Faculty of engineering - Shoubra
Benha University
Literature Review

in fulfillment of the requirements of

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

Title: -

Build a website on recent computer engineering topics

By:

	Name	Edu mail	B.N
1	Maha Ashraf alsaid	maha196073@feng.bu.edu.eg	959

Approved by:

Examiners committee	Signature
1. Dr.Ahmed Bayoumi	
2. Dr.Shady Elmashad	
3. Dr. Abdelhamid Attaby	

Name: Maha Ashraf

Alsaid B.N/: 959

Date: 2019/2020

Topic: Cryptography.

Github account: https://github.com/Maha-Ashraf/ECE006-htmlproject

Github page(published website):
https://maha-ashraf.github.io/ECE006-htmlproject/

Application brief :

The topic that I choose for my website is Cryptography.

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" 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, to transform messages in ways that are hard to decipher.

These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email.

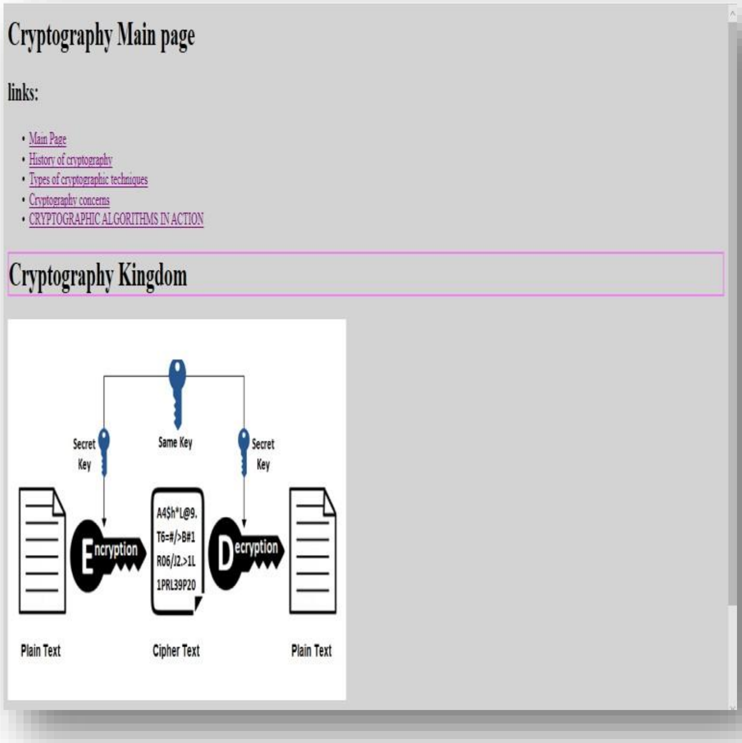
- The reason I choose this topic that:

It's a very interesting and important subject because:

- **Cryptography** provides information Security for - Defending against external/internal hackers -Defending against industrial espionage - Securing E-commerce .
- IT is also Securing bank accounts/electronic transfers- Securing intellectual property- Avoiding liability Threats to Information Security - Pervasiveness of email/networks - Online storage of sensitive information - Insecure technologies (e.g. wireless)- Trend towards paperless society - Weak legal protection of email privacy.

Screen shots for my website:(Cryptography Kingdom)

The first page (The main page)

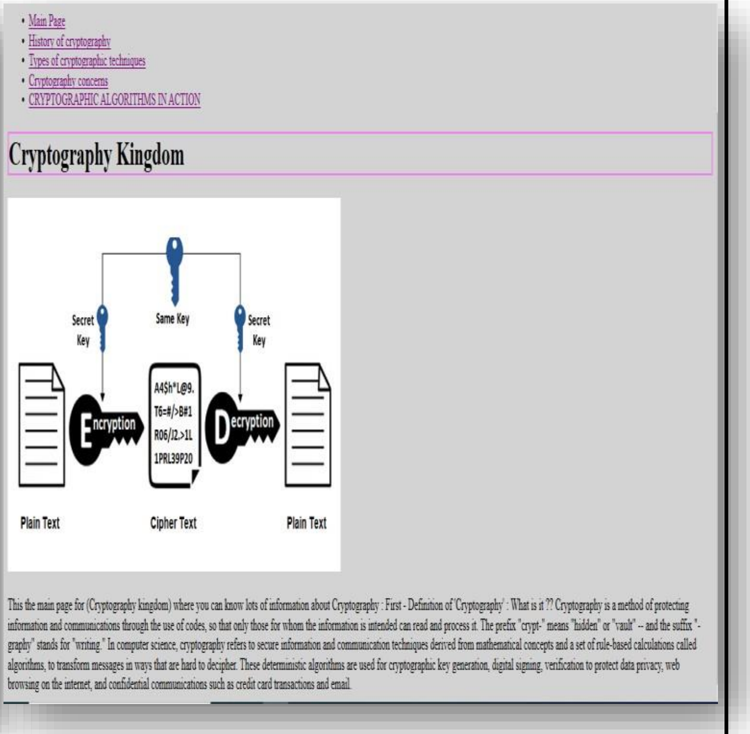


Cryptography Main page

links:

- Main Page
- History of cryptography
- Types of cryptographic techniques
- Cryptography concerns
- CRYPTOGRAPHIC ALGORITHMS IN ACTION

