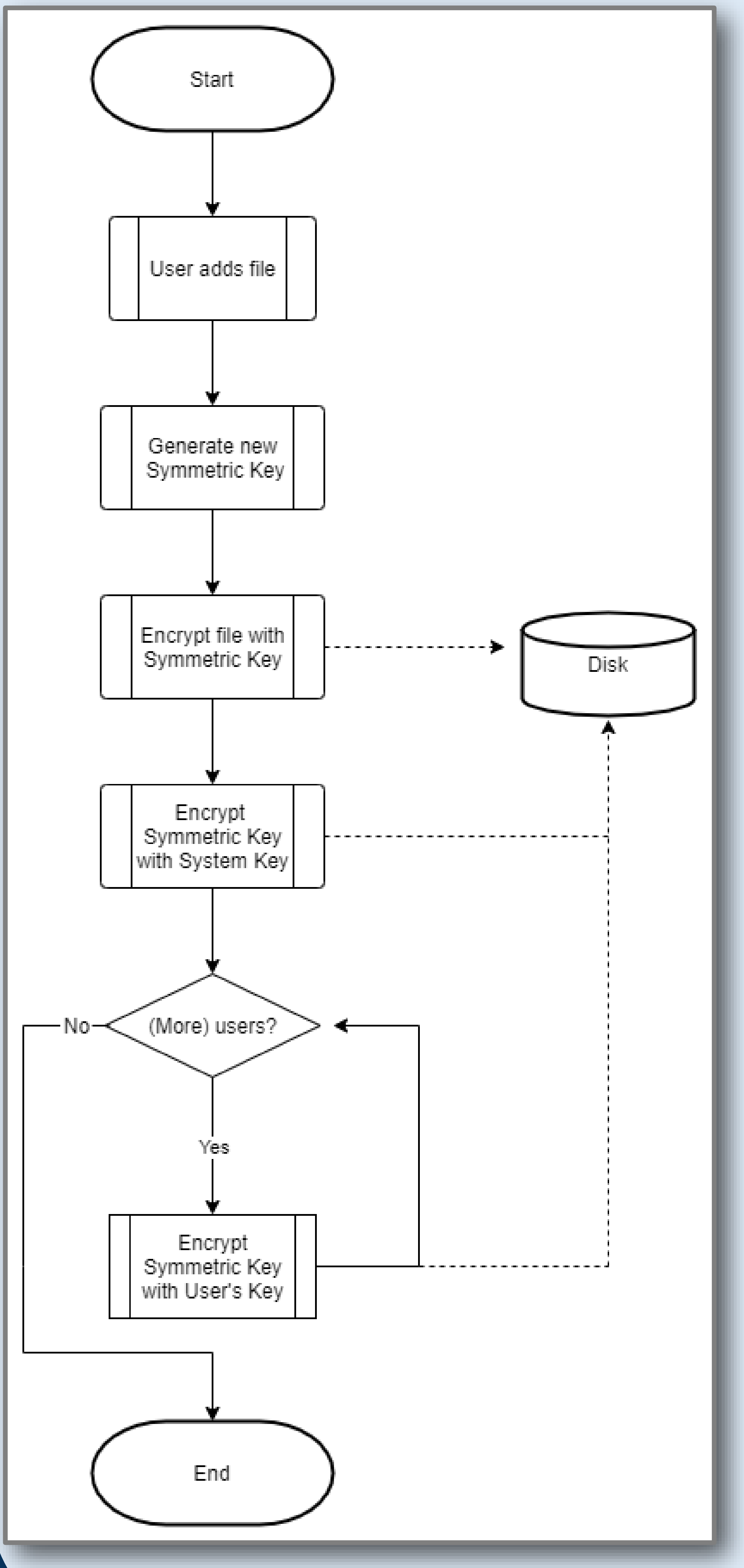
NON-SHARED KEY ENCRYPTION LOCKER FOR SHARING FILES SECURELY

INTRODUCTION

The aim of this project is to produce a non-shared key encryption software that will allow users to share files securely. Encryption is currently one of the most effective data security methods. It ensures data confidentiality by making the data not readable to unauthorised parties.[1] Encryption usually involves the use of cryptographic keys.

In conjunction with file encryption, this project will also look into how to design a system to enhance data security further by proposing a scheme where authorised parties will not need to share encryption keys in order to share files.

METHODS & TECHNOLOGY



Start

User adds file

Generate new Symmetric Key

Encrypt file with Symmetric Key

Disk

Encrypt Symmetric Key with System Key

(More) users?

No

Yes

Encrypt Symmetric Key with User's Key

End

Proposed method for this project is the use of hybrid cryptosystem as shown in the flowchart.

Both public-key system and symmetric-key system will be used. The reason is attackers could intercept the shared key if it is transmitted over the Internet alone for example and compromise data confidentiality. [2]

A combination of AES (symmetric encryption) and RSA (public-key encryption) algorithms are used.

In regards to technology used, Java programming language and Java Security API will be used.

