Cryptanalysis of Purple: the Japanese WWII Cipher Machine

GROUP: PASSWORD123

謝致仁 F01061

許有暢 112550168

蔡尚融 112550201

賴邑城 112550009

傅永威 112550107

周廷威 112550013

CONTENT

ABSTRACT

我們想要回到過去二次大戰的時代，體會一下當時破譯密碼的辛酸，了解那個年代的情報戰爭和密碼學家的巨大貢獻。這段歷史不僅展示了技術的突破，還揭示了人類智慧與勇氣的極限。這將是一段充滿敬意的回溯之旅，讓我們重新審視那些在背後默默奉獻的人們所留下的永恆遺產。

INTRODUCTION

密碼機於二次大戰期間被廣泛應用於安全通訊

紫色密碼機 (PURPLE) 是美國密碼分析師用來代稱日本在二次大戰期間所使用的97式歐文打字機

主要用於加密日本重要的外交和軍事通訊

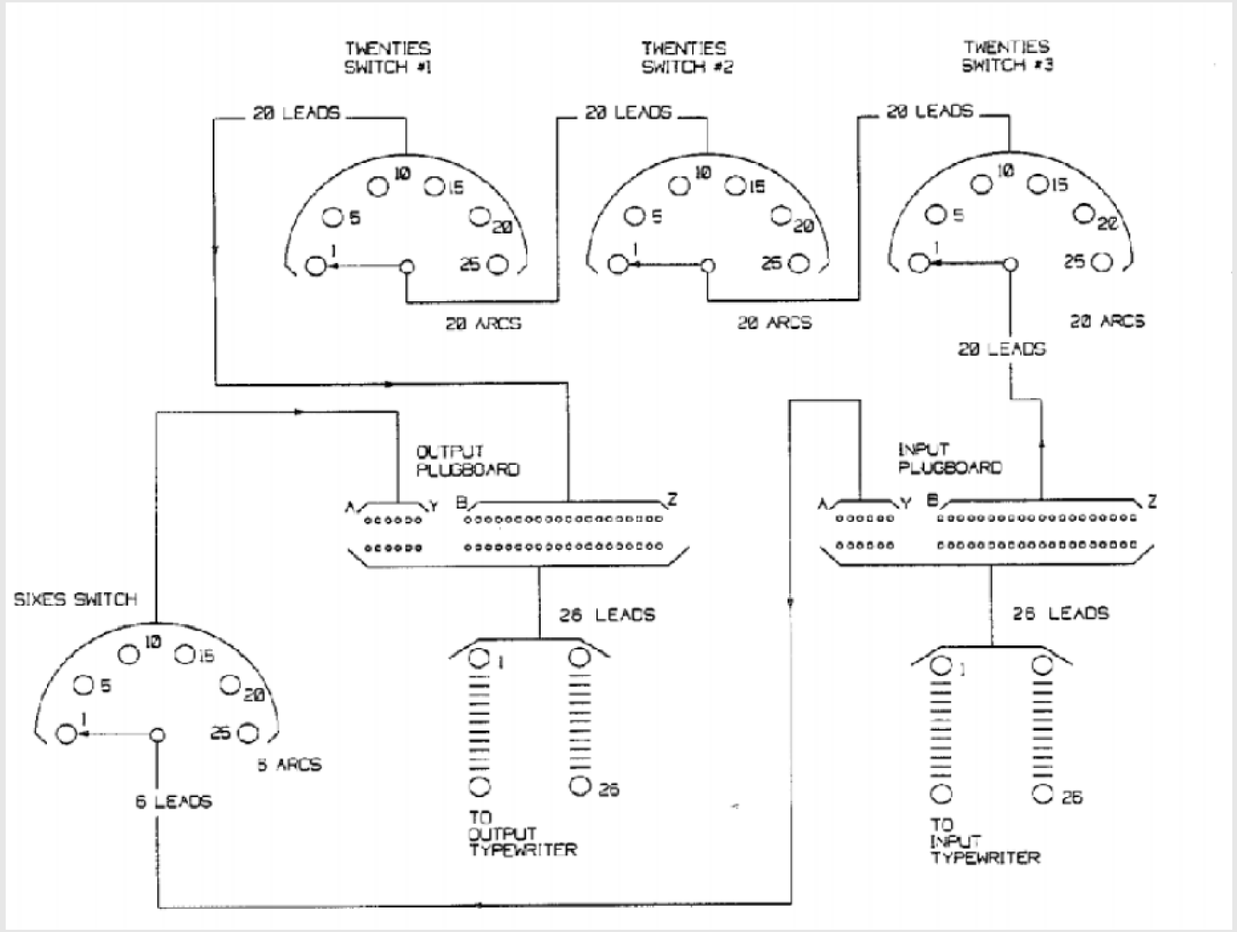
COMPONENT

輸入插線板

切換開關

輸出插線板

步進開關



SYSTEM ARCHITECTURE

CRACKING METHODS

(一) 暴力破解

- 窮舉 Key 來一一解密，比對各項結果之預測分數。
- 概念較基本。
- 用來處理 Rotor 解密。

(二) MCMC

- 使用 Markov-Chain-Monte-Carlo 演算法
- 適合處理高維度、多重可能性之樣本。較有彈性及效率。
- 用來分析 Plugboard 狀態。

EXPERIMENT

(一) 暴力破解

- 先將一串明文以隨機產生的 KEY 加密
- 測試選用的明文為 IN THE HEART OF A DENSE FOREST, DAPPLED SUNLIGHT PIERCED THE THICK CANOPY, CASTING A MOSAIC OF LIGHT AND SHADOW ON THE FOREST FLOOR.

(一) 暴力破解

- 隨機產生的 KEY：13,1,18,24,32
- 加密後的密文為

  ADJREZEEJFENYDOZGYCIQITLMEPQTE

  RSYSZUTHXCYIGGOLWPADMUQCCOTO

  NIJIHBEXBIKILYIREVXOFXVALXLVISULI

  QSGOVEHAVRTJEUB

(一) 暴力破解

- SCORING FUNCTION: BIGRAM
- 利用暴搜 ROTOR 組合 (KEY) 的方式，得到分數最高的解密字串

(一) 暴力破解

substitution.py 1, U decryption.py 2, U Force.py 2, U

final_project > codes > Force.py > ...

```python
        save_bigram(bigrams)
    text = "In the heart of a dense forest, dappled sunlight pierced the thick canopy, casting a mosaic of ligh
    pur, key = RandomPurple()
    print(f"Key: {key}")
    encrypted = pur.encrypt(filter(text))
    print(f"Encrypted: {encrypted}")
