MCS – Experiment No. 3

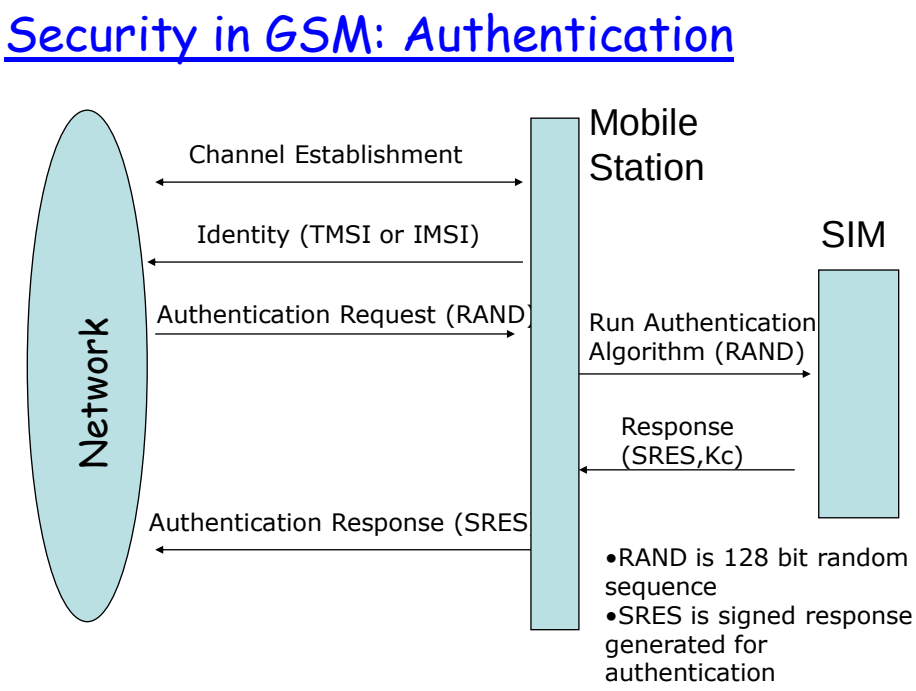
Aim : To Study Authentication in GSM Network using A3 Algorithm.

Theory :

Encryption in the GSM network utilizes a Challenge/Response mechanism.

1. The Mobile Station (MS) signs into the network.
2. The Mobile Services Switching Center (MSC) requests 5 triples from the Home Location Register (HLR).
3. The Home Location Register creates five triples utilizing the A8 algorithm. These five triples each contain:
   - A 128-bit random challenge (RAND)
   - A 32-bit matching Signed Response (SRES)
   - A 64-bit ciphering key used as a Session Key (Kc).
4. The Home Location Register sends the Mobile Services Switching Center the five triples.
5. The Mobile Services Switching Center sends the random challenge from the first triple to the Base Transceiver Station (BTS).
6. The Base Transceiver Station sends the random challenge from the first triple to the Mobile Station.
7. The Mobile Station receives the random challenge from the Base Transceiver Station and encrypts it with the Individual Subscriber Authentication Key (Ki) assigned to the Mobile Station utilizing the A3 algorithm.
8. The Mobile Station sends the Signed Response to the Base Transceiver Station.
9. The Base Transceiver Station sends the Signed Response to the Mobile Services Switching Center.
10. The Mobile Services Switching Center verifies the Signed Response.
11. The Mobile Station generates a Session Key (Kc) utilizing the A8 algorithm, the Individual Subscriber Authentication Key (Ki) assigned to the Mobile Station, and the random challenge received from the Base Transceiver Station.
12. The Mobile Station sends the Session Key (Kc) to the Base Transceiver Station.
13. The Mobile Services Switching Center sends the Session Key (Kc) to the Base Transceiver Station.
14. The Base Transceiver Station receives the Session Key (Kc) from the Mobile Services Switching Center.
15. The Base Transceiver Station receives the Session Key (Kc) from the Mobile Station.
16. The Base Transceiver Station verifies the Session Keys from the Mobile Station and the Mobile Services switching Center.
17. The A5 algorithm is initialized with the Session Key (Kc) and the number of the frame to be encrypted.
18. Over-the-air communication channel between the Mobile Station and Base Transceiver Station can now be encrypted utilizing the A5 algorithm.

