WEB-O-MANIA Application Description Paper

Name: Avinash Kadimisetty **Samgatha ID**: SAM15000007

Description:

Interface:

Since this application is Romeo-Juliet specific,

1. The applications consists of a login form which allows either Romeo or Juliet to login to the application.
2. There is no REGISTER since this is a specific application. (Romeo communicated the login details to JULIET)
3. Once a person (Romeo or Juliet) logs in, a screen containing his earlier messages and a chat box will be displayed.
4. The message box consists of the earlier messages sent or received.
5. A person can enter messages into the chat box and send it to the other.
6. A logout button on the top for destroying the session.

Inside application:

Since the chat has to be encrypted, I use the following way to encrypt and decrypt messages.

1. I select two prime numbers say a, b.
2. Now I compute their product say n=a*b;
3. Now compute another product x= (a-1)*(b-1).
4. Now select a number e, such that 1<e<x, and e is coprime to n.
5. Now choose some number d such that the following condition is satisfied.
   a. (d*e)mod (x)=1

Encryption:

For every character entered, I would take its ASCII value and then encrypt that value in the following way.

Say the character entered is c. so the encrypted message would be (c ^ e) mod (n);

For example if a=3, b=11 then n=33 and x=20. Suppose e=7 and d=3,
And if the message is 2 then the encrypted value is (2^7) mod (33) =29;

Decryption for every value I receive on the other side,

I decrypt the value like this,

Decrypted value = ((encrypted_value) ^ d) mod (n)

So for the above example the decrypted value will be (29^3) mod (33) which is 2.

For this application since the characters have ASCII values ranging from 0 to 255 the computed product of the prime numbers n should be greater than 255.

So ‘a’ and ‘b’ should be chosen in a way satisfying the above condition.

Communicate the technique to Juliet:

Romeo chooses two prime numbers of his own choice and writes a program to encrypt the message and sends the message to Juliet.

Romeo asks Juliet to decrypt the value in the above way by telling her the values of d and n.

An option for decrypting the message will also be provided in the application where in if you enter the message that is encrypted, the decrypted message is displayed.

Implementation:

Whenever the user inputs a message and presses enter the entered message is encrypted character wise and concatenated with the character `. The encryption is done within a module whose input is string and output is encrypted numbers concatenated by ( `).

On the other side if a person wants to decrypt the message he/she can do it either manually because the values of ‘d’ and ‘n’ are known, or can use the automated decryption available in the application to bring in the ease of reading.

Automated decryption module takes in input as a sequence of numbers concatenated by ` and output the corresponding decrypted message in the form of readable text.

Taking in the security concerns, the application will be more secure if Romeo can change the values of ‘a’ and ‘b’ regularly. Romeo can do this, by setting the numbers in the source code.