

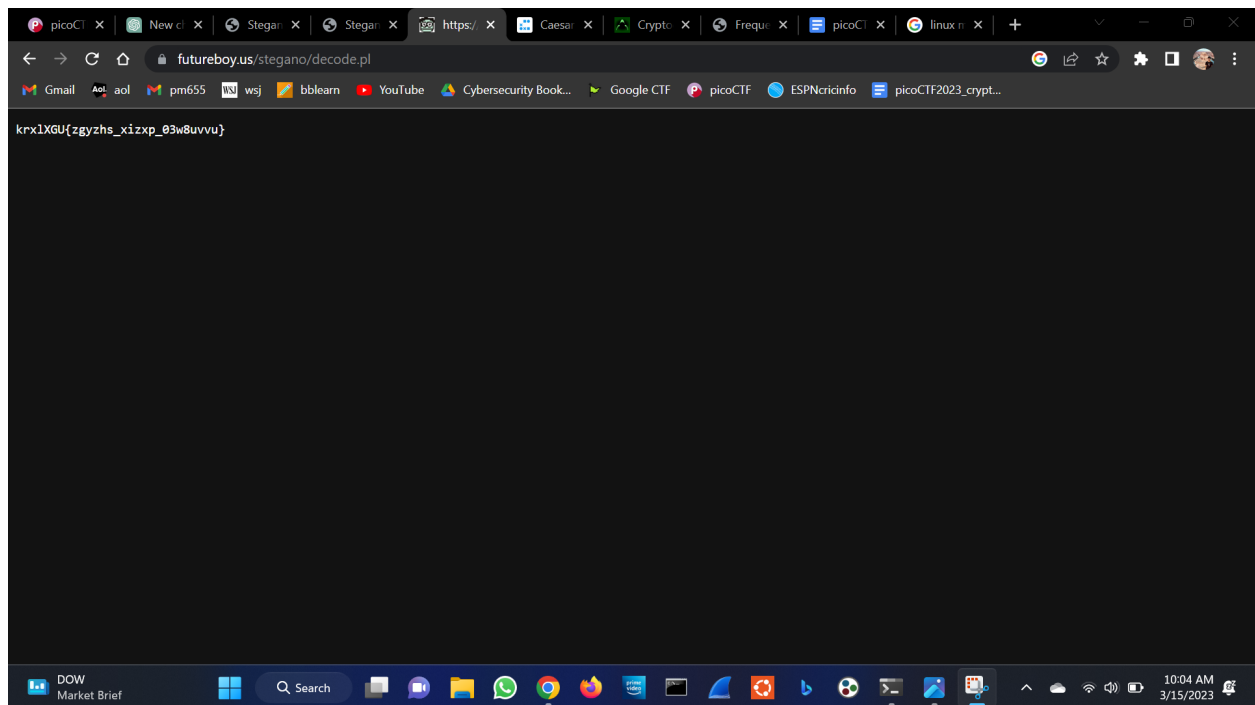
HideToSee

The screenshot shows a web browser window with the URL `futureboy.us/stegano/decinput.html`. The page title is "Steganographic Decoder". The form contains the following elements:

- A paragraph explaining the form's purpose: "This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will be asked to save the resulting payload file to disk. This form may also help you guess at what the payload is and its file type..."
- A section titled "Select a JPEG, WAV, or AU file to decode:" with a "Choose File" button and the text "atbash (4).jpg".
- A "Password (may be blank):" text input field.
- Three radio buttons for output options:
 - ☒ View raw output as MIME-type `text/plain`
 - ☐ Guess the payload
 - ☐ Prompt to save (you must guess the file type yourself.)
- A "Submit" button.
- Instructions: "To use this form, you must first [encode a file](#)." and "These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide."
- Contact information: "Please send comments or questions to [Alan Eliassen](#)." and a link "[Back to Alan's Home Server](#)".

The Windows taskbar at the bottom shows the date and time as 10:03 AM on 3/15/2023.

After submitting we get the cipher text



Decode it using the atbash cipher tool with hand or online. You get the flag as
`picotf{atbash_crack_03d8feef}`