Lodz University of Technology

Faculty of Electrical, Electronic, Computer and Control Engineering

Institute of Applied Computer Science

Engineer’s thesis

**The web application supporting encryption algorithms   
–**

**Does cryptography provide security?**

Paweł Grzegorzewski

Album number: 190116

Thesis written

under supervision of

**Justyna Żuk, PhD**

Łódź, January, 2017

# Contents

[Contents 2](#_Toc470627723)

[1. Introduction 3](#_Toc470627724)

[2. Involved technologies 5](#_Toc470627725)

[2.1 HTML5 5](#_Toc470627726)

[2.2 Cascading Style Sheets (CSS3) 6](#_Toc470627727)

[2.3 JavaScript (JS) 7](#_Toc470627728)

[2.4. JQuery 8](#_Toc470627729)

[2.5 Cryptico.js 9](#_Toc470627730)

[3. Software 9](#_Toc470627731)

[3.1 Git 10](#_Toc470627732)

[3.2 Adobe Photoshop CS6 (PS CS6) 11](#_Toc470627733)

[3.3 Notepad ++ 12](#_Toc470627734)

[3.4 Eclipse 12](#_Toc470627735)

[4. Information included in the thesis 13](#_Toc470627736)

[4.1 General cryptography issues 13](#_Toc470627737)

[4.1.1 Cryptology 13](#_Toc470627738)

[4.1.1 Cryptography 15](#_Toc470627739)

[4.1.2 Cryptanalysis 16](#_Toc470627740)

[4.2 Cryptography methods 16](#_Toc470627741)

[4.2.2 Vigenere Cipher 18](#_Toc470627742)

[4.2.3 Merkle-Hellman Cipher 18](#_Toc470627743)

[4.2.4 RSA Cipher 18](#_Toc470627744)

[4.3 Digital Signature 18](#_Toc470627745)

[5. JavaScript Cryptography Library 18](#_Toc470627746)

[**b.** **xxx** 18](#_Toc470627747)

[**c.** **xxx** 19](#_Toc470627748)

[5. The web application supporting encryption algorithms 20](#_Toc470627749)

[**a.** **Graphical user interface** 20](#_Toc470627750)

[**b.** **xxxx** 20](#_Toc470627751)

[6. Summary 21](#_Toc470627752)

[7. Appendix 22](#_Toc470627753)

[Bibliography 23](#_Toc470627754)

# 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 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. Because of that fact the special approach have been taken. There are few available webservices and applications 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 that they are dedicated for specific group of users either users who 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/ which implement a huge variety of ciphers, however there are no explanations how the encrypting algorithm works. Another example is http://rumkin.com/ implements less ciphers than previous website but also gives only laconic description of each presented cipher. There are also some web applications which are concentrating only on one particular cipher like 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 graphical block 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. This diploma thesis application was inspired by CrypTool software.

The final solution is the web application supporting the encrypting algorithms. One of the most important assumptions connected with the solution is that ordinary user may not be familiar with the cryptology or have sufficient knowledge of mathematics or computer science that is why the theoretical background was provided. 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 in the application. These sites provides all required information to understand and enable user to try how the cipher works. All the information is 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 a possibility to change important coefficients and options. The 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 the software apart from other available programs. After research of many web sites and tested few desktop applications and none of them had the connection between encryption and immediate feedback about the security level of the cryptogram.

# Involved technologies

To create an application which fulfils all stated requirements there should be involved few different technologies. To obtain proper appearance of the application, support of the inputs and operation on the provided data there was combined five different programming languages.

### 2.1 HTML5

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. There 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.

That technology was used to design and create all websites of my application. It is very easy to use and provides few very applicative properties. HTML5 was helpful with preserving whole structure of the document. Using the tags makes the administration of the 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 Javascript was used mainly for cryptography methods implementations. I have also added some functions to manage cascade style sheets for same simply animations and handling all inputs. As a main scripting technology Javascript was used for a practical workflow for all used cryptography methods.

### 2.4. JQuery

JQuery is next technology appearing in the 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.

JQuery library was used 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

Cryptico is an 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 the library was used 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.

# Software

Well suited software is very important during process of development. Software as a tool should help user with creation the code, management and edition of all project files. The more advanced the software is the more optimal the is the work. Programming process becomes much faster, and effective, there is a lover possibility to make errors, finding sources of problems and resolving them is also easier. All these aspects have to be taken in mind at the first phase of planning. During the project a lot of time had to be spent on preparation of images and animations. That is why very another type of software-graphical program, alongside these strictly connected with programming had to be used. After a consideration the following softwares were involved.

