




Taller 2 - Blockchain


1. Crear el formulario php:

dd/mm/aaaa --:--


Banco Davivienda

Cuenta Origen

Ahorros

Banco Davivienda

Cuenta Destino

Ahorros

Numero Identificación

Valor Transacción

Identificador Transacción (CUS)

Descripción

Crear Transacción

```

<div class="container p-4">
  <div class="row">
    <div class="col-md-4">

      <?php if (isset($_SESSION['message'])) { ?>
        <div class="alert alert-<?= $_SESSION['message_type']; ?> alert-dismissible fade show" role="ale
          <?= $_SESSION['message'] ?>
          <button type="button" class="btn-close" data-bs-dismiss="alert" aria-label="Close"></button>
        </div>/.alert.alert-<?= $_SESSION['message_type']; ?>.alert-dismissible.fade.show
      <?php session_unset();
    } ?>

    <div class="card card-body">
      <form action="save_tx.php" method="POST">
        <div class="form-group m-2">
          <input type="datetime-local" name="fecha-hora" class="form-control" placeholder="Fecha -
            autofocus>/form-control
          </div>/form-group.m-2
        <div class="form-group m-2">
          <select class="form-select" aria-label="Default select example" name="banco_origen">
            <option selected>Banco Davivienda</option>
            <option value="1">Bancolombia</option>
            <option value="2">Banco BBVA</option>
            <option value="3">Banco Falabella</option>
            <option value="4">Banco Caja Social</option>
          </select>/form-select
        </div>/form-group.m-2

        <div class="form-group m-2">
          <input type="number" name="cuenta_origen" class="form-control" placeholder="Cuenta Origen
            autofocus>/form-control
          </div>/form-group.m-2

        <div class="form-group m-2">
          <select class="form-select" aria-label="Default select example" name="tipo_cuenta_origen">
            <option selected>Ahorros</option>
            <option value="1">Corriente</option>
          </select>/form-select
        </div>/form-group.m-2

        <div class="form-group m-2">
          <select class="form-select" aria-label="Default select example" name="banco_destino">
            <option selected>Banco Davivienda</option>

```

Una vez creado el formulario con php, html y bootstrap 5 procedemos a crear el archivo donde ira toda la lógica del formulario para insertar la información en la base de datos

2. Inserción de transacciones en la base de datos:

```
taller_2_blockchain > save_tx.php > ...
3 include('db.php');
4
5 if (isset($_POST['save_tx'])) {
6     $fecha_hora = $_POST['fecha-hora'];
7     $banco_origen = $_POST['banco_origen'];
8     $cuenta_origen = $_POST['cuenta_origen'];
9     $tipo_cuenta_origen = $_POST['tipo_cuenta_origen'];
10    $banco_destino = $_POST['banco_destino'];
11    $cuenta_destino = $_POST['cuenta_destino'];
12    $tipo_cuenta_destino = $_POST['tipo_cuenta_destino'];
13    $numero_identificacion = $_POST['numero_identificacion'];
14    $valor_transaccion = $_POST['valor_transaccion'];
15    $cus = $_POST['CUS'];
16    $descripcion = $_POST['descripcion'];
17    $transaccion = $fecha_hora + $cuenta_origen + $cuenta_destino + $numero_identificacion + $valor_transaccion + $cus;
18
19    $start_time_cbc = microtime(true);
20    $CBC = encrypt_decrypt_cbc('cifrar', $transaccion);
21    $end_time_cbc = microtime(true);
22    $elapsed_time_cbc = ($end_time_cbc - $start_time_cbc) * 1000;
23
24
25    $start_time_ecb = microtime(true);
26    $ECB = encrypt_decrypt_ecb('cifrar', $transaccion);
27    $end_time_ecb = microtime(true);
28    $elapsed_time_ecb = ($end_time_ecb - $start_time_ecb) * 1000;
29
30    $start_time_cfb = microtime(true);
31    $CFB = encrypt_decrypt_cfb('cifrar', $transaccion);
32    $end_time_cfb = microtime(true);
33    $elapsed_time_cfb = ($end_time_cfb - $start_time_cfb) * 1000;
34
35
36    $start_time_ofb = microtime(true);
37    $OFB = encrypt_decrypt_ofb('cifrar', $transaccion);
38    $end_time_ofb = microtime(true);
39    $elapsed_time_ofb = ($end_time_ofb - $start_time_ofb) * 1000;
40
41
42    $query = "INSERT INTO `transacciones` (`Fecha - Hora`, `Banco Origen`, `Cuenta Origen`, `Tipo Cuenta Origen`, `Banco Destino`,
43    `Numero Identificacion`, `Valor Transaccion`, `CUS`, `Descripcion`, `CBC`, `Time CBC`, `ECB`, `Time ECB`, `CFB`, `Time CFB`,
44    `OFB`, `Time OFB`) VALUES ('$fecha_hora', '$banco_origen', '$cuenta_origen', '$tipo_cuenta_origen', '$banco_destino', '$cuenta_destino', '$numero_identificacion', '$valor_transaccion', '$cus', '$descripcion', '$CBC', '$elapsed_time_cbc', '$ECB', '$elapsed_time_ecb', '$CFB', '$elapsed_time_cfb', '$OFB', '$elapsed_time_ofb')";
45
46    $result = mysqli_query($con, $query);
47    if ($result) {
48        echo "Transacción guardada exitosamente";
49    } else {
50        echo "Error al guardar la transacción: " . mysqli_error($con);
51    }
52}
```

