**Report on research of Engineering of shubra department of Banha University**

**URL at gitHub : https://github.com/isramemduh**

Topic name: Intro to cryptography

ABSTRACT:

Encryption is the technique used to convert a plain text message into cipher text which is unreadable to human or machine. Encryption is of two types, namely: symmetric key encryption and asymmetric key encryption. Encryption scheme in which both the sender and receiver share the same key is referred to as symmetric key encryption scheme. Encryption scheme in which encryption and decryption are performed using different keys, i.e. a public key and a private key is referred to as asymmetric key encryption scheme. This paper presents a performance comparison between four popular and commonly used encryption algorithms: Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA). DES, 3DES, and AES are symmetric key encryption algorithms while RSA is an asymmetric key encryption algorithm. The comparative analysis is carried out based on their Architecture, Scalability, Flexibility, Reliability, Security and Limitation that are essential for secured communication (Wired or Wireless).The results achieved form a baseline in choosing an encryption algorithm that is more efficient and that have strength against cryptanalysis.

INTRODUCTION:

In this era of universal electronic connectivity, the possibility of theft of information by hackers and eavesdroppers is very high. There is indeed no time at which security does not matter. The tremendous growth in computer systems and their interconnections via networks have increased the dependence of organizations and individuals on the information stored and communicated using these systems. There is a need to protect data and resources from disclosure and to protect systems from network based attacks. For secure communication over public network data can be protected by the method of encryption. Encryption converts that data by any encryption algorithm using the ‘key’ in scrambled form. Only user having access to the key can decrypt the encrypted data. Encryption is a fundamental tool for the protection of sensitive information. The purpose of using encryption is privacy (preventing disclosure or confidentiality) in communications. The main goal of cryptography is keeping data secure from unauthorized users. Original data that is readable and understandable either by a person or by a computer is called plain text whereas the data which is unreadable to human or machine is called cipher text. The technique to convert a plain text message into cipher text is called encryption (Paar and Pelzi, 2010).

Encryption is a way of talking to someone while other people are listening, but such that other people cannot understand what you are saying. Encryption algorithms play a big role in providing data security against malicious attacks. In mobile devices security is very important and different types of algorithms are used to prevent malicious attack on the transmitted data. Encryption algorithm can be categorized into symmetric key (private) and asymmetric (public) key.

In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys (Davis, 2003). Public key is used for encryption and private key is used for decryption (e.g. Rivest-Shamir-Adleman). According to (Elminaam et al., 2008), asymmetric encryption techniques are about 1000 times slower than Symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use a stronger key than symmetric encryption technique Public key encryption is based on mathematical function, computationally intensive and is not very efficient for small mobile devices (Alexandre et al., 2006). The present scenario uses encryption which includes mobile phones, passwords, smart cards and DVDs. It has permeated everyday life and is heavily used by much web application. According to (Jeeva et al., 2012), Encryption algorithms play a vital role in information systems. The study discovers the progress of Encryption algorithms in terms of their diversity of applications. Some of the Encryption algorithms have been developed to make transmission and storage of data more secured and confidential. Different levels of securities are offered by different algorithms depending on how difficult it is to break them (Elminaam et al., 2010). If it is difficult to recover the plain text in spite of having substantial amount of cipher text then an algorithm is unconditionally secured. Dhawan (2002) compared the performance of the different encryption algorithms by conducting experiments inside .NET framework. This study provides evaluation of four of the most common encryption algorithms namely: Data Encryption Standard (DES), Triple Data Encryption Standard (3-DES), Advanced Encryption Standard (AES or Rijndael), and Rivest-Shamir-Adleman (RSA). The rest of this paper has been organized as follows: section 2 presents the research focus, section 3 presents the methodology, section 4 presents the results and discussion and section 5 presents the conclusion.

Subject:

2. REVIEW OF RELATED WORKS

This paper presents a detailed study of the popular Encryption Algorithms such as RSA, DES, 3DES and AES. The use of internet and network is growing rapidly, so there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used (Nadeem, 2006). In this paper, a survey on the existing works on the Encryption techniques has been done. To sum up, all the techniques are useful for real-time Encryption. Each technique is unique in its own way, which might be suitable for different applications and has its own significance. According to research done and literature survey it can be found that AES algorithm is most efficient in terms of speed, time, throughput, and avalanche effect. The security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data. Our future work will explore this concept and a combination of algorithms will be applied either sequentially or parallel, to setup a more secure environment for data storage and retrieval.