3.1 Git

Git is the 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. This difference is called by Git the delta.

Git was used 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 is quite big project it is very reasonable to save 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.

3.2 Adobe Photoshop CS6 (PS CS6)

Adobe Photoshop CS6 is the latest version of the most famous software for raster graphics edition. Raster graphics is the way of presenting picture by the grid of pixels. Unlike vector graphics the quality of the raster graphics picture depends on the resolution of the picture. Adobe Photoshop can be concerned as a flagship software of the Adobe Systems company. Adobe Photoshop was created by brothers Thomas and Jon Knoll in nineteen ninety, but first commercial edition was published in two thousand and three. Since four years there is the newest sixth version of the Adobe Photoshop. The source code of an application is written in C++, however first releases were written in Pascal. Files created in Photoshop have .psd extension. These files are the project files which are divided by layer and each created element is fully editable. Files have also the latest history of changes. CS which is part of name of the software comes from “Creative Suite” special extension which as merged with the major program. Creative suite added the possibility to create own shortcuts, tool for searching, filter gallery, colour matching and many other very useful tools. Photoshop is not only the most popular but also the most advanced software of that kind. It supports huge range of graphical files, also animation files like for example .gif. Unfortunately its biggest competitor GIMP has got substantially less functionalities and is less user friendly than PS CS6. There are lot of great functionalities which makes this software amazing for amateur users as well as professional graphics designers. The most important tool which I also used for preparing graphics for my thesis is “planar selection”, tool which enables user to select and then cut the part of the image.

All the pictures used in the practical part of my diploma thesis were edited in the Adobe Photoshop CS6. Some clip arts or ready elements from the internet were also used but all of them were edited and changed in the program. There are no pictures (despite pictures presenting authors of cryptography methods) which were just downloaded and put without any change within a thesis. There are also two short animations which show the operation of Vigenere and Caesar ciphers. This kind of presenting an example is more appealing to the users of the application. It helps to imagine whole process of encryption.

3.3 Notepad ++

Notepad++ is an advanced text editor based on the Scintilla project. Software is created in C++ language with the Win32 API by programmer whose pseudonym is “Don Ho”. Notepad is more advanced substitute of basic Windows tool – Notepad. It was released on two thousands and three and is still under a development. Notepad++ supports a lot of filetypes. The next great advantage is recognition and marking the syntax of the code with different colours. That makes the file presentation very clear for users. Notepad++ offers also auto completion of the code. Each edited file within the program stays in its memory till the close it in the interface of Notepad++.

I have used this program for small changes of the project. It was only used as substitute of the main software for development of my webapplication which was Jave Eclipse Mars, definitely more advanced and better suited program for creation of the application.

# 3.4 Eclipse

Eclipse is one of the most popular integrated development environment. It is the most often used software by Java developers. It is free, open-source software/ Eclipse is also written in Java programming language, the first version comes IBM rational code. It was created by Eclipse Foundation in two thousands one. Under the name of Eclipse foundation there were initially grouped many different well known brands like Borlands, IBM, Red hat, Rational Software and many more. The last stable release was rightly month ago so the software is being still at the process of development and improvement. Eclipse like other advanced programming environments enables user to create applications in many different languages. Each programming language may be added to the Eclipse by special plugin. Not only programming languages can be added, there are lot of functionalities available in form of plugins. The most important are tools for graphical user interface or IML graphs creation. Eclipse may be also extended with plugins responsible for connection with servers or databases.

Eclipse has to be considered as a main developing software which was involved in the thesis. Despite small added or edited in the previously mentioned Notepad++ all the application code was written in Eclipse. This IDE is very user friendly and helpful in the development process. Numerous helpful features provided by the software like code colouring, code suggestion, tree presentation of project files, easy and fast code refraction makes writing of the code very rapid, simple and convenient.

# Information included in the thesis

The most important assumption which must be highlighted connected with the software is to provide information understandable for any kind if user. With that in mind there was provided few sites devoted with general questions connected with the cryptology. Among them there are sites which explains what the cryptology is about, what are the differences between cryptography and cryptoanalysis and many others. It is vital to read these theoretical part before moving to the cryptography methods and encrypting to have complete view about the topic of cryptology.