Flow Diagram :



Database :

HLR :

id	MSISDN	IMSI	Services
1	9029326504	919029311986	CALL,SMS,GPRS
2	9209203394	919209494286	CALL,SMS

VLR :

id	IMSI	MSISDN	TMSI
1	919029311986	9029326504	919029908227
2	919209494286	9209203394	919209529393

AUC :

id	IMSI	Ki
1	919029311986	cd-e7-e1-f3-e7-ed-d3-db-d8-d0-c2-cd-dc-9c-cb-b6
2	919209494286	a2-9a-a6-ff-e2-f0-8a-db-be-aa-e7-a1-a0-c3-89-ad

Program :

a) Backend PHP Program :

```
<?php
/*
 * ************************************************************
 ***************  MCS EXPT3 ****************************
 ************************************************************/
 /* Designed & Developed by
 /*                                        - Shiburaj Pappu
 /* ************  S.P.I.T ***********************************
 /* ********** M.E (EXTC) Sem-II ****************************
 */
?>
<?php

include_once('Database.class.php');
define("MSCTBL","msc");
$db = new Database('localhost', 'root', 'test123', 'mscsim');
    //connect to the server
    $db->connect();

if($_GET['action']=='register' && !empty($_POST['MSISDN']) &&
!empty($_POST['IMSI'])){
    $preMSISDN =
$_POST['MSISDN'][0].$_POST['MSISDN'][1].$_POST['MSISDN'][2].$_POST['MSISDN'][3]
;
    $data['TMSI'] = "91".$preMSISDN.rand('199999','999999');
    $sql = "SELECT * FROM ".MSCTBL." WHERE `MSISDN` = '".$_POST['MSISDN']."'";
    $row = $db->query_first($sql);
    if(empty($row)){
        $error_dat['status'] = "error";
        $error_dat['reason'] = "Registration Failed...";
    }else{
        $db->query_update(MSCTBL,$data," `MSISDN` = '".$_POST['MSISDN']."' ");
        $error_dat['regdata'] = $row;
        $error_dat['regdata']['TMSI'] = $data['TMSI'];
        $error_dat['status'] = "success";
        $error_dat['reason'] = "Registration Complete...";
    }
    sleep(3);
    echo json_encode($error_dat);
}elseif($_GET['action']=='makesim' && !empty($_POST['MSISDN'])){
    $preMSISDN =
$_POST['MSISDN'][0].$_POST['MSISDN'][1].$_POST['MSISDN'][2].$_POST['MSISDN'][3]
;
    $data['IMSI'] = "91".$preMSISDN.rand('199999','999999');
    $data['IMEI'] = "956647"."894467".rand('199999','999999');
    $data['Ki'] = genRandKey(128);
    $data['NSP'] = getNSP($preMSISDN);
    $sql = "SELECT * FROM ".MSCTBL." WHERE `MSISDN` = '".$_POST['MSISDN']."'";
    $row = $db->query_first($sql);
    if(empty($row)){
        $data['MSISDN'] = $_POST['MSISDN'];
        $db->query_insert(MSCTBL,$data);
    }else{
        $db->query_update(MSCTBL,$data," `MSISDN` = '".$_POST['MSISDN']."' ");
        $data['MSISDN'] = $_POST['MSISDN'];
    }
    echo json_encode($data);
}elseif($_GET['action']=='authenticate' && !empty($_POST['MSISDN']) &&
!empty($_POST['TMSI'])){
    $sql = "SELECT * FROM ".MSCTBL." WHERE `MSISDN` = '".$_POST['MSISDN']."'
AND `TMSI` = '".$_POST['TMSI']."'";
    $row = $db->query_first($sql);
    if(empty($row)){
```

```
        $error_dat['status'] = "error";
        $error_dat['reason'] = "Device Not Registered...";
    }else{
        $error_dat['RAND'] = genRandKey(128);
        $error_dat['RES'] = resGen($error_dat['RAND'],$row['Ki'],128);
        $error_dat['status'] = "success";
        $error_dat['reason'] = "RAND Generation Complete...";
    }
    sleep(3);
