Journal of Computations & Modelling, vol.4, no.1, 2014, 349-358
ISSN: 1792-7625 (print), 1792-8850 (online)
Scienpress Ltd, 2014

Cryptool 2 in Teaching Cryptography

Major Konstantinos Loussios[1]

Abstract.

Considering the value it had in the past, has continued to the present and will continue to have, perhaps to an even greater extent in the future concealing information during transmission or transport, leads automatically to attempt to discover the importance and the value of the means, methods and techniques used to implement the concealment.

Cryptography is a branch of computer science attracts the attention with its great utility that has nowadays. Given therefore deemed necessary to standardize, analyze and present the encryption algorithms to learning and training on the operation with as efficiently and easily as possible. Having in mind that the theory must be accompanied by practice and examples that help to consolidate the syllabi material, we felt that the analytical presentation of an educational tool on learning algorithms of cryptography is a way of learning while embedding.

The learning tool cryptool 2 is an implementation of all the above, and through this we will try to show, those essential functions, which help the user with visual and practical way, to see in detail all the properties and functional details of the algorithms contained, will present representative examples of functioning algorithms, we proceed to create digital signatures and will implement the cryptanalysis algorithms.

The above is an object of study and teaching in the professional area of land, in the field of communications and transmissions-service systems.

Knowing, however, that historically since the antiquity, first we Greeks, we use encryption in a simple form, for military purposes, but later down through the years and fighting wars around the world, the art encryption and decryption evolved and became object of all armies and weapons. This created great interest, mobilizing science and development of complex thinking that eventually evolved into an autonomous discipline.

Keywords: Cryptography, Algorithms, AES, DES, RSA, Hash Function, Cryptology

[1] Hellenic Army General Staff, 5 Kleomahous Str., Chalkida 34100, Greece
E-mail: klousios@hotmail.com

1 Introduction

The issue I would mention is the software cryptool 2 and how it could be used in the teaching of cryptography to audiences - learners who have not special knowledge in computers and they have a relatively short time to digest the information provided and then use the appropriate program for the effective functioning of the body - the service to which they belong. An example of such an audience is the non-specialized in IT - communications military personnel .

2 Need to Know Cryptography

Undoubtedly is now imperative, every single computer user, information systems, networks (classified or not connected to internet) and any other devices such as mobile phones and services provided to us in many ways , be aware that the transmission of data, storage and use must be made for safety reasons the use of encryption .

Besides particularly the current deployment of wired and wireless networks and the Internet make it imperative than ever to protect data and information.

Important part of the principles and policies for an organization or company or public – government or private sector, is the consolidation of the concept of security. This is achieved by awareness of the risks involved in connection with measures and security policies to ensure the confidentiality of all interested parties.

There are three words, «Confidentiality» , i.e. non-disclosure of the contents and protect them from their enemies and prying eyes , " Integrity " , transfer - transfer to the recipient , and intact whole message content , lossless , additions or alterations and "Availability" response i.e. at any time of the program, information system or network service , refer invariably to all security policies and is wanted in the safe mode. In this one of the leading roles played by knowledge and use of cryptography.

3 Use of Cryptography in Military Science and Activity

From ancient times there was the effort to secure and content protection messages were of particular value and should be protected. Then started and the various methods for converting the format of the message to non- readable and

comprehensive format so deceived opponent . Examples are algorithms baton and Caesar with the original forms of texts, how to encrypt the final cipher . Later

followed the polyalphabetic substitution as Vigenere 's algorithm and the 19th century Hill's based on the linear algebra.

During the two world wars cryptography developed using both mathematics and electromechanical devices and appeared machines for automated encryption and greater complexity and difficulty of discovery of encryption mechanisms.

In the first World War have the appearance of the British encryption algorithm PLAYFAIR and matched by their opponents Germans in ADFGX. In both cases , starting with the provisions in letters and 5x5 tables with specific reading and filling the gaps with letters operating output of the cryptogram , using keywords and conversely decryption.

The 2nd World War role undertaken by cryptographic engines for greater complexity and speed. Examples are the German ENIGMA, the Japanese PURPLE and the American SIGABA. With the end of the conflict have been deciphered algorithms encryption keys used and all the mistakes that led to the failures of the use of cryptography.

Later we moved to another age where they no longer rely as before both in the way of structure and function of the cipher as the key length . At a time like this the " Cold War " where antagonisms -confrontation , the two different allied block West and East and the psychological impact of threats, revelations or announcements for demonstration power gave great importance to the development of potential concealment , division intelligence and create impressions .

Worthwhile references algorithms is definitely the DES (Data Encryption Stantard) symmetric algorithm with key length 56 bits, which works with the structure feistel (confusion - diffusion), the Triple DES which increases the key length and encrypts again the already encrypted part and AES (Advanced Encryption Stantard) where here cover any gaps were identified in the DES using larger keys of 128 bits and a change of the encryption process .