The main part of the application are sites dedicated to cryptography methods. It was not easy task to choose proper ciphers for the application. There were many aspects under consideration before including cipher in the application like: level of complexity, type of cryptosystem, key type, safety of cryptosystem and so on. User should learn, investigate and try ciphers which belong to different available types.

### 4.1 General cryptography issues

Cryptology itself is very broad topic. It is very important to understand some of basic information before going deeply into matter of cryptosystems and safety provided by them. Webapplication proposed as a solution of this thesis provides some sites which purpose is to explain in a very clear understandable way basic topics connected with the cryptology.

### 4.1.1 Cryptology

To understand all information presented in the thesis user should at the begging realise what the cryptology is about. Cryptology is a branch of science very closely connected with mathematics. Cryptology is generally related with the data the process of data manipulation which main purpose is to hide its true content from unwanted users. This data manipulation is a cipher – way of changing a plain text into another text, which should look like nonsense for people we want to hide information from. We can consider a cipher as an algorithm, set of steps which must be performed in order to change a text into a secret and secured information. The most important part of the cipher is a key. The key is usually a string of letters which enables receiver to retrieve the plain text from cryptogram. It must be remembered that there are two main types of keys and as a result two sorts of cryptosystems: symmetric and asymmetric. There are also two expletive and competing parts of cryptology: cryptography and cryptanalysis. The first part is responsible hiding and securing information and the second one breaks the cryptogram and retrieves plain text. Cryptology is very broad topic it is not only about ciphering data and cracking them, it covers also random key generation, key exchange protocols, digital and electronic signatures. We can state that the cryptology takes its roots in ancient Rome. All historical resources states that Roman army as a first tried to hide the meaning of the important military orders from the enemies. Roman were using cipher which names comes from currently ruling dictator, one of the most important people from whole history Gaius Julius Caesar. At the same time the opponent and complementary part of cryptology – cryptanalysis was born. Since that times both branches of this science were developing alongside. One influenced the other and vice versa. People were creating more complex and providing higher level of safety cryptography methods. There were created two types of ciphers substitution in which every character from the plaintext is replaced by ciphertext character according to the fixed rule – key. Another type of cryptosystem is known as a transposition cipher where ale used in the plain text characters are changing their positions within a ciphertext. All mentioned above ciphers belong to one family of cryptosystems –symmetric cryptosystems. Symmetric cryptosystem uses just one key in both processes: encryption and decryption. It has got advantages as well as few major drawbacks. The biggest one is that both sender and receiver of encrypted message are obliged to state the key before transmission of the messages. These cryptosystems have no protection in the case when attacker somehow steals the secret key.

The first milestone in cryptology took place during the second world war when one of the biggest inventors in the history Alan Turing as a first constructed mechanical computer. Alan and his invention not only changed the course of a war and saved millions of lives but also begin the age of computer science. That moment, since computers started to create cryptograms and break them was an enormous change for cryptology. From these days computers took the humans role. Amount of computations which computers are able to perform in a short period of time enabled us analyse, change and test giant amount of data. Evolution in computers architecture still lasts and accelerates more ad more. Speed and amount of computation performed by today machines grow very fast. That influences also both cryptography as well as cryptanalysis and motivate to development. The second huge milestone in cryptology took place in ninety seventy-six when the idea of public key ere proposed by Whitfield Diffie and Martin Hellman was proposed. This kind of cryptosystem is based on the pair of different keys. Sender uses one key for encryption and the receiver uses second one to decrypt the message. Both keys are very closely attributable to each other but it is really hard to retrieve or guess one from another. This feature solves most of the problems which are related to symmetric cryptosystems. Most of modern ciphers belong to this relatively new family of ciphers. The idea of digital signatures is also based on the asymmetric cryptography.

Nowadays cryptography overtook cryptanalysis in their ‘race’. There are few cryptography methods which provide sufficient level of safety and even the most powerful machines are not able retrieve plainext from the cryptograms. According to many scientific publications these lead will remain for next ten or fifteen years however we cannot be sure about that. The industrial and technological progress is enormously fast and there is no possibility to predict how huge power computers will have in few years.