3. Creación de la base de datos en mysql con xampp:

The screenshot shows the phpMyAdmin interface for a database named 'Blockchain'. The 'transacciones' table is selected, and its structure is displayed. A message at the top indicates that changes to the table were successful. Below the message, the SQL command for altering the table is shown: `ALTER TABLE `transacciones` CHANGE `Time CFB` `time CFB` DECIMAL(11,4) NULL DEFAULT NULL;`. The table structure is shown in two tabs: 'Estructura de tabla' (selected) and 'Vista de relaciones'. The table has 19 columns, each with a checkbox for selection. The columns are: 1. Fecha - Hora (datetime), 2. Banco Origen (text), 3. Cuenta Origen (int(11)), 4. Tipo Cuenta Origen (text), 5. Banco Destino (text), 6. Cuenta Destino (int(11)), 7. Tipo Cuenta Destino (text), 8. Numero Identificacion (int(11)), 9. Valor Transaccion (int(11)), 10. CUS (int(11)), 11. Descripción (text), 12. CBC (text), 13. Time CBC (decimal(11,4)), 14. ECB (text), 15. Time ECB (decimal(11,4)), 16. CFB (text), 17. time CFB (decimal(11,4)), 18. OFB (text), and 19. Time OFB (decimal(11,4)). The 'CUS' column is marked as the primary key. Below the table structure, there are options to print, make a backup, move columns, or normalize the table. There is also a section for creating an index, with a dropdown for the column(s) to index and a 'Continuar' button. At the bottom, there is a section for partitions, with a message indicating that no partition is defined.

#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Comentarios	Extra	Acción
<input type="checkbox"/>	1 Fecha - Hora	datetime			No	current_timestamp()			Cambiar Eliminar Más
<input type="checkbox"/>	2 Banco Origen	text	utf8mb4_unicode_ci		No	Ninguna			Cambiar Eliminar Más
<input type="checkbox"/>	3 Cuenta Origen	int(11)			No	Ninguna			Cambiar Eliminar Más
<input type="checkbox"/>	4 Tipo Cuenta Origen	text	utf8mb4_unicode_ci		No	Ninguna			Cambiar Eliminar Más
<input type="checkbox"/>	5 Banco Destino	text	utf8mb4_unicode_ci		No	Ninguna			Cambiar Eliminar Más
<input type="checkbox"/>	6 Cuenta Destino	int(11)			No	Ninguna			Cambiar Eliminar Más
<input type="checkbox"/>	7 Tipo Cuenta Destino	text	utf8mb4_unicode_ci		No	Ninguna			Cambiar Eliminar Más
<input type="checkbox"/>	8 Numero Identificacion	int(11)			No	Ninguna			Cambiar Eliminar Más
<input type="checkbox"/>	9 Valor Transaccion	int(11)			No	Ninguna			Cambiar Eliminar Más
<input type="checkbox"/>	10 CUS	int(11)			No	Ninguna	Identificador Transaccion		Cambiar Eliminar Más
<input type="checkbox"/>	11 Descripción	text	utf8mb4_unicode_ci	Sí	NULL				Cambiar Eliminar Más
<input type="checkbox"/>	12 CBC	text	utf8mb4_unicode_ci	Sí	NULL				Cambiar Eliminar Más
<input type="checkbox"/>	13 Time CBC	decimal(11,4)		Sí	NULL				Cambiar Eliminar Más
<input type="checkbox"/>	14 ECB	text	utf8mb4_unicode_ci	Sí	NULL				Cambiar Eliminar Más
<input type="checkbox"/>	15 Time ECB	decimal(11,4)		Sí	NULL				Cambiar Eliminar Más
<input type="checkbox"/>	16 CFB	text	utf8mb4_unicode_ci	Sí	NULL				Cambiar Eliminar Más
<input type="checkbox"/>	17 time CFB	decimal(11,4)		Sí	NULL				Cambiar Eliminar Más
<input type="checkbox"/>	18 OFB	text	utf8mb4_unicode_ci	Sí	NULL				Cambiar Eliminar Más
<input type="checkbox"/>	19 Time OFB	decimal(11,4)		Sí	NULL				Cambiar Eliminar Más

