Question: 4

- In AES scheme it is important to manage and share the key in a very secure manner. If the key is compromised it is very easy to decrypt the message.
- In this pocket version of AES, the key is only 16 bit long so a brute force attack is very likely to be successful.
- Unlike asymmetric algorithms, AES does not offer authentication and data integrity.