### 4.1.1 Cryptography

Cryptography is a branch of cryptology responsible for securing information. The main goal of cryptography is to cipher plaintext to provide sufficient level of safety which means that no third parties will be able to retrieve secret message. Cryptography strives to create such cryptogram which will be conditionally easy and unconditionally as difficult as possible. Conditionally easy cryptogram is such a cryptogram for which the time and amount of arithmetical operation needed to retrieve plaintext is low in a case when user owns a key. On the other side retrieving the plaintext from cryptogram without any knowledge about the used key should be as hard as possible – this is what ‘unconditionally difficult’ means.

There are many diffusions of cryptography methods regarding to different aspects, in regard to used alphabets, way of changing plain text characters but the most important is in regard to the key type. Since ninety seventy-six an idea of asymmetric cryptosystem was created. All previous ciphers use symmetric key which mean that encryption and decryption can be done by using one key. These kind of ciphers had many advantages. Computational complexity of encryption and decryption is relatively low, which is a big virtue. Drawback of symmetric cryptosystem is the users are forced to fix the key before the transmission. Having in mind that it is vital to change keys to preserve high level of security symmetric key becomes a huge disadvantage.

The totally new, asymmetric cryptosystem introduced huge change – pair of keys. In asymmetric cryptosystems users generate pair of keys: encrypting and decrypting one. Sender produces keys, and publishes key responsible for encryption. That kind of approach resolves totally problem of stating key which was present in symmetric cryptosystems. However the computational complexity is much higher than in previous case. Process of encryption and decryption lasts longer and need more resources the symmetric ciphers. What is more interesting asymmetric cryptography found application in other important area of cryptology - digital signature.

There are few very important safety aspects which cryptography may ensure. First of all is data confidentiality which is assured by process of encryption. Digital signature added to the message ensures data authenticity. Digital signature points at the true source of the received information. What is more sender cannot deny that he or she is the author of the message which fulfils third security function call non-repudiation. Last security function is the data integrity which is also supported by the signature. Digital signature is the function of the message, and includes the part of the original message. Whenever the original message will be changes, the signature will also change. Wrong validation of the signature suggest that third parties had access to the message during the transmission and the whole message was changed. Using both encryption of message and digital signature increases the level of safety enormously.

### 4.1.2 Cryptanalysis

Cryptanalysis is a second branch of cryptology which is totally opposite to cryptography. It appeared in the history almost parallel to the cryptography. As cryptography’s opponent this kind of science arose right after the first cipher. Cryptanalysis is responsible for finding and using vulnerabilities of cryptography methods. After a find and use of weakness of cipher cryptanalyst is able to retrieve plaintext from cryptogram. Each attack at cipher requires special amount of resources. There are three main which need to be considered during attack: time needed to retrieve message, computers memory needed to perform all required computations, and amount of data which cryptanalyst intercepted. All these three resources are strictly connected and they affects each other. Considering the last, the most important resource – data, there are many different situations in which cryptanalyst can collect it. There are at least four main worth to mention: situation when cryptanalyst own only ciphertext, more convenient when cryptanalyst has got both – ciphertext and corresponding plaintext, situation when cryptanalyst has got temporary access to either encrypting or decrypting machine and collect date from it.

Cryptanalyst may be considered as a danger not only for encrypted message itself but also for a transmission channel. This channel can be attacked passively or actively. In active wiretap sender is impersonates by attacker which means that the authenticity of the message is threaten. Passive wiretap is the vulnerability against the confidentiality of the message. In this kind of wiretap attacker focuses on transmission channel and tries to intercept private message.

### 4.2 Cryptography methods

One of the most significant issues concerning practical solution of the thesis was the proper chose of cryptography methods which should appear in the webapplication. Application should cover ciphers from both symmetric and asymmetric cryptography system families to show the user major differences between them. Beginning user should also start his or her adventure with the cryptology with an easy example of the cipher, that is why there are examples of the classical cryptosystems in the application. On the other hand it was necessary to put an example of modern and very powerful cryptosystem. To give the user complete view at exchanging secured messages digital signature should be also available in the application. After a research and having in mind all mentioned requirements the following cryptosystems were described and implemented in the thesis.

### 4.2.1 Caesar Cipher

One of the most basic and probably the oldest cipher in human history. This classical cipher was firstly use in ancient Rome for military purposes. Caesar Cipher belongs to the symmetric, transposition family of ciphers. The cryptogram is created by replacement of the every plain text letter by letter shifted by fixed value. The key determines the value of the alphabet shift. There are two different ways of presenting key in the Caesar cipher. We can present key as a number or as a letter. The second option goes to show the letter which the first letter of original alphabet will be replaced by. Originally Roman were using only the shift three, nowadays we can find in many places implementation with shift thirteen. Apart from the value of shift, there is also possibility to state the direction of the shift.

