

# CRYPTANALYSIS OF PURPLE, JAPANESE WWII CIPHER MACHINE

PASSWORD123

我們

周廷威 組長

資訊工程學系 112550013

賴邑城 組員

資訊工程學系 112550009

蔡尚融 組員

資訊工程學系 112550201

許有暢 組員

資訊工程學系 112550168

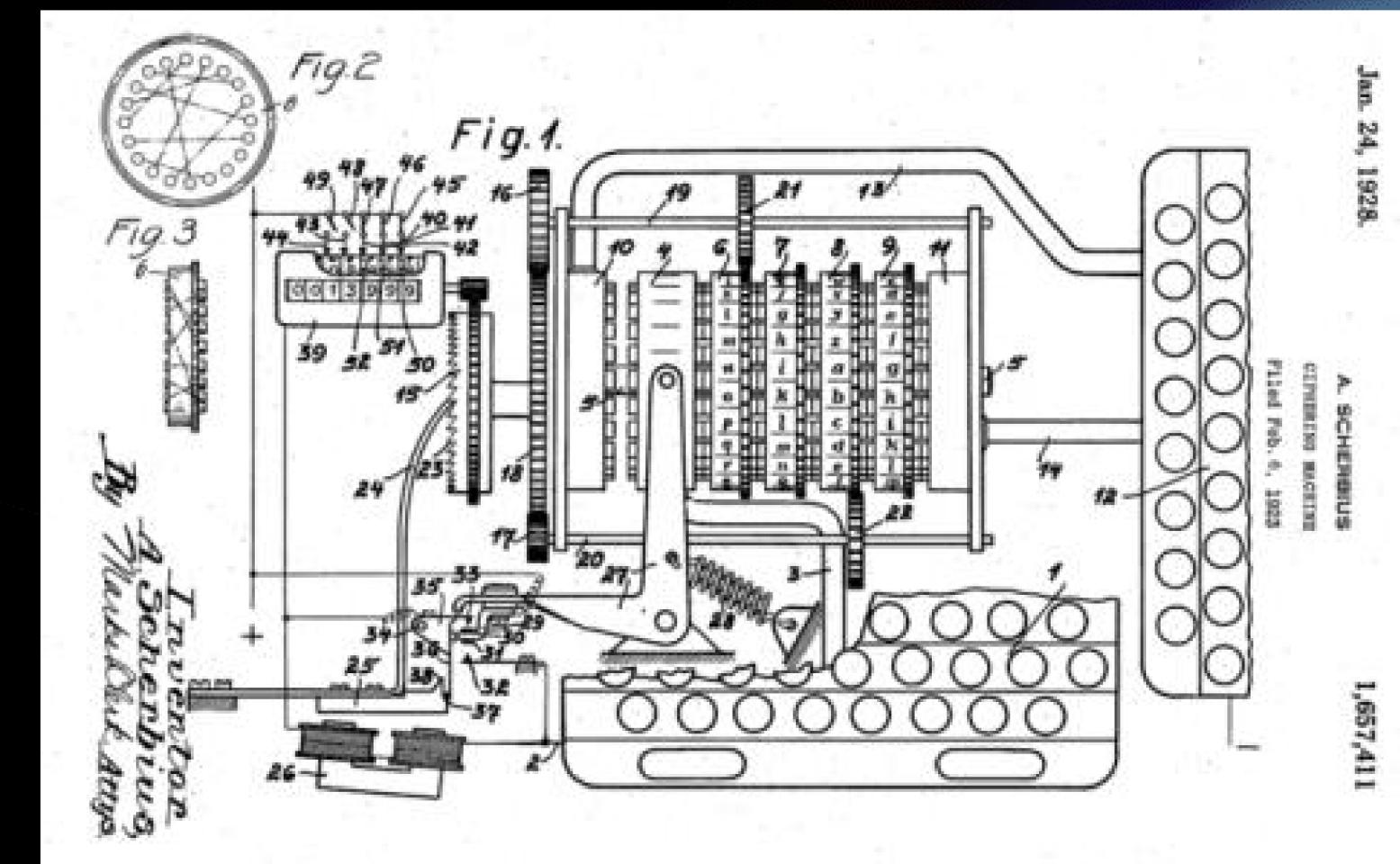
傅永威 組員

資訊工程學系 112550107

# 背景

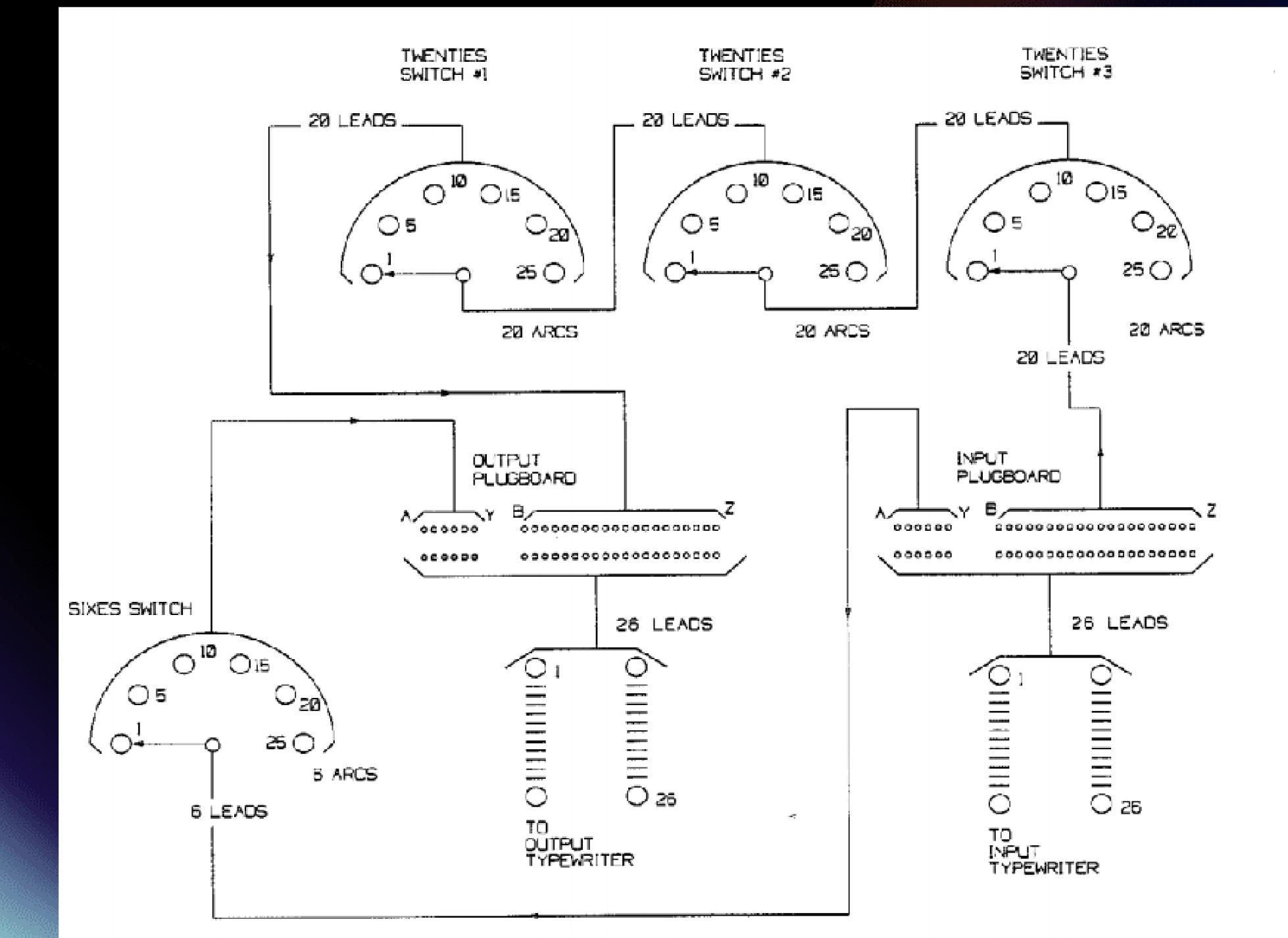
在第二次世界大戰中，密碼機被廣泛用於安全通訊。

