УДК 681.18

ТКАЧМАН М.Л.
АБАЛИЕВА А.Д.
КНУ им. Ж.Баласагына

PHP программалоо тилиндеги PHPMyAdmin базасы менен бирдикте форма жана функция куралын шифрлоодо колдонуу

ИСПОЛЬЗОВАНИЕ ИНСТРУМЕНТА ФОРМ И ФУНКЦИЙ ШИФРОВАНИЯ В ЯЗЫКЕ ПРОГРАММИРОВАНИЯ PHP СОВМЕСТНО С БАЗОЙ PHPMYADMIN

Use of the tool of forms and functions of enciphering in the PHP programming language together with the PHP MyAdmin base

Аннотация: *заманбап крип тографиялык, маалыматтык технологияларды сабактарда колдонуу, жөн гана студенттердин көңүлүнө куса болуу гана эмес, окуу процесинин негизги бөлүгү десек болот.*

Аннотация:*использование современных, криптографических информационных технологий на занятиях стало не просто способом привлечь к изучению предмета студентов, но и неотъемлемой частью образовательного процесса.*

Annotation: *use of modern cryptographic information technologies on occupations didn't become simple in the way to involve in studying of a subject of students, but also an integral part of educational process.*

Негизги сөздөр: *система; маалымат; криптография; метод; шифрлоо.*

Ключевые слова: *система; информация; криптография; метод; шифрование.*

Keywords: *system; information; cryptography; method; enciphering.*

История криптографии насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии можно использовать технологические характеристики применяемых методов шифрования.

Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам — линейному и дифференциальному криптоанализу. Однако до 1975 года криптография оставалась «классической» или же, более корректно, криптографией с секретным ключом [1].

В нашем случае также используется секретный ключ. Но каждый раз он будет произвольный, и он не будет фиксироваться ни на каком-либо носителе. А передаваться будет путем радиоданных или любым другим способом, исключая интернет передачу. Это позволит исключить перехват ключа.

И дальше в осуществлении нашего замысла подключаем информационные web-технологии на базе PHP My Admin и языка программирования PHP.

Исследование осуществляется путем создания ряда форм для ввода данных и форм получения результата, а также создание промежуточных рабочих файлов.

Составлен план осуществления замысла:

1. Создание базы данных для ввода зашифрованной информации: shifr.
2. Разработка рабочих форм, начиная с главной формы.
3. Создание файлов обработки данных, принимаемых с форм.
4. Разработка инструкции пользователя по работе для получения корректного результата.

1. Создание базы данных для ввода зашифрованной информации: shifr.

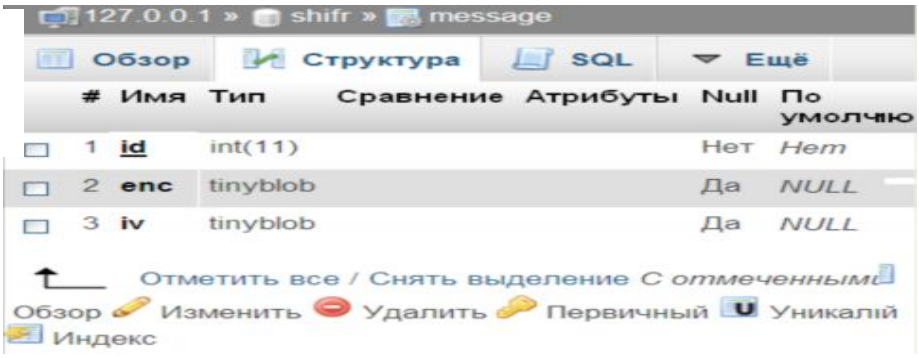

Рис.1. Базы данных: shifr.

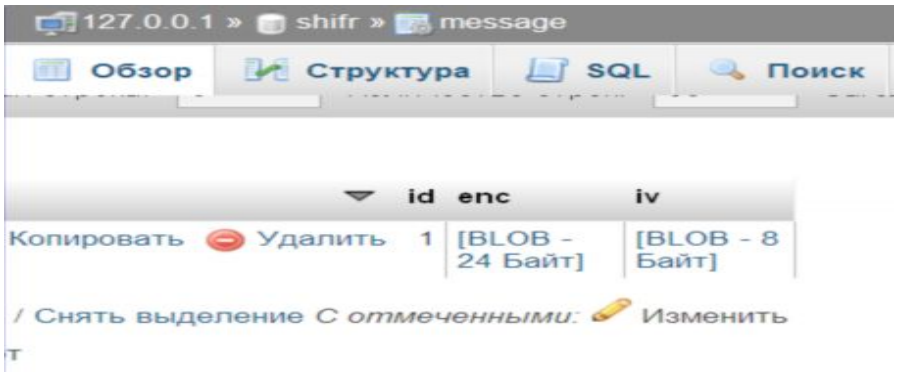

Рис.2. Базы данных с типом данных BLOB.

