Faculty of engineering - Shoubra
Benha University

Research Project

in fulfillment of the requirements of

Department	**Engineering Mathematics and Physics**
Division	**----------**
Academic Year	**2019-2020 Preparatory**
Course name	**Computer**
Course code	**ECE001**

Title: -

Cryptography By:

	Name	Edu mail	B.N
1	عمرو محمد حسن محمد قنديل	amr195646@feng.bu.edu.eg	583

Link to GitHub website:
Link to GitHub page:

Approved by:

Examiners committee	Signature
Dr. Ahmed Bayoumi	
Dr. Shady Elmashad	
Dr. Abdelhamid Attaby	

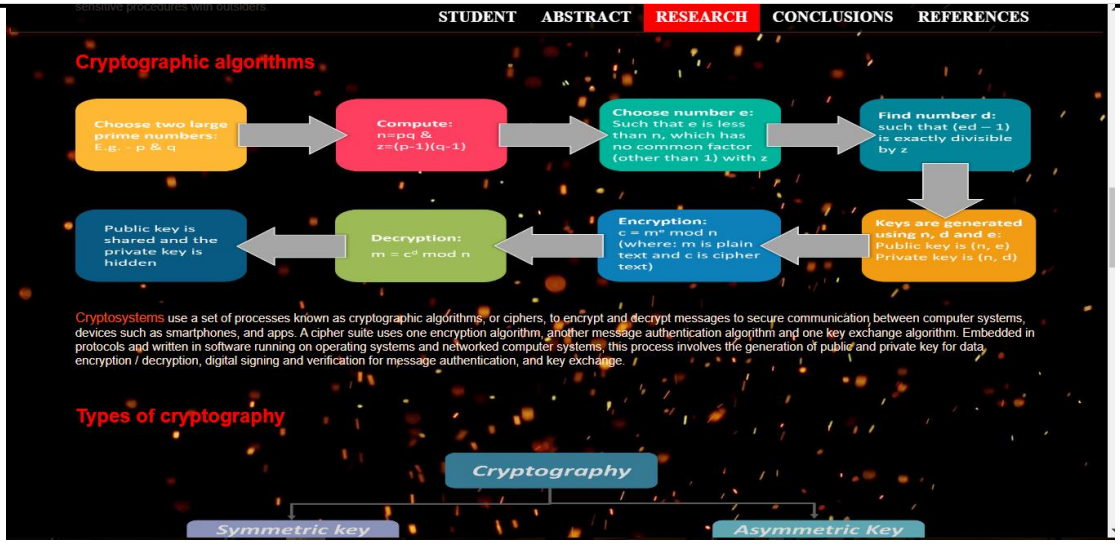
\

Application brief

Cryptography is Information Security science. The word derives from the Greek kryptos, which means hidden. Cryptography includes techniques such as microdots, merging words with images, and other ways of concealing storage or transit information. Modern cryptography intersects the disciplines of mathematics, electrical engineering and computer science. Cryptographic applications include ATM cards, computer passwords, and electronic commerce.Before the modern age cryptology was almost synonymous with encryption, the conversion of information from a readable state to apparent absurdity. The sender retained the ability to decrypt the information and thus to avoid being able to read it by unwanted persons. The methods used to perform cryptology have become increasingly complex and their application more widespread since the WWI and the advent of the computer.Modern cryptography follows a strongly scientific approach, and designs cryptographic algorithms around assumptions of computational hardness, making such algorithms difficult for an adversary to break through. In theory, such systems are not unbreakable but it is impossible to do so by any practical means. So these schemes are computationally secure. Secure schemes exist that can not be proven to be broken — an example is the one-time pad — but these schemes are harder to implement than the theoretically breakable but computationally secure mechanisms.Tags: cryptography subject, cryptography ppt, cryptography pdf, cryptography seminar, latest

seminar topic cryptography, full seminar report on cryptography, source code cryptography

