Homework 2

Encryption

Botond Lajos Perényi

Task 1: Confusion and diffusion

Part i: Encrypt THEWANDCHOOSESTHEWIZARD using Vigenère cipher with MAGIC as key: FHKECZDIPQASKAVTECQBMRJ. I used my code from the previous assignment to achieve this. (In my code I used lowercase, meaning I had to convert the message and key in my code.)

Part ii: Change one letter in the plaintext: Encrypt THEWANDCHOOSESTHELIZARD using Vigenère cipher with MAGIC as key: FHKECZDIPQASKAVTERQBMRJ. I changed one letter compared to the original message, and only one letter changed in the resulting ciphertext.

The diffusion property is when changing one bit (in this case letter) in the plaintext changes around half of the resulting ciphertext. This does not happen with Vigenère cipher, as changing one letter in the plaintext changes only one letter in the ciphertext. This means that the diffusion property is not achieved in the Vigenère cipher. (The diffusion property should not depend on which letter is changed in the plaintext.)

Part iii: Change one letter in the key: Encrypt THEWANDCHOOSESTHEWIZARD using Vigenère cipher with MANIC as key: FHRECZDPPQASRAVTEJQBMRQ. I changed one letter in the key compared to the original key, and five letters changed in the resulting ciphertext (compared with the original ciphertext).

The confusion property is when changing one bit (a letter in this case) in the key changes around half of the resulting ciphertext for a given plaintext. With this message (which is 23 letters long) the expected change should be around 11, but this does not happen with changing one letter in the key. Thus the confusion property is not properly achieved in the Vigenère cipher.

Task 2: Pseudorandom function

Task 3:

Task 4:

Task 5: