Yücel Özdemir - 220201009

Number of pages	Memory usage (kB)	Execution time (ns)
1000	13482	190443900
100	2909	10330800
10	1701	1628600
1	1476	895100

```
Text 1000 execution time: 190443900 nanoseconds
Memory usage: 13482 kB

Text 100 execution time: 10330800 nanoseconds
Memory usage: 2909 kB

Text 10 execution time: 1628600 nanoseconds
Memory usage: 1701 kB

Text 1 execution time: 895100 nanoseconds
Memory usage: 1476 kB
```

- **Frequency analysis:** Because I'm just using a secret key, this encryption system is not very secure. If a text is very long like 1000 pages, this way is not secure, because secret key on a long text can be broken easily using frequency analysis, so we must use short texts which is encrypted with different secret keys as possible.
- **Short key size:** 56-bit key is too short for security.
- **Brute-force attack:** It is vulnerable to brute-force search of the whole key space, either by large collections of general-purpose machines or even more quickly by specialized hardware. Combining this weakness with the key complement weakness, DES can be broken using 2^{55} encryptions.
- We can increase security using 3DES with 2 or 3 different secret keys instead of DES. No practical attacks are known.

Statistical attacks which are faster than brute-force attack:

- **Differential cryptanalysis:** Differential cryptanalysis is like linear cryptanalysis; differential cryptanalysis aims to map bitwise differences in inputs to differences in the output in order to reverse engineer the

action of the encryption algorithm. It is again aiming to approximate the encryption algorithm looking to find a maximum likelihood estimator of the true encryption action by altering plaintexts or (looking at different plaintexts) and analyzing the impact of changes to the plaintext to the resulting ciphertext. Differential cryptanalysis is therefore a chosen plaintext attack. Differential cryptanalysis has been revealed that the designers of DES already knew about this type of attack and designed S-boxes and chose 16 as the number of rounds to make DES specifically resistant to this type of attack. It has been shown that DES can be broken using differential cryptanalysis if we have 2^{47} chosen plaintexts or 2^{55} known plaintexts. Although this looks more efficient than a brute-force attack, finding 2^{47} chosen plaintexts or 2^{55} know plaintexts is impractical. Therefore, we can say that DES is resistant to differential cryptanalysis.

- **Linear cryptanalysis:** DES is more vulnerable to linear cryptanalysis than to differential cryptanalysis, probably because this type of attack was not known to the designers of DES. S-boxes are not resistant to linear cryptanalysis. It has been shown that DES can be broken using 2^{43} pairs of known plaintexts. However, from the practical point of view, finding so many pairs are very unlikely.

- **Related key attacks:** Related-key attack is any form of cryptanalysis where the attacker can observe the operation of a cipher under several different keys whose values are initially unknown, but where some mathematical relationship connecting the keys is known to the attacker. For example, the attacker might know that the last 80 bits of the keys are always the same, even though they don't know, at first, what the bits are. This appears, at first glance, to be an unrealistic model; it would certainly be unlikely that an attacker could persuade a human cryptographer to encrypt plaintexts under numerous secret keys related in some way.