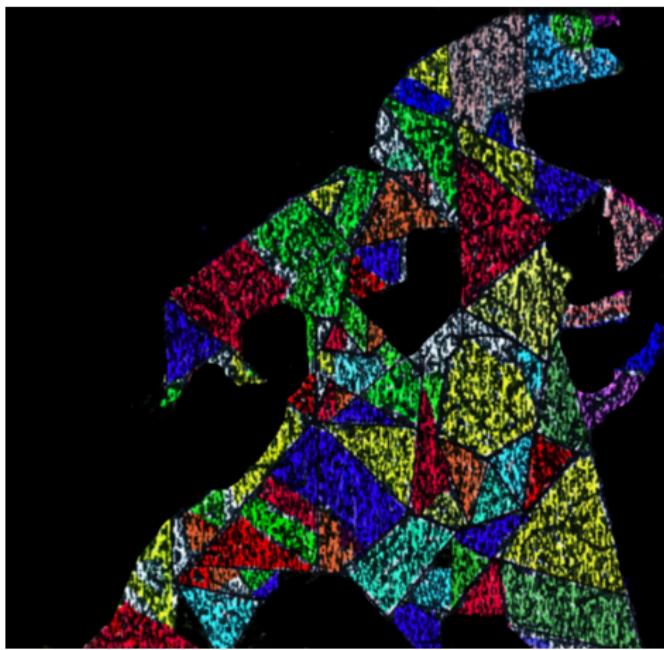


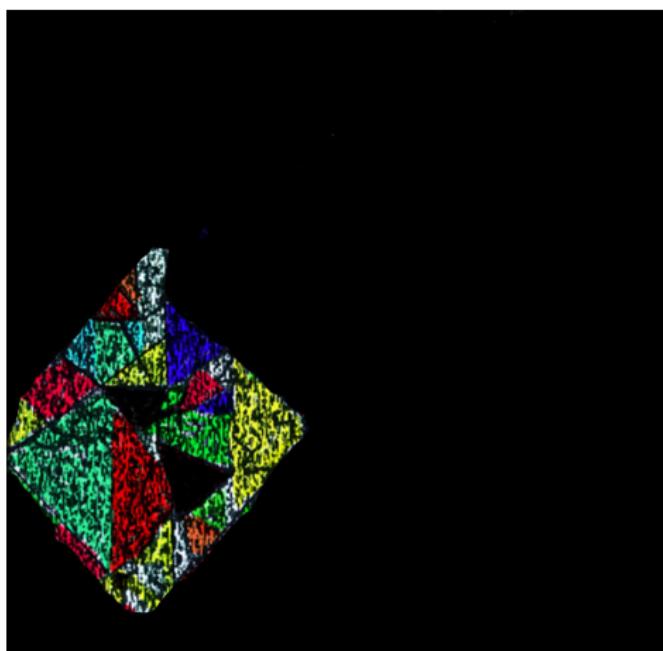


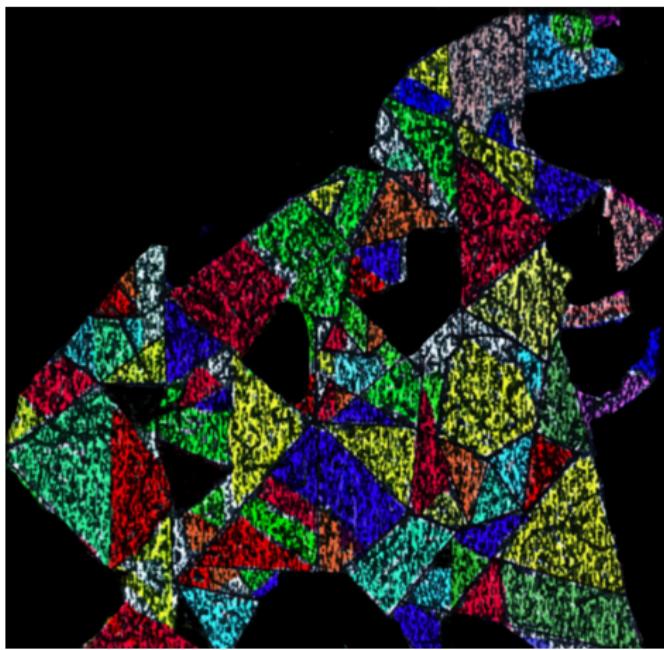


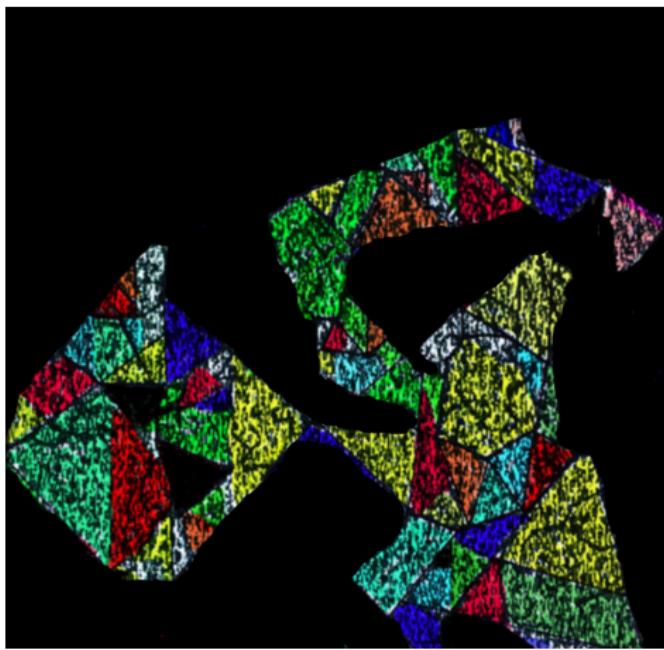


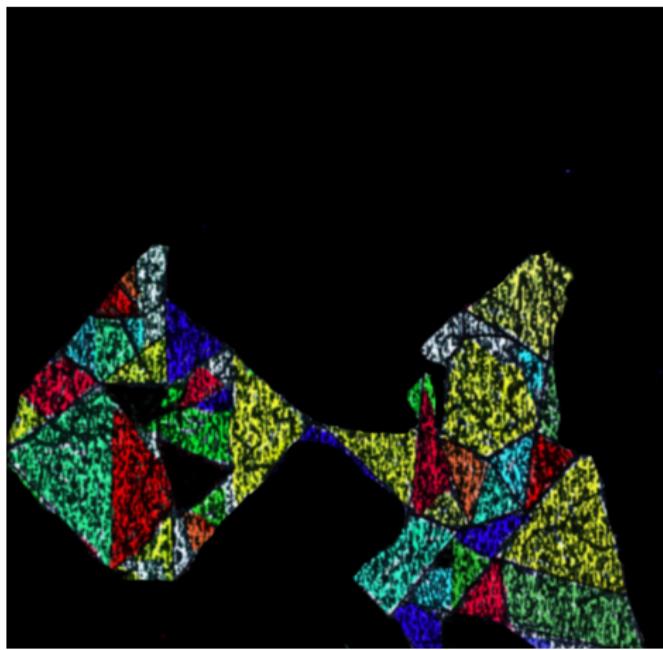


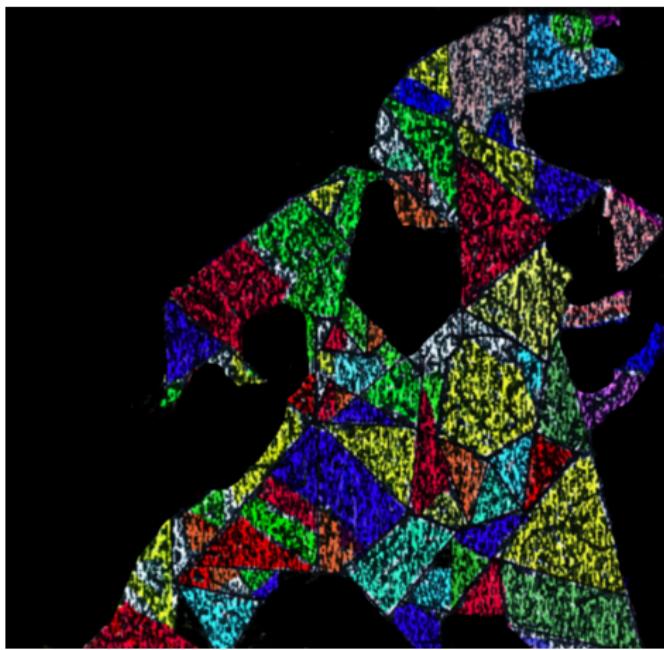




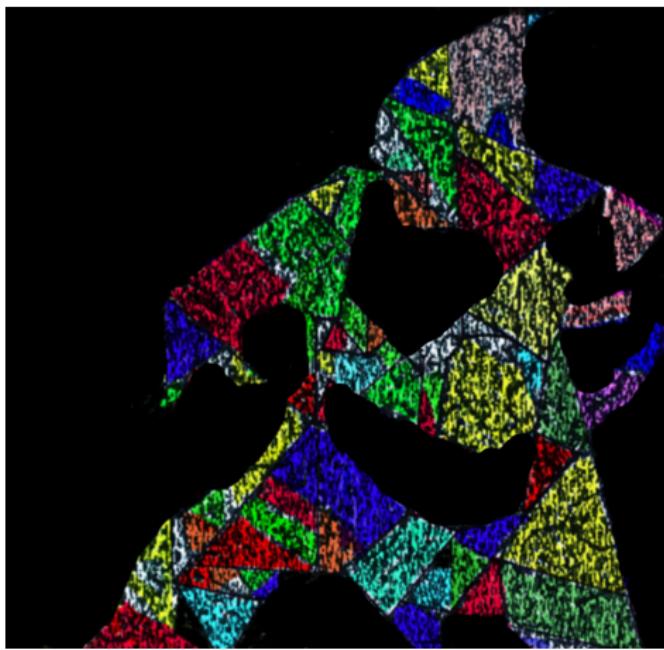


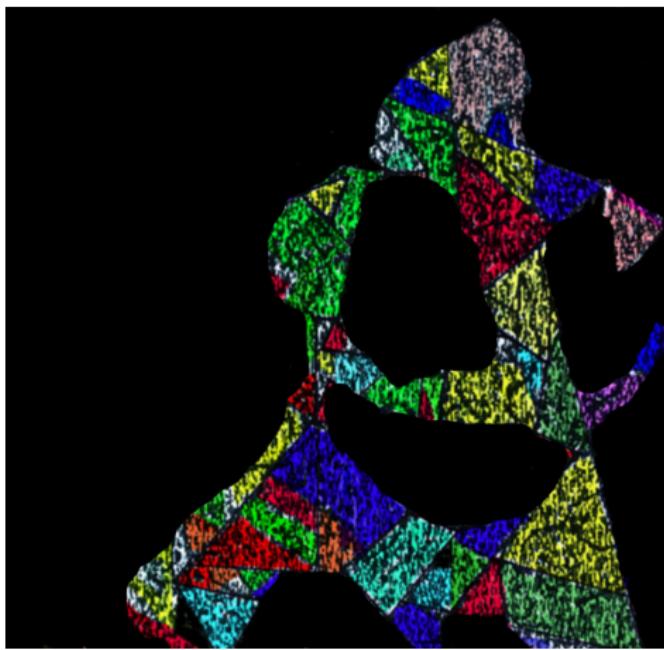


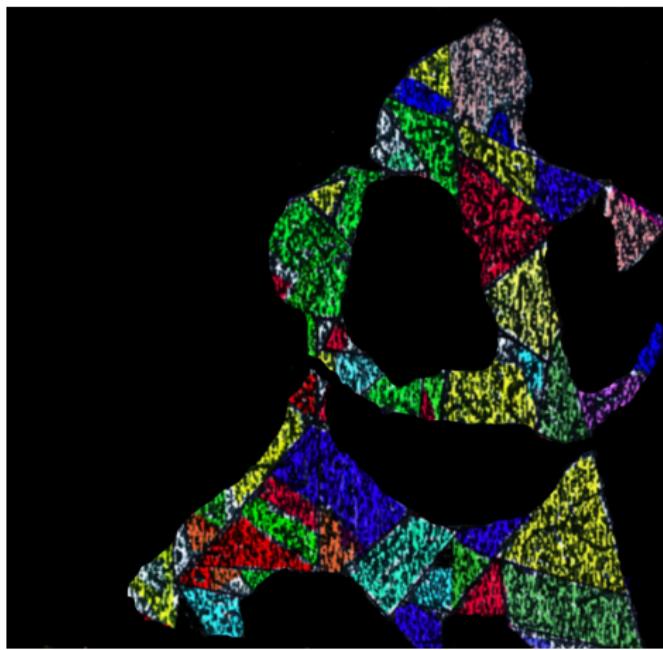


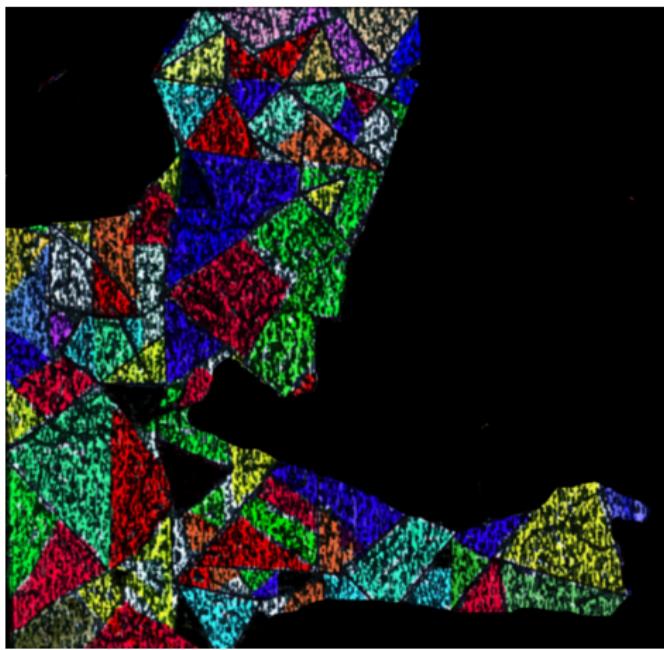


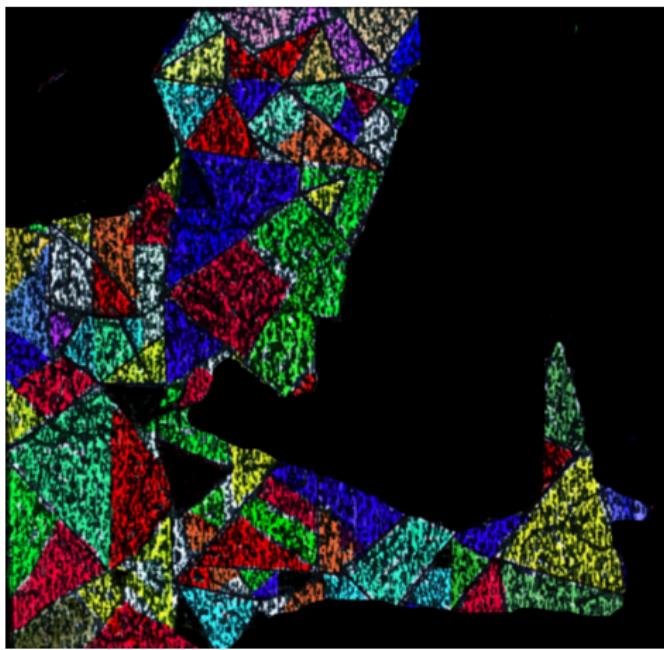


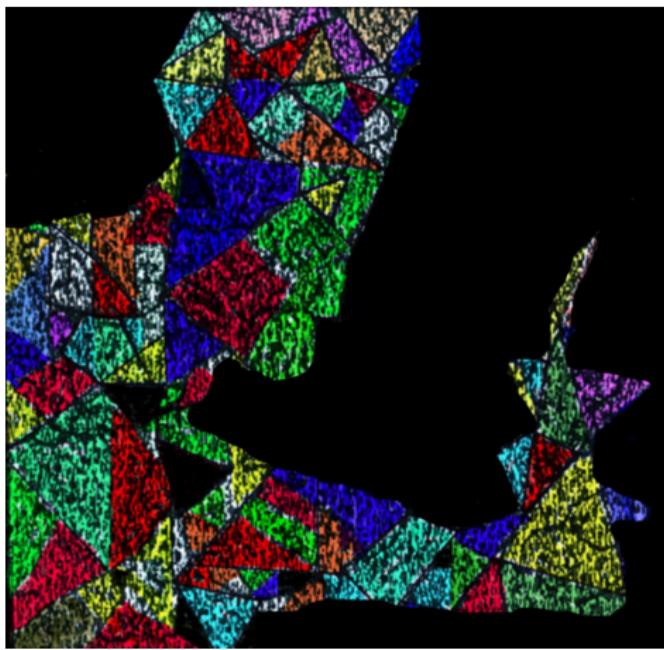


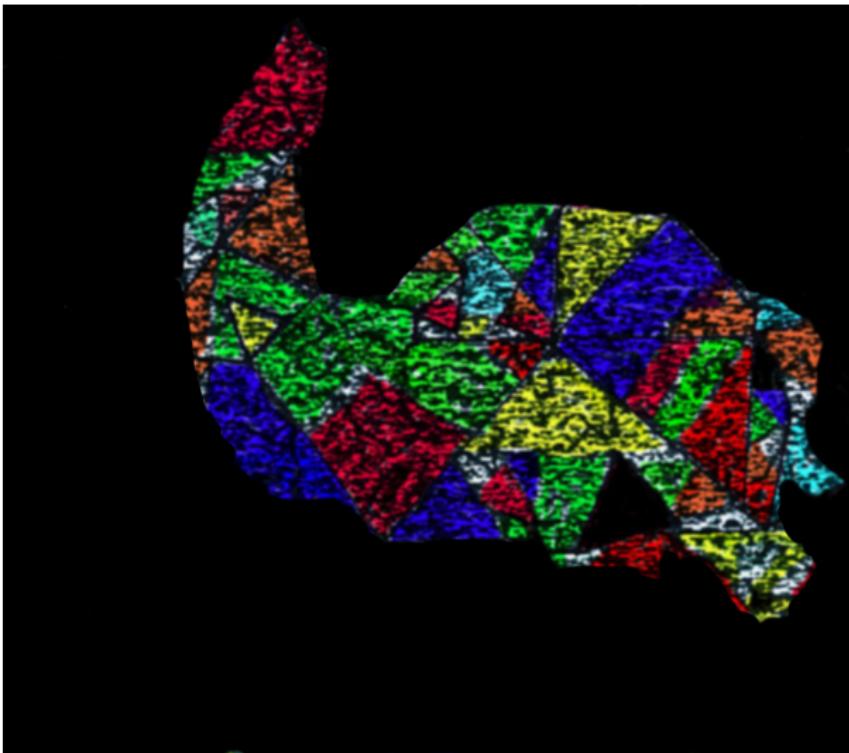


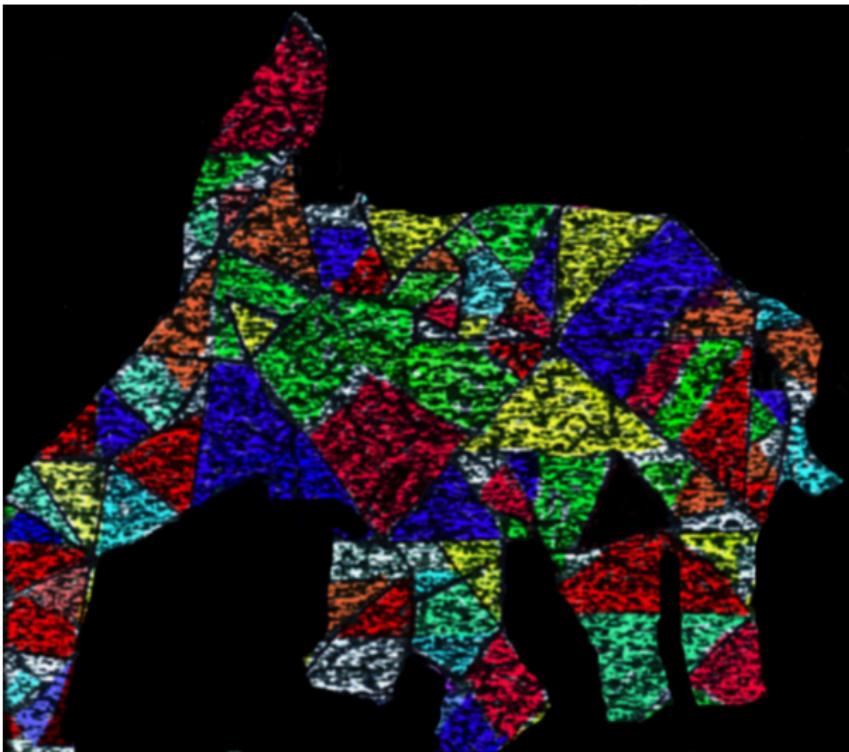


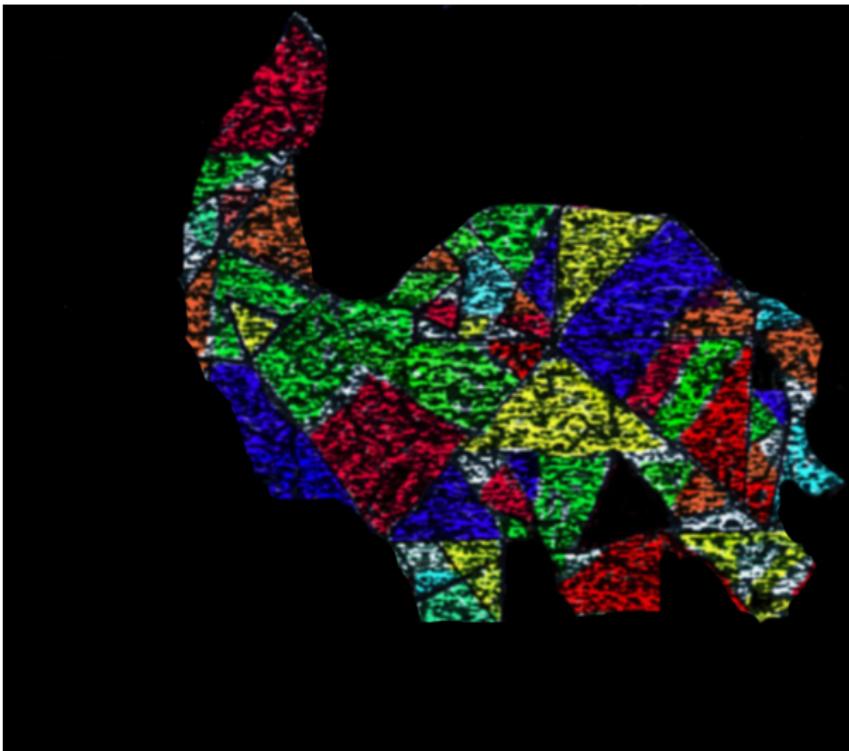


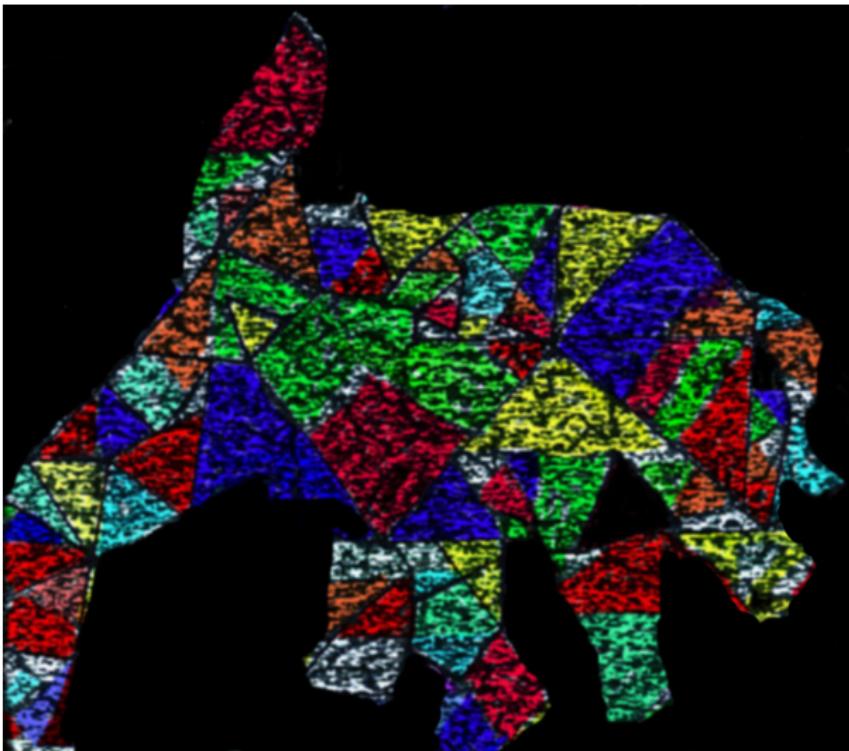


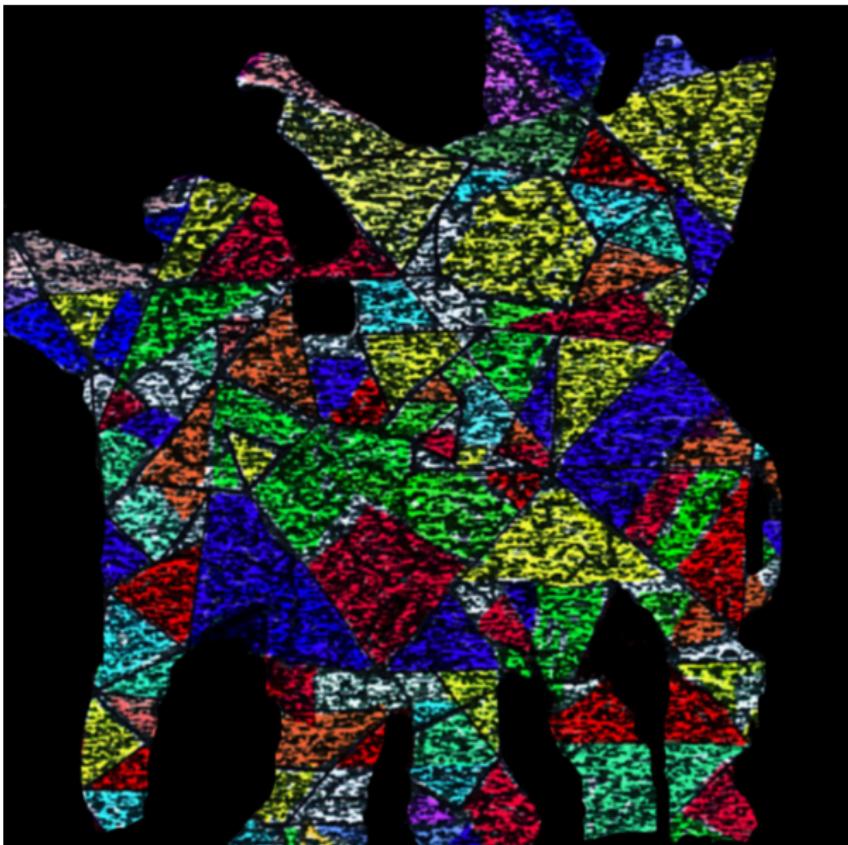






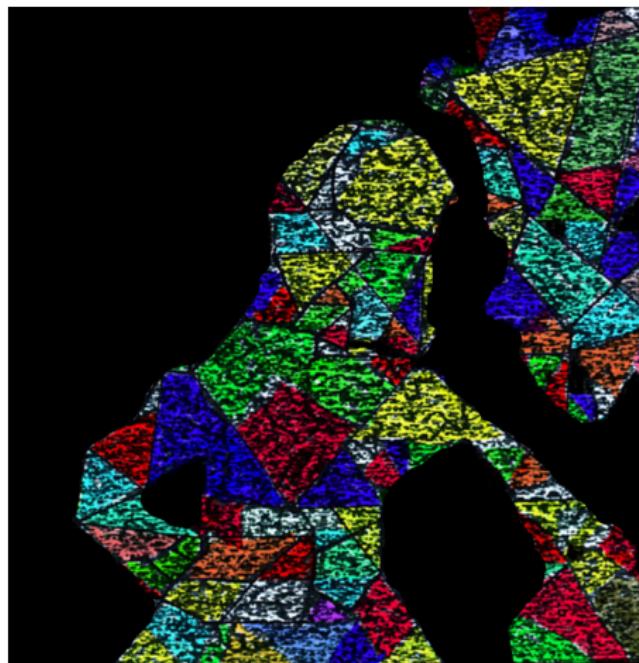