    pur = Purple97().from_key_sheet(key)
    print(f"The cypher should be decrypt like this: {pur.decrypt(encrypted)}")
    best_text = ""
    best_score = -float('inf')
    for i in tqdm.tqdm(range(1,pow(25,4)), desc="Decyphering"):
        for m in range(1, 6):
            key = f"{i%25+1}-{i//25%25+1},{i//625%25+1},{i//15625%25+1}-{sw_fast_slow[m]}"
            depur = Purple97().from_key_sheet(key)
            decrypted = depur.decrypt(encrypted)
            score = grade(decrypted, bigrams)
            if score > best_score:
                best_score = score
                best_text = decrypted
    print(f"Best score: {best_score}, text: {best_text}")
```

PROBLEMS 5 OUTPUT DEBUG CONSOLE TERMINAL PORTS GITLENS COMMENTS

```
(base) PS C:\Users\userwei\Desktop\Coding\GitHub\NYCU_Cryptography-Engineering\final_project\codes> python -u "c:\Users\userwei\Desktop\Coding\GitHub\NYCU_Cryptography-Engineering\final_project\codes\Force.py"
Bigram scores loaded from bigram_scores.json
Key: 13-1,18,24-32
Encrypted: ADJREZEEJFENYDOZGYCIQITLMEPQTERSYSZUTHXCYIGGOLWPADMUQCCOTONIJIHBEXBIKILYIREVXOFXVALXLVISULIQSGOVEHAVRTJEUB
The cypher should be decrypt like this: INTHEHEARTOFADENSEFORESTDAPPLEDSUNLIGHTPIERCEDTHETHICKCANOPYCASTINGAMOSAICOFLIGHTANDSHADOWONTHEFORESTFLOOR
Decyphering: 100%|██████████| 390624/390624 [04:12<00:00, 1546.39it/s]
Best score: -663.0997415503504, text: IKNBEVEAVLOBABETKEROMELSNAHNFEDMUTBITDPMIENRENGFEFTISSRATOPYFAWGILBACOBAIGOHPIWRTATGSDANOJOMBLECONETHPBOOB
```

