Introduction to Security (WS2017/18) Prof. Matteo Maffei

Project 3 – Cryptography

TU Wien

Submission by **Markus Peitl (01526724)**

During the development of the project solutions, I have discussed problems, solutions, and other questions with the following other students:

-

Cryptography

It was asked to develop a method to extract the key of an encrypted text, only by using the ciphertext, which could be extracted with an eavesdropping attack.
Used was an encryptio scheme where the letters of a plaintext were replaced by the letters of an encryption key in the first step, while on the next letter of the
plaintext the alphabet or key (depending on encryption decryption) was rotated and replaced by the rotated key.

Through this the effective key used to encrypt the plaintext changes with every letter, which prevents us from performing a frequency analysis on the whole text.
However the alphabet and the encryption key used both have a fixxed size of 44 characters and by performing a cyclic and linear rotation of the key, we can easily see
that the encryption key reaches the same position every 44 characters, which would be the same as using the same key multiple times, while giving us the ciphertext
ultimately making the text vulnerable to a frequency analysis.

For this we first divide the text into 44 bins, where we put the strings that use the same encryption key, then we can just perform frequency analysis for the letter E on this
text, by counting how often every character occurs in one of those bins and sorting the distribution. This will likely result in one letter occurring the most in this
distribution, if the text is long enough to perform frequency analysis on 1/44th of the text and uses english language , which would then be the encrypted letter for ‘E‘ .

So now we can just repeat that for every one of the 44 ciphertext bins, which will give us the other parts of the key, because this key is only shifted by one position every step,
giving us access to the other characters of the encryption scheme.

Lastly when we have extracted every 44 characters of the encryption key, we need to shift the key by 4 steps as we want the key to align with A in its first initial position, as
E is located as the 5th character of the alphabeth.

EFGH.....
>>>>
ABCDEFG

Which finally gives us the encryption key of cipher, we need, to decrypt the secret text.

The instructions to testing the implementation are located in ReadMe.txt, which containes the command to the shell script that will decrypt the secret by
executing the java code that does the frequency analysis and decryption-encryption, which source is located in
/security_cipher_breaker/src/sample
in the classes Main.java and CipherManager.java.