Cryptography Kingdom

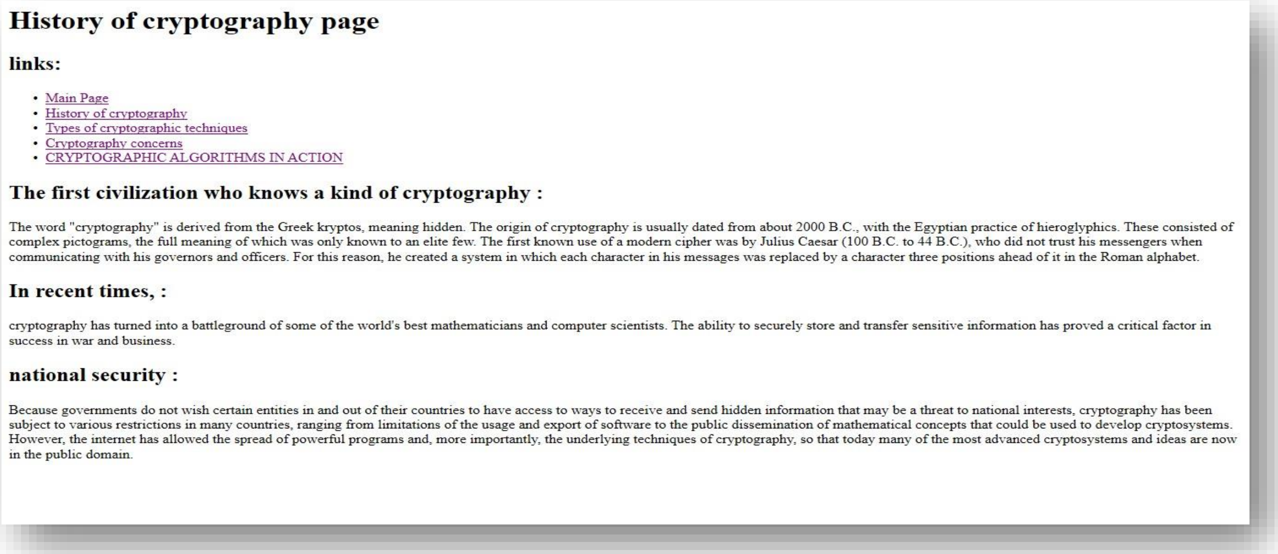


- Main Page
- History of cryptography
- Types of cryptographic techniques
- Cryptography concerns
- CRYPTOGRAPHIC ALGORITHMS IN ACTION

Cryptography Kingdom

This the main page for (Cryptography kingdom) where you can know lots of information about Cryptography : First - Definition of 'Cryptography' : What is it ?? Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" 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, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email.

The second page :(History of cryptography page)



History of cryptography page

links:

- Main Page
- History of cryptography
- Types of cryptographic techniques
- Cryptography concerns
- CRYPTOGRAPHIC ALGORITHMS IN ACTION

The first civilization who knows a kind of cryptography :

The word "cryptography" is derived from the Greek kryptos, meaning hidden. The origin of cryptography is usually dated from about 2000 B.C., with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to an elite few. The first known use of a modern cipher was by Julius Caesar (100 B.C. to 44 B.C.), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

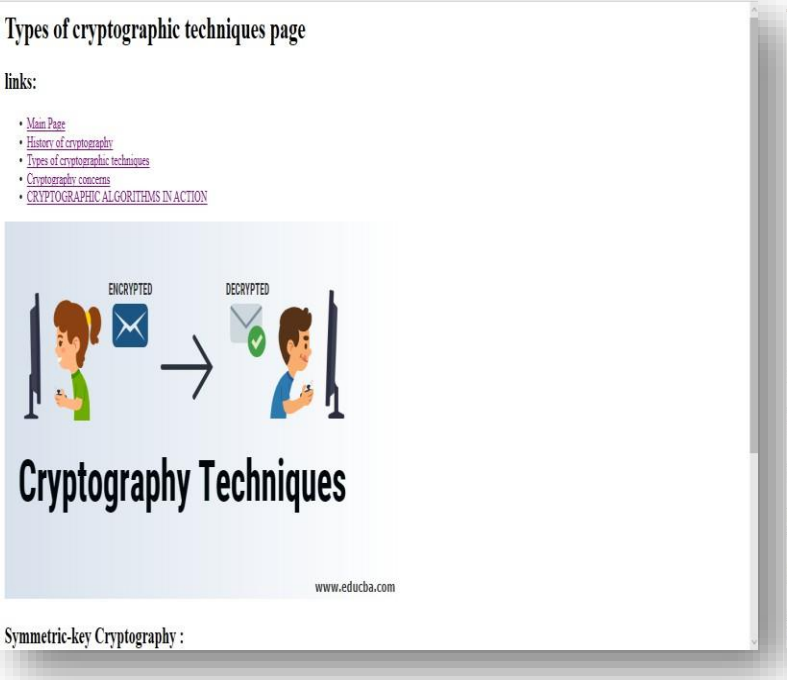
In recent times, :

cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

national security :

Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems. However, the internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain.

The third page: (Types of cryptographic techniques page)

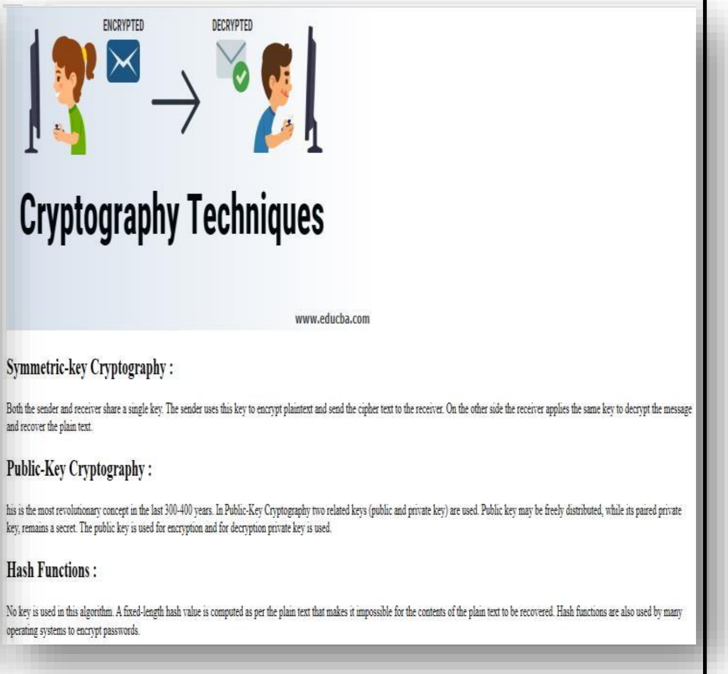


Types of cryptographic techniques page

links:

- Main Page
- History of cryptography
- Types of cryptographic techniques
- Cryptography concerns
- CRYPTOGRAPHIC ALGORITHMS IN ACTION

Symmetric-key Cryptography :



Symmetric-key Cryptography :

Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

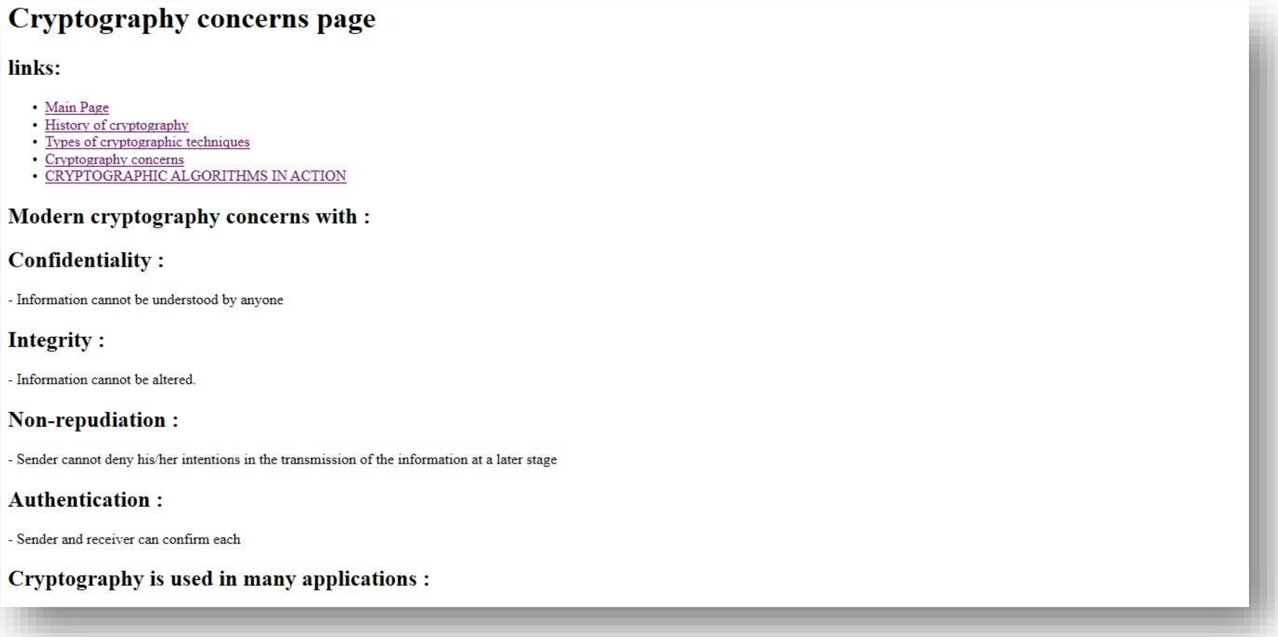
Public-Key Cryptography :

his is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

Hash Functions :

No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

The fourth page: (Cryptography concerns page)



Cryptography concerns page

links:

- Main Page
- History of cryptography
- Types of cryptographic techniques
- Cryptography concerns
- CRYPTOGRAPHIC ALGORITHMS IN ACTION

Modern cryptography concerns with :

Confidentiality :

- Information cannot be understood by anyone

Integrity :

- Information cannot be altered.

Non-repudiation :

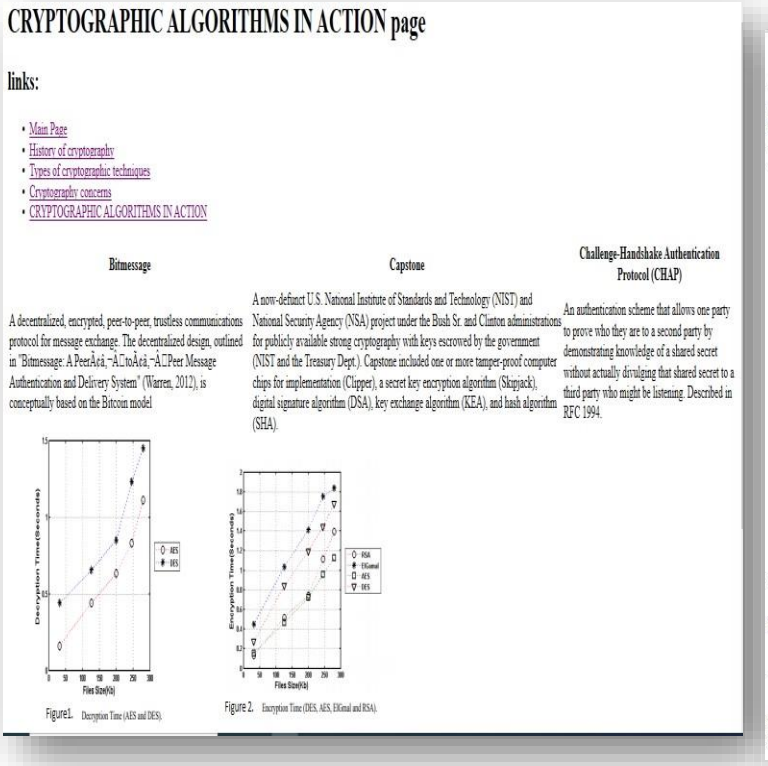
- Sender cannot deny his/her intentions in the transmission of the information at a later stage

Authentication :

- Sender and receiver can confirm each

Cryptography is used in many applications :

The fifth page: (CRYPTOGRAPHIC ALGORITHMS IN ACTION page)



CRYPTOGRAPHIC ALGORITHMS IN ACTION page

links:

- Main Page
- History of cryptography
- Types of cryptographic techniques
- Cryptography concerns
- CRYPTOGRAPHIC ALGORITHMS IN ACTION

Bitmessage

A decentralized, encrypted, peer-to-peer, trustless communications protocol for message exchange. The decentralized design, outlined in "Bitmessage: A PeerÃ¢â‚¬Â□toÃ¢â‚¬Â□Peer Message Authentication and Delivery System" (Warren, 2012), is conceptually based on the Bitcoin model