Encryption in the Caesar cryptography system is described by the following formula:

Where:

E(i) − i-th character of encrypted text

D(i) − i-th character of plain text

k – shift value

Decryption looks almost exactly the same, the only difference is the opposite sign in the formula

Unfortunately Caesar cipher does not provide any acceptable level of safety. Because of the fact that all characters of the cryptogram are only shifted by one value from the original message the secured message may be cracked in no more than few minutes by everyone who has got pen and piece of paper. This simple cryptography method is weak against all available types of attack. Its space of keys which means how many possible keys may be used are determined by the length of used alphabet.

### 4.2.2 Vigenere Cipher

Vigenere cipher is strongly connected with the Caesar cipher. This cipher belongs to a polialphabetic, substitution family of ciphers. It is also based on the idea of using shifted alphabet but is more advance than its ancestor. Vigenere cipher can be realized with the tool invented by Johannes Trithemius-Tabula Recta. Tabula Recta is a two dimensional square array. Each row contains all characters from the alphabet in proper order however each consecutive row has higher shift than previous one. Tabula consist of twenty-six rows and includes all possible shifts of the alphabet and with vertical and horizontal headers which contains not shifted alphabets . Trithemius basing on his own invention created also very basic cipher. During the encryption each consecutive character of plain text cipher with the shifted alphabet where value of the shift was equal to the index of the plain text character. Around fifty years later in fifty fifty-three true inventor of Vigenere cipher Giovan Battista Bellaso described his invention in the book ‘La Ciphra del. Sig. Giovan Battista Bellaso’. Bellaso added one improvement to Trithemius cryptography system which was remarkable amelioration-the key. Key was a string of characters used during encryption. When user of Vigenere Cipher want to encrypt something with the Tabula Recta her just need to look at the row or column where header shows the letter to encrypt and the column or row with the header with key character. Cipher text character is in the place where both row and column are crossed. In the case when the lengths of plaintext and the key are not equal, key need to be shorten or copied to adjust to amount of plaintext characters. Blaise the Vigenere also added something to this famous cryptography method – new type of key which is called autokey. Autokey is just a letter or short phrase to which user has to add almost whole original message to make the plain text and the key equal in terms of length.

From the mathematical point of view process of encryption can be described by the following formula:

where:

C(i) − i-th character of ciphertext

D(i) − i-th character of plaintext

K(i) − i-th character of key

Decryption process looks almost exactly the same like the encryption process. It is described according to the formula:

Vigenere cipher may be considered as a cryptography system which provides very high protection level. What is more, under three constraint Vigenere cipher can count as a perfect one. If the key is as long as a plain text, it is totally random and used for only on encryption then the cipher may be considered as unbreakable. Encryption which fulfils all these three constraints are known as a one-time-pad encryption. This method was invented and described at the first time in eighteen eighty-two by Fran Miller. However it was reinvented and patented in nineteen nineteen by American cryptologist Gilbert Vernam. He is also inventor of polialphabetic known as Vernam cipher.

There are few different methods of attack at the Vigenere cipher. The first one invented by Friedrich Kasiski is about finding repetitions in the ciphertext. Kasiski assumed that the same occurrences of part of ciphertext may be encrypted with the same key. Finding the distance between these repetitions can denote the possible lengths of the key. After find the length of key the frequency analysis can be applied. This kind of attack is about counting the number of occurrences of certain character and matching them to possible plaintext letters knowing the fact how probable the character is within a language.

