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. There are few available webservices designed for learning and presenting the process of encryption of few cryptography methods. Few of them are prepared for learning basics of cryptography and others are used for academical purposes. There are lots of problems connected with them, the most common is they are dedicated for specific group of users either users how have no previous contact with cryptography or for users who have at least intermediate experience with this topic. There are also few websites which enables user to encrypt and decrypt information but gives no theoretical background. The great example is French site [*http://www.dcode.fr/*](http://www.dcode.fr/)which implement a huge variety of ciphers, however there are no explanations how the encrypting algorithm works. Another example is [*http://rumkin.com/*](http://rumkin.com/) implements less ciphers than previous website but also gives only laconic description of the cipher. There are also some web applications which are concentrating only on one particular cipher like [*http://www.xarg.org/tools/caesar-cipher/*](http://www.xarg.org/tools/caesar-cipher/)(there is only one cryptography method among many other small programs like calculators).

The most advanced web application of that kind is CrypTool. CrypTool is not only a web application, there are also version of the application designed for a Windows, Linux and MacOs operating systems. It is a great application which provides both theory and practical implementations of huge variety of ciphers. It also gives information about digital and electronic signatures, key exchange protocols, random key generators many more. It covers almost all topics connected with the cryptology. The author of CrypTool is Bernhard Esslinger. There were many university workers involved in the project from universities of Darmstadt, Duisburg-Essen, Kassel and Siegen. The first version was released in ninety ninety-eight, two years ago the newest application CrypTool 2 was released. It provides modern graphical user interface. It realises all ciphers with block graphical workflows. It is very nice feature because user can see every step of encryption or decryption process. However this approach makes encryption pipeline more difficult than filling in required coefficient in a cipher’s form in the previous version of CrypTool. Both version have their advantages and drawbacks but none of them provides theory part. Cipher descriptions are available on web version of CrypTool – CrypTool Online. It is suited for any kind of users, no one should have any problems with using it. It has almost every feature which such a service should be equipped with. Thanks to accessible characterizations and clear, and professional approach to the practical presentation of ciphers online version outwent other versions. My diploma thesis application was inspired by CrypTool software.

The final solution is 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. These sites provides all required information to understand and enable user to try how the cipher works. All the information are presented in such a way that everyone will understand operation of the cryptography system: people acquainted with the topic as well as these who read about ciphers for the first time. The second part of the application is focused on the application of the cryptography systems. Within these sites user is able to use the ciphers. Each cipher is editable, there is possibility to change important coefficients and options. Application has got functionalities of encryption and decryption of arbitrary text. One of the most important aspects concerning the practical part is the section describing safety of the cryptosystem. Application not only gives the general information about the safety of the cryptography system but also reacts to the provided input. The output about the safety depends closely on the all the provided data. This functionality gives the real filling about the cipher, user can try lot of examples, modifications of the cipher and compare achieved outputs. This is the feature which set my software apart from other available programs. I have visited many web sites and tested few desktop applications and none of the had the connection between encryption and immediate feedback about the security level of the cryptogram.

**2.Technologies**

**2.1 HTML5** – Hypertext Markup Language is the newest version of the programming language used for creation internet sites. Initial release of that standard was published on twenty-eighth of October two thousand fourteen. It takes it roots from the previous version HTML4 and its XML version XHTML1. HTML5 like the previous versions uses the special mark-ups to make the content of the document structured and make it visually distinguishable. Thare are three main categories of markup language: presentational, procedural and descriptive markup language. The first type is responsible to preprocess document in such a way that both printed document and electronic version on the computer screen will look exactly the same. Procedural markup supplies the document with the tags which give the instructions to the processor how to edit the text. HTML belongs to the descriptive family of the markup languages. The aim if the descriptive markup is to label and divide the document. Semantics allows the special presentation of the created document. It does not provide any specific instruction about the processing of the file. However it states the role of the text. All the information about edition and formatting is usually stated in the separate place by a Cascade Style Sheets. The modification stated by the tag affects part of the text placed between opening and ending tags.

HTML5 makes the websites less static, it influences the level of interactivity of the site. It provides new semantic elements like: <section>, <article>, <header> and <footer>, graphic elements like <canvas> and multimedia elements <audio> and <video>. New features of the HTML for storing data in the browser are “localstorage” and more powerful “indexedDB”. One of the most important aspects of the new standard is the improved error handling. Browsers supporting current version of HTML are checking the correctness of the syntax. HTML5 is also compatible with older versions of the webbrowsers which just ignore new unknown tags.