    echo json_encode($error_dat);
}elseif($_GET['action']=='gensres' && !empty($_POST['RAND']) &&
!empty($_POST['Ki'])){
    $error_dat['SRES'] = resGen($_POST['RAND'],$_POST['Ki'],128);
    $error_dat['status'] = "success";
    $error_dat['reason'] = "RAND Generation Complete...";
    sleep(3);
    echo json_encode($error_dat);
}elseif($_GET['action']=='sendsres' && !empty($_POST['SRES']) &&
!empty($_POST['RES'])){
    if($_POST['SRES']==$_POST['RES']){
        $error_dat['status'] = "success";
        $error_dat['reason'] = "Authentication Successfull...";
    }else{
        $error_dat['status'] = "error";
        $error_dat['reason'] = "Authentication Failed...";
    }

    sleep(3);
    echo json_encode($error_dat);
}


function genRandKey($length=128){
    $count = round($length/8);
    $binData = "";
    for($i=1;$i<=$count;$i++){
        $binData .= dechex(rand('128','255'))."-";
    }
    $binData = trim($binData,"-");
    return $binData;
}

function getNSP($preMSISDN){
    $NSP = array('9821'=>'Loop Mobile','9870'=>'Loop Mobile','9773'=>'Loop
Mobile',
                '9664'=>'Loop Mobile','8082'=>'Loop Mobile',
                '9819'=>'Vodafone','9820'=>'Vodafone','9833'=>'Vodafone',
                '9920'=>'Vodafone','9930'=>'Vodafone','9769'=>'Vodafone',
                '9619'=>'Vodafone','9167'=>'Vodafone','8879'=>'Vodafone',
                '7506'=>'Vodafone Essar Ltd',
                '9029'=>'Tata GSM','8097'=>'Tata GSM','8976'=>'Tata GSM',
                '7208'=>'Tata GSM','8655'=>'Tata GSM',
                '9869'=>'MTNL','9969'=>'MTNL','9757'=>'MTNL',
                '9022'=>'Reliance (GSM)','9699'=>'Reliance
(GSM)','8080'=>'Reliance (GSM)',
                '7666'=>'Reliance (GSM)','8767'=>'Reliance
(GSM)','7303'=>'Reliance (GSM)',

'9867'=>'Airtel','9892'=>'Airtel','9967'=>'Airtel','9987'=>'Airtel',
                '9004'=>'Airtel','7738'=>'Airtel',
                '9702'=>'Idea','9594'=>'Idea','8108'=>'Idea','8652'=>'Idea',
                '7302'=>'Idea',
                '9768'=>'Aircel','8898'=>'Aircel','8286'=>'Aircel',
                '9076'=>'Videocon','8828'=>'Videocon','8268'=>'Videocon',
                '9320'=>'Reliance(CDMA)','9321'=>'Reliance(CDMA)',
'9322'=>'Reliance(CDMA)',
                '9323'=>'Reliance(CDMA)', '9324'=>'Reliance(CDMA)',
'7498'=>'Reliance(CDMA)',
                '8448'=>'Reliance(CDMA)',
                '9220'=>'Tata (CDMA)','9221'=>'Tata (CDMA)','9222'=>'Tata
(CDMA)',
```

```
                    '9223'=>'Tata (CDMA)','9224'=>'Tata (CDMA)','9209'=>'Tata
(CDMA)'
                );

    if($NSP[$preMSISDN]){
        return $NSP[$preMSISDN];
    }else{
        return "Other";
    }

}

function resGen($rand,$ki,$length=128){
    $count = round($length/16);
    $rand_arr = explode("-",$rand);
    $ki_arr = explode("-",$ki);
    for($i=0;$i<$count;$i++){
        $left = hexdec($rand_arr[$i]) ^ hexdec($ki_arr[$i+$count]);
        $right = hexdec($ki_arr[$i]) ^ hexdec($rand_arr[$i+$count]);
        $res64[$i] = $left ^ $right;
    }
    $count2 = round($count/2);
    for($i=0;$i<$count2;$i++){
        $res32[$i] = dechex($res64[$i] ^ $res64[$count2+$i]);
    }
    return implode('-',$res32);
}
?>
```

b) Frontend HTML & Javascript :

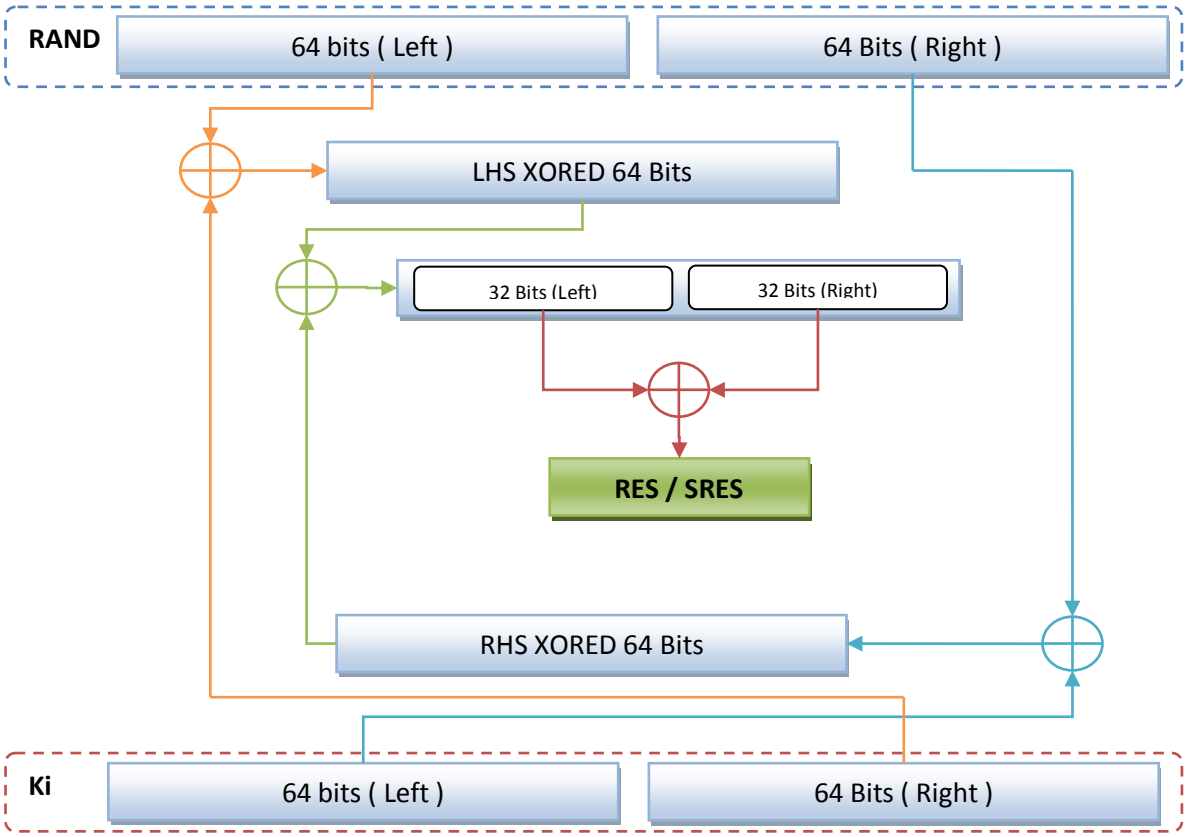
```
<?php
/*
 * ************************************************************
 ***************  MCS EXPT3 ******************************
 ************************************************************/
 /* Designed & Developed by
 /*                                        - Shiburaj Pappu
 /* ************  S.P.I.T ************************************
 /* ********** M.E (EXTC) Sem-II ****************************
 */
?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=Cp1252">
 <link type="text/css" href="style.css" rel="stylesheet" />
 <script type="text/javascript" src="jquery.js"></script>
 <script type="text/javascript">
        jQuery(document).ready(function() {

            ////////////////////////////////////////////////////////////
            ////////////////////  Making Sim ///////////////////////////
            ////////////////////////////////////////////////////////////
            $('#mkSIM').removeAttr('disabled');
            $('#msisdn').removeAttr('disabled');
            $('#register').attr('disabled','disabled');
            $('#authenticate').attr('disabled','disabled');
            $('#mearea').attr('value','');
            $('#mscarea').attr('value','');

            $('#direcImg').css('display','none');
            $('#mkSIM').click(function(){
                var simMSISDN = $('#msisdn').attr('value');

$.post('functions.php?action=makesim',{'MSISDN':simMSISDN},function(data){
                    $('#simvars').css('display','block');
                    $('#simMSISDN span').html(data.MSISDN);
                    $('#simIMSI span').html(data.IMSI);
                    $('#simIMEI span').html(data.IMEI);
```

```
                    $('#simKival').attr('value',data.Ki);
                    $('#simKiMSC span').html(data.Ki);
                    $('#simNSP span').html(data.NSP);
                    $('#mkSIM').attr('disabled','disabled');
                    $('#register').removeAttr('disabled');
                    $('#msisdn').attr('disabled','disabled');
                },"json");
            });

            ////////////////////////////////////////////////////////////
            ////////////////////   Registering on Netwrok   ////////////////
            ////////////////////////////////////////////////////////////
            $('#register').click(function(){
                var temp = $('#mearea').attr('value');
                $('#register').attr('disabled','disabled');
                $('#mearea').attr('value',temp + '>> Registering on
Network...');