Capstone

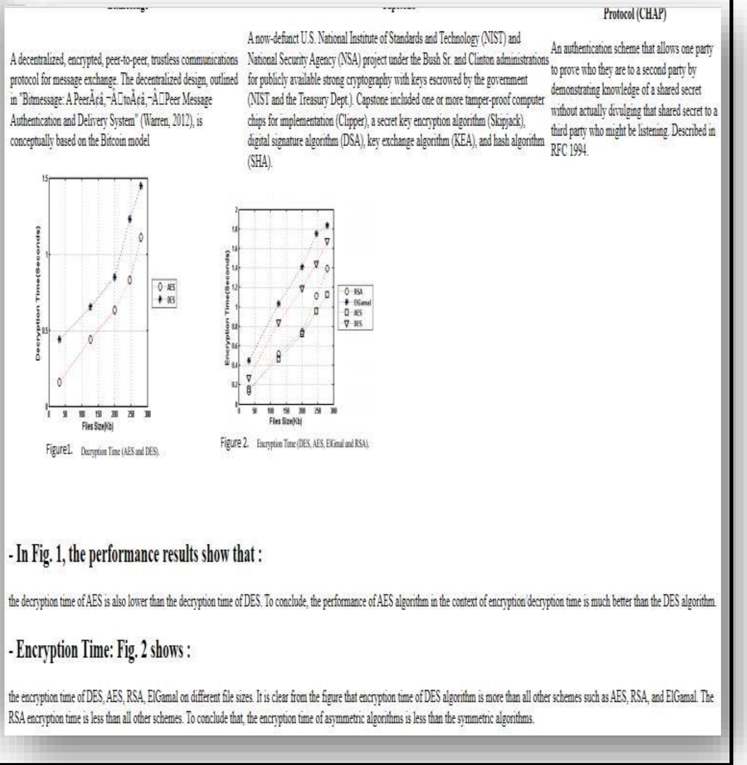
A now-defunct U.S. National Institute of Standards and Technology (NIST) and National Security Agency (NSA) project under the Bush Sr. and Clinton administrations for publicly available strong cryptography with keys escrowed by the government (NIST and the Treasury Dept.). Capstone included one or more tamper-proof computer chips for implementation (Clipper), a secret key encryption algorithm (Skipjack), digital signature algorithm (DSA), key exchange algorithm (KEA), and hash algorithm (SHA).

Challenge-Handshake Authentication Protocol (CHAP)

An authentication scheme that allows one party to prove who they are to a second party by demonstrating knowledge of a shared secret without actually divulging that shared secret to a third party who might be listening. Described in RFC 1994.

Figure1. Decryption Time (AES and DES).

Figure 2. Encryption Time (DES, AES, ElGmal and RSA).



Protocol (CHAP)

A decentralized, encrypted, peer-to-peer, trustless communications protocol for message exchange. The decentralized design, outlined in "Bitmessage: A PeerÃ¢â‚¬Â□toÃ¢â‚¬Â□Peer Message Authentication and Delivery System" (Warren, 2012), is conceptually based on the Bitcoin model

A now-defunct U.S. National Institute of Standards and Technology (NIST) and National Security Agency (NSA) project under the Bush Sr. and Clinton administrations for publicly available strong cryptography with keys escrowed by the government (NIST and the Treasury Dept.). Capstone included one or more tamper-proof computer chips for implementation (Clipper), a secret key encryption algorithm (Skipjack), digital signature algorithm (DSA), key exchange algorithm (KEA), and hash algorithm (SHA).

An authentication scheme that allows one party to prove who they are to a second party by demonstrating knowledge of a shared secret without actually divulging that shared secret to a third party who might be listening. Described in RFC 1994.

Figure1. Decryption Time (AES and DES).

Figure 2. Encryption Time (DES, AES, ElGmal and RSA).

- In Fig. 1, the performance results show that :

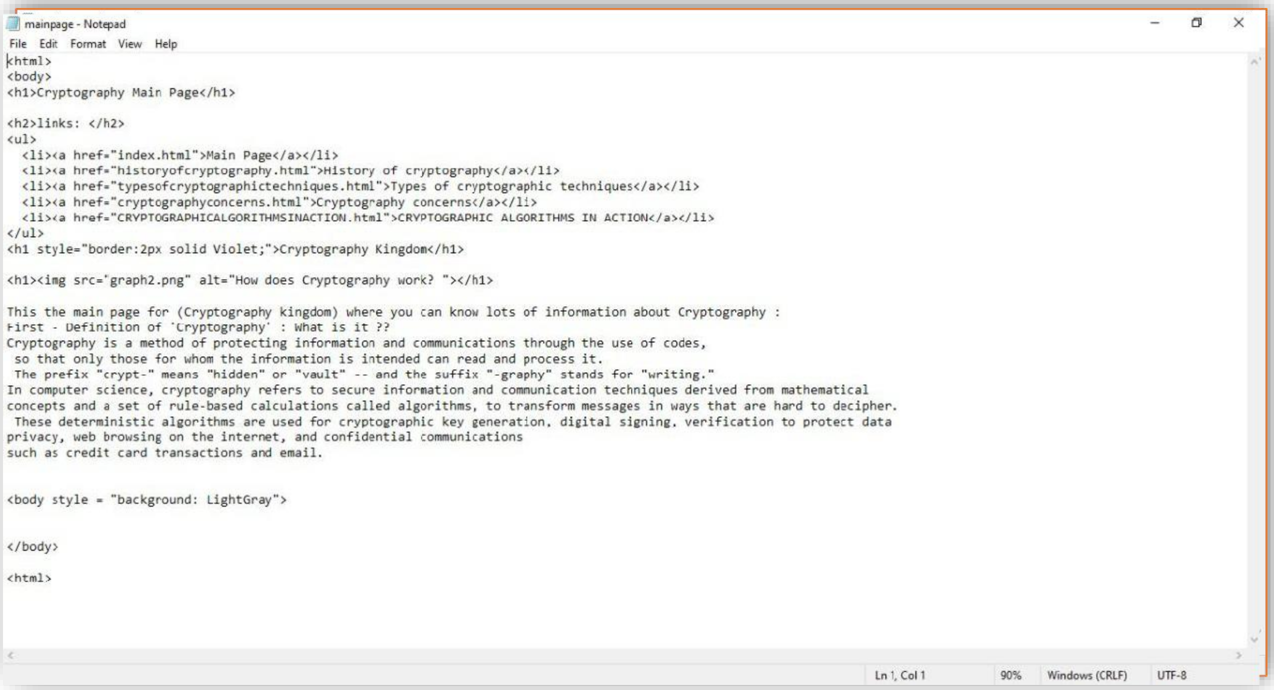
the decryption time of AES is also lower than the decryption time of DES. To conclude, the performance of AES algorithm in the context of encryption/decryption time is much better than the DES algorithm.

