1. Consider the ADFGX cipher with keyword crypto and matrix

\[
\begin{array}{c|cccc}
A & D & F & G & X \\
\hline
A & a & m & x & r & b \\
D & t & w & q & i & e \\
F & n & f & z & c & l \\
G & g & o & h & v & k \\
X & u & y & d & p & s \\
\end{array}
\]

(a) Encrypt the plaintext ourtargetisalice.
(b) Decrypt the ciphertext XGFXGADDGDAFDAAG.

2. Consider the Hill cipher with encoding matrix \( M = \begin{pmatrix} 10 & 1 & 7 \\ 16 & 2 & 11 \\ 19 & 8 & 14 \end{pmatrix} \).

(a) Encrypt the plaintext cryptography.
(b) Decrypt the ciphertext IULZGMMUY.

3. Consider the four-square cipher whose plaintext squares are in normal alphabetical order, and whose lower-left ciphertext square is generated with the keyword computerizably and whose upper-right ciphertext square is generated with the keyword troublemakings.

(a) Encrypt the plaintext disqualification.
(b) Decrypt the ciphertext NNNPSYKZBUCUHG.

4. (Non-Collaboration Problem) Alice implements a Hill cipher on her computer, but fails to check that the encoding matrix is invertible modulo 26. She sends Bob the plaintext message test using the matrix \( M = \begin{pmatrix} 0 & 3 \\ 2 & 5 \end{pmatrix} \).

(a) Find Alice’s ciphertext.
(b) In addition to the plaintext test, there are three other plaintexts that also encode to the same message. Find them.
(c) If Alice instead sent a 40-character message to Bob, how many possible decodings would Bob have to search through in order to find Alice’s message?
5. In this problem, we will study the “affine Hill cipher”: given an \( n \times n \) matrix \( M \) that is invertible modulo 26 and a row vector \( b \), the plaintext vector \( x \) is encoded as the ciphertext vector \( y = xM + b \).

(a) Encrypt the message \textit{onetwofour} using the matrix \( M = \begin{pmatrix} 11 & 17 \\ 12 & 7 \end{pmatrix} \) and vector \( b = \langle 4, 11 \rangle \).

(b) Describe the decryption procedure for the affine Hill cipher.

(c) Decode the ciphertext \textit{BUERQA} that was encoded using the matrix \( M = \begin{pmatrix} 6 & 19 \\ 21 & 4 \end{pmatrix} \) and vector \( b = \langle 17, 12 \rangle \).

(d) Eve has acquired the encoding machine for a \( 3 \times 3 \) affine Hill cipher and wishes to extract the matrix \( M \) and the vector \( b \). She inputs the message \textit{aaabaaabaaab} and receives as output \textit{DGLFQAQZZHHC}. Determine the matrix \( M \) and the vector \( b \).

6. Alice is using the ADFGX cipher to send messages to Bob. She intends to send a 33-character message, but, by accident, only types the first 12 characters before accidentally hitting “send”. She retypes the message but accidentally presses “send” again after typing the first 19 characters. She then correctly sends the full message. Bob therefore receives the following three ciphertexts (of lengths 24, 38, and 66 characters respectively):

1. AFDGADDFFDDGFGAAFXDXXFD
2. AFDGACXDDDFAAFGDFXDDDCAFXAXXFDXFFGDXD
3. AFDGACXAFXGFDADAFAAXGKDDFXDDAXXFFFDAAFXAXXADXXFDGXDGGFG

(a) Eve is spying on this interaction, and based on the three messages she suspects that Alice may have sent partial versions of the final message followed by the full one. Explain why Eve might draw this conclusion based on the three messages she recorded.

(b) Find the length of Alice’s keyword.

(c) What are the lengths of the columns in each of the 3 messages? Use this information to determine which columns have which lengths in each message.

(d) Eve intercepts a list of possible keywords for this message: \textit{abedc, acbed, abcde, baecd, bcade}, \textit{beadc, cabled, cdeba, daceb, debac, eacdb, ecabd}. Which one is the correct key? [Hint: Use the results of part (c) to eliminate all but one possibility.]