                $('#direcImg').css('display','block');
                var temp = $('#mearea').attr('value');
                $('#mearea').attr('value',temp + '\n>> Sending IMSI & MSISDN
...');
                var simMSISDN = $('#simMSISDN span').html();
                var simIMSI = $('#simIMSI span').html();
                var temp = $('#mscarea').attr('value');
                $('#mscarea').attr('value',temp + '>> Recieving Registeration
Request ...');
                $('#regvars').css('display','block');
                $('#recdMSISDN span').html(simMSISDN);
                $('#recdIMSI span').html(simIMSI);

$.post('functions.php?action=register',{'MSISDN':simMSISDN,'IMSI':simIMSI},func
tion(data){
                    $('#direcImg').attr('src','left.png');
                    var temp = $('#mscarea').attr('value');
                    $('#mscarea').attr('value',temp + '\n>> Registration
Successfull ...');
                    var temp = $('#mscarea').attr('value');
                    $('#mscarea').attr('value',temp + '\n>> Sending TMSI
number...');
                    $('#simTMSI span').html(data.regdata.TMSI);

                    $('#genTMSI span').html(data.regdata.TMSI);
                    var temp = $('#mearea').attr('value');
                    $('#mearea').attr('value',temp + '\n>> Recieved TMSI
Number,Registration Successfull ...');
                    $('#authenticate').removeAttr('disabled');
                },"json");
            });


            ////////////////////////////////////////////////////////////
            ////////////////////   Authenticating on Netwrok   ////////////////
            ////////////////////////////////////////////////////////////
            $('#authenticate').click(function(){
                var temp = $('#mearea').attr('value');
                $('#authenticate').attr('disabled','disabled');
                $('#mearea').attr('value',temp + '\n>> Requesting
Authentication of Device...');
                $('#direcImg').attr('src','right.png');
                var temp = $('#mearea').attr('value');
                $('#mearea').attr('value',temp + '\n>> Sending TMSI...');
                var simTMSI = $('#simTMSI span').html();
                var simMSISDN = $('#simMSISDN span').html();
                var temp = $('#mscarea').attr('value');
                $('#mscarea').attr('value',temp + '\n>> Recieving
Authentication Request ...');
                $('#regvars').css('display','none');
                $('#authvars').css('display','block');
                $('#recdTMSI span').html(simTMSI);
```

