|  |  |  |
| --- | --- | --- |
| **ipn** | **INSTITUTO POLITÉCNICO NACIONAL**  **ESCUELA SUPERIOR DE CÓMPUTO** |  |

**Cryptography**

**“DES/AES Image Cypher”**

Abstract

The digital information safety is a concern that has been since the usage of the computers to process and save data, so, it is important to know how we can implement encryption standards in order to protect any kind of sensible information that we’re working with.

**By:**

**Reyes Valenzuela Alejandro**

Professor:

MSc. NIDIA ASUNCIÓN CORTEZ DUARTE

September 2019

To validate this report it is necessary to include the corresponding seal

**Index**

Content

[Introduction: 1](#_Toc476313175)

[Literature review: 1](#_Toc476313176)

[Software (libraries, packages, tools): 1](#_Toc476313177)

[Procedure: 1](#_Toc476313178)

[Results 1](#_Toc476313179)

[Discussion: 1](#_Toc476313180)

[Conclusions: 2](#_Toc476313181)

[References: 2](#_Toc476313182)

[Code 2](#_Toc476313183)

# Introduction:

[1] The information leakage is a vulnerability when information is exposed to unauthorized agents, specially, application sensitive data from users, such as:

* Account identifiers
* Email addresses
* File System Structure
* Bank information
* Database structure
* Medical history

Among others, those vulnerabilities, if discovered, can result in a massive money loss, especially for the bank information, where we’re working with accounts from around the world, that’s why our data can’t be processed as plain text. If an external agent intercepts our communication with the system, the attacker will gain access to information that could affect both our integrity and the image from the system’s developers.

[2] Since the Ancient Greek’s era, there has been some encryption techniques that allows us to “cover up” the information in order to assure that only the receiver could understand and work with it, so, the extern agents won’t have an idea of what’s on the message and how could you use it without the sender permission, being the ancient method recorded, the “Scytale”, an small rod that was wrapped with leather, where the information was written on in a manner that only the people with the same rod diameter could read the message.

Write your own concise introduction. It should explain the outlines of the work, what results have been determined, and salient points about the work. Remember that an introduction “tells the reader what he/she is going to be reading.”

# Literature review:

The literature needs to provide an understanding of the conceptual and theoretical and mathematical background, context and justification of your work.

You should include diagrams, formulas, algortithms, …

should be referenced using

# Software (libraries, packages, tools):

\* Make a list of ALL items used in the lab. Alternatively, materials can be included as part of the procedure.

# Procedure:

\* Flowchart / block diagram  
\* Add details (step-by-step) of your procedure in such a way that anyone else could repeat the experiment.

# Results

\* This section should include any data tables, observations, images.   
\* All tables, graphs and charts should be labeled appropriately.

This section describes but does not explain your results

Since you are presenting your results, not the figures which represent the results, you should ensure you refer explicitly to your results and not just to your data figures (graphs, tables). As you describe particular results in the text of your results section, make **sure you refer to the corresponding figure in brackets after you have mentioned the results**. The figures should be inserted into the text as soon as possible after you mention them.

# Discussion:

Your discussion section has two fundamental aims:

* to interpret and explain the results of your study,
* to explore the significance of your study’s findings. [qualify and explore](https://unilearning.uow.edu.au/report/2bvi.html) the theoretical importance/significance of your results.

The discussion is also the place in a report where any qualifications or reservations you have about the research should be aired.

# Conclusions:

\* List one thing you learned and describe how it applies to a real-life situation.   
\*Discuss possible errors that could have occurred in the collection of the data (experimental errors)

\*How generally do your results apply?

\*Were their any defects in your experimental design or procedure?

# References:

<https://affinity-it-security.com/what-is-information-leakage/>

<https://www.gemalto.com/review/Pages/a-brief-history-of-encryption.aspx>

# Code

Include all source code, comment all the reused code and also show the references

You must use the next link to format your code

<http://www.planetb.ca/syntax-highlight-word>

\*About figures or tables\*

Using figures such as diagrams, tables, graphs, charts or maps can be a very useful way to show and emphasise information in your report.

Figures essential to the report should be smoothly and correctly integrated and should be explained and referred to in the main body of the report.

Example:

