



SECURE ELECTRONIC COMMERCE [INTE1070]

Assignment Report

Akshay Sunil Salunke
S37304440

Introduction

In this assignment, I had to create a shopping website which worked on client server model. We were expected to work in HTML, JavaScript and PHP. The learning outcome of this assignment was application of encryption/decryption algorithms while transferring data between client and server.

Body

The assignment is divided into 4 parts,

Registration

The requirements for this part were

- The password should be at least 6 characters.
- On successful signup, the password sent to server should be hashed and not plaintext.
- The username and hashed password are saved in database/users.txt.

For the first requirement, I created a JavaScript function in register.html called checkpwd(). This function was called on 'oninput' event on the password input field. The function checks the length of input field and enables the 'Register' button only if the length is greater than or equal to 6.

When user clicks register button, the username and SHA256 hashed password is POSTed to server's register.php, which then saves this information in users.txt file using fwrite().

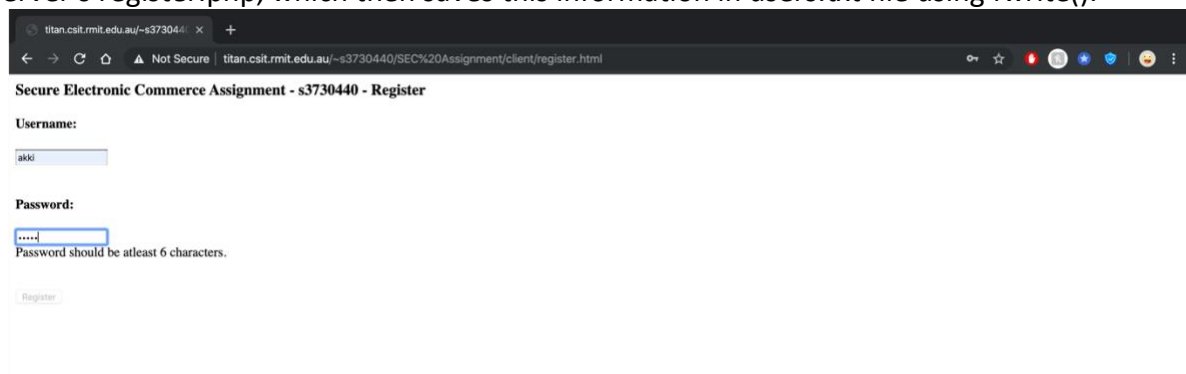


Figure 1. register.html

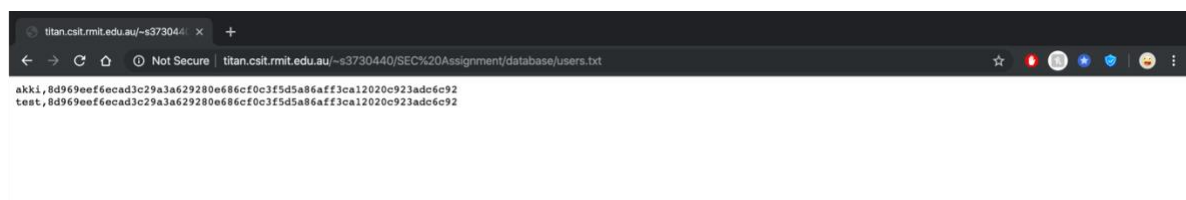


Figure 2 users.txt

Login

When the user enters username and password in login.html, the information is POSTed to server's login.php, which then checks if the username exists in users.txt, if it does, the hashed password is matched and if matched, login is successful.

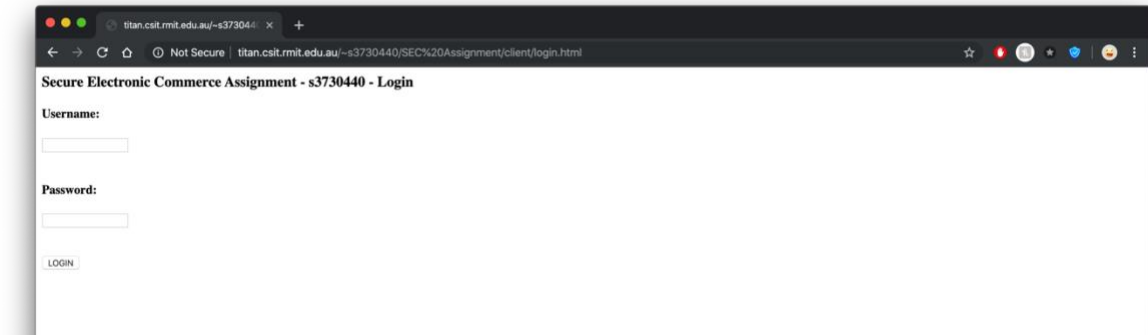


Figure 3 login.html

Shopping Cart

Requirements for shopping cart are:

- Cart can be accessed only if user is logged in.
- Cart updates when quantity of any item changes.

