Common Datasets for Baby AES Testing:

1. **Random Dataset:**
   - Contains randomly generated plaintext and keys, simulating a diverse range of inputs.
   - Used for general performance evaluation and testing basic encryption/decryption functionality.
2. **Avalanche Key Dataset:**
   - Contains key pairs with a high Hamming distance (many bit differences), ensuring a small change in the key causes a significant change in the ciphertext.
   - Used to assess the avalanche effect, a desirable property in secure ciphers.
3. **Low Density with Key Dataset:**
   - Contains plaintexts with a low density of 1s (more 0s), paired with a variety of keys.
   - Used to evaluate how the cipher handles different data patterns and key combinations.
4. **High Density with Key Dataset:**
   - Contains plaintexts with a high density of 1s (more 1s), paired with a variety of keys.
   - Similar purpose as the low density dataset, but focusing on different data patterns.
5. **Low Density with Plaintext Dataset:**
   - Contains a variety of keys paired with plaintexts that have a low density of 1s.
   - Used to assess how key variations affect encryption with specific data patterns.
6. **High Density with Plaintext Dataset:**
   - Contains a variety of keys paired with plaintexts that have a high density of 1s.
   - Similar purpose as the low density plaintext dataset, but with different data patterns.
7. **CBC (Cipher Block Chaining) Dataset:**
   - Contains plaintext blocks specifically designed to test the security of the CBC mode of operation.
   - CBC involves chaining blocks together, and this dataset helps evaluate its resistance to specific attacks.

Purposes of Using These Datasets:

- **Analyzing Diffusion and Confusion:**
  - Datasets with different densities help assess how effectively baby AES mixes up data and obscures patterns, key properties of a secure cipher.
- **Evaluating Key Sensitivity:**
  - Avalanche key datasets measure how sensitive the cipher is to small changes in the key, ensuring resilience against brute-force attacks.
- **Testing Resistance to Attacks:**
  - Datasets like those for CBC mode help evaluate the cipher's ability to withstand specific attack techniques that target its mode of operation.
- **Identifying Weaknesses:**
  - By analyzing results with different datasets, researchers can pinpoint potential vulnerabilities in baby AES and suggest improvements.

Random Bit Test on Each Dataset:

1. **Random Dataset:**
   - **Test Description:** Randomly select a bit position in each ciphertext and check its value.
   - **Output:** If the selected bit is equally likely to be 0 or 1 across all ciphertexts, the test passes.
2. **Avalanche Key Dataset:**
   - **Test Description:** For each key pair, modify one bit in the plaintext and observe the change in the corresponding bit in the ciphertext.
   - **Output:** If modifying one bit in the key causes a significant change in the corresponding bit of the ciphertext, the test passes.
3. **Low Density with Key Dataset:**
   - **Test Description:** Randomly select a bit position in each ciphertext and check its value.
   - **Output:** If the selected bit is equally likely to be 0 or 1 across all ciphertexts, the test passes.
4. **High Density with Key Dataset:**

- **Test Description:** Randomly select a bit position in each ciphertext and check its value.
- **Output:** If the selected bit is equally likely to be 0 or 1 across all ciphertexts, the test passes.

5. **Low Density with Plaintext Dataset:**
   - **Test Description:** Randomly select a bit position in each ciphertext and check its value.
   - **Output:** If the selected bit is equally likely to be 0 or 1 across all ciphertexts, the test passes.
6. **High Density with Plaintext Dataset:**
   - **Test Description:** Randomly select a bit position in each ciphertext and check its value.
   - **Output:** If the selected bit is equally likely to be 0 or 1 across all ciphertexts, the test passes.
7. **CBC (Cipher Block Chaining) Dataset:**
   - **Test Description:** Randomly select a bit position in each ciphertext and check its value.
   - **Output:** If the selected bit is equally likely to be 0 or 1 across all ciphertexts, the test passes.

Tests for Baby AES:

1. **Avalanche Test:**
   - **Test Description:** Measure the sensitivity of Baby AES to changes in the input plaintext by modifying one bit at a time and observing the impact on the ciphertext.
   - **Output:** If a small change in the input results in a significant change in the output, the test passes.
2. **Strict Avalanche Test:**
   - **Test Description:** Similar to the Avalanche Test, but also includes checking the impact of changes in the key.
   - **Output:** If modifying one bit in the input plaintext or key causes a significant change in the output, the test passes.
3. **Completeness Test:**
   - **Test Description:** Evaluate the behavior of Baby AES by changing one bit at a time in the input and observing the impact on the output.
   - **Output:** If changing any bit in the input results in a detectable change in the output, the test passes.