Other attack known as a Friedman test is based on index of coincidence. This index measures how similar a frequency distribution is to the uniform distribution Index of coincidence can be counted from the following formula:

http://latex.codecogs.com/gif.latex?IC%20=%20\frac%7b\sum_%7b0%7d%5e%7b26%7d%7bf%7bi%7d(f%7bi%7d%20-%201)%7d%7d%7bN(N-1)%7d

where:

IC – index of coincidence

fi – count of the letter

N – amount of characters in the encrypted text

### 4.2.3 Merkle-Hellman Cipher

Merkle-Hellman cipher belongs to asymmetric cryptosystems family with public key. Is it one of the first asymmetric ciphers in the history. It was invented in ninety seventy-eight by Ralph Merkle and Martin Hellman. Cipher is also one out of many ‘knapsack’ ciphers. The name comes from the mathematical problem which has got the same name. The problem is defined as follows: for a given set of numbers A the goal is to find any subset of numbers B which gives the sum S. Merkle-Hellman cryptosystem is based on the special case of sum of subset problem – whole set of numbers has to superincreasing, That means the each consecutive member of the set is higher than sum of all previous numbers from the set. It is very important aspect because in traditional knapsack question there are usually more than one subsets which fulfills the problem. That would mean that there are more than one solutions which could give plaintext or there are more than one possible plaintexts which is also a nonsense.

Keys are the two different set of numbers and two additional elements. Private key is a superincreasing set of numbers. To generate public key which is also set of numbers, user has to find the sum of private set and choose arbitrary number which has to be cooprime with the sum. Each element of public key is the result of modulo operation of the sum from the result of multiplication of element from private set and chosen multiplier. Both multiplier and sum of private set are part of public and private keys.

To perform encryption user is obliged to convert the message into the binary string. After that all consecutive numbers need to be multiplied by the consecutive elements of the key set. The cipher text is the sum of all results of multiplications. Depending on lengths of plain text and key, ciphertext may consist of one or more numbers. The process of encryption can be described by the formula:

https://latex.codecogs.com/gif.latex?%5Csmall%20c%20%3D%20%5Csum_%7Bi%20%3D%200%7D%5E%7Bn%7D%5Calpha_%7Bi%7D%20*%20%5Cbeta%20_%7Bi%7D

where:

c – ciphertext character

αi =i-th bit of the plaintext

βi – i-th element of the public key set

Process of decryption is a bit more complicated than encryption. Receiver of encrypted message at the beginning has to perform modulo operation of sum from result of multiplication of number representing ciphertext by modulo reverse of multiplier. The result of the operation is the number which has to find in the knapsack problem. Each element which is part of the ciphertext sum gives bit ‘1’ and the other give ‘0’. The last step is just to convert given bits into characters string. Process of decryption based on solving superincreasing sum of subset problem is described by the following formula:

https://latex.codecogs.com/gif.latex?%5Csmall%20m%20%3D%20%5Csum_%7Bi%20%3D%200%7D%5E%7Bn%7D%5Calpha_%7Bi%7D%20*%20w_%7Bi%7D

where:

m – plaintext character

wi – i-th element of the private key set

In terms of safety Merkle-Hellman cryptography system like other knapsack ciphers provides very high level of secure against brute force attack. Brute force attack is computational ineffective method for this cipher. Its computational complexity is θ2n which for big n gives very time consuming problem to resolve. However there was found a vulnerability connected with the knapsack cipher. Adi Shamir co-author of the one of the most popular and safe cryptography system used the dynamic programming and wrote the algorithm which solves the knapsack problem in pseudo-polynomial time. Because of this loophole Merkle-Hellman cipher does not find application nowadays.

### 4.2.4 RSA Cipher

RSA is one of the most popular asymmetric cryptography system with public keys. It was invented in ninety seventy-seven by three cryptologists Ron Rivest, Adi Szamir and Leonard Adleman. RSA cipher is very universal, it finds application not only in message encryption but also may be used for creating digital signatures. Message encrypted with RSA with signature with the same cryptosystem fulfills all important safety aspects. It provides confidentiality, integrity, authenticity, and non-reputability. RSA cipher is based on the difficulty of factoring of result of multiplication of two very large prime numbers. Multiplication of numbers is not a problem even for very large integers, however difficulty arises for opposite side operation which is factoring. That kind of computation is very hard and resources consuming even for very powerful computers. There are no algorithm which would significantly speed up the whole process. That makes RSA very powerful cryptography tool which under few constraints may be considered as a perfect cipher.

The security level depends mostly on the length of the key The longest known broken key used in RSA was 768 bit. It was achieved at the beginning of two thousand ten. The whole process of cracking the key was performed by a huge cluster of computers which consists of hundreds of machines. The time spent on cracking took around two years of computations. There are no published information about cracking longer key. Because of the fact who hard and resources consuming the cryptanalysis process for RSA is the most common implementations of this cryptosystem have between 1024 and 4096 bit long keys. According to many predictions in around ten to twenty years 1024 bit key long can be considered as not enough safe. However the technology development is enormously fast and computers computational power is growing year over the year what may result that cracking longer keys may be achieved faster than the all predictions say.