For the first requirement, we check if the SESSION variable is set. If not, it shows an error and link to login.html. To update cart every time user changes item, we call the updateCart() function with onchange() event call on productQuantity input field.

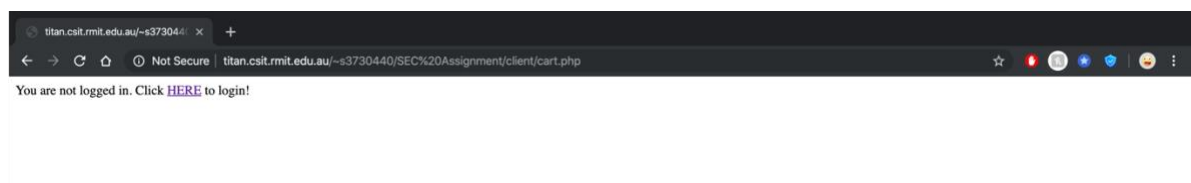
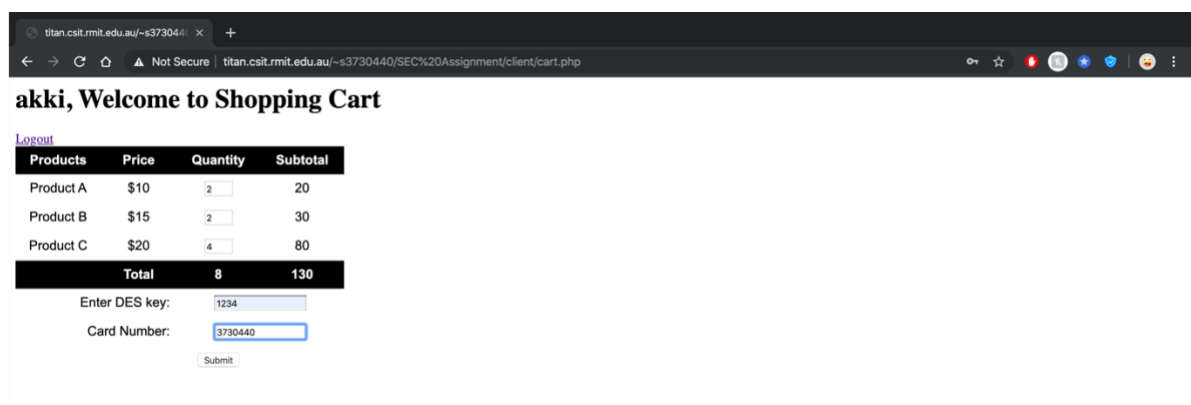


Figure 4 cart.php



Products	Price	Quantity	Subtotal
Product A	\$10	2	20
Product B	\$15	2	30
Product C	\$20	4	80
Total		8	130