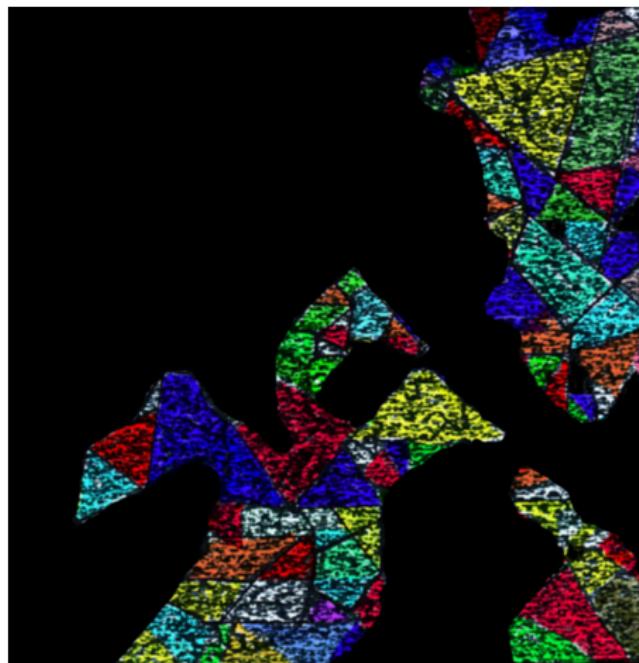


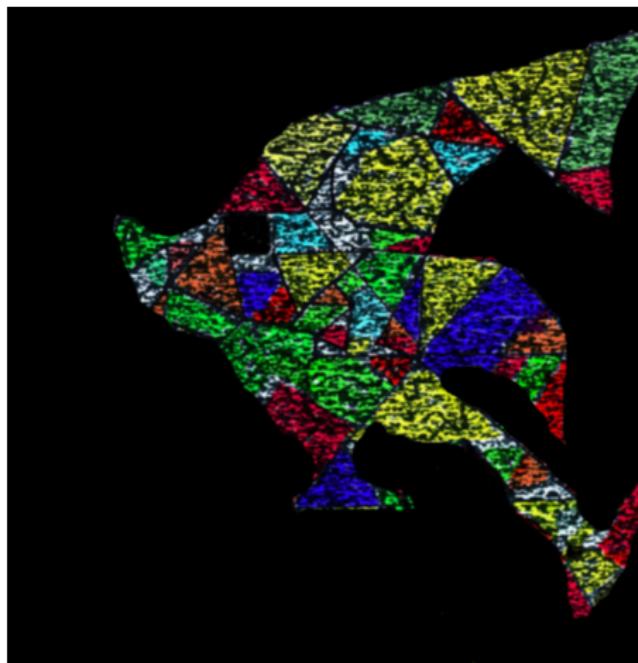


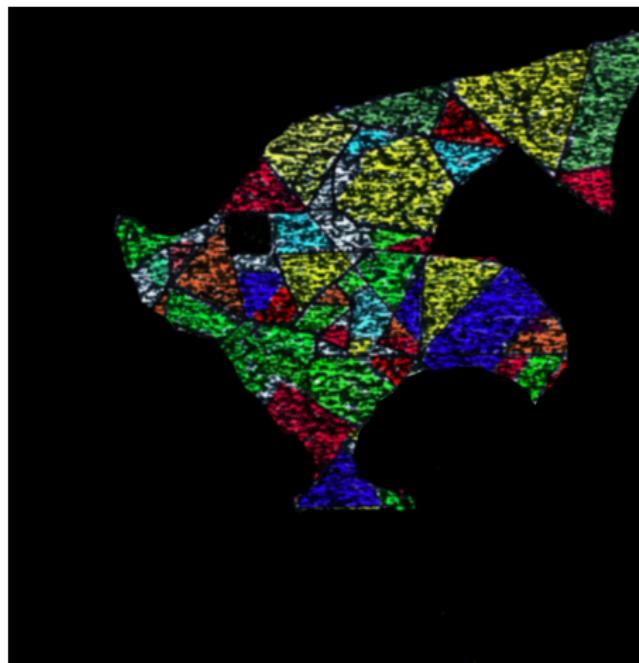


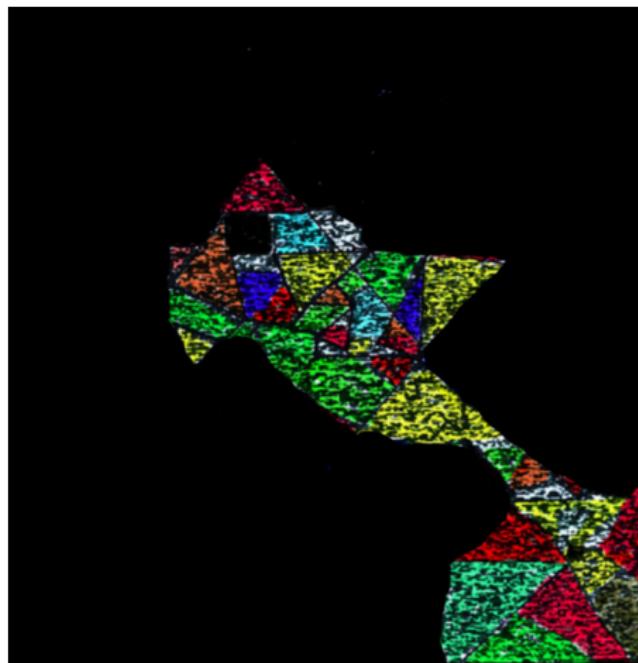


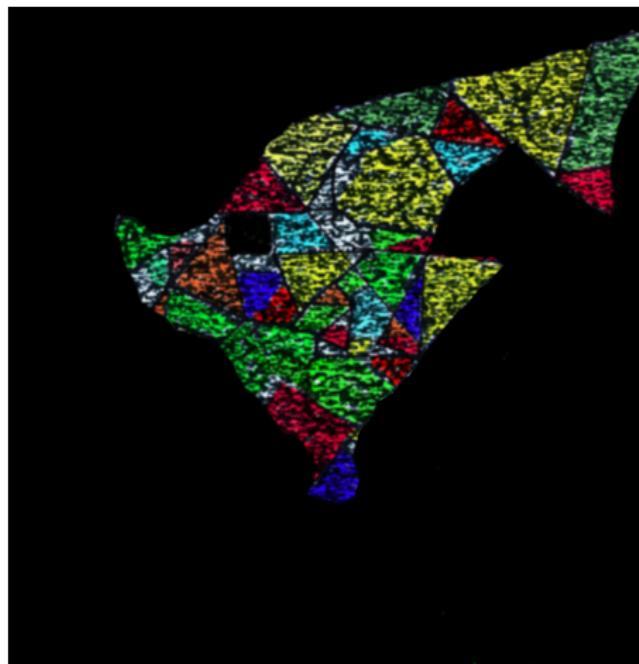


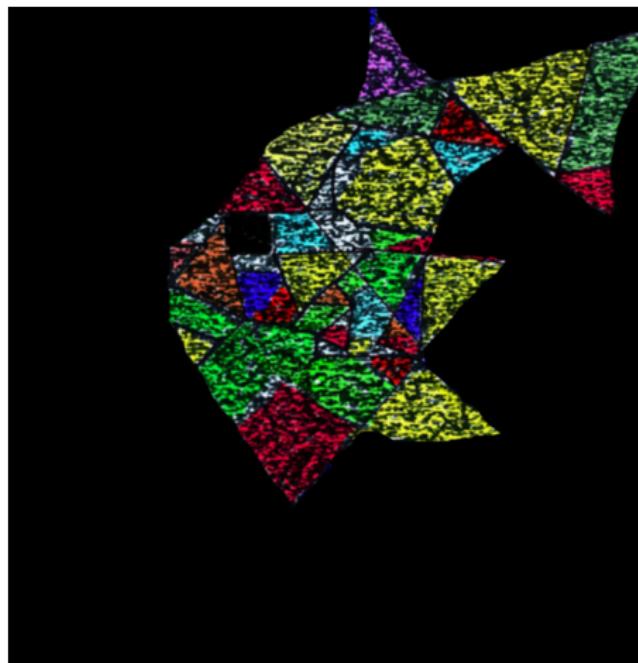


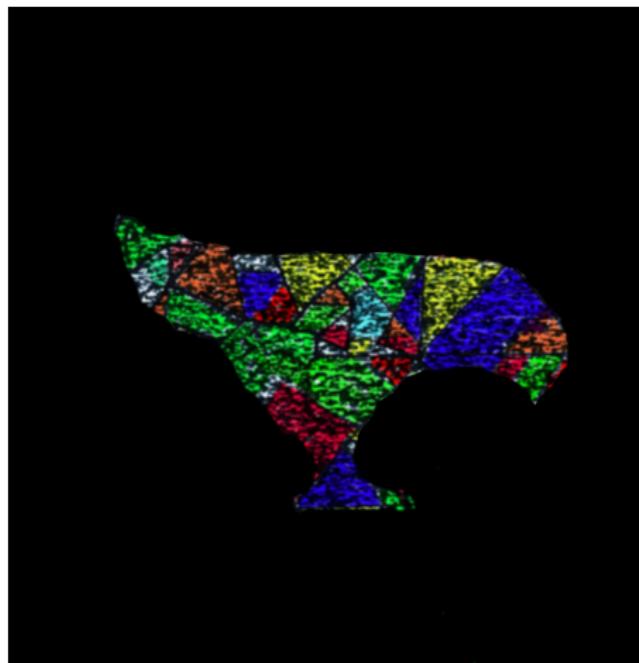


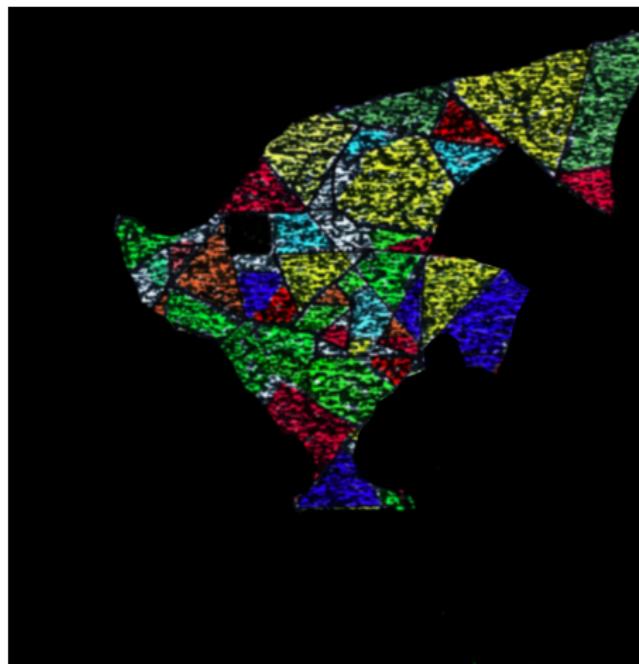


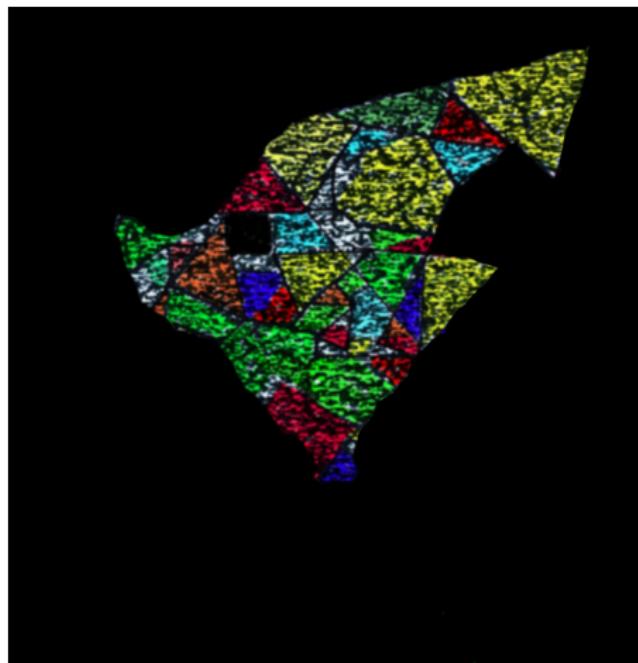


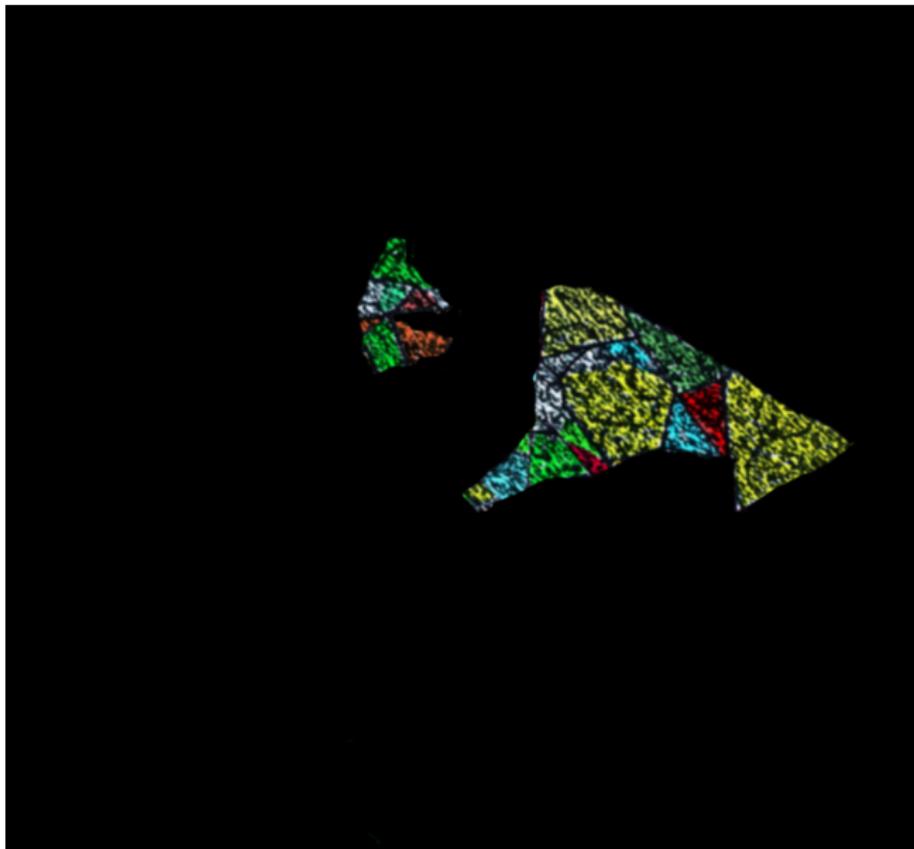












Criptografía, significa escritura secreta y se define como el estudio de todas las técnicas matemáticas relacionadas con aspectos de la seguridad de información, tales como la confidencialidad, integridad de datos, autenticación de identidad y autenticación del origen de datos.