2.1 Overview of Various Encryption Algorithms Thakur et al. (2011) discussed a fair comparison between three most common symmetric key cryptography algorithms: DES, AES and Blowfish. The main concern was the performance of the algorithms under different settings, the presented comparisons takes into consideration the behavior and performance of the algorithms when different data loads are used. The comparison was made on the basis of these parameters: speed, block size, and key size. Simulation program was implemented using java programming. It was concluded that blowfish has better performance than other common encryption algorithms used. Marwaha et al. (2013) discussed three algorithms DES, 3DES and RSA. DES and 3DES are symmetric key cryptographic algorithms and RSA is an asymmetric key cryptographic algorithm. Algorithms have been analyzed on their ability to secure data, time taken to encrypt data and throughput the algorithm requires. Performance of different algorithms was different according to the inputs. It was concluded that confidentiality and scalability provided by 3DES over DES and RSA is much higher and makes it suitable even through DES consumes less power memory and time to encrypt and decrypt the data but on security from DES can be easily broken by brute force technique as compared to 3DES and RSA, making it the last secure algorithm.

Alam et al. (2013) discussed performance and efficiency analysis of different block cipher algorithms (DES, 3DES, CAST-128, BLOWFISH, IDEA and RC2) of symmetric key cryptography. Block cipher algorithms has been compared based on the factors: input size of data(in the form of text, audio and video), encryption time, decryption time, throughput of encryption and decryption of each block cipher and power consumption. It was concluded that 3DES has more power consumption and less throughput than the DES due to its triple phase characteristics. Saini (2014) make a performance analysis of various algorithmsDES, AES, RC2, Blowfish, 3DES and RC6. It was concluded from the simulation outcomes that best algorithm are those that are well known and well documented because they are well tested and well-studied. A good cryptographic system strikes a balance between what is possible and what is acceptable. Alanazi et al. (2010) has done the comparative analysis of three Encryption Algorithms (DES, 3DES and AES) within nine factors such as Key Length, Cipher Type, Block Size, Security, Possible Keys, Possible ASCII printable character keys and Time required to check all possible keys at 50 billion keys per second etc. Study shows that AES is better than DES and 3DES.r

1 DES Algorithm It was developed in the early 1975 at IBM labs by Horst Fiestel. The DES was approved by the NBS (National Bureau of Standards, now called NIST –National Institute of Standards and Technology) in 1978. The DES was standardized by the ANSI (American National Standard Institute) under the name of ANSI X3.92, better known as DEA (Data Encryption Algorithm). The DES was once a predominant symmetric-key algorithm for the encryption of electronic data. But now it is an outdated symmetric key data encryption method. DES uses 56 bits key for encryption and decryption. It completes the 16 rounds of encryption on each 64 bits block of data. Data encryption standard works on a particular principle. Huang (2008) explains that Data encryption standard is a symmetric encryption system that uses 64-bit blocks, 8 bits (one octet) of which are used for parity checks (to verify the key's integrity). Each of the key's parity bits (1 every 8 bits) is used to check one of the key's octets by odd parity, that is, each of the parity bits is adjusted to have an odd number of '1's in the octet it belongs to. The key therefore has a real useful length of 56 3bits, which means that only 56 bits are actually used in the algorithm. So it would take a maximum of 256 or 72,057,594,037,927,936 attempts to find the correct key (Coppersmith, 1994). DES uses 16 rounds of a Feistel like encryption method to encrypt plain text. A key schedule is used to derive 16 keys for the successive rounds of encryption from the original key. The block diagram of one round of DES is shown in Figure 2. Even so, DES remained a trusted and widely used encryption algorithm through the mid1990s (Islam et al., 2008).

Summary:

[Cryptography](https://www.sciencedirect.com/topics/computer-science/cryptography) is the science of encrypting and decrypting data. Based on complex mathematics, cryptography provides several important information security services such as authentication, confidentiality, integrity, and [non-repudiation](https://www.sciencedirect.com/topics/computer-science/nonrepudiation). [Cryptographic protocols and applications](https://www.sciencedirect.com/topics/computer-science/cryptographic-application) make cryptography user-friendly and enable users to secure their data without having to carry out the complex mathematics themselves. [Modern cryptography](https://www.sciencedirect.com/topics/computer-science/modern-cryptography) relies on cryptographic keys, usually a short string of text, for encoding and decoding messages in combination with [cryptographic algorithms](https://www.sciencedirect.com/topics/computer-science/cryptographic-algorithm). Based on the type of keys used, cryptography is classified as either symmetric or asymmetric [key cryptography](https://www.sciencedirect.com/topics/computer-science/key-cryptography). Both symmetric and asymmetric key cryptography provide [data confidentiality](https://www.sciencedirect.com/topics/computer-science/data-confidentiality). Asymmetric key encryption is sometimes called [public key encryption](https://www.sciencedirect.com/topics/computer-science/public-key-encryption). Digital signatures, one of the by-products of [public key cryptography](https://www.sciencedirect.com/topics/computer-science/public-key-cryptography), enable the verification of authenticity, integrity, and non-repudiation.