- Encryption Time: Fig. 2 shows :

the encryption time of DES, AES, RSA, ElGamal on different file sizes. It is clear from the figure that encryption time of DES algorithm is more than all other schemes such as AES, RSA, and ElGamal. The RSA encryption time is less than all other schemes. To conclude that, the encryption time of asymmetric algorithms is less than the symmetric algorithms.

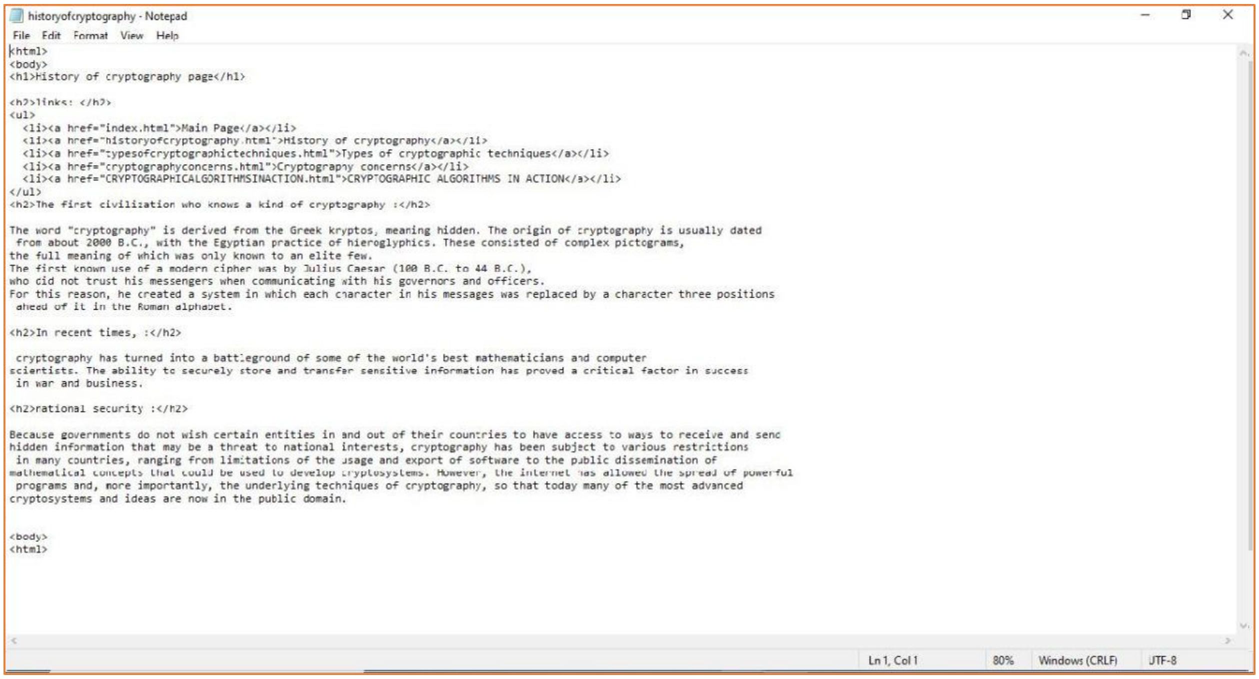
Source code screen shots:

The first page (The main page: Cryptography Kingdom):



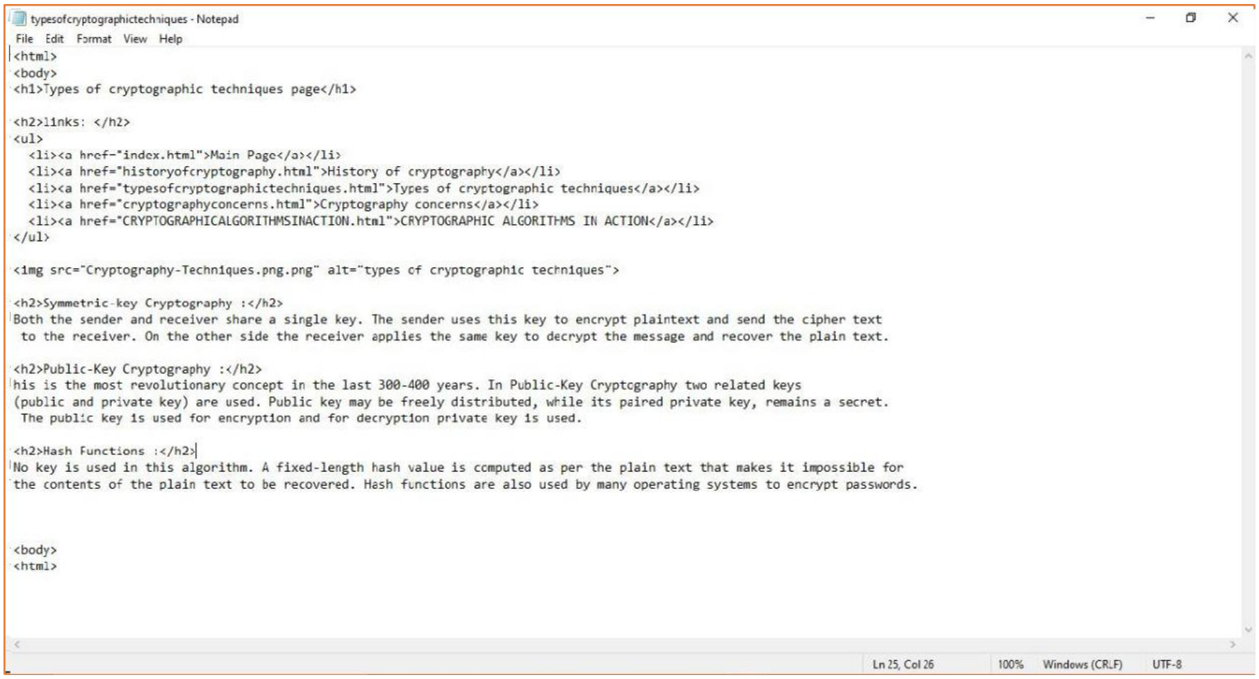
```
<html>
<body>
<h1>Cryptography Main Page</h1>

<h2>links: </h2>
<ul>
  <li><a href="index.html">Main Page</a></li>
  <li><a href="historyofcryptography.html">History of cryptography</a></li>
  <li><a href="typesofcryptographictechniques.html">Types of cryptographic techniques</a></li>
  <li><a href="cryptographyconcerns.html">Cryptography concerns</a></li>
  <li><a href="CRYPTOGRAPHICALGORITHMSINACTION.html">CRYPTOGRAPHIC ALGORITHMS IN ACTION</a></li>
</ul>
<h1 style="border:2px solid Violet;">Cryptography Kingdom</h1>

<h1><img src="graph2.png" alt="How does Cryptography work? "></h1>

This the main page for (Cryptography kingdom) where you can know lots of information about Cryptography :
First - Definition of 'Cryptography' : What is it ??
Cryptography is a method of protecting information and communications through the use of codes,
 so that only those for whom the information is intended can read and process it.
 The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" 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, to transform messages in ways that are hard to decipher.
 These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data
privacy, web browsing on the internet, and confidential communications
such as credit card transactions and email.


<body style = "background: LightGray">


</body>

<html>
```