Los principales metas que se persiguen al construir un sistema de seguridad son las siguientes :

- Confidencialidad,
- Integridad de los datos,
- Autenticación y autenticación del origen de los datos,
- No-rechazo.

Los principales metas que se persiguen al construir un sistema de seguridad son las siguientes :

- Confidencialidad,
- Integridad de los datos,
- Autenticación y autenticación del origen de los datos,
- No-rechazo.

Los principales metas que se persiguen al construir un sistema de seguridad son las siguientes :

- Confidencialidad,
- Integridad de los datos,
- Autenticación y autenticación del origen de los datos,
- No-rechazo.

Los principales metas que se persiguen al construir un sistema de seguridad son las siguientes :

- Confidencialidad,
- Integridad de los datos,
- Autenticación y autenticación del origen de los datos,
- No-rechazo.

La **confidencialidad** es un servicio usado para mantener el contenido de la información alejado de todo individuo que no posea una autorización.

La **Integridad** es un servicio que tiene como principal objetivo proteger los datos de una alteración no autorizada. Para asegurar la integridad de los datos, se debe tener la habilidad de detectar la manipulación de los datos por partes no autorizadas. La manipulación de los datos incluyen aspectos tales como la inserción, eliminación y sustitución de datos.

La autenticación es un servicio relacionado con la identificación. Esta función es aplicada tanto a las partes que están compartiendo una información como a la información misma. Una parte debe poderse identificar con la otra. La información entregada a través de un canal debe ser autenticada así como su procedencia, el origen de los datos, su contenido, el tiempo del envío de los datos, etc. La autenticación del origen de los datos asegura implícitamente la integridad de los datos.

No-rechazo, es un servicio que previene a una entidad de acciones de desconocimiento. Esto es, en el caso de que existan disputas debido a que ciertas acciones realizadas producen la negación de una entidad, es necesario tener los medios que las resuelvan. Por ejemplo, si una entidad da autorización a un agente de intermediación para comprar una propiedad y después tal autorización es negada se debe resolver la disputa por medio de un procedimiento que involucre una tercera parte.