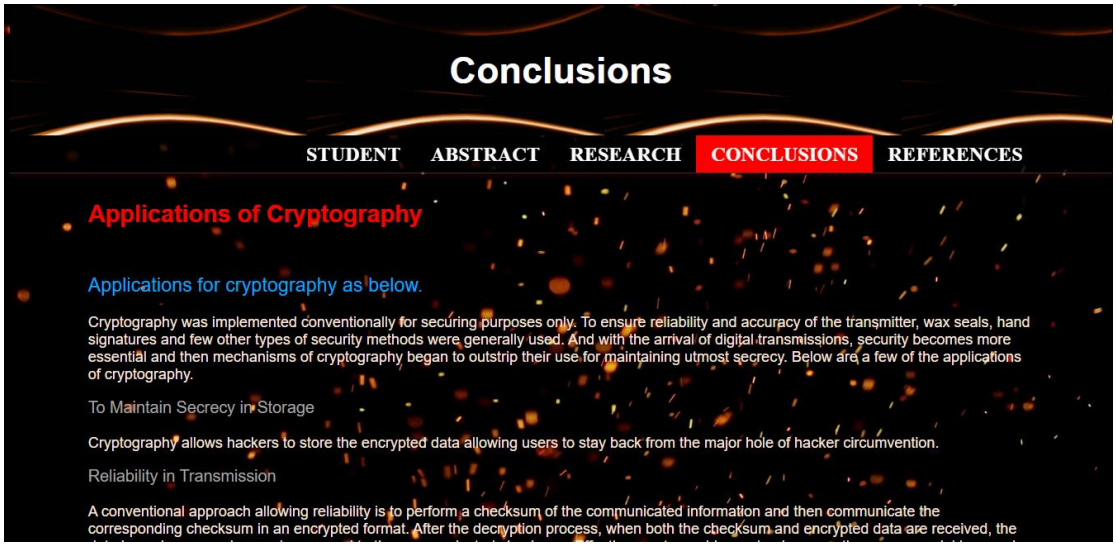
Screen shots


STUDENT ABSTRACT RESEARCH CONCLUSIONS REFERENCES
Cryptographic algorithms
Choose two large prime numbers: E.g. - p & q
Compute: n=pq & z=(p-1)(q-1)
Choose number e: Such that e is less than n, which has no common factor (other than 1) with z
Find number d: such that (ed − 1) is exactly divisible by z
Keys are generated using n, d and e: Public key is (n, e) Private key is (n, d)
Encryption: c = m^e mod n (where: m is plain text and c is cipher text)
Decryption: m = c^d mod n
Public key is shared and the private key is hidden
Cryptosystems use a set of processes known as cryptographic algorithms, or ciphers, to encrypt and decrypt messages to secure communication between computer systems, devices such as smartphones, and apps. A cipher suite uses one encryption algorithm, another message authentication algorithm and one key exchange algorithm. Embedded in protocols and written in software running on operating systems and networked computer systems, this process involves the generation of public and private key for data encryption / decryption, digital signing and verification for message authentication, and key exchange.
Types of cryptography
Cryptography
Symmetric key
Asymmetric Key


STUDENT ABSTRACT RESEARCH CONCLUSIONS REFERENCES
Cryptography tools are more useful in the situations of signature confirmation, code signing and to perform other cryptography activities. Here are the extensively used cryptography tools.
1. Security Token
This token is used for user verification. To execute a protected exchange of information, a security token must be encrypted. Also, the HTTP protocol provides complete statefulness. So, a browser uses the server-side formulated token to go on with the state. In general, remote authentication is the method that moves.
2. JCA
That is the tool used to authorize the process of encryption. This tool could be called Cryptographic Java libraries. These Java libraries are included with predefined activities where prior to implementation they need to be imported. Despite being the Java library, it works in proportion to other frameworks and thus supports multiple application development.
3. SignTool.exe
This is Microsoft's popular tool mostly used to sign the files. The prominent feature supported by this tool is the addition of a signature and time stamp to any kind of file. This holds the ability to authenticate the file with the time mark in the file. The entire functionality in SignTool.exe ensures increased file reliability.
4. Docker
One can build huge applications using the docker. The information kept in the docker is entirely in encrypted format. Cryptography must be strictly followed in this, in order to move with data encryption. In addition, both files and information are encrypted, so that no one can access the things that do not have an exact access key. Docker is also envisaged as a cloud storage that allows users to manage the information on a dedicated or shared server.
5. CertMgr.exe
This is the file to install as it is in the.exe-extension format. CertMgr holds good handling of different certificates. In addition, it even handles CRLs where those are lists for the revocation of certificates. The aim of cryptography in the development of certificates is to ensure that the information exchanged between the parties is more protected and this tool supports the addition of additional bits in protection.
6. Authentication Using Key
Here, the encrypted information needs to be decrypted via keys. Everyone can easily understand the normal information whereas the encrypted information is known only to the intended user. There are two types of encryption techniques in this tool and these are:
CSymmetric Key Cryptography
Asymmetric Key Cryptography
So, cryptography tools are mostly used in every secured activity and there are many tools available where users can choose the one depending on their necessities.