The second page (History of cryptography page)



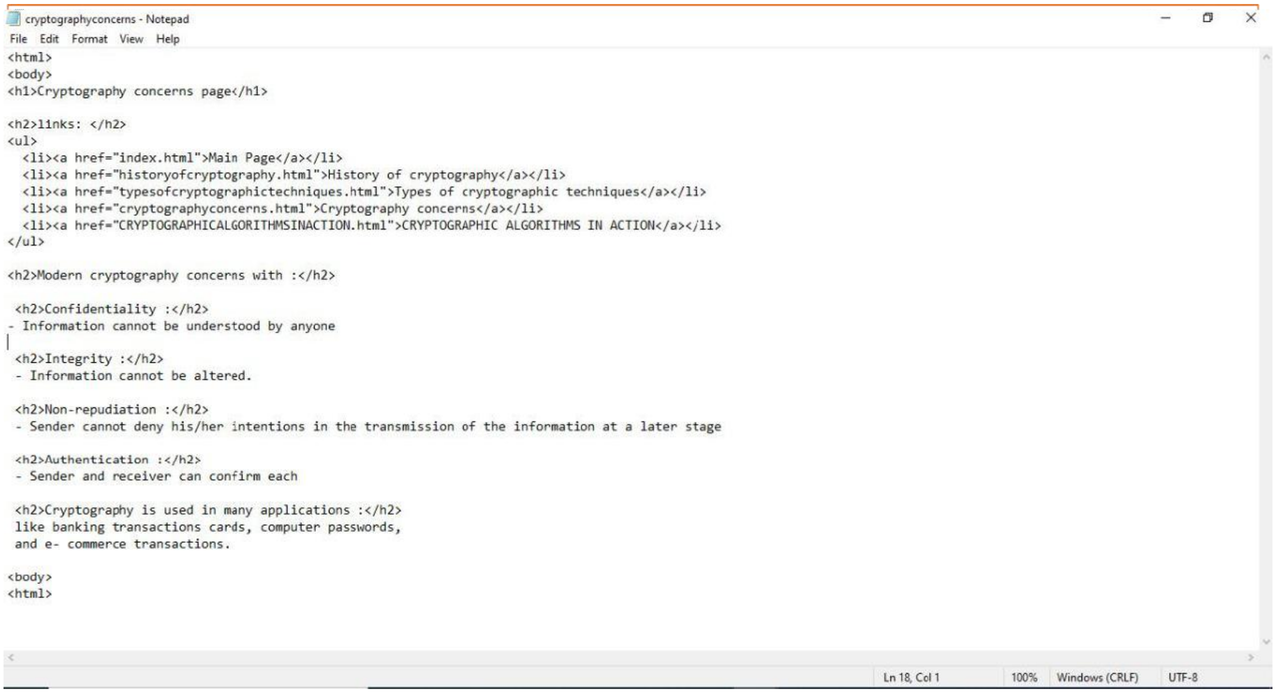
```
<html>
<body>
<h1>History of cryptography page</h1>

<h2>links: </h2>
<ul>
  <li><a href="index.html">Main Page</a></li>
  <li><a href="historyofcryptography.html">History of cryptography</a></li>
  <li><a href="typesofcryptographictechniques.html">Types of cryptographic techniques</a></li>
  <li><a href="cryptographyconcerns.html">Cryptography concerns</a></li>
  <li><a href="CRYPTOGRAPHICALGORITHMSINACTION.html">CRYPTOGRAPHIC ALGORITHMS IN ACTION</a></li>
</ul>
<h2>The first civilization who knows a kind of cryptography :</h2>

The word "cryptography" is derived from the Greek kryptos, meaning hidden. The origin of cryptography is usually dated
 from about 2000 B.C., with the Egyptian practice of hieroglyphics. These consisted of complex pictograms,
the full meaning of which was only known to an elite few.
The first known use of a modern cipher was by Julius Caesar (100 B.C. to 44 B.C.),
who did not trust his messengers when communicating with his governors and officers.
For this reason, he created a system in which each character in his messages was replaced by a character three positions
 ahead of it in the Roman alphabet.

<h2>In recent times, :</h2>

 cryptography has turned into a battleground of some of the world's best mathematicians and computer
scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success
 in war and business.

<h2>national security :</h2>

Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send
hidden information that may be a threat to national interests, cryptography has been subject to various restrictions
 in many countries, ranging from limitations of the usage and export of software to the public dissemination of
mathematical concepts that could be used to develop cryptosystems. However, the internet has allowed the spread of powerful
 programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced
cryptosystems and ideas are now in the public domain.


<body>
<html>
```

The third page: (Types of cryptographic techniques page)


typesofcryptographictechniques - Notepad
File Edit Format View Help
Ln 25, Col 26
100%
Windows (CRLF)
UTF-8