(一) 暴力破解

- 解密後的字串為

IKNBEVEAVLOBABETKEROMELSNAHNF

EDMUTBITDPMIENRENGFEFTISSRATOP

YFAWGILBACOBAIGOHPIWRTATGSDAN

OIOMBLECONETHPBOOB

(二) MCMC

經插線板加密後密文：

OF ZIT ITQKZ GY Q RTFLT YGKTLZ, RQHHSTR LXFSOUIZ HOTKETR ZIT ZIOEA EQFGHN, EQLZOFU Q DGLQOE GY SOUIZ QFR LIQRGV GF ZIT YGKTLZ YSGGK. Q UTFZST WKTTMT VIOLHTKTR ZIKGXUI ZIT STQCTL, EQKKNOFU VOZI OZ ZIT LETFZ GY VOSRYSGVTKL QFR RQDH TQKZI....

(二) MCMC

substitution.py 1, U | decryption.py 2, U | Force.py 2, U

final_project > codes > substitution.py > ...

```python
class MCMC_sub:
    def decrypt(self,text:str,iterations:int=10000) -> str:
                    if check_dict(best_text,self.cipher,self.words) > 0.5:
                        print(f"New best score: {best_score}, Text: {best_text}")

        return best_text

if __name__ == "__main__":
    text = "Of zit itqkz gy q rtflt ygktlz, rqhhstr lxfsouiz hotketr zit zioea eqfghn, eqlzofu q dglqoe gy soui
    text = text.upper()
    tt = ""
    for c in filter_plaintext(text):
        tt += c
    mcmcsub = MCMC_sub(tt)
    print(mcmcsub.decrypt(tt))
```

PROBLEMS 5 | OUTPUT | DEBUG CONSOLE | TERMINAL | PORTS | GITLENS | COMMENTS

```
(base) PS C:\Users\userwei\Desktop\Coding\GitHub\NYCU_Cryptography-Engineering\final_project\codes> python -u "c:\Users\userwe
i\Desktop\Coding\GitHub\NYCU_Cryptography-Engineering\final_project\codes\substitution.py"
Bigram scores loaded from bigram_scores.json
100%|██████████| 10000/10000 [00:01<00:00, 5804.32it/s]
INTHEHEARTOFADENSEFORESTDAPPLEDSUNLIGHTPIERCEDTHETHICKCANOPYCASTINGAMOSAICOFLIGHTANDSHADOWONTHEFORESTFLOORAGENTLEBREEXEWHISPER
EDTHROUGHTHELEAZESCARRYINGWITHITTHESCENTOFWILDFLOWERSANDDAMPEARTHBIRDSCHIRPEDMELODIOUSLYFROMHIDDENPERCHESADDINGTOTHESERENESYMP
HONYOFNATUREAMIDSTTHISTRANQUILSETTINGASMALLCURIOUSFOVPOKEDITSHEADFROMBEHINDABUSHITSBRIGHTEYESSCANNINGTHESURROUNDINGSWITHAMIVOF
CAUTIONANDWONDERASITZENTUREDFURTHERTHERUSTLEOFITSSTEPSMINGLEDWITHTHESOFTSOUNDSOFTHEFORESTCREATINGAPEACEFULHARMONYWITHTHEWILDER
NESS
```

(二) MCMC

SCORING FUNCTION: BIGRAM

解密後明文：

INTHEHEARTOFADENSEFORESTDAPPLEDS
UNLIGHTPIERCEDTHETHICKCANOPYCASTI
NGAMOSAICOFLIGHTANDSHADOWONTHEF
ORESTFLOORAGENTLEBREEXEWHISPERED
THROUGHTHELEAZESCARRYINGWITHITTH
ESCENTOFWILDFLOWERSAND....

PROSPECT

將破解 ROTOR 與 PLUGBOARD 的方法結合，搭配其他的 SCORING FUNCTION（合法字串長度平方等），得到最有文句特性字串作為破解的結果。

CONTRIBUTION

破解 PURPLE 密碼機的期末專題展示了現代密碼分析技術的顯著進步，不僅增強了對歷史密碼學的理解，也為改進現代信息安全措施提供了寶貴的見解。

除此之外，這也有助於加強加密技術的發展，提升數據保護水平，並提供更強的抵禦潛在威脅的能力。

Q&A

THANKS FOR LISTENING!!