To generate key user at the beginning need to choose to prime numbers. The higher these numbers are the higher safety will be assured. Next step is to multiply both these coefficients and the result ‘n’ becomes one of the common factor for both private and public key. Next important factor Ф(n) is the result of multiplication of both previously chosen factors decreased by one. To obtain public key user has to choose one more coefficient ‘e’. This coefficient need to be coprime with the n coefficient. Two numbers are coprime when the only positive common divisor for them is equal one. The last step of key generation is to get second parameter for private key ‘d’. To determine ‘d’ coefficient user has to perform the Extended Euclidean algorithm. Parameter ‘d’ is the greatest common divisor of ‘e’ and Ф(n). As mentioned before, keys pairs of numbers public key is the pair (n, e) and the private one is (n, d).

RSA encryption process can be described by the following formula:

c ≡ me mod n

where :

c – cipher text character

m – plaintext character

e – e parameter of the public key

n – n parameter of the public key

Decryption is described by very similar formula which is as follows:

m ≡ cd mod n

where:

d – d parameter of the private key.

RSA as very effective cryptography system finds many different applications. RSA is regularly used in internet browsers, in applications based on exchanging data like email, chat applications. Virtual private networks and for user identification.

### 4.3 Digital Signature

Digital signature is an another method used for data security. It is strictly connected with the cryptography systems, it uses Mathematics to achieve authenticity of electronic documents. Digital signature was firstly described in the nineteen seventy-six by Whitfield Diffie and Martin Hellman as a possible application of their great invention which is asymmetric cryptography. It was only theoretical solution, they did not present any practical implementation of the signature. The first proof that asymmetric cryptography system can implement digital signature made inventors of RSA cipher Ron Rivest, Adi Szamir and Leonard Adleman. Digital signature is based on the asymmetric cryptography, however it is realised in an opposite way to the ciphers. During the ciphering sender uses public key of the receiver to encrypt the message and receiver uses his private key to decrypt the document. In the case of signature, sender uses his private key to generate his signature and receiver of the message verifies the authenticity by using public version of the sender key.

Similarly to the ciphers there can be distinguished three main phases connected with digital signature scheme. First phase is a creation of the pair of keys, firstly random private key is generated from the all possible keys. Basing on the private key the other from the pair is calculated. Second phase is signing the document. User performs signature function on the document in order to sign it. Last phase is on the receiver side – signature verification. In the process of verification involved is public key of sender which states if the signature belongs to the proper person or not. Process of verification gives also more important information which will be explained later.

There are some cryptography systems which can applied to both encryption and signing the electronic documents and mentioned before RSA is a great example. Previously discussed ciphers provide data confidentiality, which means that message was readable only for people who were allowed to do that. Only people who have access to the key can read the true content of the encrypted message. Digital signature does not provide data confidentiality however it fulfils other very important aspects of data protection. First and foremost digital signature like traditional written signature verifies the author of the signature. This feature is called authentication. The second very important feature – non-repudiation states that sender of the message cannot deny that message comes from him or her. The last important feature tells the receiver that the original message was not altered by third parties during the data transmission. Digital signature finds application mostly in electronic signature implementation.

### 4.4 Electronic signature

# JavaScript Cryptography Library

Functions and implemented algorithms

……………………………………………………………. … ……………… ……………….

Possible modifications

……………………………………………………………. ………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ………………… ……………….

* 1. **xxx**

……………………………………………………………. ………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ………………… ……………….

* 1. **xxx**

……………………………………………………………. ………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ………………… ……………….

# The web application supporting encryption algorithms

……………………………………………………………. ……….…………………

* 1. **Graphical user interface**

Graphical user interface (GUI), is a type of user interface that allows users …

* 1. **xxxx**

……………………………………………………………. ……….………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ………………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ….. ………………… ……………….

* + - * 1. **xxx**

……………………………………………………………. ………. ………………… ……………….

* + - * 1. **xxx**

……………………………………………………………. …….. …………………

* + - 1. **xxx**

……………………………………………………………. ……….. ………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ……… ………………… ……………….

* + - 1. **xxx**

……………………………………………………………. ….. …………………… ……………….

# Summary

……………………………………………………………. ………………… ……………….

