

Lab 7 – Hand-on DH algorithm

Aim

Try to use DH algorithm to improve the security during login process.

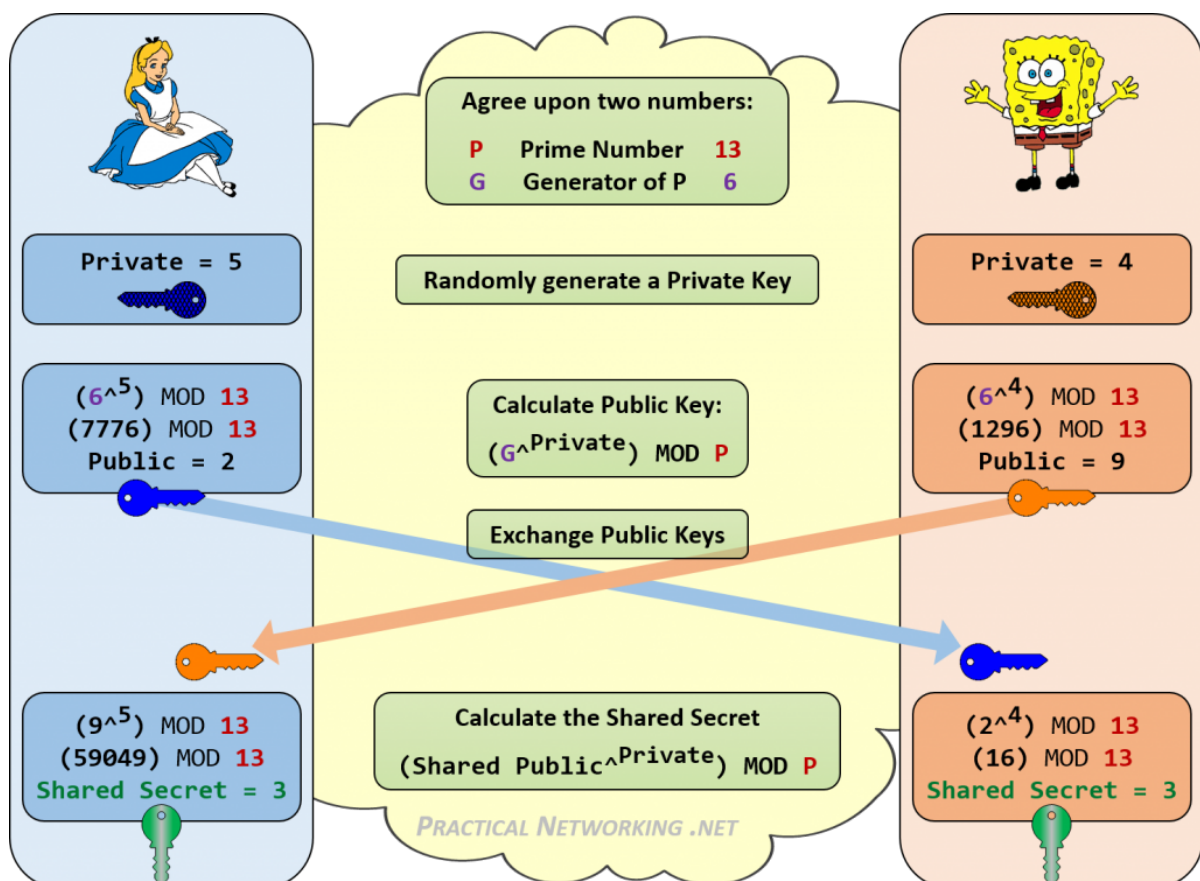
Resources

1. You should continuously use the all settings of last lab.

Tips:

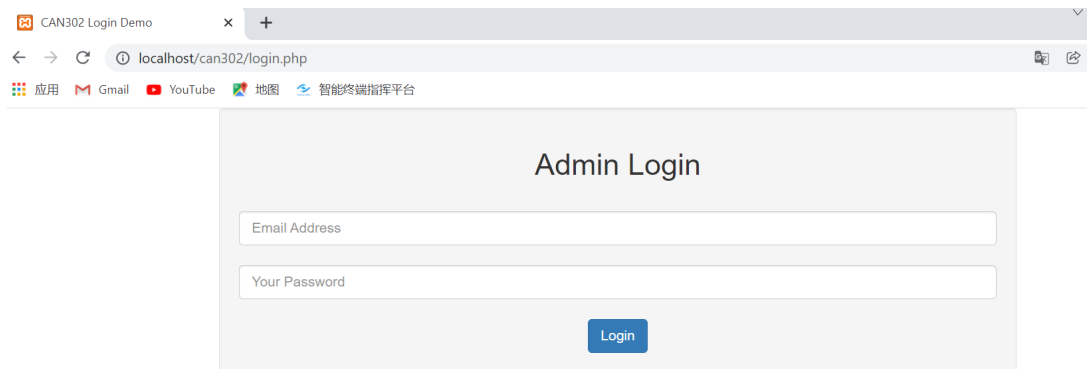
1. If you are not sure why you are doing something, ask a TA. This is what they are here for.
2. The forums are available for questions and discussions.
3. These labs are expected take more than the 2 allocated hours. You should complete them in your own time before the next lab. Practice makes perfect!

