work2

姓名：吴浩哲

学号：2223612444

1. 简述ENIGMA密码机是如何组成，以及如何保证加解密一致性。

组成结构

1. **键盘**：用于输入明文字母。
2. **转子**：核心加密部件，通常由3-4个可旋转的圆盘组成，每个转子内部有26个电触点，对应字母A-Z，通过内部连线实现字母替换。转子会随每次按键转动，改变加密路径。
3. **反射器**：固定不动的圆盘，将电流反射回转子，确保加密和解密路径对称。
4. **插线板**：通过电缆交换字母对（如A-B），进一步增加密钥空间。
5. **指示灯/显示器**：显示加密后的字母。

加解密一致性保证

1. **对称设计**：反射器的存在使得加密和解密路径完全一致。输入字母A加密为D时，输入D必解密为A。
2. **密钥同步**：收发双方需预先约定相同的初始设置，包括：
   - 转子排列顺序。
   - 转子初始方向。
   - 插线板连线方式。
3. **动态加密**：每次按键后转子转动，改变字母映射关系，但双方机器同步转动，确保解密时路径还原。

工作流程示例

1. **加密**：明文输入→通过插线板→经转子多层替换→反射器反射→反向通过转子→插线板→输出密文。
2. **解密**：密文输入时，电流沿相同路径反向流动，还原明文。

2. 若接线板有10条连接线，扰频器（转子）5选3，计算密钥个数，哪个部件对密钥空间的扩大起的作用更大?

计算密钥个数

ENIGMA密码机的密钥空间由以下三部分组成：

(1) 转子（扰频器）的排列与初始位置

- **转子选择**：从5个转子中选3个，排列方式为排列数 $A_5^3 = 5 \times 4 \times 3 = 60$ 种。
- **初始位置**：每个转子有26个可能的位置，因此初始位置组合数为 $26^3 = 17576$ 种。
- **总转子密钥空间**：$A_5^3 \times 26^3 = 60 \times 17576 = 1054560$ 种。

(2) 接线板的连接方式

- 接线板交换10对字母（即10条连接线），需从26个字母中选择20个字母（10对），剩余6个字母不交换。
- 计算公式为：
- $$\frac{26!}{(26-20)! \times 10! \times 2^{10}} = \frac{26!}{6! \times 10! \times 1024}$$
- 具体数值约为 150738274937250 种。

(3) 总密钥空间

将转子部分和接线板部分相乘：

$$1054560 \times 150738274937250 \approx 1.59 \times 1020$$

哪个部件对密钥空间贡献更大?

- **接线板**的密钥空间约为 1.5×10^{14} 种，而**转子**部分仅为约 1.05×10^6 种。
- 接线板的贡献是转子的约 **1500亿倍**，因此**接线板对密钥空间的扩大起决定性作用。**

3. 阐述扰频器和线路接线板是如何被破译的?

扰频器的破译

（1）数学建模与置换理论

- **波兰数学家雷杰夫斯基**通过分析ENIGMA的加密过程，发现**转子状态与字母替换的循环圈规律。**他证明：
  - 每条电文开头的6个字母（通信密钥重复两次加密）生成的字母对应表，其**循环圈的数量和长度仅由转子顺序和初始位置决定**，与接线板无关。

- 通过穷举$26^3 = 17576$种转子初始位置，结合循环圈特征建立“指纹库”，大幅缩小密钥空间。

（2）操作漏洞利用

- **密钥重复加密**：德军要求操作员将通信密钥（如`PGH`）输入两次（如`PGHPGH`），但仅第一个转子转动，导致重复加密的密文存在规律性关联，雷杰夫斯基通过统计密文对破解转子状态。
- **反射器特性**：ENIGMA的反射器设计确保字母**不会加密为自身**，这一特性被用于排除无效密钥组合。

线路接线板的破译

（1）分离接线板的影响

- 雷杰夫斯基发现，**接线板的字母交换不影响循环圈的结构**（如循环圈数量、长度）。破译时先确定转子状态，再反向推导接线板的连接方式。
- 例如，若接线板交换了字母A/L，但循环圈`A→F→W→A`仍保持3个字母长度，仅具体字母变化。

（2）已知明文攻击

- **固定报文格式**：德军在电文中频繁使用固定短语（如“Heil Hitler”或天气预报“wetter”），通过猜测明文与密文对应关系，可推断接线板配置。
- **“炸弹”机辅助**：英国图灵团队设计的“炸弹”机（Bombe）自动化测试可能的接线板组合，结合已知明文快速筛选有效配置。