Due to the complicity of the nowadays life, people need to do several things at the same time in work, at home. This can be done only if personal resource can be accessed securely where they are located in computers at home or in office. This paper presents an algorithm of accessing securely a desktop computer (DC) at home remotely to perform some tasks using a mobile phone (MP), transferred tokens were protected by use of RC5 encryption code. The obtained results show that proposed algorithm can be applied to perform tasks to help people in work or at home simultaneously.

**KEYWORDS:** MP, remote DC, resource access, RC5.
Fig. 3. shows messages exchange between remote DC and a MP, messages are exchanged through SIM cards integrated in both systems, the MP send a message were remote DC return an ACK.

2.3 Message configuration
Messages to be send from any HP have to be configured first in the proposed system. Few messages are chosen for testing noting that any type of message can work. Menu of configuring the system is shown in Fig. 4. Message id, command and descriptions have to give to the system.

2.4 MP(SIM₁) connection to Remote DC(SIM₂)
The MP was integrated with the SIM₁, it works in any local coverage, simply information such as dial Remote DC number, message id, the command type for selected message and its description will be shown. Fig. 5. shows sending message menu by the MP. Message is directly sent to the Remote DC.

2.5 Message receiving by remote DC (SIM₂)
The remote DC with an integrated SIM card, it can receive a message and store it into a directory prepared for that proposes, that is if and only if the remote DC (SIM₂) is within the local coverage.

2.6 Message Loading in remote DC (SIM₂) directory
A program written in VBasic is used to load a received message and consult a database to select the suitable action. Instruction are written in a VBase code and fill into a data base, each instruction was numbered, once the received number matches the database an action is taken by the remote DC. Actions are numbered (01 to 07). Remote DC peeps if it receives a message code equals to “06”. To perform action reset DC, the received message must be “01” and so on as described in Table 1.

2.7 ACK to MP of action performance.
Any received message must have its corresponding in data base that easily helps in performing proper action by the remote DC. Then an ACK of performing the required action have to be sent to the MP (SIM₁) and displayed on its screen.

2.8 ACK to MP of wrong choice
In case a DC (SIM₁) receives un valid message which means receiving any text or number which is not in database an ACK of wrong message is prepared and sent back to MP (SIM₁).

2.9 Data Protection
Data transferred between DC and MP have to be encrypted when it sent and decrypted at time it received, hence the proposed algorithm uses RC5 for encryption/decryption of data. In MP a pair of public key is produced (public key and private key), then send public key to the remote DC. Remote DC uses it to encrypt the RC5 secret key and send it to MP. MP decrypts the received key and uses it for any further encryption/decryption between them.

To avoid an authorized access, each command sent by MP to DC is encrypted with a shared key between the two parties and using RC5 algorithm. A replay is received using same procedure. Noting that with use of symmetric encryption algorithm will protect data and wont delay the system.

3. RESULTS
Testing the proposed system it gives good results. As mentioned in the previous paragraph the received is load in the directory and a written program is consulted to select the proper action. As shows in Fig. 6, the remote DC (SIM₂) received a message with value “05” from MP (SIM₁) which means run a calculator.

4. RESULT ANALYSIS
As shown in results it easy to invoke a remote DC where it was located in office at home to copy to do some work and no need to use internet to do so, just use the MP with a local coverage to perform certain work. Results shows among hundred messages, the proposed system recognizes ninety seven of them were by the remote makes 97% were as shown in the field correct and recognized (CR) in the
Table 2 and only 3 messages did not recognized due to distortion caused by bad coverage. Table 2, shows performance results obtained by the proposed system.

Table 2. Proposed system Acceptance and Rejection

<table>
<thead>
<tr>
<th>No.</th>
<th>MT</th>
<th>NM</th>
<th>R</th>
<th>NR</th>
<th>CR</th>
<th>WR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DT</td>
<td>50</td>
<td>49</td>
<td>1</td>
<td>98%</td>
<td>2%</td>
</tr>
<tr>
<td>2</td>
<td>ST</td>
<td>50</td>
<td>48</td>
<td>2</td>
<td>96%</td>
<td>4%</td>
</tr>
<tr>
<td>3</td>
<td>TM</td>
<td>100</td>
<td>97</td>
<td>3</td>
<td>97%</td>
<td>3%</td>
</tr>
</tbody>
</table>

Where:
MT message type, NM number of messages, R recognized, NR non recognized, CR correct and recognized, WR wrong not recognized, DT different type, ST same message and TM total messages.

5. RELATED WORK
The idea of this work is similar to the work provided by [7] and [8] that is accessing a remote desktop computer using hand phone. The mentioned works use a Wi-Fi network in establishing a connection between the DC and MP, where in the proposed system uses local MP coverage and this gives the proposed system an advantage in enhancing the mobility by increasing the access range and secure data transaction between two parties.

6. CONCLUSION
A secure system of accessing a remote DC using a MP was presented main while paper investigates similar systems. Paper also shows how to secure messages sent to the DC remotely.

REFERENCES