This document outlines the general concept of the project, development process and how this process is split, prerequisites in terms of base knowledge, obstacles that may present themselves in the project and the overall learning outcomes.

The overall concept for the project is to create an Android application that uses anonymity techniques such as encryption and timed 'self destruct' messaging. The application will primarily be used to exchange messages, files and potentially quick, anonymous transactions between users.

The project will involve research regarding cryptography techniques, cryptocurrency wallet implementation and compression algorithms such as Huffman Encoding alongside market research in comparison to other similar applications such as WhatsApp and Telegram.

The final product of this project can be used in several different ways. The product could be used to exchange messages or files that contains sensitive information whilst preserving users privacy. Another example of use could be for making fast transactions of any size without having to exchange bank details.

Due to the fact that the largest messaging applications don't support any transactions amongst users combined with the rise of cryptocurrency in mainstream media, there could be a surge in demand for a product like this in the near future which is the primary reason for pursuing the development of this application. The application could also be turned into a profitable model by charging a small amount of commission for every transaction or including advertising within it..

The development process for the application is split into two sections. Core Use and Additional Features. The core aspects of the application will be prioritised and implemented first and the Additional Features will be evaluated and (dependant on time constraints) implemented secondly.

- **User Account Sign Up**

- **Search Users Bar**

- **Encrypt and Compress Messages**

- **User Profiles**

- **Timed ‘Self Destruct’ Messages**

- **Wallet Implementation for Cryptocurrency(s)**

!

#

- **File Transfers**

$

The fundamental skills required to carry out the project have been identified and broken down into the following sections.

; %&' #() *+*

; * "#!

;, ! + - !

;. *"

The majority of the skills required will derive from pre-existing knowledge, further research will be required to ensure that the development of the project is carried out successfully. The key areas for research include; encryption techniques such as RSA or Needham-Schroeder Protocol, Cryptocurrency Wallets and how to implement them, compression algorithms such as Huffman Encoding and a general overview of Android Studio. Further online resources have been amended to the reference section which contain information regarding these skills.

Several obstacles may arise during the course of the project development. For the core part of the development, the biggest obstacle will be ensuring that encryption works across messages and for files. Research into handling different file types must be conducted to ensure that this doesn't happen.

Another obstacle will be to ensure that messages have a long enough time delay before they delete themselves from the database. This could be overcome by setting a time allowance per amount of words or by allowing users to adjust the time delay themselves after initially reading a message.

In regards to the additional features, the main obstacle will be with the implementation of cryptocurrency wallets. The initial research conducted will be to implement Bitcoin, however this may change to a different cryptocurrency as Bitcoin is known to have slow transaction times. This implementation must be tested vigorously to minimise bugs and prevent financial loss.

Although additional learning outcomes may come from the development of the project, the expected ones are as follows;

c / "

c 0

c # *

c,

This gives a firm basic understanding of cyber security in a practical use which is increasingly in demand alongside modern technological skills such as working with cryptocurrency and Android application development.

!

Android Studio. 'Android Developers Manual'. [online] Android. Available at: https://developer.android.com/develop/index.html [Accessed 6th Dec. 2017]

Ireland, D. (2016). 'RSA Algorithm'. [online] DI Management. Available at: http://www.geeksforgeeks.org/rsa-algorithm-cryptography [Accessed 6th Dec. 2017]

Marshall, D. (2001). 'Huffman Coding'. [online] Cardiff School of Computer Science & Informatics. Available at: https://users.cs.cf.ac.uk/Dave.Marshall/Multimedia/node210.html [Accessed 6th Dec. 2017]

Unknown. 'CoinSpark for Developers'. [online] CoinSpark. Available at: http://coinspark.org/developers [Accessed 6th Dec. 2017]