Enigma 破译 实验报告

陈庆之 2021011819

2023 年 4 月 9 日

1 算法原理

1.1 Enigma 原理

1.2 Rejewski 的方法

1.3 Turing 的方法

2 实际攻击样例

2.1 Rejewski 的方法

2.2 Turing 的方法

3 代码结构与文档

3.1 代码结构

本次实验的代码部分包括以下文件：

1. `enigma.py`: 实现了支持选择转子顺序、插线板、转子设置、初始值设置的 Enigma I 密码机。密码机会存储最开始的设置，并支持 `reset()` 方法。密码机的转子数量、可用转子排列等可以被简单地扩展。
2. `rejewski.py`: 实现了 Rejewski 的破解方法。其中的 `make_catalogue()` 可以在当前目录下生成 `catalogue.json`（相当于波兰人**建立目录**的过程），之后使用 `decypher(...)` 方法可以对特定的重复密钥序列进行破解。
3. `turing.py`: 实现了 Turing 的破解方法。使用其中的 `decypher(...)` 方法并传入已发现的环，方法会返回所有可能的转子序列和初始位置。