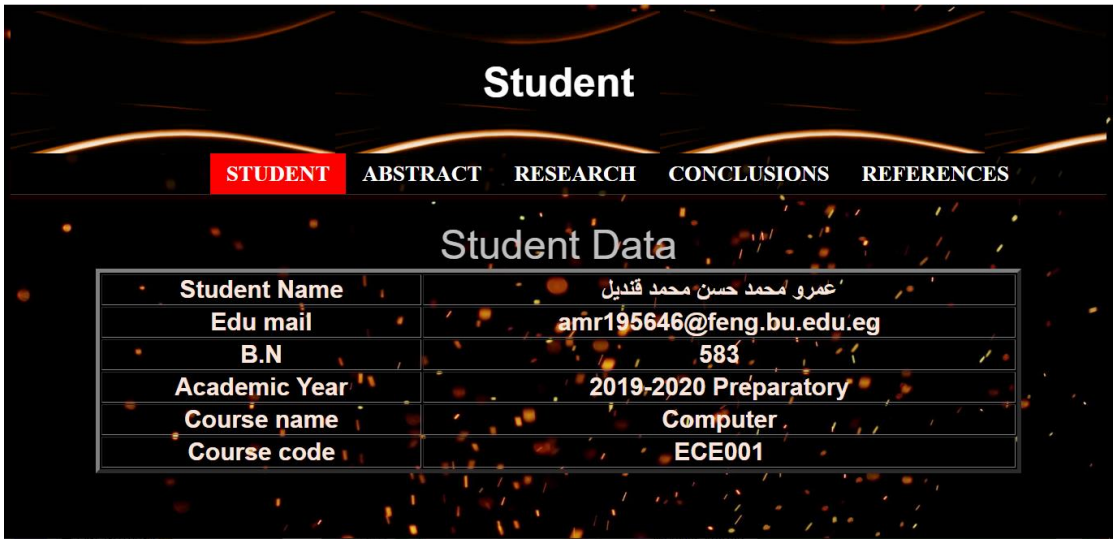
Abstract

Conclusions



References

Student



Source code

Style

```
<!DOCTYPE HTML>
<html>
    <head>
     <title>Research</title>
      <meta charset="utf-8"
    </head>
    <style>
body {

        background-image: url(
        https://img.uxfree.com/wp-content/uploads/2018/02/waves-or-yellow-and-orange-embers-floating-on-dark-back
        ground-in-4k.jpg);
        background-repeat: no-repeat;
        background-attachment: fixed;
        background-size: 100% 100%;
}
.header {

        padding: 25px;
        text-align: center;
        background-image: url(https://sfwallpaper.com/images/black-and-orange-backgrounds-6.jpg);
        color: white;
        font-size:25px;
        font-family: Arial, Helvetica, sans-serif,"Times New Roman", Times, serif;
}
a{
        color: white;
        font-size:27px;
        text-decoration: none
}
```

```
}
a{
        color: white;
        font-size:27px;
        text-decoration: none
}
a:hover{
        color: white;
        font-weight: bold;
        font-size:32px
}
a:active{
         color:white;
        color: #4D5656  ;
        font-weight: normal
}
.header2{
        font-family: Arial, Helvetica, sans-serif,"Times New Roman", Times, serif;
        color:  #f00;
        margin: 10px 100px ;
    padding: 5px;;
    }

.paragraph{
 color: #FCE6DE;
  font-family: Arial, Helvetica, sans-serif,"Times New Roman", Times, serif;
  font-size: 20px;
  margin: 10px 100px ;
  padding: 5px;
```

```
}
 nav{


  width: 100%;
  height: 50px;
  background: rgba(0,0,0,.8);
  border-top: 1px solid rgba(255,255,255,.2);
  border-bottom: 1px solid rgba(255,255,255,.2);
  position:sticky;
  top:0;
  left:0;
  border-top:0;
  box-shadow: -1px 6px 1px rgba(198, 0, 0, 0.1);

 }
nav ul{
 display: flex;
 margin: 0;
 padding: 0 100px;
 float:right;
}
nav ul li{
 list-style: none;

}
nav ul li a{
 display: block;
 color: #fff;
 padding: 0 20px;
 text-decoration: none;
 text-transform: uppercase;
 font-weight: bold;
 line-height: 50px;
}
```

```
 text-decoration: none;
 text-transform: uppercase;
 font-weight: bold;
 line-height: 50px;
}
nav ul li a:hover,
nav ul li a.active{

 background: #f00;
}
.img{text-align: center;
margin: 10px 100px ;
   padding: 5px;}

</style>
```

