

**Ways to Hide Weak Implementations of   
Strong Crypto Algorithms**

**Project Plan/Strategy**

**Submitted by: Kevin Tan Wei Loong  
Matriculation Number: U1821147D**

**Supervisor: Dr Tay Kian Boon**

School of Computer Science & Engineering

**2020**

**INTRODUCTION**

In our day to day activities that involves the use of technology, the transfer and storage of data is always happening around us. As such, this raises the concern for privacy and security issues. In this case, the most common and popular solution is the use of strong crypto algorithms to protect our data though encryption. However, the use of such algorithms does not mean that there is no vulnerability to break the system.

**PROJECT OBJECTIVES**

The objectives of this project are to explore different ways to hide weak implementations of strong crypto algorithms. If there is any part in the cryptosystem that is weakly implemented (either ignorantly or deliberately), encrypted data using strong algorithms can be retrieved easily without the user’s knowledge.

**PROJECT PLAN / STRATEGY**

The project plan first involves researching on the different types of strong crypto algorithms used for data encryption such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA). Next, a program is to be written to implement the algorithm and create an environment at the same time to test out the different types of keys being used to encrypt the data.

The strategy here is to test out smaller keys first to reduce the entropy of the keys which makes it easier to brute-force. These can be carried out by the following methods: have the program to read only the first 2 or 3 characters of the password/message, using timestamp as the key or creating a random key generator with weak entropy.

Exploration of different ways to exploit the system can be done thereafter, by taking advantage of the types of weakness each algorithm has, ultimately creating a malicious program to trick the user and learning how the mind of a black hat hacker works.