Definición

Un sistema Criptográfico o Criptosistema S es una sextupla

$$(\mathcal{A}, \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}).$$

\mathcal{A} es el alfabeto de definición (ejemplo $\{0, 1\}$),

\mathcal{P} es un conjunto finito de textos en claro, el cual consta de listas finitas de elementos del alfabeto,

\mathcal{C} es un conjunto finito de textos cifrados (consta de listas finitas de un alfabeto no necesariamente \mathcal{A}),

\mathcal{K} es el conjunto o espacio finito de claves o llaves,

Definición

Un sistema Criptográfico o Criptosistema S es una sextupla

$$(\mathcal{A}, \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}).$$

\mathcal{A} es el alfabeto de definición (ejemplo $\{0, 1\}$),

\mathcal{P} es un conjunto finito de textos en claro, el cual consta de listas finitas de elementos del alfabeto,

\mathcal{C} es un conjunto finito de textos cifrados (consta de listas finitas de un alfabeto no necesariamente \mathcal{A}),

\mathcal{K} es el conjunto o espacio finito de claves o llaves,

Definición

Un sistema Criptográfico o Criptosistema S es una sextupla

$$(\mathcal{A}, \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}).$$

\mathcal{A} es el alfabeto de definición (ejemplo $\{0, 1\}$),

\mathcal{P} es un conjunto finito de textos en claro, el cual consta de listas finitas de elementos del alfabeto,

\mathcal{C} es un conjunto finito de textos cifrados (consta de listas finitas de un alfabeto no necesariamente \mathcal{A}),

\mathcal{K} es el conjunto o espacio finito de claves o llaves,

Definición

Un sistema Criptográfico o Criptosistema S es una sextupla

$$(\mathcal{A}, \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}).$$

\mathcal{A} es el alfabeto de definición (ejemplo $\{0, 1\}$),

\mathcal{P} es un conjunto finito de textos en claro, el cual consta de listas finitas de elementos del alfabeto,

\mathcal{C} es un conjunto finito de textos cifrados (consta de listas finitas de un alfabeto no necesariamente \mathcal{A}),

\mathcal{K} es el conjunto o espacio finito de claves o llaves,

Definición

Un sistema Criptográfico o Criptosistema S es una sextupla

$$(\mathcal{A}, \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}).$$

\mathcal{A} es el alfabeto de definición (ejemplo $\{0, 1\}$),

\mathcal{P} es un conjunto finito de textos en claro, el cual consta de listas finitas de elementos del alfabeto,

\mathcal{C} es un conjunto finito de textos cifrados (consta de listas finitas de un alfabeto no necesariamente \mathcal{A}),

\mathcal{K} es el conjunto o espacio finito de claves o llaves,

Definición

Un sistema Criptográfico o Criptosistema S es una sextupla

$$(\mathcal{A}, \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}).$$

\mathcal{A} es el alfabeto de definición (ejemplo $\{0, 1\}$),

\mathcal{P} es un conjunto finito de textos en claro, el cual consta de listas finitas de elementos del alfabeto,

\mathcal{C} es un conjunto finito de textos cifrados (consta de listas finitas de un alfabeto no necesariamente \mathcal{A}),

\mathcal{K} es el conjunto o espacio finito de claves o llaves,

Definición

Un sistema Criptográfico o Criptosistema S es una sextupla

$$(\mathcal{A}, \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}).$$

\mathcal{A} es el alfabeto de definición (ejemplo $\{0, 1\}$),

\mathcal{P} es un conjunto finito de textos en claro, el cual consta de listas finitas de elementos del alfabeto,

\mathcal{C} es un conjunto finito de textos cifrados (consta de listas finitas de un alfabeto no necesariamente \mathcal{A}),

\mathcal{K} es el conjunto o espacio finito de claves o llaves,

Reglas de ciframiento

Para $K \in \mathcal{K}$, existe una regla de ciframiento $e_K : \mathcal{P} \rightarrow \mathcal{C} \in \mathcal{E}$ y una correspondiente regla de desciframiento

$d_K : \mathcal{C} \rightarrow \mathcal{P} \in \mathcal{D}$, tales que

$$d_K(e_K(x)) = x, \text{ para todo texto en claro } x.$$

Reglas de ciframiento

Para $K \in \mathcal{K}$, existe una regla de ciframiento $e_K : \mathcal{P} \rightarrow \mathcal{C} \in \mathcal{E}$ y una correspondiente regla de desciframiento

$d_K : \mathcal{C} \rightarrow \mathcal{P} \in \mathcal{D}$, tales que

$$d_K(e_K(x)) = x, \text{ para todo texto en claro } x.$$

Reglas de ciframiento

Para $K \in \mathcal{K}$, existe una regla de ciframiento $e_K : \mathcal{P} \rightarrow \mathcal{C} \in \mathcal{E}$ y una correspondiente regla de desciframiento

$d_K : \mathcal{C} \rightarrow \mathcal{P} \in \mathcal{D}$, tales que

$$d_K(e_K(x)) = x, \text{ para todo texto en claro } x.$$

Reglas de ciframiento

Para $K \in \mathcal{K}$, existe una regla de ciframiento $e_K : \mathcal{P} \rightarrow \mathcal{C} \in \mathcal{E}$ y una correspondiente regla de desciframiento

$d_K : \mathcal{C} \rightarrow \mathcal{P} \in \mathcal{D}$, tales que

$$d_K(e_K(x)) = x, \text{ para todo texto en claro } x.$$

El cifrado por desplazamiento

Este cifrado es una generalización del cifrado Cesar. En este caso

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n, n \text{ fijo}$$

Para $K \in \mathbb{Z}_n$ se tiene que

$$e_k(x) = x + K \bmod n,$$

$$d_k(x) = x - K \bmod n.$$

El cifrado por desplazamiento

Este cifrado es una generalización del cifrado Cesar. En este caso

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n, n \text{ fijo}$$

Para $K \in \mathbb{Z}_n$ se tiene que

$$e_k(x) = x + K \bmod n,$$

$$d_k(x) = x - K \bmod n.$$

El cifrado por desplazamiento

Este cifrado es una generalización del cifrado Cesar. En este caso

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n, n \text{ fijo}$$

Para $K \in \mathbb{Z}_n$ se tiene que

$$e_k(x) = x + K \bmod n,$$

$$d_k(x) = x - K \bmod n.$$

El cifrado por desplazamiento

Este cifrado es una generalización del cifrado Cesar. En este caso

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n, n \text{ fijo}$$

Para $K \in \mathbb{Z}_n$ se tiene que

$$e_k(x) = x + K \bmod n,$$

$$d_k(x) = x - K \bmod n.$$

El cifrado por desplazamiento

Este cifrado es una generalización del cifrado Cesar. En este caso

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n, n \text{ fijo}$$

Para $K \in \mathbb{Z}_n$ se tiene que

$$e_k(x) = x + K \bmod n,$$

$$d_k(x) = x - K \bmod n.$$

El cifrado por desplazamiento

Este cifrado es una generalización del cifrado Cesar. En este caso

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n, n \text{ fijo}$$

Para $K \in \mathbb{Z}_n$ se tiene que

$$e_k(x) = x + K \bmod n,$$

$$d_k(x) = x - K \bmod n.$$

Ejemplo

Si $K = 11$ y $n = 26$, entonces el texto en claro

wewillmeetatmidnight

Se cifra convirtiendo el texto en una sucesión de enteros

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19.

Adicionamos 11 a cada valor para obtener

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4.

HPHTWWXPPELEXTOYTRSE es el texto cifrado.

Ejemplo

Si $K = 11$ y $n = 26$, entonces el texto en claro

wewillmeetatmidnight

Se cifra convirtiendo el texto en una sucesión de enteros

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19.

Adicionamos 11 a cada valor para obtener

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4.

HPHTWWXPPELEXTOYTRSE es el texto cifrado.

Ejemplo

Si $K = 11$ y $n = 26$, entonces el texto en claro

wewillmeetatmidnight

Se cifra convirtiendo el texto en una sucesión de enteros

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19.

Adicionamos 11 a cada valor para obtener

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4.

HPHTWWXPPELEXTOYTRSE es el texto cifrado.

Ejemplo

Si $K = 11$ y $n = 26$, entonces el texto en claro

wewillmeetatmidnight

Se cifra convirtiendo el texto en una sucesión de enteros

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19.

Adicionamos 11 a cada valor para obtener

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4.

HPHTWWXPPELEXTOYTRSE es el texto cifrado.

Ejemplo

Si $K = 11$ y $n = 26$, entonces el texto en claro

wewillmeetatmidnight

Se cifra convirtiendo el texto en una sucesión de enteros

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19.

Adicionamos 11 a cada valor para obtener

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4.

HPHTWWXPPELEXTOYTRSE es el texto cifrado.

Ejemplo

Si $K = 11$ y $n = 26$, entonces el texto en claro

wewillmeetatmidnight

Se cifra convirtiendo el texto en una sucesión de enteros

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19.

Adicionamos 11 a cada valor para obtener

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4.

HPHTWWXPPELEXTOYTRSE es el texto cifrado.

Ejemplo

Si $K = 11$ y $n = 26$, entonces el texto en claro

wewillmeetatmidnight

Se cifra convirtiendo el texto en una sucesión de enteros

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19.

Adicionamos 11 a cada valor para obtener

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4.

HPHTWWXPPELEXTOYTRSE es el texto cifrado.