links, headers, images & paragraphs

```
    <body>
<div class="header">
 <h1>Cryptography</h1>
  </div>
    <nav>
<ul>
   <li><a href="Student.html">Student</a></li>
   <li><a href="Abstract.html">Abstract</a></li>
   <li><a style=""class="active"" href="index.html">Research</a></li>
   <li><a href="Conclusions.html">Conclusions</a></li>
   <li><a href="References.html">References</a></li>
 </ul>
  </nav>



   <div class="header2">
    <h1>Introduction</h1>
   </div>

   <div class="img"> <img src="2.png" width="100%" height="400">
   </div>
   <div class="paragraph">
   <p><span style="color: #FF4F0A;font-size: 1.1em;text-decoration: underline">Cryptography</span> is a method of protecting
   information and communication through the use of codes, so it can be read and processed only by those for whom the
   information is intended. The "crypt-" prefix means "hidden" or "vault" – and the "-graphy" suffix stands for "writing."In
   computer science, cryptography refers to secure information and communication techniques derived from mathematical
   concepts, and a set of rule-based calculations called algorithms, transforming messages in hard-to-decipher ways. These
   deterministic algorithms are used for key generation cryptography, digital signing, data privacy protection verification,
   internet web browsing, and confidential communications such as credit card transactions and e-mail.</p>
  </div>

   <div class="header2">
     <h1>Cryptography Techniques</h1>
    </div>
```

```
 <div class="header2">
  <h1>Applications of Cryptography</h1>
 </div>


<div class="paragraph">
<p><span style="color: #0AA9FF;font-size: 1.3em">Applications for cryptography as below.</span><br><br> Cryptography was impl
<p><span style="color: #A4A5A5;font-size: 1.1em">To Maintain Secrecy in Storage</span><br><br> Cryptography allows hackers to
<p><span style="color: #A4A5A5;font-size: 1.1em">Reliability in Transmission</span><br><br>A conventional approach allowing r
<p><span style="color: #A4A5A5;font-size: 1.1em">Authentication of Identity</span><br><br> Cryptography is strongly linked to

</div>


<div class="header2">
  <h1>Examples</h1>
 </div>


<div class="paragraph">
<p><span style="color: #0AA9FF;font-size: 1.3em">The examples of cryptography include the following.</span><br><br>
End-to - end encryption in WhatsApp is one of the prominent examples of cryptographic encryption these days. This feature is
</p>

</div>
```