Una vez creada la base de datos con todos los datos, procedemos a crear la conexión con php mediante el archivo bd.php

4. Conexión Mysql con PHP

```
taller_2_blockchain > db.php
1  <?php
2
3  session_start();
4
5  $conn = mysqli_connect(
6      'localhost',
7      'root',
8      '',
9      'Blockchain'
10 );
11 // if(isset($conn)){
12 //     echo 'DB is connected';
13 // }
14 ?>
```

5. Realizamos la primera inserción sin realizar la encriptación:

05/10/2023 00:54

Banco Davivienda

123123

Ahorros

Banco Davivienda

999999

Ahorros

1000589224

10000

1

Primera Transacción

Crear Transacción

Fecha/Hora	Banco Org	Cuenta Org	Tipo Cuenta Org	Banco Dest	Cuenta Dest	Tipo Cuenta Dest	# Identificación	Valor Tx	CUS	Descripción	CBC	Time CBC	ECB	Time ECB	CFB	Time CFB	OFB	Time OFB
2023-10-05 00:54:00	Banco Davivienda	123123	Ahorros	Banco Davivienda	999999	Ahorros	1000589224	10000	1	Primera Transacción								

Ya que validamos que funciona la conexión y podemos realizar la inserción de datos, procedemos a implementar el programa visto en clase utilizando los 4 tipos de encriptación solicitados en el taller

6. Implementación función de encriptación con los 4 tipos solicitados y su respectiva medición de tiempos con la función **microtime**

```
$start_time_cbc = microtime(true);
$CBC = encrypt_decrypt_cbc('cifrar', $transaccion);
$end_time_cbc = microtime(true);
$elapsed_time_cbc = ($end_time_cbc - $start_time_cbc) * 1000;

$start_time_ecb = microtime(true);
$ECB = encrypt_decrypt_ecb('cifrar', $transaccion);
$end_time_ecb = microtime(true);
$elapsed_time_ecb = ($end_time_ecb - $start_time_ecb) * 1000;

$start_time_cfb = microtime(true);
$CFB = encrypt_decrypt_cfb('cifrar', $transaccion);
$end_time_cfb = microtime(true);
$elapsed_time_cfb = ($end_time_cfb - $start_time_cfb) * 1000;

$start_time_ofb = microtime(true);
$OFB = encrypt_decrypt_ofb('cifrar', $transaccion);
$end_time_ofb = microtime(true);
$elapsed_time_ofb = ($end_time_ofb - $start_time_ofb) * 1000;
```

Una vez encriptado de las 4 formas almacenamos el tiempo de cada encriptación y su respectivo texto encriptado en la base de datos junto con los datos de la transacción:

7. Creación de la transacción con sus respectivos encriptaciones (4) y toma de tiempos:

05/10/2023 02:38

Banco Davivienda

123214521

Ahorros

Banco Davivienda

124215124

Ahorros

1000589224

23000

22

Prueba Tiempos

Crear Transacción

Evidenciamos la inserción de los datos en la base de datos y en la tabla:

Fecha/Hora	Banco Org	Cuenta Org	Tipo Cuenta Org	Banco Dest	Cuenta Dest	Tipo Cuenta Dest	# Identificación	Valor Tx	CUS	Descripción	CBC	Time CBC	ECB	Time ECB	CFB	Time CFB	OFB	Time OFB
2023-10-05 00:54:00	Banco Davivienda	123123	Ahorros	Banco Davivienda	999999	Ahorros	1000589224	10000	1	Primera Transacción								
2023-10-05 00:55:00	Banco Davivienda	321321	Ahorros	Banco Davivienda	789789	Ahorros	1000589224	20000	2	Segunda Transacción								
2023-10-05 02:09:00	Banco Davivienda	12344512	Ahorros	Banco Davivienda	9876523	Ahorros	1000589224	100000	10	Transacción Cifrada	H+aXM6IMTuxqQCRXdTatA==		H+aXM6IMTuyfMMJ6VopjsQ==		UfN64tzCouxMmg==		UfN64tzCouxL2A==	
2023-10-05 02:38:00	Banco Davivienda	123214521	Ahorros	Banco Davivienda	124215124	Ahorros	1000589224	103000	20	Prueba Tiempos	GtekQgsi1NYxuoYOloucuQ==	5.5559	GtekQgsi1NbbMZVIPYaC6Q==	0.0410	UfF86NTBo+4zlg==	0.3338	UfF86NTBo+4D2A==	0.1740
2023-10-05 02:44:00	Banco Davivienda	42151251	Ahorros	Banco Davivienda	909701924	Ahorros	1000589224	23000	22	Prueba Tiempos	qkM5vsS+LbQHpJNN3pgBA==	3.4931	qkM5vsS+LaCH9MC3HrA==	0.0229	Ufp94HfP+M3rg==	0.1781	Ufp94HfP+MG3g==	0.1500
2023-10-10 15:30:00	Banco Davivienda	123456789	Ahorros	Bancolombia	987654321	Corriente	1234567890	500000	555	Transferencia de fondos	Valor CBC		Valor ECB		Valor CFB		Valor OFB	

