Solution to Hw1.1: The plaintext is ‘itwouldbesotemptingtojustwritecanyouhearmenow’ and the Caesar Key was 10.

Solution to Hw1.2 The plaintext is ‘iamintheresomewherehidinginthatlonglistofgibberish’ and the key was \( a = 5 \) and \( b = 14 \); in other words, 

\[
\text{ciphertext} = 5 \times \text{plaintext} + 14 \mod 26, \quad \text{and} \quad \\
\text{plaintext} = 21 \times \text{ciphertext} + 18 \mod 26.
\]

Solution to Hw1.3 The plaintext is ‘thetipofthemonthistobuylowandsellhighaaa’ and the key was the matrix

\[
\begin{bmatrix}
24 & 1 & 3 & 7 \\
23 & 9 & 5 & 5 \\
10 & 21 & 5 & 0 \\
23 & 0 & 15 & 19
\end{bmatrix}
\]

Solution to Hw1.4 See the accompanying MATLAB file crackvigenere.m.

The first plaintext is the Gettysburg Address by Abraham Lincoln, and it was encrypted with the Vigenere key \([12, 4, 18, 5, 9, 20]\).

The second plaintext is the lyrics to the song Stairway to Heaven, and it was encrypted with the Vigenere key \([2, 5, 3, 19, 7, 21, 6]\) (by the way, no one really knows the exact lyrics since they are not entirely discernable in the song—some might say the singing was a form of encryption—so you discovered something that no one but Led Zeppelin knew).

The third plaintext is the poem Jabberwocky by Lewis Carrol, and it was encrypted with the Vigenere key \([16, 7, 3]\). The fact that you found it means that it meets English letter frequency proportions, although it somehow doesn’t quite seem to be English.

The fourth plaintext is an article by Jim Litke, the beginning segment of the plaintext is ‘byjimlitkeinjuriesareanoccupationalhazardineverybigtimesportbutsomuchsoinskiing’... and it was encrypted with the vigenere key \([13, 9, 7, 21, 22, 15, 6, 7, 2, 11, 18]\).

Solution to Hw2.1

a) Suppose \( c_1 = DES_K(m_1) + L \) and \( c_2 = DES_K(m_2) + L \); adding these yields \( c_1 + c_2 = DES_K(m_1) + DES_K(m_2) \) since \( L + L = 0 \) removes the \( L \) part of the key. Thus Eve can try all \( 2^{64} \) possible values of \( K \) until \( c_1 + c_2 = DES_K(m_1) + DES_K(m_2) \) is satisfied, and then \( L \) is \( c_1 + DES_K(m_1) \). Our success came from first canceling part of the key’s effect and focussing on the other part of the key.

b) Suppose \( c_1 = DES_K(m_1 + L) \) and \( c_2 = DES_K(m_2 + L) \). The critical trick here is to recall that
the decryption of DES is precisely the encryption of DES with reversal of order in round keys. Thus

taking $\text{DES}_K(\cdot)$ of both sides yields $\text{DES}_K(c_1) = m_1 + L$ and $\text{DES}_K(c_2) = m_2 + L$, which means that $m_1 = \text{DES}_K(c_1) + L$ and $m_2 = \text{DES}_K(c_2) + L$, and the exact trick of part a can be employed; adding, we get $m_1 + m_2 = \text{DES}_K(c_1) + \text{DES}_K(c_2)$ which yields $K$ by trying all $2^{64}$ possibilities, and then $L$ is $m_1 + \text{DES}_K(c_1)$.

**Solution to Hw2.2** See the accompanying MATLAB file crackhill.m.

The first plaintext is the Gettysburg Address and it was encrypted with the Hill Key

$$\begin{bmatrix}
10 & 9 & 18 & 4 \\
10 & 11 & 13 & 18 \\
17 & 15 & 20 & 25 \\
21 & 14 & 12 & 20
\end{bmatrix}$$

The second plaintext is the lyrics to Stairway to Heaven and it was encrypted with the Hill Key

$$\begin{bmatrix}
10 & 8 & 21 & 21 \\
12 & 12 & 24 & 15 \\
23 & 15 & 15 & 18 \\
15 & 4 & 0 & 2
\end{bmatrix}$$

The third plaintext is Jabberwocky and it was encrypted with the Hill key

$$\begin{bmatrix}
14 & 9 & 7 & 24 & 12 \\
3 & 21 & 23 & 1 & 7 \\
13 & 1 & 2 & 6 & 17 \\
3 & 15 & 1 & 25 & 24 \\
20 & 24 & 6 & 5 & 19
\end{bmatrix}$$

The fourth plaintext is the article by Jim Litke and it was encrypted with the Hill key

$$\begin{bmatrix}
3 & 13 & 17 & 3 & 18 & 22 & 20 \\
16 & 4 & 8 & 4 & 14 & 19 & 15 \\
24 & 5 & 7 & 23 & 24 & 9 & 4 \\
21 & 5 & 18 & 3 & 8 & 18 & 0 \\
24 & 16 & 24 & 16 & 18 & 4 & 7 \\
8 & 1 & 3 & 6 & 24 & 24 & 25 \\
6 & 5 & 1 & 5 & 15 & 5 & 24
\end{bmatrix}$$

**Solution to Hw2.3** The command plaintext=subscribe('ukpesahcdyrizbljwxfmotvgq',ciphertext) will return the plaintext, which is the first part of the classic book The Hitchhiker's Guide to the
Galaxy by Douglas Adams. (It is the first book of a five book trilogy.)
For the extra credit problem, the command plaintext=substitute('shbpjtaxcuqomgrnwdvzfifkey',ciphertext)
will return the plaintext, which is the United States Constitution. This was a little trickier because
Ye’ Olde English and the legal terminology of the era somewhat complicated frequency analysis.