Используется база данных, как источник для безопасного хранения данных.

2. Разработка рабочих форм, начиная с главной формы.

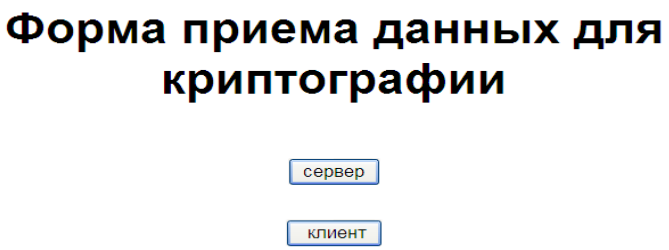

Рис.3. Главная форма. [Исходный код формы 1]

Исходный код формы 1:

```
<html>
<head>
<title>Форма приема данных для криптографии</title>
</head>
<body>
  <br>
<h1 align="center">Форма приема данных для криптографии </h1>
```

```
  <br>
  <table align="center" border="1"   >
<form  action="form_cript1.php"   method="post">
<table align="center">
<tr>
<td colspan=2>
<input type="submit" value="сервер" name="send"/>
</td>
</tr>
</table>
</form>
<form  action="form_client.php"   method="post">
<table align="center">
<tr>
<td colspan=2>
<input type="submit" value=" клиент" name="send"/>
</td>
</tr>
</table>
</form>
</table>
</body>
</html>
```

2.1. Разрабатывается рабочая форма ввода данных для сервера:

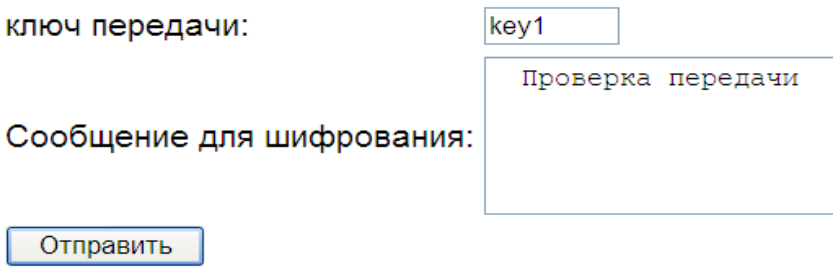

Рис.4. Рабочая форма ввода данных для сервера.
[Исходный код формы 2]

Исходный код формы 2:

```
<html>
<head>
<title>Форма для криптографии</title>
</head>
<body>
<form  action="shifr_in.php"   method="post">
<table>
<tr>
<td>ключпередачи:</td><td><input  type="text"  size="5"  value=""  name="name"
/><br/></td>
```

```
</tr>
<tr>
<td>Сообщение для шифрования:</td><br/>
<td><textarea rows="5" cols="40" name="message"></textarea><br/></td>
</tr>
<tr>
<td colspan=2>
<input type="submit" value="Отправить" name="send"/>
</td>
</tr>
</table>
</form>
</body>
</html
```

2.2. Исходный код файла обработки передаваемых данных для шифрования 3:

```
<?php
$text = $_POST['message'];
$key = $_POST['name'];
$iv = mcrypt_create_iv(mcrypt_get_iv_size(MCRYPT_DES, MCRYPT_MODE_ECB), MCRYPT_RAND);
$enc = mcrypt_encrypt(MCRYPT_DES, $key, $text, MCRYPT_MODE_ECB, $iv);
include("file_per.php");
?>
```

2.3. Исходный код файла обработки передаваемых данных для шифрования в файле include("file_per.php").

```
<?php
include("config.php");
$q1=mysql_query("TRUNCATE TABLE `message");
$q="INSERT INTO `message` (`enc`,`iv`)VALUES ('$enc','$iv')";
$q1=mysql_query($q);
echo'Сообщениеотправлено';
echo"<br>";
mysql_query("SET NAMES utf8");
$query = "SELECT * from message";
$sort=@mysql_query($query);
$row = @mysql_fetch_array($sort);
echo$row[enc];
echo"<br>";
echo$row[iv];
echo"<br>";
$dctext = mcrypt_decrypt(MCRYPT_DES, $key, $enc, MCRYPT_MODE_ECB, $iv);
$v=$dctext;
echo'$v='.$v;
?>
<form action="index.php" method="post">
<table>
<tr>
<td colspan=2>
<input type="submit" value="сервер" name="send"/>
</td>
```

```
</tr>
</table>
</form>
```

Результат передачи данных:

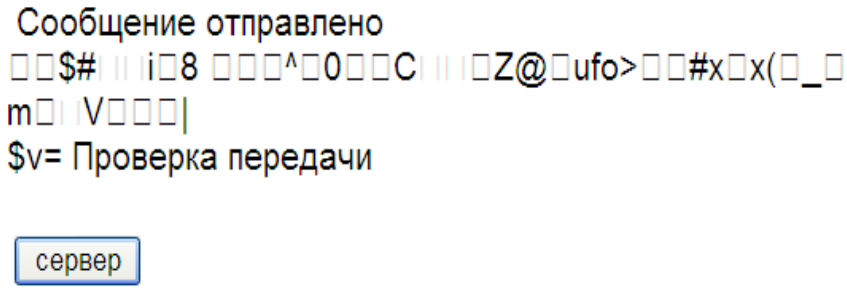

Рис.4. Результат передачи данных [Исходный код формы 3].