Code of the project:

<!DOCTYPE html>

<html>

<head>

<meta charset="utf-8" />

<meta http-equiv="X-UA-Compatible" content="IE=edge">

<title>Home</title>

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" type="text/css" media="screen" href="style.css" />

<link rel="icon" type="image/x-icon" href="1.png" />

</head>

<body>

<header>

<div class="image1">

<img src="1.png" alt="banha university" width="300px" height="200px">

<h2 id="h23"> Research for <br> Faculty of engineering - Shoubra Benha University <h2>

<ul>

<li> <a href="Main\_page.html"> Home</a> </li>

<li> <a href="Abstract.html"> Abstract </a> </li>

<li> <a href="Intro.html"> Introduction </a> </li>

<li> <a href="Subject.html"> Subject </a> </li>

<li> <a href="Summary.html"> Summary </a> </li>

<li> <a href="Personal\_info.html"> Personal Information </a> </li>

</ul>

</div>

</header>

<div class="content" id="box1">

<table class="T0" id="T1">

<tr>

<td> Department </td>

<td> Engineering mathematics and physics </td>

</tr>

<tr>

<td> Devision</td>

<td> ----------- </td>

</tr>

<tr>

<td> Academic year </td>

<td> 2020-2021 Perparatory </td>

</tr>

<tr>

<td> Course name </td>

<td> Computer </td>

</tr>

<tr>

<td> Course code </td>

<td> ECE001 </td>

</tr>

</table>

<h2 id="h24"> Examiers Commitee </h2>

<table class"T0" id="T2">

<tr>

<td> 1 </td>

<td> Dr.Ahmed Bayoumi </td>

</tr>

<tr>

<td> 2</td>

<td> Dr.Shady Elmashad</td>

</tr>

<tr>

<td> 3 </td>

<td> Dr. Abdelhamid Attaby </td>

</tr>

</table>

</div>

<div class="content" id="box2">

<h2 id="h24"> Research guidelines and special notes </h2>

<h2>The research is to build a simple HTML website about one of the following topics </h2>

<article class="AR0" id="AR1">

- Artificial Intelligence

- Big Data

- Database Systems

- Programming Languages

- Internet of Things

- Mobile Computing

- Cryptography

- Operating Systems

- Computer Architecture

- Computer Engineering Role in COVID-19 Pandemic?

</article>

<h2> Instructions to student </h2>

<article class="AR0" id="AR2">

1. Discuss the selected topic and its applications into the report.

2. The website should contain images, tables, lists and multiple web pages related

and linked to each other. (At least four web pages in addition to the home

page).

3. Add part of your website source code and screenshots to the report to present

your work.

4. Create github account <a href="https://github.com">https://github.com/</a> ,follow video

<a href="https://youtu.be/8faIUlJHik">https://youtu.be/8faIUlJHik </a>

5. Upload your website source code into your github account.

6. Upload your website to <a href="https://pages.github.com/"> https://pages.github.com/ </a> to make it visible.

7. Add a link of your github web site to the report.

8. Submit a zip file contains your report as word file and source code.

9. You can use Google <a href="www.google.com">(www.google.com)</a> or the Egyptian knowledge bank

<a href="www.ekb.com">(www.ekb.com)</a>

</article>

</div>

<p id="h24"> Material selected : Cryptography </P>

<footer>

<div class="Personal\_info">

<span class="span0" id="h22"> Esraa Mamduh Ezat </span><hr>

<span class="span0" id="h22"> Dr.Ahmed Bayoumi </span><hr>

<span class="span0" id="h22"> Dr.Shady Elmashad </span><hr>

<span class="span0" id="h22"> Dr. Abdelhamid Attaby </span><hr>

</div>

</footer>

</body>

</html>