The topic of this thesis is a triangulation algorithm and its use in cryptanalysis.
First of all we will define a non-linear equation system on which we can apply triangulation algorithm and we will explain what its output is. Then we will demonstrate its application in cryptanalysis, more specificaly during the attack on the Rinjdael cifer. We will illustrate this attack by a search of collision for our hash function, created for this purpose in Davies-Mayer mode using Rijndael cipher
This thesis also contains a practical part in which we will demonstrate the search of collision for our hash function mention before.