# Assignment 1 - Encryption, Memory and secure Programming

**Learning Objective:** to identify and extract an encryption key from a RAM dump.

**Rationale**: All programs that use variables have those variables stored in RAM memory during execution of the program. The Data Encryption Standard (DES) is a symmetric algorithm which means that it uses the same key for encryption and decryption. In the Microsoft implementation of DES, the implementation on which the assignment is based, the key is automatically generated by the program itself and will be stored in RAM memory during execution of the program code. Your task is to make a copy of the RAM and then analyse that copy, identify and extract the key. This is not as straight forward as it may seem and requires you to research solutions. Additionally, a significant amount of malware uses data encryption to hide from malware checkers that seek out malware based on a footprint.

Visual Studio is already installed on the image that is supplied to you for this course by the Institute. <https://connect.lyit.ie/EricomXML/AccessPortal/start.html#/app/dashboard>

**Useful Links**

[**https://kb.acronis.com/content/27931**](https://kb.acronis.com/content/27931)

[**https://cqureacademy.com/blog/forensics/memory-dump-analysis**](https://cqureacademy.com/blog/forensics/memory-dump-analysis)

[**https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf**](https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf)

[**https://medium.com/@zemelusa/first-steps-to-volatile-memory-analysis-dcbd4d2d56a1**](https://medium.com/@zemelusa/first-steps-to-volatile-memory-analysis-dcbd4d2d56a1)

[**https://stackoverflow.com/questions/1263350/cryptography-best-practices-for-keys-in-memory**](https://stackoverflow.com/questions/1263350/cryptography-best-practices-for-keys-in-memory)

**Papers**

[**https://cryptome.org/0003/RAMisKey.pdf**](https://cryptome.org/0003/RAMisKey.pdf)

[**https://www.researchgate.net/profile/Christopher\_Hargreaves/publication/221548532\_Recovery\_of\_Encryption\_Keys\_from\_Memory\_Using\_a\_Linear\_Scan/links/53e3ae820cf21cc29fc5f5fe/Recovery-of-Encryption-Keys-from-Memory-Using-a-Linear-Scan.pd**](https://www.researchgate.net/profile/Christopher_Hargreaves/publication/221548532_Recovery_of_Encryption_Keys_from_Memory_Using_a_Linear_Scan/links/53e3ae820cf21cc29fc5f5fe/Recovery-of-Encryption-Keys-from-Memory-Using-a-Linear-Scan.pd)

[**https://www.sciencedirect.com/science/article/pii/S1742287609000486**](https://www.sciencedirect.com/science/article/pii/S1742287609000486)

[**https://ee.stanford.edu/~hellman/publications/36.pdf**](https://ee.stanford.edu/~hellman/publications/36.pdf)

**Caveat**

IF you are doing the assignment on your laptops rather than the VM. In order to install and run Visual Studio, the machine you are using must meet or exceed the minimum hardware specification (see below). If you run into difficulties with running the programme, please see the specifications below.

**Hardware Specification**

* 1.6 GHz or faster **processor**.
* 1 GB of **RAM** (for x86) or 2 GB of **RAM** (for x64); an **additional** 512 MB **RAM recommended** if running a virtual machine.
* 200 MB of available **hard disk space**.
* 5400 RPM **hard disk** drive.
* **DirectX** 9-capable **video card** that runs at 1024 x 768 or higher display **resolution**.

With the image provided by the college this should not be a problem any longer.

**Software Specification**

* Visual Studio 2019 (C# and perhaps Python)

# Steps

1. **Visual Studio**

The image provided by the institute has a preinstalled version of Visual Studio.

1. **Running the program in Visual Studio**

1. Create the directory **C:\Data\Temp**

2. Create a short text file (1/2 page of text), save it as **MyData.txt** in the directory specified in step 1.

3. Start **Visual Studio**. The program will run in Visual Studio 2019 in the image environment

supplied by the Institute. Go to **Start** -> **All Programs** -> **Visual Studio 2019**

4. Create a N**ew Project**, **Scroll** and select **Console Application (.NET Framework)** (using the **Visual**

**C#** template), highlight and press next.

5. Give the application a name **CryptoProgA** and change the Framework to **.NET Framework 4.7.2**

6.  **Delete** the code on the console window and paste the **Crypto Program code** (see assignment

folder and code document) into the console window.

7. Comment out those lines that have the function of deleting the key from memory.

8. Simply click **Start** on the Main Menu to run the program.

1. **Performing a RAM Dump**

1. Perform a memory dump of machine’s RAM.

2. Analyse dump using forensics tools and visual inspection and see if you can find the key.

1. **Key Management in memory**

The program contains 2 lines of code:

ZeroMemory(gch.AddrOfPinnedObject(), sSecretKey.Length \* 2);

gch.Free();

Provide an explanation for both lines of code, what does the code do and how? **Note:** these

lines should be commented out prior to beginning your assignment.

1. **Finding the key**

**Hnt:** Use breakpoints.

# What you are required to submit

You are required to submit **1 zip file** per team consisting of:

A five to eight minute video explaining the nature and substance of the key found, explaining why this may or may not be the key and why the key can/cannot be used to decrypt the encrypted message. What might be one alternative method of decrypting the message? Absolute maximum length 8 minutes.

There must be evidence of both team member’s contributions to the assignment.

# Rubric

1. The key (and explanation of the key) 40%
2. Is the key found the decryption key? 25%
3. Decryption of the encrypted message? 15%
4. Alternative for decrypting the message? 10%
5. Evidence of Depth and breadth of research 5%
6. Academic presentation 5%

The submission should be submitted once by a single member of the team and must be submitted by **16th November**. Please note: Team members share equal responsibility for the production of the video, there must be evidence of contribution from both team members and marks will reflect this. Inter-team work is not permitted and individuality is expected. There will be an assignment in Cryptographic Maths also. Submission dates for this element of the module will be discussed by my co-lecturer.

**I hope this clarifies any misconceptions**