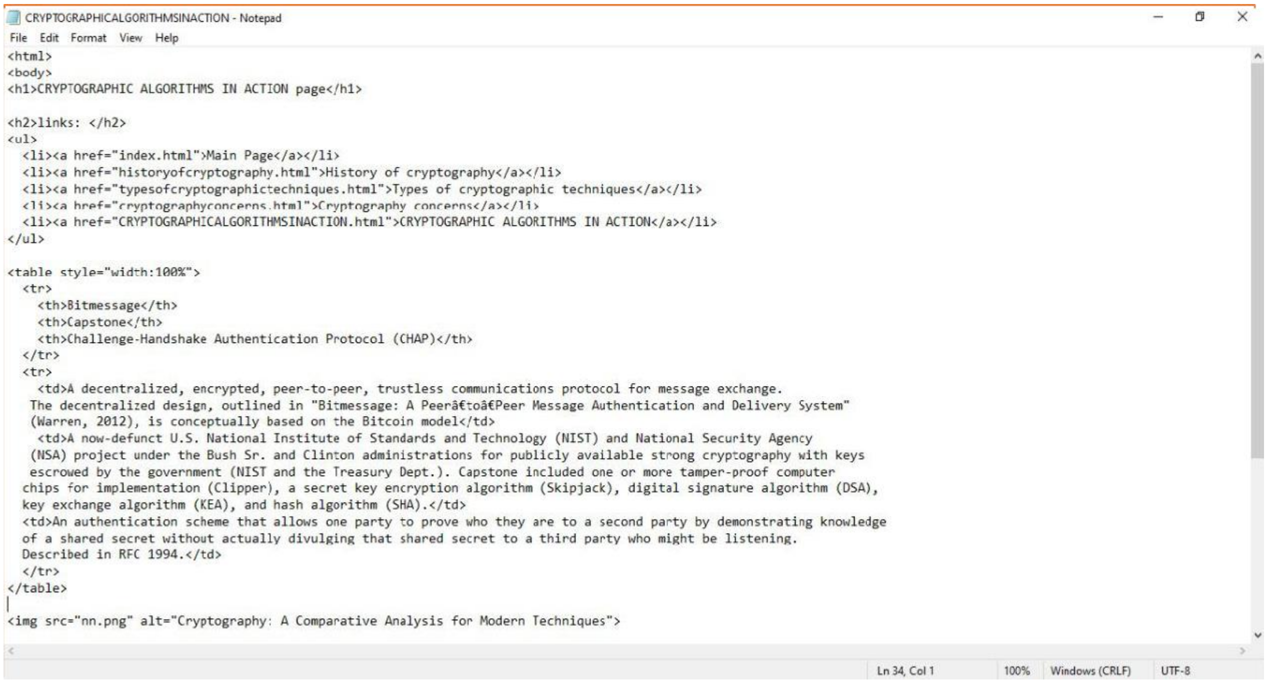
```
<html>
<body>
<h1>Types of cryptographic techniques page</h1>

<h2>links: </h2>
<ul>
  <li><a href="index.html">Main Page</a></li>
  <li><a href="historyofcryptography.html">History of cryptography</a></li>
  <li><a href="typesofcryptographictechniques.html">Types of cryptographic techniques</a></li>
  <li><a href="cryptographyconcerns.html">Cryptography concerns</a></li>
  <li><a href="CRYPTOGRAPHICALGORITHMSINACTION.html">CRYPTOGRAPHIC ALGORITHMS IN ACTION</a></li>
</ul>

<img src="Cryptography-Techniques.png.png" alt="types of cryptographic techniques">

<h2>Symmetric-key Cryptography :</h2>
Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text
 to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

<h2>Public-Key Cryptography :</h2>
his is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys
(public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret.
 The public key is used for encryption and for decryption private key is used.

<h2>Hash Functions :</h2>
No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for
the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.



<body>
<html>
```

The fourth page: (Cryptography concerns page)

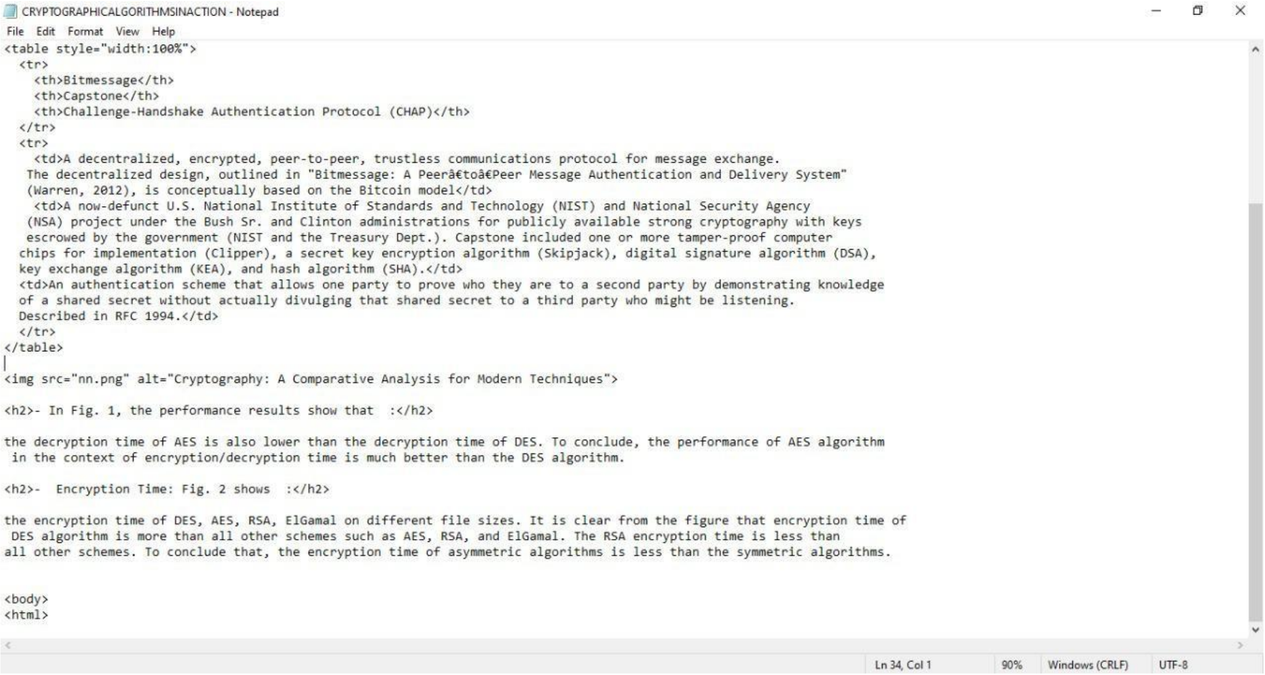


```
<html>
<body>
<h1>Cryptography concerns page</h1>

<h2>links: </h2>
<ul>
  <li><a href="index.html">Main Page</a></li>
  <li><a href="historyofcryptography.html">History of cryptography</a></li>
  <li><a href="typesofcryptographictechniques.html">Types of cryptographic techniques</a></li>
  <li><a href="cryptographyconcerns.html">Cryptography concerns</a></li>
  <li><a href="CRYPTOGRAPHICALGORITHMSINACTION.html">CRYPTOGRAPHIC ALGORITHMS IN ACTION</a></li>
</ul>

<h2>Modern cryptography concerns with :</h2>

 <h2>Confidentiality :</h2>
- Information cannot be understood by anyone

 <h2>Integrity :</h2>
 - Information cannot be altered.

 <h2>Non-repudiation :</h2>
 - Sender cannot deny his/her intentions in the transmission of the information at a later stage

 <h2>Authentication :</h2>
 - Sender and receiver can confirm each

 <h2>Cryptography is used in many applications :</h2>
 like banking transactions cards, computer passwords,
 and e- commerce transactions.

<body>
<html>
```

