二重の格子
解　説

本問題は、Vigenère暗号とPlayfair暗号を組み合わせた二重暗号の解読を題材としています。外側のVigenère暗号を解読すると、内側のPlayfair暗号の鍵が判明します。 Vigenère暗号は16世紀にフランスの外交官Blaise de Vigenèreによって広められた多表式換字暗号です。単一換字暗号とは異なり、平文の各文字を鍵の対応する文字に基づいて異なるシフト量で暗号化します。

鍵が繰り返し使用されるため、同じ平文でも鍵の位置によって異なる暗号文になります。この特性により、単純な頻度分析では解読が困難ですが、Kasiski検定や一致指数法によって鍵長を特定し、列ごとに頻度分析を行うことで解読が可能です。

Playfair暗号は1854年にイギリスの科学者Charles Wheatstoneが考案した二字組換字暗号です。

鍵から生成した5×5のアルファベット表を用いて、平文を2文字ずつのペアに分割して暗号化します。同じ文字が連続する場合はXなどのパディング文字を挿入します。暗号化規則は、2文字が同じ行にある場合は右隣の文字に、同じ列にある場合は下隣の文字に、それ以外の場合は矩形の対角にある文字に置換します。

第一次世界大戦ではイギリス軍が実際に使用しました。

まず暗号文を確認します。

```
  EFLVK OVLJP MWQEQ NHIJR TTLIE TCHLT WCJNW SEFBT WHJVM JMSTV LRKMR KGDGH JVITR WUDMC
TFEYW JZGWK ACTUE DTQHI HUKBU SHBXR YEREZ XHYCS CKYYO GBUZG OZIIL ANXKM YRNEK HU
```

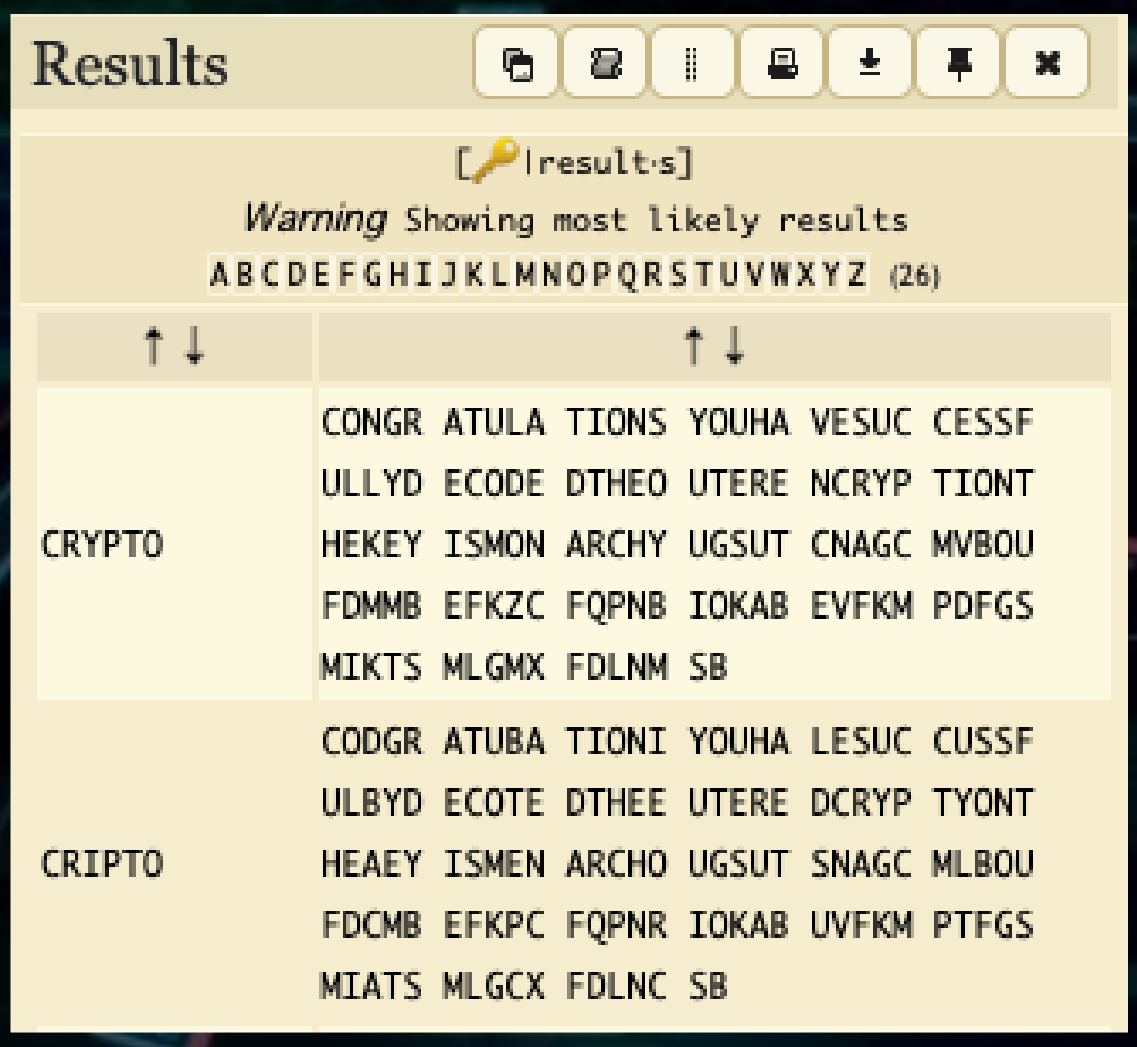
暗号文は5文字区切りで表記されて
おり、これはVigenère暗号の典型的な
形式です。問題文から、外側の暗号を
解読すると内側の暗号の鍵が判明
することがわかります。5文字区切り
の表記と二重暗号という構造から、
外側の暗号はVigenère暗号と推測
できます。Vigenère Solver で検索
すると、Vigenère暗号を復号できる
サイトがあり、こちらで復号を試して
みます。