Lists

```
    </div>
    <div class="paragraph">
    <p><span style="color: #FF4F0A;font-size: 1.1em">Cryptography</span> tools are more useful in the situations of signature confirmation, code
    signing and to perform other cryptography activities. Here are the extensively used cryptography tools.
      <ol>
    <li><span style="color: #63bee8;font-size: 1.2em;text-decoration: underline">Security Token</span><br>This token is used for user verification.
    To execute a protected exchange of information, a security token must be encrypted. Also, the HTTP protocol provides complete statefulness. So, a
    browser uses the server-side formulated token to go on with the state. In general, remote authentication is the method that moves. </li><br>
    <li><span style="color: #63bee8;font-size: 1.2em;text-decoration: underline">JCA </span><br>That is the tool used to authorize the process of
    encryption. This tool could be called Cryptographic Java libraries. These Java libraries are included with predefined activities where prior to
    implementation they need to be imported. Despite being the Java library, it works in proportion to other frameworks and thus supports multiple
    application development.
    </li><br>
    <li><span style="color: #63bee8;font-size: 1.2em;text-decoration: underline">SignTool.exe</span><br>
    This is Microsoft's popular tool mostly used to sign the files. The prominent feature supported by this tool is the addition of a signature and
    time stamp to any kind of file. This holds the ability to authenticate the file with the time mark in the file. The entire functionality in
    SignTool.exe ensures increased file reliability.</li> <br>
    <li><span style="color: #63bee8;font-size: 1.2em;text-decoration: underline">Docker </span><br>One can build huge applications using the docker.
    The information kept in the docker is entirely in encrypted format. Cryptography must be strictly followed in this, in order to move with data
    encryption. In addition, both files and information are encrypted, so that no one can access the things that do not have an exact access key.
    Docker is also envisaged as a cloud storage that allows users to manage the information on a dedicated or shared server.
    </li><br>
    <li><span style="color: #63bee8;font-size: 1.2em;text-decoration: underline">CertMgr.exe</span><br>
    This is the file to install as it is in the.exe-extension format. CertMgr holds good handling of different certificates. In addition, it even
    handles CRLs where those are lists for the revocation of certificates. The aim of cryptography in the development of certificates is to ensure
    that the information exchanged between the parties is more protected and this tool supports the addition of additional bits in protection.
    </li><br>
    <li><span style="color: #63bee8;font-size: 1.2em;text-decoration: underline">Authentication Using Key</span><br>
    Here, the encrypted information needs to be decrypted via keys. Everyone can easily understand the normal information whereas the encrypted
    information is known only to the intended user. There are two types of encryption techniques in this tool and these are:<ul>
    <li><span style="color: #A4A5A5;font-size: 0.9em">CSymmetric Key Cryptography</span></li>
    <li><span style="color: #A4A5A5;font-size: 0.9em">Asymmetric Key Cryptography</span></li></li>
  </ul>
    So, cryptography tools are mostly used in every secured activity and there are many tools available where users can choose the one depending on
    their necessities.
    </li><br>
  </ol>
    </p>
    </div>
```

```
    </div>
    <div class="paragraph">
    <ol>
    <li><a href="https://www.elprocus.com/cryptography-and-its-concepts/">Elprocus</a></li><br>
    <li><a href="https://searchsecurity.techtarget.com/definition/cryptography">Searchsecurity</a></li><br>
    <li><a href="https://061076e0q-1105-y-https-academic-eb-com.mplbci.ekb.eg/levels/collegiate/article/cryptography/472150">Ekb.e
    <li>Katz, J., & Lindell, Y. (2014). Introduction to modern cryptography. CRC press.</li><br>
    <li>Menezes, A. J., Katz, J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography. CRC press.</li>
  </ol>
    </div>
```

Tables

```
        <br>
        <div class="paragraph">
        </table>

        <table border="5" style="width:100%"  >
         <caption>Student Data</caption>
    <tr>
      <th style="font-size:30px ">Student Name</th>
      <th style="font-size:30px ">عمرو محمد حسن محمد قنديل</th>
    </tr>
    <tr>
      <td>Edu mail</td>
      <td>amr195646@feng.bu.edu.eg</td>
    </tr>
    <tr>
      <td>B.N</td>
      <td>583</td>
    </tr>
    <tr>
      <td>Academic Year</td>
      <td>2019-2020 Preparatory  </td>
    </tr>
    <tr>
      <td>Course name</td>
      <td>Computer</td>
    </tr>
    <tr>
      <td>Course code</td>
      <td>ECE001</td>
    </tr>
  </table>
        <div/>
```

```
tbody td {text-align: center;
font-weight: bold;
font-size: 30px;
color: #FCE6DE
}
table caption{font-size: 2.5em;
color: #C1C1C1}
```