

by: Stefan More <[smore@student.tugraz.at](mailto:smore@student.tugraz.at)>  
Adviser: Dieter Bratko

### Problem:

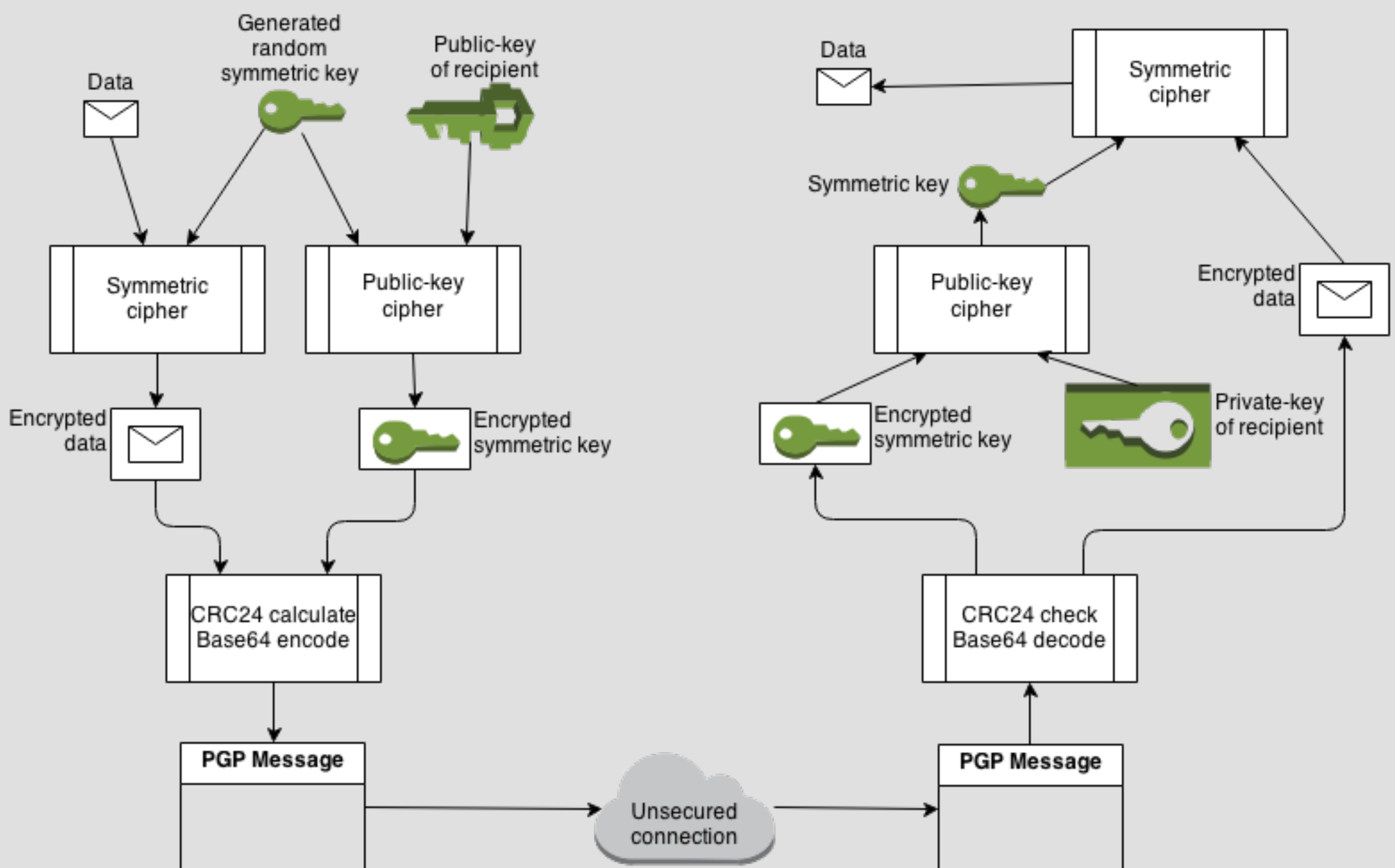
OpenPGP is a non-proprietary protocol for encrypting data. It combines public-key and symmetric cryptography.

IAIK's set of Java-based tools lacks an implementation of PGP. Yet.

### Goals:

- Implement RFC 4880 (OpenPGP) in Java
- Test Interoperability with other implementations
- Integrate OpenPGP in IAIK-JCE
- Implement a user interface to demo the lib

### Principle of OpenPGP encryption & decryption:



### Resources:

- *RFC 4880 (OpenPGP Message Format)*: <https://tools.ietf.org/html/rfc4880>
- *IAIK Java Cryptography Extension*: <https://jce.iaik.tugraz.at>
- *This project's source code*: <http://jpg.2904.cc>