紫色密碼機（PURPLE）是美國密碼分析師用來代稱日本在二戰期間使用的97式歐文打字機。這臺機器主要用於加密日本的重要外交和軍事通訊。



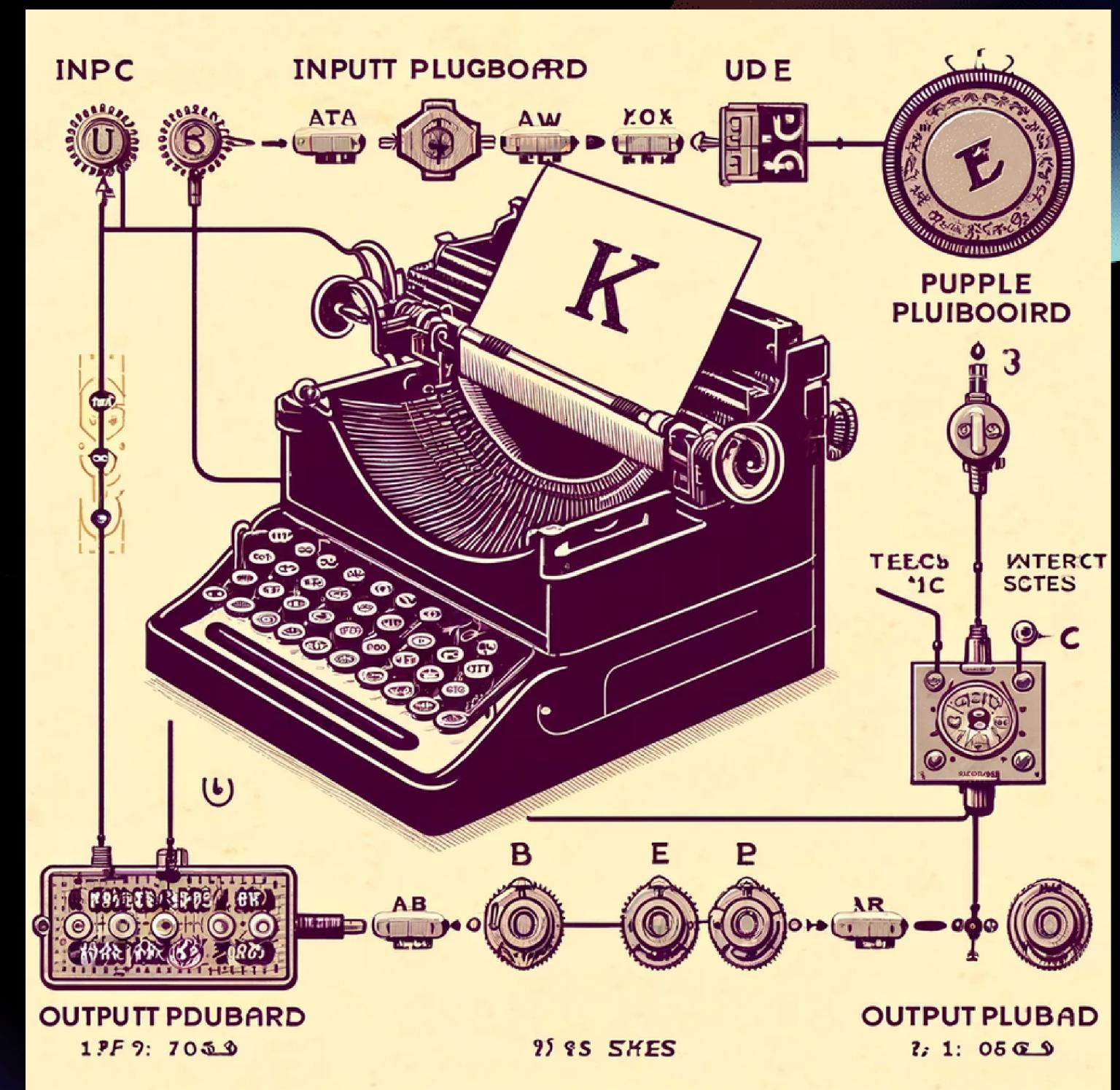
# 紫色密碼機組件

- 輸入插線板
- 切換開關
- 輸出插線板
- 步進開關



# 加密示例

- 外部輸入
- 輸入插線板
- 轉輪加密
- 輸出插線板



# 弱點與攻擊手段

- 機器的結構弱點
  - 內部字母表分割
  - 轉輪位置變換頻率
- 實施的攻擊策略
  - 已知明文攻擊
  - 密文唯一攻擊



# 參考資料

- LAMI, B., KALLCO, G., GUO, N., & SHI, S. (2019). CRYPTANALYSIS OF PURPLE, JAPANESE WWII CIPHER MACHINE.
- OPENAI. (2024). CHATGPT (4) [LARGE LANGUAGE MODEL].  
[HTTPS://CHAT.OPENAI.COM](https://chat.openai.com)
- 解密恩尼格碼密碼機——《科學月刊》. (2016, JANUARY 27).  
[HTTPS://PANSOI.ASIA/ARCHIVES/92180](https://pansci.asia/archives/92180)

謝謝聆聽！