3. Создание файлов обработки данных, принимаемых с форм.

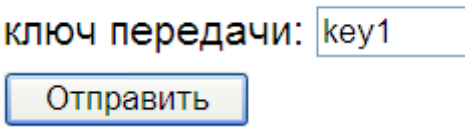

Рис.5. Форма приема данных.

Исходный код файла 4:

```
<html>
<head>
<title>Форма приема данных для криптографии</title>
</head>
<body>
<form  action="priem_mess.php"   method="post">
<table>
<tr>
<td>ключпередачи:</td><td><input type="text" value="" name="name" /><br/></td>
</tr>
<td colspan=2>
<input type="submit" value="Отправить" name="send"/>
</td>
</tr>
</table>
</form>
</body>
</html>
```

Результат расшифровки переданного сообщения:

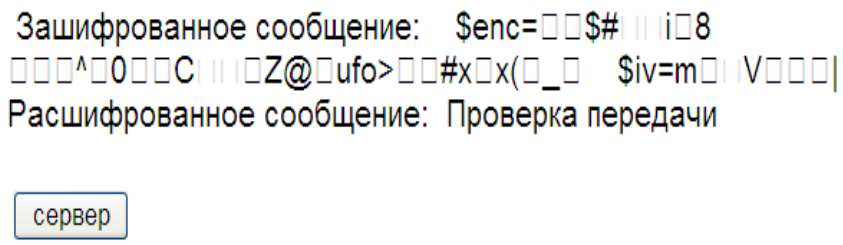

Рис.6. Результат расшифровки переданного сообщения.[Исходный код формы 4]

Исходный код файла приема сообщения:

```
<?php
$key="";

include("config.php");
$query = "SELECT * from message";
$sort=@mysql_query($query);
$row = @mysql_fetch_array($sort);
$key = $_POST['name'];
$enc=$row[enc];
echo'Зашифрованноесообщение:';
echo"    ";
echo'$enc='.$enc;
echo"    ";
$iv=$row[iv];
echo'$iv='.$iv;
echo"<br>";
$dctext = mcrypt_decrypt(MCRYPT_DES, $key, $enc, MCRYPT_MODE_ECB, $iv);
echo'Расшифрованное сообщение:';
echo" ";
echo$dctext;
?>
<form action="index.php"  method="post">
<table>
<tr>
<td colspan=2>
<input type="submit" value="сервер" name="send"/>
</td>
</tr>
</table>
</form>
```

4. Разработка инструкции пользователя по работе для получения корректного результата.

Данная инструкция была разработана в полном объеме.

Выводы по статье «Использование инструмента форм и функций шифрования в языке программирования PHP совместно с базой PHPMyAdmin».

В результате работы был выявлен ряд положительных свойств функций шифрования:

$iv = mcrypt_create_iv(mcrypt_get_iv_size (MCRYPT_DES, MCRYPT_MODE_ECB), MCRYPT_RAND);

$enc = mcrypt_encrypt(MCRYPT_DES, $key, $text, MCRYPT_MODE_ECB, $iv);

Идешифрования:

$dctext = mcrypt_decrypt (MCRYPT_DES, $key, $enc, MCRYPT_MODE_ECB, $iv); которые способствуют функциональности надежного шифрования и дешифрования

отправленных данных. Хранение осуществлено в базе данных. Хранимая зашифрованная информация не отображается в базе, за счет применения типа данных BLOB.

Литература

1. Панасенко. С. / С. Панасенко. Алгоритмы шифрования.
2. *[1]*- https://ru.wikipedia.org/wiki/Шифрование
3. Э. Гамма, Р. Хелм, Р. Джонсон, Дж. Влиссидес Приемы объектно-ориентированного проектирования. Паттерныпроектирования (*Design Patterns: Elements of Reusable Object-Oriented Software*).
4. МэттЗандстра (Matt Zandstra) PHP. Объекты, шаблоны и методики программирования (*PHP Objects,Patterns, and Practice*).
5. Нигель Смарт Криптография.
6. Саймон Сингх Книга шифров
7. Дэвид Кан Взломщики кодов
8. Брюс Шнайер Секреты и ложь. Безопасность данных в цифровом мире.
9. Сидельников В.М. Криптография и теория кодирования / В.М. Сидельников.
10. Баричев С.Г., Серов Р.Е. Основы современной криптографии / С.Г. Баричев., Р.Е.Серов.