1. (Modular Arithmetic, 5 pts x 4) Recall the definition of congruence: \( a \equiv r \pmod{m} \) \( \iff \ a = qm + r \), where \( a, q, r \in \mathbb{Z}, m \in \mathbb{Z}^+, \) and \( 0 \leq r < m \).
   (a) Prove that
   \[ (a \cdot b) \mod{m} = ((a \mod{m}) \cdot (b \mod{m})) \mod{m}. \]  
   (1)
   (b) Based on the result in (a), compute \( 4^{102} \mod{101} \).
   (c) Suppose that \( a, m > 0, \) and \( a \not\equiv 0 \pmod{m} \). Prove that
   \[ (-a) \mod{m} = m - (a \mod{m}) \]  
   (2)
   (d) Prove that \( a \mod{m} = b \mod{m} \) if and only if \( a \equiv b \mod{m} \). (Hint: check online how to prove an “if and only if” statement.)

2. (Shift Cipher, 10 pts) Use exhaustive key search to decrypt the following ciphertext, which was encrypted using a Shift Cipher:
   (Hint: a Matlab/Python script can save you plenty of time.)

   BERAKPYDJXUQYHYJIIQRYHTYJIQPBQDUYJIIFUHCQD.

3. (Affine Cipher, 5 pts x 2) Suppose that \( K = (5, 21) \) is a key in an Affine Cipher over \( \mathbb{Z}_{29} \).
   (a) Express the decryption function \( d_K(y) \) in the form \( d_K(y) = a'y + b' \), where \( a', b' \in \mathbb{Z}_{29} \).
   (b) Prove that \( d_K(e_K(x)) = x \) for all \( x \in \mathbb{Z}_{29} \).

4. (Affine Cipher, 5 pts x 3) An involutory key is a key \( K \) such that \( e_K(x) = d_K(x) \) for any message \( x \). See Chapter 1 of Stinson, Problem 6.
   (a) Suppose that \( K = (a, b) \) is a key in an Affine Cipher over \( \mathbb{Z}_n \). Prove that \( K \) is an involutory key if and only if \( a^{-1} \mod{n} = a \) and \( b(a + 1) \equiv 0 \pmod{n} \).
(b) Determine all the involuntary keys in the Affine Cipher over $\mathbb{Z}_{15}$.

(c) Suppose that $n = pq$, where $p$ and $q$ are distinct odd primes. Prove that the number of involuntary keys in the Affine Cipher over $\mathbb{Z}_n$ is $n + p + q + 1$.

5. (Hill Cipher, 5 pts x 2) Determine the inverses of the following matrices over $\mathbb{Z}_{26}$.

(a) \[
\begin{pmatrix}
2 & 5 \\
9 & 5 \\
\end{pmatrix}
\]

(b) \[
\begin{pmatrix}
1 & 11 & 12 \\
4 & 23 & 2 \\
17 & 15 & 9 \\
\end{pmatrix}
\]

6. (Permutation Cipher, 5 pts x 2)

(a) Suppose that $\pi$ is the following permutation of $\{1, ..., 8\}$:

\[
\begin{array}{cccccccc}
x & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
\pi(x) & 4 & 1 & 6 & 2 & 7 & 3 & 8 & 5 \\
\end{array}
\]

Compute the permutation $\pi^{-1}$.

(b) Decrypt the following ciphertext, for a Permutation Cipher with $m = 8$, which was encrypted using the key $\pi$:

```
TGEEMNELNIDROBOAHDOETCSHAEIRLM.
```
You are given the following plaintext/ciphertext relationship table:

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Plaintext</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>b</td>
</tr>
<tr>
<td>F</td>
<td>a</td>
</tr>
<tr>
<td>L</td>
<td>y</td>
</tr>
<tr>
<td>T</td>
<td>u</td>
</tr>
<tr>
<td>O</td>
<td>f</td>
</tr>
<tr>
<td>Q</td>
<td>i</td>
</tr>
<tr>
<td>U</td>
<td>d</td>
</tr>
<tr>
<td>J</td>
<td>o</td>
</tr>
</tbody>
</table>

Using your linguistic skills (which may include the knowledge of frequencies of occurrence of letters) and command of the English language, decode the sentence correctly. (Hint, this is about the recent senate inquiry about the fiscal policies of the US federal reserve.)

Note: please provide brief steps.