Figure 5 cart.php - Update cart feature

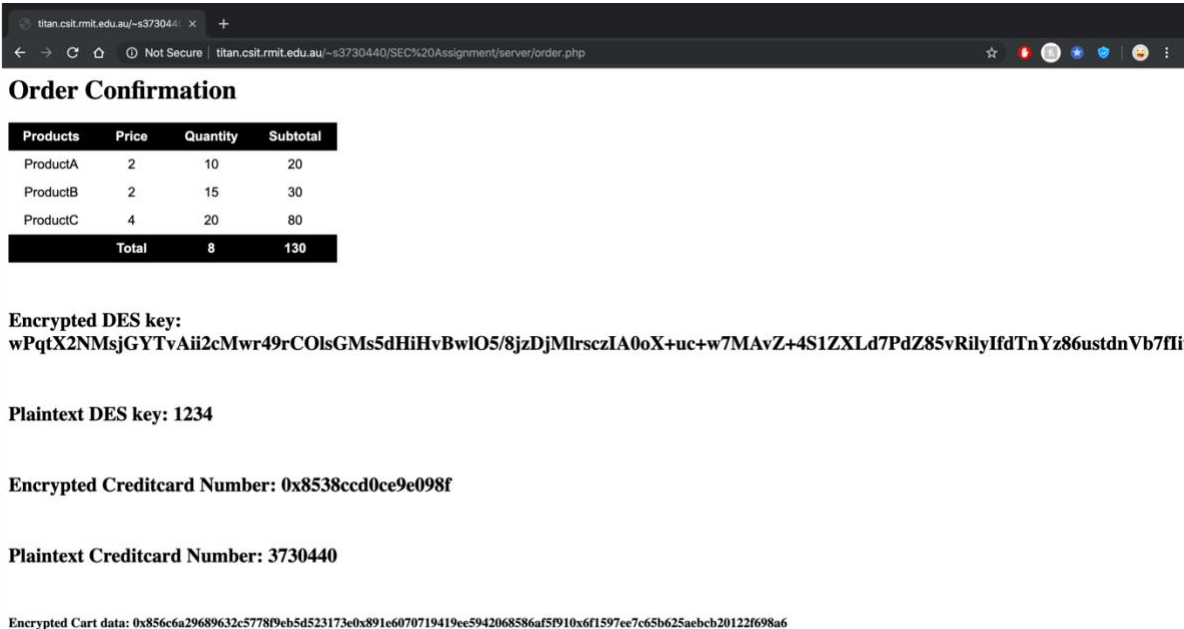
Posting information to server

Requirements for this are:

- Credit card number should be encrypted using DES.
- Encrypt DES key with RSA public key.
- Encrypt shopping cart data with DES.

We are encrypting the credit card number and shopping cart data(product name, quantity, subtotal) with DES key entered by user, by using the `javascript_des_encryption()`. We also encrypt the user entered DES key with server's RSA public key. We then replace the plain form data in html with encrypted data and then post it to `order.php` on server.

We decrypt the received encrypted DES key with server's private RSA key and then decrypt the credit card number and shopping cart data using this decrypted DES key. We then save all the decrypted information into `orders.txt`.



Order Confirmation

Products	Price	Quantity	Subtotal
ProductA	2	10	20
ProductB	2	15	30
ProductC	4	20	80
Total		8	130

Encrypted DES key:
wPqtX2NMsjGYTVAii2cMwr49rCOlsGMS5dHiHvBwlO5/8jzDjMlrsczIA0oX+uc+w7MAvZ+4S1ZXLd7PdZ85vRilyIfdTnYz86ustdnVb7fIi

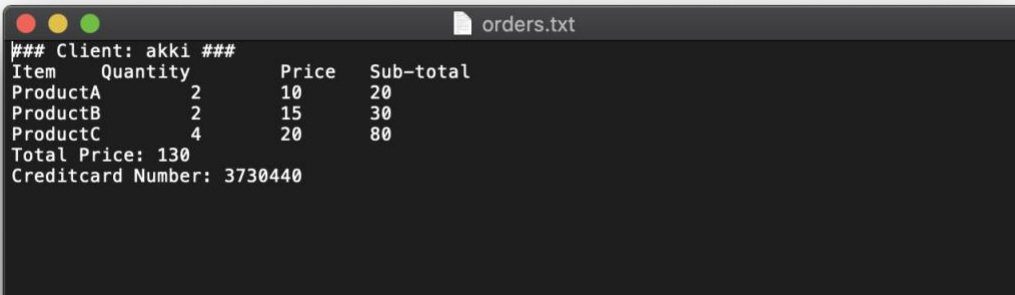
Plaintext DES key: 1234

Encrypted Creditcard Number: 0x8538ccd0ce9e098f

Plaintext Creditcard Number: 3730440

Encrypted Cart data: 0x856c6a29689632c5778f9eb5d523173e0x891e6070719419ee5942068586af5f910x6f1597ee7c65b625aebcb20122f698a6

Figure 6 order.php



```
### Client: akki ###
Item    Quantity    Price    Sub-total
ProductA    2        10        20
ProductB    2        15        30
ProductC    4        20        80
Total Price: 130
Creditcard Number: 3730440
```

Figure 7 orders.txt

Data Flow Diagram