El cifrado por desplazamiento se puede atacar haciendo una búsqueda exhaustiva de la clave, por ejemplo

JBCRCLQRWCRVNBJENBWRWN, puede ser descifrado haciendo

jbcrcrlqrwcrvnbjenbwrwn

iabqbkpqvbjqumaidmavqvm

hzapajopuaptlzhclzupul

gyzozinotzoskygbkytotk

fxynyhmnsynrjxfajxsnsj

ewxmxglmrxmqiweziwrmri

dvwlwfklqlphvdyhvqlqh

El cifrado por desplazamiento se puede atacar haciendo una búsqueda exhaustiva de la clave, por ejemplo

JBCRCLQRWCRVNBJENBWRWN, puede ser descifrado haciendo

jbcrcrlqrwcrvnbjenbwrwn

iabqbkpqvbqumaidmavqvm

hzapajopuaptlzhclzupul

gyzozinotzoskygbkytotk

fxynyhmnsynrjxfajxsnsj

ewxmxglmrxmqiweziwrmri

dvwlwfklqlphvdyhvqlqh

El cifrado por desplazamiento se puede atacar haciendo una búsqueda exhaustiva de la clave, por ejemplo

JBCRCLQRWCRVNBJENBWRWN, puede ser descifrado haciendo

jbcrcrlqrwcrvnbjenbwrwn

iabqbkpqvbjqumaidmavqvm

hzapajopuaptlzhclzupul

gyzozinotzoskygbkytotk

fxynyhmnsynrjxfajxsnsj

ewxmxglmrxmqiweziwrmri

dvwlwfklqlphvdyhvqlqh

El cifrado por desplazamiento se puede atacar haciendo una búsqueda exhaustiva de la clave, por ejemplo

JBCRCLQRWCRVNBJENBWRWN, puede ser descifrado haciendo

jbcrcrlqrwcrvnbjenbwrwn

iabqbkpqvbqumaidmavqvm

hzapajopuaptlzhclzupul

gyzozinotzoskygbkytotk

fxynyhmnsynrjxfajxsnsj

ewxmxglmrxmqiweziwrmri

dvwlwfklqlphvdyhvqlqh

El cifrado por desplazamiento se puede atacar haciendo una búsqueda exhaustiva de la clave, por ejemplo

JBCRCLQRWCRVNBJENBWRWN, puede ser descifrado haciendo

jbcrcrlqrwcrvnbjenbwrwn

iabqbkpqvbqumaidmavqvm

hzapajopuaptlzhclzupul

gyzozinotzoskygbkytotk

fxynyhmnsynrjxfajxsnsj

ewxmxglmrxmqiweziwrmri

dvwlwfklqlphvdyhvqlqh

El cifrado por desplazamiento se puede atacar haciendo una búsqueda exhaustiva de la clave, por ejemplo

JBCRCLQRWCRVNBJENBWRWN, puede ser descifrado haciendo

jbcrcrlqrwcrvnbjenbwrwn

iabqbkpqvbqumaidmavqvm

hzapajopuaptlzhclzupul

gyzozinotzoskygbkytotk

fxynyhmnsynrjxfajxsnsj

ewxmxglmrxmqiweziwrmri

dvwlwfklqlphvdyhvqlqh

El cifrado por desplazamiento se puede atacar haciendo una búsqueda exhaustiva de la clave, por ejemplo

JBCRCLQRWCRVNBJENBWRWN, puede ser descifrado haciendo

jbcrcrlqrwcrvnbjenbwrwn

iabqbkpqvbqumaidmavqvm

hzapajopuaptlzhclzupul

gyzozinotzoskygbkytotk

fxynyhmnsynrjxfajxsnsj

ewxmxglmrxmlqiweziwrmri

dvwlwfklqlphvdyhvqlqh

El cifrado por desplazamiento se puede atacar haciendo una búsqueda exhaustiva de la clave, por ejemplo

JBCRCLQRWCRVNBJENBWRWN, puede ser descifrado haciendo

jbcrcrlqrwcrvnbjenbwrwn

iabqbkpqvbqumaidmavqvm

hzapajopuaptlzhclzupul

gyzozinotzoskygbkytotk

fxynyhmnsynrjxfajxsnsj

ewxmxglmrxmqiweziwrmri

dvwlwfklqlphvdyhvqlqh

El cifrado por desplazamiento se puede atacar haciendo una búsqueda exhaustiva de la clave, por ejemplo

JBCRCLQRWCRVNBJENBWRWN, puede ser descifrado haciendo

jbcrcrlqrwcrvnbjenbwrwn

iabqbkpqvbqumaidmavqvm

hzapajopuaptlzhclzupul

gyzozinotzoskygbkytotk

fxynyhmnsynrjxfajxsnsj

ewxmxglmrxmqiweziwrmri

dvwlwfklqlphvdyhvqlqh

El cifrado por desplazamiento se puede atacar haciendo una búsqueda exhaustiva de la clave, por ejemplo

JBCRCLQRWCRVNBJENBWRWN, puede ser descifrado haciendo

jbcrcrlqrwcrvnbjenbwrwn

iabqbkpqvbqumaidmavqvm

hzapajopuaptlzhclzupul

gyzozinotzoskygbkytotk

fxynyhmnsynrjxfajxsnsj

ewxmxglmrxmqiweziwrmri

dvwlwfklqlphvdyhvqlqh

cuvkvejkpvkogucxgupkpg

btujudijoujnftbwftojf

astitchintimesavesnine

cuvkvejkpvkogucxgupkpg

btujudijoujnftbwftojf

astitchintimesavesnine

cuvkvejkpvkogucxgupkpg

btujudijoujnftbwftojf

astitchintimesavesnine

En esta sección describiremos las rutinas-MatLab que nos permitirán hacer un ataque eficiente al sistema de desplazamiento.

En principio debemos definir el alfabeto, en nuestro caso:

$$L = \{A, B, C, D, \dots, Z\}.$$

```
>> abet = 'ABCDEFGHIJKLMNPQRSTUVWXYZ'
```

Podemos verificar la asignación realizada a cada letra en este alfabeto, evaluando la función en ella;

```
>> abet(3)
```

```
ans =
```

```
C
```

En principio debemos definir el alfabeto, en nuestro caso:

$$L = \{A, B, C, D, \dots, Z\}.$$

```
>> abet = 'ABCDEFGHIJKLMNPQRSTUVWXYZ'
```

Podemos verificar la asignación realizada a cada letra en este alfabeto, evaluando la función en ella;

```
>> abet(3)
```

```
ans =
```

```
C
```

En principio debemos definir el alfabeto, en nuestro caso:

$$L = \{A, B, C, D, \dots, Z\}.$$

```
>> abet = 'ABCDEFGHIJKLMNPQRSTUVWXYZ'
```

Podemos verificar la asignación realizada a cada letra en este alfabeto, evaluando la función en ella;

```
>> abet(3)
```

ans =

C

En principio debemos definir el alfabeto, en nuestro caso:

$$L = \{A, B, C, D, \dots, Z\}.$$

```
>> abet = 'ABCDEFGHIJKLMNPQRSTUVWXYZ'
```

Podemos verificar la asignación realizada a cada letra en este alfabeto, evaluando la función en ella;

```
>> abet(3)
```

ans =

C

Ahora debemos hacer una asignación del tipo

$$A \rightarrow 0, \quad B \rightarrow 1, \quad C \rightarrow 2 \dots Z \rightarrow 25.$$

definiendo la función;

```
>> letters = @(x) abet(x + 1);
```

Tal definición puede ser verificada realizando el cálculo:

```
>> letters(2)
```

```
ans =
```

```
C
```

Ahora debemos hacer una asignación del tipo

$$A \rightarrow 0, \quad B \rightarrow 1, \quad C \rightarrow 2 \dots Z \rightarrow 25.$$

definiendo la función;

```
>> letters = @(x) abet(x + 1);
```

Tal definición puede ser verificada realizando el cálculo:

```
>> letters(2)
```

```
ans =
```

```
C
```

Ahora debemos hacer una asignación del tipo

$$A \rightarrow 0, \quad B \rightarrow 1, \quad C \rightarrow 2 \dots Z \rightarrow 25.$$

definiendo la función;

```
>> letters = @(x) abet(x + 1);
```

Tal definición puede ser verificada realizando el cálculo:

```
>> letters(2)
```

```
ans =
```

```
C
```

Ahora debemos hacer una asignación del tipo

$$A \rightarrow 0, \quad B \rightarrow 1, \quad C \rightarrow 2 \dots Z \rightarrow 25.$$

definiendo la función;

```
>> letters = @(x) abet(x + 1);
```

Tal definición puede ser verificada realizando el cálculo:

```
>> letters(2)
```

```
ans =
```

```
C
```

La función MatLab, **Itable**, realiza la acción inversa, por ejemplo;

```
>> Itable('C')
```

```
ans =
```

```
2
```

La función MatLab, **Itable**, realiza la acción inversa, por ejemplo;

```
>> Itable('C')
```

```
ans =
```

```
2
```

Veamos ahora como MatLab realiza un ciframiento por desplazamiento:

Elijamos el mensaje a cifrar, por ejemplo

```
>> message = 'ATTACK AT DAWN'
```

```
message =
```

```
ATTACK AT DAWN
```

Veamos ahora como MatLab realiza un ciframiento por desplazamiento:

Elijamos el mensaje a cifrar, por ejemplo

```
>> message = 'ATTACK AT DAWN'
```

```
message =
```

```
ATTACK AT DAWN
```