The fifth page: (CRYPTOGRAPHIC ALGORITHMS IN ACTION page)


CRYPTOGRAPHICALGORITHMSINACTION - Notepad
File Edit Format View Help
Ln 34, Col 1
100%
Windows (CRLF)
UTF-8

```
<html>
<body>
<h1>CRYPTOGRAPHIC ALGORITHMS IN ACTION page</h1>

<h2>links: </h2>
<ul>
  <li><a href="index.html">Main Page</a></li>
  <li><a href="historyofcryptography.html">History of cryptography</a></li>
  <li><a href="typesofcryptographictechniques.html">Types of cryptographic techniques</a></li>
  <li><a href="cryptographyconcerns.html">Cryptography concerns</a></li>
  <li><a href="CRYPTOGRAPHICALGORITHMSINACTION.html">CRYPTOGRAPHIC ALGORITHMS IN ACTION</a></li>
</ul>

<table style="width:100%">
  <tr>
    <th>Bitmessage</th>
    <th>Capstone</th>
    <th>Challenge-Handshake Authentication Protocol (CHAP)</th>
  </tr>
  <tr>
    <td>A decentralized, encrypted, peer-to-peer, trustless communications protocol for message exchange.
   The decentralized design, outlined in "Bitmessage: A Peerâ€toâ€Peer Message Authentication and Delivery System"
   (Warren, 2012), is conceptually based on the Bitcoin model</td>
    <td>A now-defunct U.S. National Institute of Standards and Technology (NIST) and National Security Agency
   (NSA) project under the Bush Sr. and Clinton administrations for publicly available strong cryptography with keys
   escrowed by the government (NIST and the Treasury Dept.). Capstone included one or more tamper-proof computer
  chips for implementation (Clipper), a secret key encryption algorithm (Skipjack), digital signature algorithm (DSA),
  key exchange algorithm (KEA), and hash algorithm (SHA).</td>
  <td>An authentication scheme that allows one party to prove who they are to a second party by demonstrating knowledge
  of a shared secret without actually divulging that shared secret to a third party who might be listening.
  Described in RFC 1994.</td>
  </tr>
</table>

<img src="nn.png" alt="Cryptography: A Comparative Analysis for Modern Techniques">
```


CRYPTOGRAPHICALGORITHMSINACTION - Notepad
File Edit Format View Help
Ln 34, Col 1
90%
Windows (CRLF)
UTF-8

```
<table style="width:100%">
  <tr>
    <th>Bitmessage</th>
    <th>Capstone</th>
    <th>Challenge-Handshake Authentication Protocol (CHAP)</th>
  </tr>
  <tr>
    <td>A decentralized, encrypted, peer-to-peer, trustless communications protocol for message exchange.
   The decentralized design, outlined in "Bitmessage: A Peerâ€toâ€Peer Message Authentication and Delivery System"
   (Warren, 2012), is conceptually based on the Bitcoin model</td>
    <td>A now-defunct U.S. National Institute of Standards and Technology (NIST) and National Security Agency
   (NSA) project under the Bush Sr. and Clinton administrations for publicly available strong cryptography with keys
   escrowed by the government (NIST and the Treasury Dept.). Capstone included one or more tamper-proof computer
  chips for implementation (Clipper), a secret key encryption algorithm (Skipjack), digital signature algorithm (DSA),
  key exchange algorithm (KEA), and hash algorithm (SHA).</td>
  <td>An authentication scheme that allows one party to prove who they are to a second party by demonstrating knowledge
  of a shared secret without actually divulging that shared secret to a third party who might be listening.
  Described in RFC 1994.</td>
  </tr>
</table>

<img src="nn.png" alt="Cryptography: A Comparative Analysis for Modern Techniques">
```

```
<h2>- In Fig. 1, the performance results show that  :</h2>

the decryption time of AES is also lower than the decryption time of DES. To conclude, the performance of AES algorithm
 in the context of encryption/decryption time is much better than the DES algorithm.

<h2>-  Encryption Time: Fig. 2 shows  :</h2>

the encryption time of DES, AES, RSA, ElGamal on different file sizes. It is clear from the figure that encryption time of
 DES algorithm is more than all other schemes such as AES, RSA, and ElGamal. The RSA encryption time is less than
all other schemes. To conclude that, the encryption time of asymmetric algorithms is less than the symmetric algorithms.


<body>
<html>
```

References:

1-

https://thesai.org/Downloads/Volume8No6/Paper_59-Cryptography_A_Comparative_Analysis_for_Modern_Techniques.pdf

2-

https://www.garykessler.net/library/crypto.html

3-

https://economictimes.indiatimes.com/definition/cryptography

4-

https://searchsecurity.techtarget.com/definition/cryptography