# Appendix

Source code…

# Bibliography

Badley, Linda. *Writing Horror and the Body. The fiction of Stephen King, Clive Barker and Anne Rice.* Westport: Greenwood Press, 1966.

Benefiel, Candace E., “Blood Relations: The Gothic Perversion of the Nuclear Family in Anne Rice's *Interview with the Vampire*.” *The Journal of Popular Culture,*Vol. 38, No. 2 (2004): 261-273.

Hoppenstand, Gary, and Ray B. Browne. “Vampires, Witches, Mummies, and Pother Charismatic Personalities: Exploring the Anne Rice Phenomenon.” *The Gothic World of Anne Rice.* ed. Hoppenstand, Gary, and Ray B. Browne. Bowling Green: Bowling Green State University Popular Press, 1996.

Ingebretsen, Edward J. “Anne Rice: Raising Holy Hell, Harlequin Style”. *The Gothic World of Anne Rice.* ed. Hoppenstand, Gary, and Ray B. Browne. Bowling Green: Bowling Green State University Popular Press, 1996.

Schneier, Bruce „Kryptografia dla praktyków”, WNT 2002 2.

Schneier, Bruce „Applied Cryptography. Protocols, Algorithms and source code in C".

Menezes, Alfred J., van Oorschot, Paul C., Vanstone, Scott A. „Handbook of Applied Cryptography”, CRC Press,1997. (Kryptografia stosowana, WNT 2005.

Stallings, William „Ochrona danych w sieci i intersieci w teorii i praktyce”, WNT, Warszawa 1997.

Stallings, William „Cryptography and network security: principles and practice”, Pearson/Prentice Hall, 2011.

Helen Fouche Gaines' Cryptanalysis: A Study of Ciphers and Their Solution.

Klander, L. „Hacker proof czyli jak się bronić przed intruzami" Mikom Warszawa 1998.

Mitnick, Kevin D., Simon, William L., and Wozniak, Steve „The Art of Deception: Controlling the Human Element of Security”, Wiley, 2003.

Mitnick, Kevin, and Simon, William „Sztuka podstępu. Łamałem ludzi, nie hasła”, Helion 2003.

Stallings, William „Cryptography and network security: principles and practice”, Pearson/Prentice Hall, 2011

Gaines, Helen Fouche „Cryptanalysis: A Study of Ciphers and Their Solution.

Swenson, Christopher „Modern Cryptanalysis: Techniques for Advanced Code Breaking”

Ferguson, Niels „Cryptography Engineering: Design Principles and Practical Applications”

**Web resources**

**Abstract**

**Keywords: cryptology, cryptography, safety, cipher, webapplication,**

Załącznik

do Regulaminu Studiów w PŁ

z dnia 29 marca 2006 roku

Łódź, dnia …………………… r.

Paweł Grzegorzewski

(IMIĘ I NAZWISKO STUDENTA)

190116

(NR ALBUMU)

Computer Science

(KIERUNEK STUDIÓW)

Inżynierskie, stacjonarne

(RODZAJ I FORMA STUDIÓW)

OŚWIADCZENIE

Świadomy odpowiedzialności karnej za składanie fałszywych zeznań oświadczam, że przedkładana praca magisterska / ~~inżynierska~~ / ~~licencjacka~~ (\*)na temat:

*„The web application supporting encryption algorithms   
– Does cryptography provide security?”*

*Aplikacja internetowa wspierająca algorytmy szyfrowania   
– czy kryptografia zapewnia bezpieczeństwo?*

została napisana przeze mnie samodzielnie.

Jednocześnie oświadczam, że ww. praca:

* nie narusza praw autorskich w rozumieniu ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. z 2000 r. nr 80, poz. 904, z późniejszymi zmianami) oraz dóbr osobistych chronionych prawem cywilnym, a także nie zawiera danych i informacji, które uzyskałem w sposób niedozwolony,
* nie była wcześniej podstawą żadnej innej urzędowej procedury związanej z nadawaniem dyplomów wyższej uczelni lub tytułów zawodowych.

Jestem także świadomy, że praca zawiera rezultaty stanowiące własność intelektualną Politechniki Łódzkiej, które nie mogą być udostępniane innym osobom i instytucjom bez zgody Uczelni.

……………………………………………………………

(PODPIS STUDENTA)

(\*) - niepotrzebne skreślić