以降はVIGENERE CIPHERというサイトを使用して解説します。

(参考: https://www.dcode.fr/vigenere-cipher)

Vigenere ciphertext の欄に暗号文を入力し、

[AUTOMATIC DECRYPTION]を選択します。 左側サイドバーにResultが表示されます。



CRYPTOという鍵文字列でCONGR ATULA TIONS (CONGRATULATIONS)という綴りが確認できます。復号に成功しました。

```
CONGR ATULA TIONS YOUHA VESUC CESSF ULLYD ECODE DTHEO UTERE NCRYP TIONT HEKEY ISMON
ARCHY UGSUT CNAGC MVBOU FDMMB EFKZC FQPNB IOKAB EVFKM PDFGS MIKTS MLGMX FDLNM SB
```

整形後のテキストは以下のとおりです。

```
CONGRATULATIONS YOU HAVE SUCCESSFULLY DECODED THE OUTER ENCRYPTION THE KEY IS MONARCHY
UGSUTCNAGCMVBOUFDMMBEFKZCFQPNBIOKABEVFKMPDFGSMIKTSMLGMXFDLNMSB
```

次に、内側の暗号を解読します。

問題文で
「古典暗号を二重に用いた」と
あることから、内側の暗号も古典暗号であると考えられます。

鍵「MONARCHY」という英単語から連想される19世紀イギリスの暗号方式として、Playfair暗号が候補に挙がります。 Playfair Solverで検索すると、 先程と同様にPlayfair暗号を復号できるサイトがあり、こちらで復号を試してみます。

(参考:https://www.dcode.fr/playfair-cipher)

PlayFair ciphertextに以下を入力します。

```
UGSUTCNAGCMVBOUFDMMBEFKZCFQPNBIOKABEVFKMPDFGSMIKTSMLGMXFDLNMSB
```

次に、Playfair暗号で使用する 5×5 のグリッド（Playfair Grid） を生成します。Playfair暗号ではアルファベット26文字のうちＪを除外し、25文字で処理を行う点が特徴です。

本問題では鍵とし「MONARCHY」が指定されています。そのため、まず重複を除いた形で鍵文字を先頭に配置し、その後に残りの

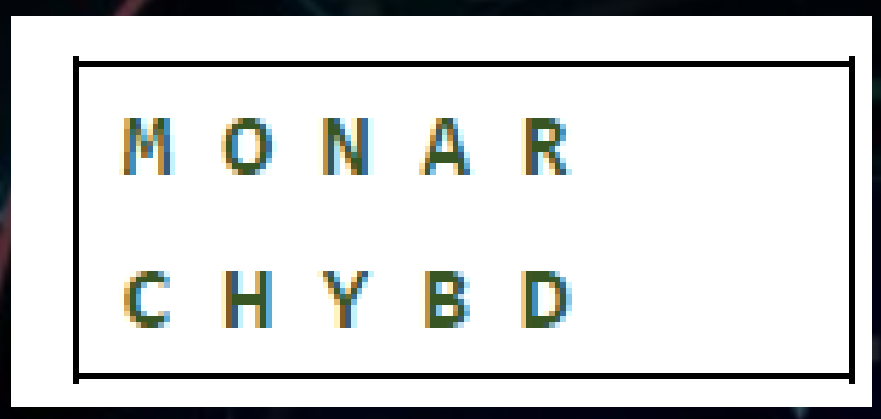
アルファベットを辞書順で埋めることで、対応するグリッドを構築します。

その結果、本問題で使用する

Playfair Gridは

「MONARCHYBDEFGIKLPQSTUVWXZ」

を入力します。



[DECRYPT PLAYFAIR]を押して

復号します。左側サイドバーに

Resultが表示されます。

```
WELXLDONEYOUHAVECRACKEDTHEPLAYFAIRCIPHERTHEFLAGISQUEENVICTORIA
```

単語毎に分けた結果が以下のとおりです。

```
WELXL DONE YOU HAVE CRACKED THE PLAYFAIR CHIPHER THE FLAG IS QUEEN  VICTORIA
```

冒頭に現れる「WELXLDONE」は、Playfair暗号における埋字（パディング）の影響によるものです。Playfair暗号では、暗号化・復号の処理単位は常に2文字（ダイグラフ）です。そのため、平文を2文字ずつ区切っていく際、同一のアルファベットが同じペア内に並んでしまう場合は、その間に埋字として「X」を挿入します

例えば「WELL DONE」を2文字ずつ区切ると、「WE」「LL」「DO」「NE」となりますが、「LL」は同一文字が同一ペア内に存在するため、Playfairの規則により「LXL」に分割され、結果として「WE」「LX」「LD」「ON」「E」となります。

このため、復号結果には「WELXLDONE」という形で「X」が現れます。

この「X」は意味を持たない埋字であるため、文脈上不要なものとして削除し、最終的に「WELL DONE」と読み取ります。

一方で「QUEENVICTORIA」のように、「EE」が連続していても「SQ」「UE」「EN」「VI」「CT」「OR」「IA」のように異なるペアに分かれている場合は、同一ペア内での重複ではないため、埋字は挿入されません。上記のルールを埋字（パディング）を取り除いた文字列は以下になります。

```
WELL DONE YOU HAVE CRACKED THE PLAYFAIR CHIPHER THE FLAG IS QUEEN  VICTORIA
```

フラグが確認できました。

flag{queenvictoria}