DH algorithm:



Remember the DH algorithm? If not, you should try to work it out before coding.

Improve the login function:



So far, our login page is as the above one. We send the passwd in plain text to the server. It is very dangerous since the communication could be sniffed by crazy EVE.

Let's use DH algorithm to against EVE in the following way:

Define the prime number by the web server and use the current time (timestamp) as the generator. Choosing a private key for the web server and let the user input a private key manually.

During loading the web page, put the timestamp and the corresponding public key of server as two hidden elements.

Then in the web page, we can use the private key inputted by user, timestamp and prime number to calculate the corresponding public key of client.

Next, we use the public key of server and private key of client to calculate the sharing secret.

Then, we calculate the hash value of password with the sharing secret as the "salt".

So, the form will finally submit the public key of client and hash value for the password with salt.

On the server side, it needs to calculate the sharing secret by using the public key of client and the private key of server.

Then, server can calculate the hash value of password store in database with the sharing secret as the salt.

Finally, server can compare both hash values to confirm the password is correct or not.

Some code hints as:

```
1 <?php
2
3 function mydh($remaind, $generator, $prv){
4     $prime = 99991;
5     if ($prv == 1){
6         $remaind = ($remaind * $generator) % $prime;
7         return $remaind;
8     }
9     else{
10        $prv -= 1;
11        $remaind = ($remaind * $generator) % $prime;
12        return mydh($remaind, $generator, $prv);
13    }
14 }
15 |
16
17 ?>
```

```

5 include("functions/dh.php");
6 $timestamp = time();
7 $serverkey = mydh(1, $timestamp, 302);
8 if (isset($_POST['login'])) {
9     $email = mysqli_real_escape_string($con,$_POST['email']);
10    $pass = mysqli_real_escape_string($con,$_POST['pass']);
11    $clientkey = mysqli_real_escape_string($con,$_POST['clientkey']);
12    $remaind = mydh(1, $clientkey, 302);
13    $get_admin = "SELECT * FROM admin WHERE email='$email'";
14    $run_admin = mysqli_query($con, $get_admin);
15    $count = mysqli_num_rows($run_admin);
16    if ($count==1) {
17        $row_admin = mysqli_fetch_array($run_admin);
18        $passwd = sha1($row_admin['passwd'].$remaind);
19        if ($passwd==$pass){
20            $_SESSION['can302'] = $email;
21            session_regenerate_id();
22            echo "<script>alert('Welcome ".$row_admin['nickname']."'</script>";
23            echo "<script>window.open('index.php?dashboard','_self')</script>";
24        }
25        else{
26            echo "<script>alert('Password is Wrong!')</script>";
27        }
28    }
29    else{
30        echo "<script>alert('Email is Wrong!')</script>";
31    }
32 }
33

```

```

46 <script src="https://cdn.bootcdn.net/ajax/libs/jshashes/1.0.8/hashes.js"></script>
47 <script>
48     function jsdh(remaind, generator, prv){
49         var prime = 99991;
50         if (prv == 1){
51             remaind = (remaind * generator) % prime;
52             return remaind;
53         }
54         else{
55             prv -=1;
56             remaind = (remaind * generator) % prime;
57             return jsdh(remaind, generator, prv);
58         }
59     }
60
61     function security(){
62         var pass = document.getElementById("pass").value;
63         var clientkey = Number(document.getElementById("clientkey").value);
64         var serverkey = Number(document.getElementById("serverkey").value);
65         var timestamp = Number(document.getElementById("timestamp").value);
66         var remaind = jsdh(1, timestamp, clientkey);
67         document.getElementById("clientkey").value = remaind;
68         remaind = jsdh(1, serverkey, clientkey);
69         pass = pass + remaind;
70         var SHA1 = new Hashes.SHA1;
71         document.getElementById("pass").value = SHA1.hex(pass);
72     }
73 </script>
74

```

Please try to make the rest part.

Extend questions:

1. Try to use timestamp to against the re-play attack.
2. Try to use AES function to encrypt the password by using the sharing secret as the encryption key.