I have used this technology to design and create all websites of my application. It is very easy to use and provided few very useful properties. HTML5 helped me to preserve the structure of the document. Using the tags makes the administration of whole project very easy and fast. Changes for particular part of the project such as for example sections or headers may be applied in few seconds. Using the same frame in the all documents of the project makes them consistent and gives the impression of professionalism.

**2.2 Cascading Style Sheets (CSS3)** – Is the latest version of the language used for describing and providing user defined presentation of the websites. CSS was inspired by the Document Style Semantics and Specification Language (DSSSL) which was the first language created for the purpose of defining style and look of the documents. The inventor of the Cascading Style sheets is the Norwegian computer scientist Hakon Wium Lie. He described his idea in the book “Cascading Style Sheets: Designing for the Web”. It was published in 1994. Cascading style sheets works perfectly along the HTML mark-ups. CSS3 is perfectly compatible with its previous versions. We can split whole language into many modules where old version of CSS is also treated as a module. The most important among all are: Text Effects, Animations, Selectors, Background, Borders. CSS file consists of the list of rules and directives bound with specified part of the documents. The greatest module which enable proper choose of the elements to edit is Selectors. It has been developed in the CSS3 by adding more constituents which allow to make more precise selection. Next new module introduced by the latest standard I want to concentrate on are “Media Queries”. Media Queries enables user to control the behaviour of the website on different resolutions of the screen. We can choose range of screen sizes and state adequate scaling of websites elements. Thanks to that preparing there is no need to separate versions for mobile devices, appearance of the website is adjusted within the media queries.

To easily administrate and manage the whole project CSS and HTML files should be separated. However there is also possibility to inject CSS code into HTML file, however if there is also reference to the CSS file user has to remember about the priorities of processing the directives. In that kind of situation there may occur overlay of rules, that is why it is vital to place the CSS directives in the separated file.

**2.3 JavaScript (JS)** – It is the most popular scripting language aimed at web development. JavaScript language was created by the Netscape company in the May of ninety ninety-five. As a main author and originator of the language should be considered American programmer and hacker Java script is based on the ECMAScript which was created by Sum Microsystems. JavaScript is considered as a high-level, dynamic, untyped and interpreted programming language. Three technologies: HTML, CSS and JavaScript are present in the majority of World Wide Web projects. Within a years many different implementations of the JavaScript were created. There were no official standardization. What is more different browsers had their own interpretation of Document Object Model (DOM), that is why it was not possible to create website which will look and behave identically on all the most popular webbrowsers. Luckily W3C organization crated standardized model DOM and a in two thousand and nine finally the common version of JS was published.

Language cannot be treated as a classical object-oriented programming language. Instead of classes JavaScript uses prototypes. The instance of the prototype is an associative array. The other property of the JS is the way of typing. In JavaScript we are not stating the type of the variable explicitly. The type is set with the assignation of the value to the variable, however it may be retyped at any time appropriately to the needs. JavaScript relies on a run-time environment to provide interaction between the script and a website DOM. This feature is essential to enable importing the scripts to the HTML documents. Whole operation of the JS is based on the call stack. JS is able to process one message form a queue at the time. Each time the message is processed the adequate function is called. It is placed with proper arguments on the stack and waits till the moment all the previously called functions end their operation. The function stack resizes during the run within the website.

The purpose of using JavaScript is to add dynamic to HTML sites. The code may manipulate all elements of Document Object Model. The most popular application of the code are: manipulation of the browser bookmarks, adding animations, creation of dialogs and control predefined style sheets and form validation. The last thing can be easily achieved by regular expressions which are supported by JavaScript. Programming code can be included in the HTML document in two different ways. It may be placed between two special tags ‘<script>’ which are created to introduce code in any scripting language. But the more elegant way is to again separate code and place them in a file with ‘js’ extension. Inside the HTML document should be attached only function calls.

In the practical solution of my diploma thesis I used JavaScript mainly for cryptography methods implementations. I have also added some functions to manage cascade style sheets and for same simply animations.

**2.4 JQuery –** next technology appearing in my thesis which is library designed for JavaScript. It is the most popular JS library. JQuery first release took place in August two thousand six. JQuery is still under process of development, last stable release was in September of a current year. It is an open-source, free software. There are many applications of that library but one of the most important is the improved way of selecting elements of the Document Object Model for which JQuery prepared totally new syntax. Second very important functionality of JQuery is the ability of animation creation. Library is also equipped with simple API for realisation AJAX requests. It realises them with two built-in functions ‘jQuery.get’ and ‘jQuery .post’. Like in the case of JavaScript itself JQuery is compatible with all popular webbrowsers however the effects may slightly differ on each of them.

