README: Vigenère Cipher Brute Forcer v1.0

Overview

The **Vigenère Cipher Brute Forcer** is a web-based application that assists with solving encrypted messages using the Vigenère cipher. This tool provides options to brute force potential decryption keys, manually solve ciphers, and analyze decrypted outputs for common patterns, valid words, or multi-word results.

This is **version 1**, a work-in-progress app developed over three days, aimed at assisting with the Felcycle Puzzle and other decryption tasks.

Features

1. **Brute Force Decryption**:
    - Attempts to decrypt the cipher using all possible keys based on user-defined parameters like key length and filtering options.
    - Includes optional features to:
        - Add a "Zeroth" row in the Vigenère table.
        - Remove specific letters (D and R) from the alphabet.
        - Filter results based on repeated letters, common words, or an extended word list.
2. **Manual Solve**:
    - Allows users to input a cipher and a manual key to directly decrypt a message.
3. **Word List Integration**:
    - Fetches and combines two lists:
        - **Common words** from an external API.
        - **Extra words** from a customizable local word list (e.g., Felcycle-related terms).
    - Enables filtering results using the combined word list.
4. **Anagram Generator**:
    - Processes decrypted results to find valid anagrams based on the combined word list.

   - Supports both single and multi-word anagram generation.

5. **Progress Tracking**:
   - Displays a real-time progress bar and estimated time remaining during brute force and anagram generation.
   - Provides interactive feedback such as "Just getting started," "Over halfway there," and "Almost done!"

6. **Output Sections**:
   - Displays:
     - Decrypted results.
     - Filtered keys.
     - Filtered decrypted results.
     - Results containing 4+ words or keys.
     - Multi-word results.
     - Full word results (8-character keys).
     - Generated anagrams.

7. **Dynamic Reset and Pause/Resume**:
   - Includes a reset button to clear all inputs and outputs.
   - Brute force can be paused and resumed as needed.

How to Use

1. **Launch the App**:
   - Open index.html in any modern browser.

2. **Input Parameters**:
   - Enter the encrypted message (cipher word) in the **Cipher Word** field.
   - Optionally, provide a **partial key** to narrow down brute force attempts.

3. **Select Key Length**:
   - Choose a key length (2-8 characters) for the brute force process.

4. **Apply Filters** (optional):
   - Enable one or more filters to refine results:

        - **Add Zeroth**: Includes an extra row in the Vigenère table starting with the full alphabet.
        - **Remove D and R**: Excludes letters D and R from the alphabet.
        - **Only Keys with Repeated Letters**: Filters keys that have repeated characters.
        - **Only Keys with Common Words**: Filters keys that contain common dictionary words.
        - **Use Word List Keys Only**: Uses the preloaded word list for potential keys.
        - **Only Results with Letters Repeated Twice**: Filters decrypted results that repeat any letter exactly twice.

5. **Decrypt**:
    - **Manual Solve**: Enter a key to decrypt directly.
    - **Brute Force**: Click the "Brute Force" button to initiate the decryption process.
6. **Track Progress**:
    - Monitor the progress bar and estimated time remaining.
    - View decrypted results in real time as they are processed.
7. **Generate Anagrams**:
    - After decryption, click **Generate Anagrams** to analyze decrypted results for valid anagrams.
8. **Reset**:
    - Clear all inputs and outputs using the **Reset** button.

Word List Management

- **Custom Word List**:
    - The extra-words.js file contains additional terms specific to your needs, such as Felcycle-related keywords.
    - Modify this file to add/remove words as needed.
    - The app combines these extra words with a common word list fetched from the Datamuse API.

Technical Notes

- **Vigenère Table**:
  - The app dynamically creates the Vigenère table based on the selected filters (e.g., removing specific letters).
- **Performance Considerations**:
  - Brute force and anagram generation can be resource-intensive for longer key lengths or large input data. Use filters to optimize performance.
  - Progress updates are throttled to prevent browser freezing.

Known Limitations (v1.0)

- **Performance**:
  - Brute force decryption may slow down for key lengths >6 without filters.
- **API Dependency**:
  - Requires an internet connection to fetch the common word list from the Datamuse API.
- **Interface**:
  - Currently designed for desktop browsers. Mobile compatibility may require adjustments.

Planned Improvements

- Enhance performance for long keys by parallelizing computations.
- Add a mobile-friendly layout.
- Improve anagram generation for large datasets.
- Introduce save/load functionality for decrypted results.

File Structure

- **HTML**: index.html - Main user interface.
- **JavaScript**:

  - app.js - Core logic for brute force decryption, word list management, and anagram generation.
  - extra-words.js - Additional word list customization.
- **CSS**: styles.css - Application styling.

This app is intended for personal use and is actively being improved. Contributions and feedback are welcome as we progress toward future versions.