Ioanna Miriam Pashalidi Kozelj
nnp18llf@bangor.ac.uk

PRIFYSGOL BANGOR UNIVERSITY

SUPERVISOR:
Cameron Gray
c.gray@bangor.ac.uk

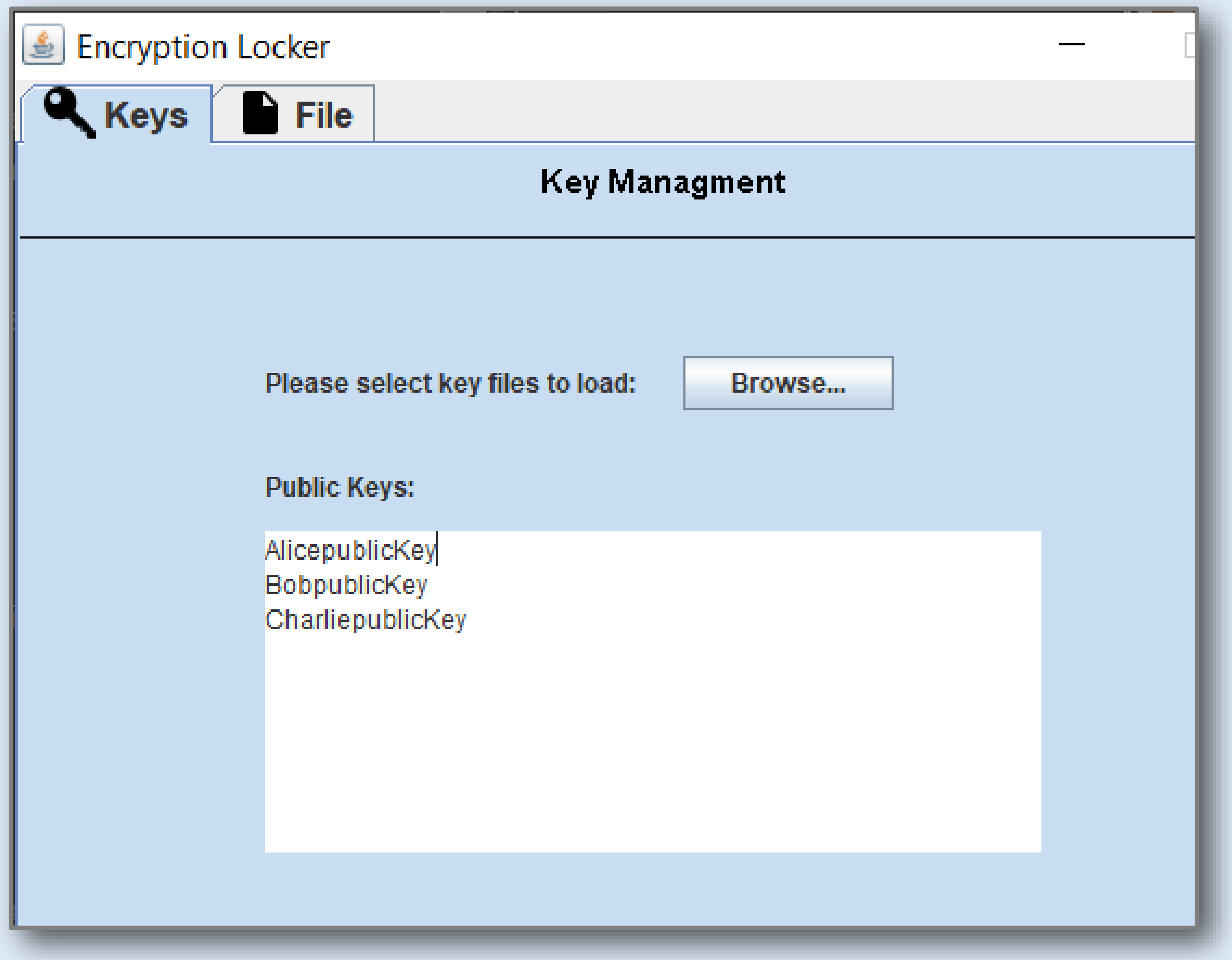
LITERATURE CITED

[1] - S. Bangera, P. Billava and S. Naik, "A Hybrid Encryption Approach for Secured Authentication and Enhancement in Confidentiality of Data," *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 2020, pp. 781-784, doi: 10.1109/ICCMC48092.2020.ICCMC-000145. Available at: https://ieeexplore.ieee.org/document/9076412

[2]—Y. Liu, W. Gong and W. Fan, "Application of AES and RSA Hybrid Algorithm in E-mail," *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, Singapore, 2018, pp. 701-703, doi: 10.1109/ICIS.2018.8466380.
Available at: https://ieeexplore.ieee.org/document/8466380

IMPLEMENTATION

Users will be able to interact with the software through graphical user interface shown in the figure below. The application will allow users to share files securely with a group of people by providing a key management feature where user could load other member's public keys that will be used as a part of file encryption process. The application also offers a decryption feature option so that the authorised members could decrypt The file using their own private keys.



Encryption Locker

Keys | File

Key Managment

Please select key files to load: Browse...

Public Keys:

AlicepublicKey
BobpublicKey
CharliepublicKey

CONCLUSIONS

As the files are being shared among users and individuals mostly across insecure channels (e.g. the internet), it becomes more challenging to ensure file security. The proposed hybrid cryptosystem that will be part of the project's software seems to solve some of the problems regarding data security as it offers efficiency of the symmetric-key encryption and convenience of the public-key encryption, meaning that the users do not need to share a key between them but simply use their own keys.