phpMyAdmin

Mostrar ventana de consultas SQL

Mostrando filas 0 - 5 (total de 6, La consulta tardó 0.0009 segundos)

SELECT * FROM `transacciones` WHERE 1;

Perfilando [Editar en línea] [Editar] [Explicar SQL] [Crear código PHP] [Actualizar]

Mostrar todo | Número de filas: 25 | Filtrar filas: Buscar en esta tabla | Ordenar según la clave: Ninguna

Operaciones extra

	Fecha - Hora	Banco Origen	Cuenta Origen	Banco Destino	Cuenta Destino	Tipo Cuenta Destino	Numero Identificación	Valor Transacción	CUS	Descripción	CBC	Time CBC	ECB	Time ECB	CFB	Time CFB	OFB	Time OFB
<input type="checkbox"/>	2023-10-05 00:54:00	Banco Davivienda	123123	Banco Davivienda	999999	Ahorros	1000589224	10000	1	Primera Transacción	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL
<input type="checkbox"/>	2023-10-05 00:55:00	Banco Davivienda	321321	Banco Davivienda	789789	Ahorros	1000589224	20000	2	Segunda Transacción	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL
<input type="checkbox"/>	2023-10-05 02:09:00	Banco Davivienda	12344512	Banco Davivienda	9876523	Ahorros	1000589224	100000	10	Transacción Cifrada	H+aXM6IMTuxqQCRXdTatA==	NULL	H+aXM6IMTuyfMMJ6VopjsQ==	NULL	UfN64tzCouxMmg==	NULL	UfN64tzCouxL2A==	NULL
<input type="checkbox"/>	2023-10-05 02:38:00	Banco Davivienda	123214521	Banco Davivienda	124215124	Ahorros	1000589224	103000	20	Prueba Tiempos	GtekQgsi1NYxuoYOloucuQ==	5.5559	GtekQgsi1NbbMZVIPYaC6Q==	0.0410	UfF86NTBo+4zlg==	0.3338	UfF86NTBo+4D2A==	0.1740
<input type="checkbox"/>	2023-10-05 02:44:00	Banco Davivienda	42151251	Banco Davivienda	909701924	Ahorros	1000589224	23000	22	Prueba Tiempos	qkM5vsS+LbQHpJNN3pgBA==	3.4931	qkM5vsS+LaCH9MC3HrA==	0.0229	Ufp94HfP+M3rg==	0.1781	Ufp94HfP+MG3g==	0.1500
<input type="checkbox"/>	2023-10-10 15:30:00	Banco Davivienda	123456789	Bancolombia	987654321	Corriente	1234567890	500000	555	Transferencia de fondos	Valor CBC	NULL	Valor ECB	NULL	Valor CFB	NULL	Valor OFB	NULL

Operaciones sobre los resultados de la consulta

CUADRO COMPARATIVO:

CBC	Time CBC	Tamaño Bloque	ECB	Time ECB	Tamaño Bloque	CFB	Time CFB	Tamaño Bloque	OFB	Time OFB	Tamaño Bloque
GtekQgsl1NYx uoYOiofcuQ==	5,555 9	24	GtekQgsl 1NbbMZ VIPYaC6 Q==	0,04 10	24	UfF86N TBo+4z lg==	0,3338	16	UfF86NTBo+4D2A==	0,1740	16
qkM5vsS+Llb QHpJNN3pqB A==	3,493 1	24	qkM5vsS +LlaC1H 9MC3Hsr A==	0,02 29	24	Ufp94tH Fp+M3r g==	0,1781	16	Ufp94tHFp+MG3g==	0,1500	16

Conclusiones:

- El algoritmo más eficiente en tiempo es el ECB
- El algoritmo menos eficiente en tiempo es el CBC con gran diferencia de los demás
- El algoritmo más completo es el ECB dado que es más eficiente en tiempo y además genera un bloque cifrado más largo por lo tanto más seguro.

Características Máquina Utilizada:

- RAM: 8gb
- CPU: Chip M1
- Memoria: 256 Gb

Link código y script: https://github.com/DanielHurtado-040801/Blockchain-Taller_2.git