La función MatLab **findstr** elimina los espacios que hay entre palabras, de la siguiente forma:

```
>> message(findstr(message, ' ')) = []
```

```
message =
```

```
ATTACKATDAWN
```

La función MatLab **findstr** elimina los espacios que hay entre palabras, de la siguiente forma:

```
>> message(findstr(message, ' ')) = []
```

```
message =
```

```
ATTACKATDAWN
```

Ahora usamos la función MatLab **Itable** para convertir los caracteres del mensaje en números enteros, de la siguiente forma:

```
>> ptext = Itable(message)
```

```
ptext =  0  19  19  0  2  10  0  19  3  0  22  13
```

Ahora usamos la función MatLab **Itable** para convertir los caracteres del mensaje en números enteros, de la siguiente forma:

```
>> ptext = Itable(message)
```

```
ptext =  0  19  19  0  2  10  0  19  3  0  22  13
```

La siguiente función, nos permitirá realizar un cifrado del tipo $x + b \text{ mód } 26$;

```
>> f = @(x, b) mod(x + b, 26);
```

Por ejemplo si queremos encriptar el mensaje ATTACK AT DAWN usando 17 como clave, debemos realizar la siguiente instrucción:

```
>> ctext = f(ptext, 17)
```

```
ctext = 17 10 10 17 19 1 17 10 20 17 13 4
```

La siguiente función, nos permitirá realizar un cifrado del tipo $x + b \text{ mód } 26$;

```
>> f = @(x, b) mod(x + b, 26);
```

Por ejemplo si queremos encriptar el mensaje ATTACK AT DAWN usando 17 como clave, debemos realizar la siguiente instrucción:

```
>> ctext = f(ptext, 17)
```

```
ctext = 17 10 10 17 19 1 17 10 20 17 13 4
```

La siguiente función, nos permitirá realizar un cifrado del tipo $x + b \text{ mód } 26$;

```
>> f = @(x, b) mod(x + b, 26);
```

Por ejemplo si queremos encriptar el mensaje ATTACK AT DAWN usando 17 como clave, debemos realizar la siguiente instrucción:

```
>> ctext = f(ptext, 17)
```

```
ctext = 17 10 10 17 19 1 17 10 20 17 13 4
```

La siguiente función, nos permitirá realizar un cifrado del tipo $x + b \text{ mód } 26$;

```
>> f = @(x, b) mod(x + b, 26);
```

Por ejemplo si queremos encriptar el mensaje ATTACK AT DAWN usando 17 como clave, debemos realizar la siguiente instrucción:

```
>> ctext = f(ptext, 17)
```

```
ctext = 17 10 10 17 19 1 17 10 20 17 13 4
```

Ahora convertimos la secuencia numérica en un mensaje cifrado, mediante la siguiente instrucción:

```
>> ctext = letters(ctext)
```

```
ctext =
```

```
RKKRTBRKURNE
```

Ahora convertimos la secuencia numérica en un mensaje cifrado, mediante la siguiente instrucción:

```
>> ctext = letters(ctext)
```

```
ctext =
```

```
RKKRTBRKURNE
```

Para descifrar el mensaje, lo primero que debemos hacer es convertir el texto en una secuencia numérica:

```
>> ctext = ltable(ctext)
```

```
ctext = 17 10 10 17 19 1 17 10 20 17 13 4
```

calculamos la operación inversa para realizar una secuencia numérica descifrada:

```
>> ptext = f(ctext,-17)
```

```
ptext = 0 19 19 0 2 10 0 19 3 0 22 13 el texto  
claro o plano se puede recuperar via la función letters:
```

```
>> ptext = letters(ptext)
```

ptext = ATTACKATDAWN

Para descifrar el mensaje, lo primero que debemos hacer es convertir el texto en una secuencia numérica:

```
>> ctext = ltable(ctext)
```

```
ctext = 17 10 10 17 19 1 17 10 20 17 13 4
```

calculamos la operación inversa para realizar una secuencia numérica descifrada:

```
>> ptext = f(ctext,-17)
```

```
ptext = 0 19 19 0 2 10 0 19 3 0 22 13 el texto  
claro o plano se puede recuperar via la función letters:
```

```
>> ptext = letters(ptext)
```

```
ptext = ATTACKATDAWN
```

Para descifrar el mensaje, lo primero que debemos hacer es convertir el texto en una secuencia numérica:

```
>> ctext = ltable(ctext)
```

```
ctext = 17 10 10 17 19 1 17 10 20 17 13 4
```

calculamos la operación inversa para realizar una secuencia numérica descifrada:

```
>> ptext = f(ctext,-17)
```

```
ptext = 0 19 19 0 2 10 0 19 3 0 22 13 el texto  
claro o plano se puede recuperar via la función letters:
```

```
>> ptext = letters(ptext)
```

ptext = ATTACKATDAWN

Para descifrar el mensaje, lo primero que debemos hacer es convertir el texto en una secuencia numérica:

```
>> ctext = ltable(ctext)
```

```
ctext = 17 10 10 17 19 1 17 10 20 17 13 4
```

calculamos la operación inversa para realizar una secuencia numérica descifrada:

```
>> ptext = f(ctext,-17)
```

```
ptext = 0 19 19 0 2 10 0 19 3 0 22 13 el texto  
claro o plano se puede recuperar via la función letters:
```

```
>> ptext = letters(ptext)
```

ptext = ATTACKATDAWN

Para realizar el ataque aun texto cifrado obtenido con este sistema, por ejemplos si le capturamos a nuestro enemigo el texto;
LYHXYTPIOMUNGXCXHCABN

Actuamos usando MatLab de la siguiente forma:

```
>> ctext = 'LYHXYTPIOMUNGXCXHCABN';
```

```
>> ctext = ltable(ctext)
```

```
ctext =
```

11	24	7	23	24	19	15	8	14	12	20	13	6	2	23	7
2	0	1	13												

Para realizar el ataque aun texto cifrado obtenido con este sistema, por ejemplos si le capturamos a nuestro enemigo el texto;
LYHXYTPIOMUNGXCXHCABN

Actuamos usando MatLab de la siguiente forma:

```
>> ctext = 'LYHXYTPIOMUNGXCXHCABN';
```

```
>> ctext = ltable(ctext)
```

```
ctext =
```

11	24	7	23	24	19	15	8	14	12	20	13	6	2	23	7
2	0	1	13												

Para realizar el ataque aun texto cifrado obtenido con este sistema, por ejemplos si le capturamos a nuestro enemigo el texto;
LYHXYTPIOMUNGXCXHCABN

Actuamos usando MatLab de la siguiente forma:

```
>> ctext = 'LYHXYTPIOMUNGXCXHCABN';
```

```
>> ctext = ltable(ctext)
```

```
ctext =
```

11	24	7	23	24	19	15	8	14	12	20	13	6	2	23	7
2	0	1	13												

El siguiente ciclo del tipo **for** generará todos los posibles textos planos:

```
>> for b = 0 : 25
    ptext = f(ctext, -b);
    ptext = letters(ptext)
    fprintf('·/· s · / · 2 · 0 f · / · s \n', 'b = ', b, ptext)
end
```

El siguiente ciclo del tipo **for** generará todos los posibles textos planos:

```
>> for b = 0 : 25
    ptext = f(ctext, -b);
    ptext = letters(ptext)
    fprintf('·/·s · / · 2 · 0f · / · s \n', 'b = ', b, ptext)
end
```

- $b = 0$ LYHXYTPIOMUNGXCXHCABN
 $b = 1$ KXGWXSOHNLTMFNBWGBZAM
 $b = 2$ JWFVWRNGMKSLEAVFAYZL
 $b = 3$ IVEUVQMFLJRKDZUEZXYK
 $b = 4$ HUDETUPLEKIQJCYTDYWXJ
 $b = 5$ GTCSTOKDJHPIBXSCXVWI
 $b = 6$ FSBRSNJCIGOHAWRBWUVH (1)
 $b = 7$ ERAQRMIHFNGZVQAVTUG
 $b = 8$ DQZPQLHAGEMFYUPZUSTF
 $b = 9$ CPYOPKGZFDLEXTOYTRSE
 $b = 10$ BOXNOJFYECKDWSNXSQRD
 $b = 11$ ANWMNIEXDBJCVRMWRPQC
 $b = 12$ ZMVLMHDWCAIBUQLVQOPB

- $b = 13$ YLUKLGCVBZHATPKUPNOA
 $b = 14$ XKTJKFBUAYGZSOJTMNZ
 $b = 15$ WJSIJEATZXFYRNISNLMY
 $b = 16$ VIRHIDZSYWEXQMHRMKLX
 $b = 17$ UHQGHCYRXVDWPLGQLJKW
 $b = 18$ TGPFGBXQWUCVOKFPKIJV
 $b = 19$ SFOEFAWPVTBUNJEJOJHIU (2)
 $b = 20$ RENDEZVOUSATMIDNIGHT
 $b = 21$ QDMCDYUNTRZSLHCMHFGS
 $b = 22$ PCLBCXTMSQYRKGBLGEFR
 $b = 23$ OBKABWSLRPXQJFAKFDEQ
 $b = 24$ NAJZAVRKQOWPIEZJECDP
 $b = 25$ MZIYZUQJPNVVOHDYIDBCO