Software Security
Assignment 1: Vigenère Cryptanalysis
Autors: Vikhman Roman 348111014, Evgeniy Lyalin 347384281

Question 1. Assume that encryption Triple-Vigenère is defined, that is $Ek1\ (Ek2\ (Ek3(x)))$, where $k1$, $k2$, $k3$ are the keys of the length m letters., x is the plaintext and Eki is the encryption wit the key ki. Is this encryption more secure than the original Vigenère? Explain

Answer:
Yes, Triple-Vigenère encryption is generally more secure than the original single Vigenère cipher, if the keys k1,k2,k3 are independent and random and of the same length m. This increases security compared to the original Vigenère cipher because it adds multiple layers of substitution, making it harder for attackers to perform frequency analysis or other cryptanalysis techniques that rely on single-key patterns. However, if the keys k1,k2,k3 are related or derived from the same source, the security gain may be limited.

Question 2. Will the answer to the previous question be changed if the keys $k1$, $k2$, $k3$ will be of different lengths? Explain

Answer:
Yes, using different key lengths improves security and makes the cipher significantly harder to break.

When the keys k1,k2,k3 have different lengths (e.g., m1,m2,m3), the periodicity of the final encryption becomes the least common multiple (LCM) of the three lengths. This longer effective period:

- Makes frequency analysis more difficult
- Reduces the effectiveness of attacks based on repeating patterns (like the Kasiski or Friedman test)
- Increases the apparent randomness of the ciphertext

The best result occurs when the key lengths are relatively prime, such as 7, 9, and 10(for example), as this maximizes their LCM.

So, Triple-Vigenère with keys of different lengths is more secure than with equal-length keys.