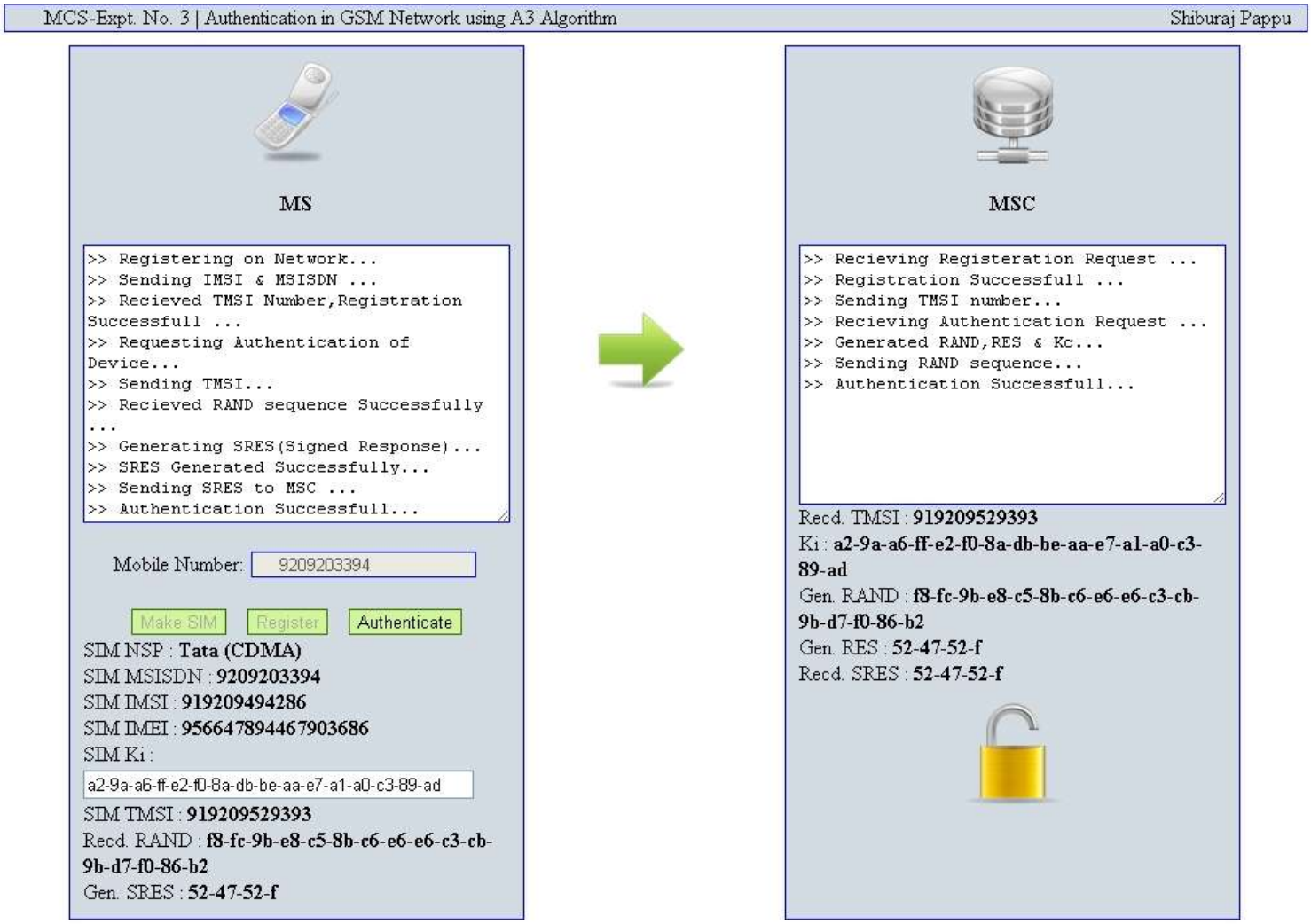
```
$.post('functions.php?action=authenticate',{'MSISDN':simMSISDN,'TMSI':simTMSI},
function(data){
                    $('#direcImg').attr('src','left.png');
                    var temp = $('#mscarea').attr('value');
                    $('#mscarea').attr('value',temp + '\n>> Generated RAND,RES
& Kc...');
                    var temp = $('#mscarea').attr('value');
                    $('#mscarea').attr('value',temp + '\n>> Sending RAND
sequence...');
                    $('#genRAND span').html(data.RAND);
                    $('#simRAND span').html(data.RAND);
                    $('#genRES span').html(data.RES);
                    var temp = $('#mearea').attr('value');
                    $('#mearea').attr('value',temp + '\n>> Recieved RAND
sequence Successfully ...');


                    var simRAND = $('#genRAND span').html();
                    var simKi = $('#simKival').attr('value');
                    var temp = $('#mearea').attr('value');
                    $('#mearea').attr('value',temp + '\n>> Generating
SRES(Signed Response)...');

                    // generate SRES

$.post('functions.php?action=gensres',{'RAND':simRAND,'Ki':simKi},function(data
){

                        var temp = $('#mearea').attr('value');
                        $('#mearea').attr('value',temp + '\n>> SRES Generated
Successfully...');
                        $('#simSRES span').html(data.SRES);
                        var temp = $('#mearea').attr('value');
                        $('#mearea').attr('value',temp + '\n>> Sending SRES to
MSC ...');

                        //// Sending SRES
                        mscRES = $('#genRES span').html();
                        $('#recdSRES span').html(data.SRES);
                        $('#direcImg').attr('src','right.png');

$.post('functions.php?action=sendsres',{'SRES':data.SRES,'RES':mscRES},function
(data){
                            $('#authImg').css('display','block');
                            if(data.status == 'success'){
                                var temp = $('#mearea').attr('value');
                                $('#mearea').attr('value',temp + '\n>>
'+data.reason);
                                $('#authImg img').attr('src','unlocked.png');
                                var temp = $('#mscarea').attr('value');
                                $('#mscarea').attr('value',temp + '\n>>
'+data.reason);
                            }else{
                                var temp = $('#mearea').attr('value');
                                $('#mearea').attr('value',temp + '\n>>
'+data.reason);
                                $('#authImg img').attr('src','locked.png');
                                var temp = $('#mscarea').attr('value');
                                $('#mscarea').attr('value',temp + '\n>>
'+data.reason);
                            }


                        },"json");
                    },"json");

                    $('#authenticate').removeAttr('disabled');
                },"json");
```

```
            });
        });

 </script>
<title>MCS-Expt3 | Authentication in GSM Network</title>
</head>
    <body>
        <div style="width: 100%;border:1px solid
blue;background:#D3DCE3;height: 20px;">
            <div style="width: 50%;float: left;text-align: center;">MCS-Expt.
No. 3 | Authentication in GSM Network using A3 Algorithm</div>
            <div style="width: 50%;float: right;text-align: right;">Shiburaj
Pappu   </div>
        </div>
        <div class="col1">
            <div class="box">
                <div><img src="phone.png" width="80" height="80" /></div>
                <div><h4>MS</h4></div>
                <div><textarea id="mearea" class="codearea"
readonly="readonly">hi</textarea></div><br />
                <div>Mobile Number:
                    <input type="text" name="msisdn" id="msisdn" /><br /><br />
                    <input type="button" id="mkSIM" class="btn" value="Make
SIM" />  
                    <input type="button" id="register" class="btn"
value="Register" />  
                    <input type="button" id="authenticate" class="btn"
value="Authenticate" />
                </div>
                <div id="simvars">
                    <div id="simNSP">SIM NSP : <span>--</span></div>
                    <div id="simMSISDN">SIM MSISDN : <span>--</span></div>
                    <div id="simIMSI">SIM IMSI : <span>--</span></div>
                    <div id="simIMEI">SIM IMEI : <span>--</span></div>
                    <div id="simKi">SIM Ki : <input type="text" name="simKival"
value="" id="simKival" /></div>
                    <div id="simTMSI">SIM TMSI : <span>--</span></div>
                    <div id="simRAND">Recd. RAND : <span>--</span></div>
                    <div id="simSRES">Gen. SRES : <span>--</span></div>
                </div>
            </div>
        </div>
        <div class="col2">
            <div><img id="direcImg" src="right.png" width="80" height="80"
/></div>
        </div>
        <div class="col3">
            <div class="box">
                <div><img src="msc.png" width="80" height="80" /></div>
                <div><h4>MSC</h4></div>
                <div><textarea id="mscarea" class="codearea"
readonly="readonly"></textarea></div>
                <div id="regvars">

                    <div id="recdMSISDN">Recd. MSISDN : <span>--</span></div>
                    <div id="recdIMSI">Recd. IMSI : <span>--</span></div>
                    <div id="genTMSI">Gen. TMSI : <span>--</span></div>
                </div>
                <div id="authvars">
                    <div id="recdTMSI">Recd. TMSI : <span>--</span></div>
                    <div id="simKiMSC">Ki : <span>--</span></div>
                    <div id="genRAND">Gen. RAND : <span>--</span></div>
                    <div id="genRES">Gen. RES : <span>--</span></div>
                    <div id="recdSRES">Recd. SRES : <span>--</span></div>
                </div>
                <div id="authImg"><img src="locked.png" width="80" height="80"
/></div>
            </div>
        </div>
    </body>
</html>
```

A3 Algorithm Logic:



Graphic User Interface :



Conclusion : **Thus we have studied Authentication in GSM Network using A3 Algorithm.**