This problem set concerns linear algebra in a context where the scalars are the nonnegative integers 0, 1, ..., \(m-1\) for some “modulus” \(m\) (and then with all arithmetic done “modulo \(m\)”). The application will be to “crack” a cipher, specifically, a Hill cipher.

See the handout *Hill Ciphers and Modular Linear Algebra* for the mathematics involved and the principles of Hill ciphers.

1. We use a 29-letter alphabet (including period, question mark, and space); its characters are in list `alf` in notebook *About Hill*.

Define a new function named `encipher` that enciphers text using a Hill cipher. This function takes two arguments and is used in the form

```
encipher[plaintxt, A]
```

where `plaintxt` is a character string of elements from `alf`; \(A\) is, for some integer \(n > 1\), an \(n \times n\) matrix with entries in \(\mathbb{Z}_m\), where \(m\) is the length of `alf`; and the result is the ciphertext string that results from applying Hill encipherment to `plaintxt` with key matrix \(A\). For example:

```
encipher["EXAMPLE", {{9,8},{0,2}}]
```

```
RRJYUWKI
```

Define `encipher` so that it expresses in MATHEMATICA what you would do by hand:

- Convert the plaintext characters into corresponding code numbers (their locations in `alf`).
- Form the \(n\)-row matrix with columns formed from code numbers (and remember to pad it with repetitions of the last code number as needed to fill out the final column).
- Apply the key matrix to the columns of code numbers to get the coded version of the ciphertext; you should be able to do this with a single matrix multiplication.
- Convert the coded ciphertext back into actual text.
Define auxiliary functions that do some of these steps, or parts of these steps.

Validate \texttt{encipher} by using package \texttt{Vdencipher} according to the instructions in \texttt{About Hill.nb}.

After validating \texttt{encipher}, you will be ready to solve the following problems about Hill ciphers.

For each problem you will need custom-made data—text (plain and/or cipher) and/or a key matrix. To get this data, see the instructions in notebook \texttt{About Hill.nb}.

You should \textit{define a function for any procedure that you apply several times, and for any procedure that someone working with Hill ciphers would want to have available.}

2. You are given the inverse of the key matrix for a Hill cipher along with some ciphertext. You must decipher this text, that is, find the corresponding plaintext.

3. You are given the key matrix for a Hill cipher and a piece of ciphertext. You must decipher the ciphertext.

4. You have learned the size \textit{n} for a certain Hill cipher. You are given a piece of “captured” plaintext along with the corresponding ciphertext. You will do two things with that:

\begin{enumerate}
\item If possible, find some set of length-\textit{n} polygraphs among the plaintext that are linearly independent, that is, whose corresponding numerical plaintext vectors are linearly independent (modulo the length of \texttt{alf}). Be sure to check for linear independence!
\item If (a) can be done, then use the answer to (a) to determine the inverse key for this cipher.
\end{enumerate}