1. **Introduction:**

Topic of data security is known for a centuries. There are many reasons to hide true meaning of the text against inappropriate receivers. The first documented appearance of secured information comes from ancient Rome. It is easy to predict that the reason was to send secret military orders and to make them readable only for proper allied commanders. Disclosure of this kind of information was very dangerous. Here we came to the roots of cryptography. We do not know who exactly came with the idea of manipulating the characters of the message using the secret algorithm. This algorithm known only for sender and the receiver we name “a key”. Thanks to that key sender is able to encrypt plain text and get a cryptogram. Key gives also the opportunity to retrieve true meaning of the cryptogram. The algorithm used in that process is a cipher. At the very beginning no one expected that message which at the first sight consists of totally random characters can hide the secret but within a years people learnt how to break the cryptogram without the key. And here we have to introduce cryptoanalysis – the branch of science which is about analyzing cryptograms and finding its corresponding plain text. One is the opposite of the other, and both of them are affect each other. Cracking the cipher force the people to invent more complex encrypting algorithms to provide higher level of security.

Demand for better and more ciphers is still present. Within a years knowledge and technology progressed enormously. Nowadays we do not use piece of paper and a pen to solve problems connected with cracking the data. Computers enabled us to make huge amount of computations in a short period of time. We can say that computers started totally new age for cryptology. Having in mind the speed of computations we have to ask the question which known ciphers may be considered as these which may provide sufficient level of security for our message? What are the constraints of these ciphers? Which factors may positively affect the encrypting algorithm and which may make our cipher useless. This will be the main goal of this thesis – analyse existing encrypting methods and judge if messages encrypted with them may be easily broken or not. Unfortunately topic of data protection and cryptology itself is not well known among the people that is why I had to use specific approach.

The final solution will be the web application supporting the encrypting algorithms. I suppose that the user may not be familiar with the cryptology or have sufficient knowledge of mathematics or computer science that is why I had to provide theoretical background. The application is divided into two main parts: theoretical and practical. The theoretical part of the application explains the basis related to the subject of cryptology and gives the introductions to each cipher used by me.