There are two ways of using JQuery. First of them is using ‘$’ function which is very useful design pattern – factory method which enables to use chainability of the code. All function with ‘$’ return objects of type JQuery. Second method is using ‘$.’ utility function which do not operate upon JQuery object straight away.

Very useful feature of library which I mentioned above is the chaining of the code. Because of the fact that the result of the result of JQuery function is object of a type JQuery we can easily bind many functions together. Thanks to that we are able to shorten our code by lots of lines preserving at the same time clarity of the code. Functions which occupy several lines of code in JQuery often may be rewrited into two or three lines. This functionality is usually used for manipulation of CSS. It is achieved by passing selector to the function on call the proper methods on it.

I have used this library few times to add some simply animations. It influenced the appearance of the web application and made it more pleasing to the eye and user friendly.

**2.5 Cryptico.js** – open-source JavaScript library dedicated for RSA encryption. It implements one of the most popular and very safe cryptography algorithm. Cryptico.js enables user not only encrypt or decrypt message with the RSA but also to sign whole message. Library uses few important secondary libraries. The most important are “jsbn.js” and “aes.js”. First one implements necessary type for the implementation of RSA cryptography method which is big integer and mathematical operations with these numbers. It is required to use very high primary numbers to make the cipher hard to break and it was the only possibility to use that implementation of big integers. As the RSA is asymmetric cipher it needs pair of asymmetric keys. Cryptico.js uses Tom Wu’s RSA encryption library which implements random key generation, keys are also encrypted with the AES cryptography method. RSA cipher provided by the Cryptico.js enables user to choose between five different available lengths of the key. They are 512, 1024, 2048, 4096 and the longest possible 8192 bit key length. All of them provides very high security level, all encrypted messages cannot be cracked on theory by a personal computer.

Implementation of the RSA cipher is not an easy task that is why I have used this library to implement this cryptography method for users. I used its interface in two different places, site about the cipher itself and in the second place about digital signature. In that place I have mixed both processes of encryption and signing the message to show the more complex way of creation secured message.

**3.Software**

**3.1 Git –** one of the most popular software for version control. Git is a distributed revision control system with own Source Control Management (SCM) and is aimed for speed, data integrity and non-linear workflows. The author of the Git is Linus Torvalds a Finnish software engineer, who is also known as a one of the major developer of Linux kernel. Another important person attributable with a git software is Junio Hamano, the programmer responsible for maintenance of the software. The first release of this free software was in April of two thousand and five. As a distributed control system each created Git directory is an outright repository. There are no main repository like in client server type of version control systems. Every repository has got full revision history and tracking abilities. We can distinguish three main stages of the Git. First one is a Working Directory where user is working on his/her version of code. Before publishing the revision it is unique code which is only available on users computer. The second stage is named Staging Area which is a pre-commit stage. All the changes which are made since the last fetch of a code may be administrated and manipulated at this stage. User may choose which changes should be pushed and which should be discarded for some reason. The last stage is a Git Commit, part responsible for publishing the code and resolving all emerged conflicts.

What is huge advantage of Git there is no need to access network or a central server to be able to work on repository. It is one of the essential kind of software in every information technology projects. Git is very fast in comparison to competitive softwares and very scalable. It finds great application in any kind of project, for projects administrated by only few people as well as for huge commercial projects which involves tens or hundreds of Information Technology specialists. Git’s strong point is the process of branch creation and merging which is also visualised in special tool. It has got also great approach to the branches – they are only references to a commit, the logical structures which makes branch very light. There are many ways to publish the repository, it may be accomplished by Hypertext Transfer Protocol (HTTP) , Secure Shell (SSH), File Transfer Protocol (FTP). Each revision is not the whole copy of the code because after some time of development whole project becomes huge and storing code at each revision memory cost would be enormously high. That is why revision remembers only the change in regard to last version.

I was using Git via the most popular Git repository hosting service GitHub. It enables user to oneself some of the features on the web. As the diploma thesis was my the biggest project which I was the only author I wanted to have whole revision history. Using a Git repository was a kind of self protection against loosing or breaking the software. GitHub played also another very important role during the process of creation the thesis. GitHub provides not only the whole history of revisions but also shares the graph presenting the amount of changes within the time. This chart was a great motivator to further work and to make the graph only ascending. It is incredible how huge impart to my project made so trivial thing like this progress graph.