Pinnacle of evolution are asymmetric algorithms where using the theory of primes we get to using public and private key. Example is the RSA (Rinest-Shamir-Adleman The co-authors of the algorithm). Asymmetric cryptography maximized security levels and has potential for further applications of cryptography.

The establishment at Allied and global levels of the fourth dimension of operations (net of land -sea - air - space) added cyberspace , historical past incidents of cyber attacks against networks and threats to critical infrastructure of each country through the corresponding attack information systems as a characteristic of today's reality .

In addition to the routine handling numerous information privacy , business , financial and industrial elements that affect vital defense and security and normalcy to a human society contribute to the pursuit of improving the safety and use of cryptography and the applications in management of risks.

4 Cryptool Portal

To learn and be trained there are many ways. One of these is the use of internet. The cryptool portal, is the way that everyone can study according to their features cryptography and cryptanalysis. Both of them constitute the science of cryptology.

Thus one can see the results of using the algorithms to cryptool on line, to ascertain the mode of each algorithm and learn summarized historical data.

5 Cryptool 2

The cryptool 2 is supplied free program with which each person installing the computer to experiment with encryption. Create their own provisions, to test the algorithms and study the results.

5.1 Basic Description

More specifically, a description of the basic steps are the following: Select an algorithm determines what kind of work will be performed (encryption - decryption), place the input data (text - file, picture , etc) appropriate type keys according to the algorithm , we form connections in the interface and the output connectors where the result will look and if everything is as it should be - if not, the program does not allow the completion of connections and not running - and then displayed after the execution result. The results obtained are thereafter studied , and compared or used in new encryption or decryption.

5.2 Original Image

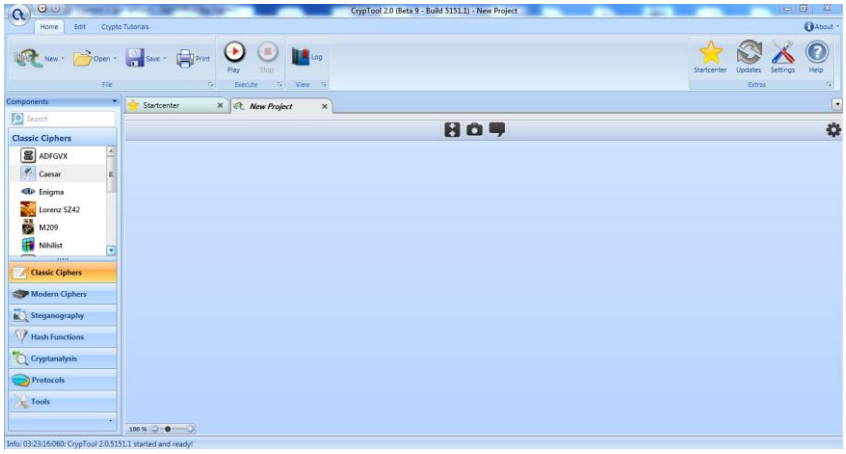

Figure 1

Figure 1 shows the original image of the program before making any choice. The horizontal space on the upper side is the menu options on the known functions of storage, file selection, updates, settings, and program execution.

The vertical left side is the toolbox of options the remaining space is the work area and the implementation of connecting the necessary parties.

5.3 Options of the Software

Figure 2

Detail in Figure 2 is what is included in the toolbox on the left side. We see all the classic algorithms, all current algorithms, hash functions, steganography , protocols and types of inputs - outputs needed to run an algorithm . With the right "click" on all these elements, when introduced into the work area , given by the program even more information on how to use and operate.

5.3 Details of Algorithms

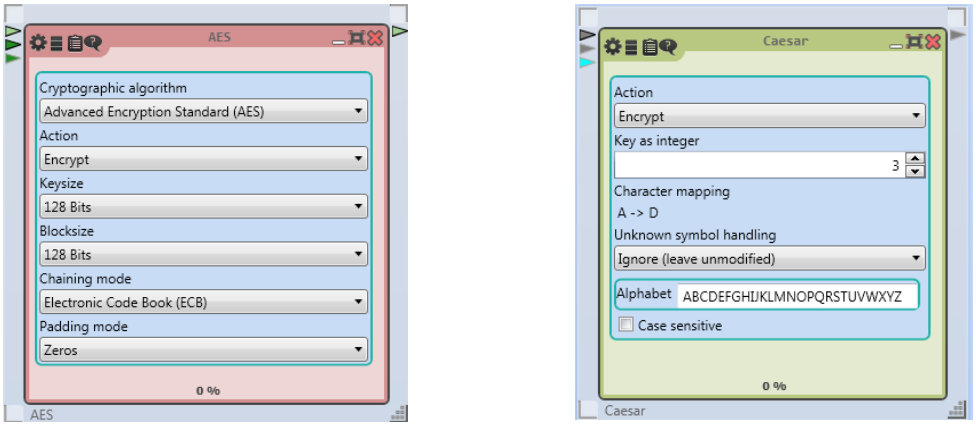

Figure 3

The icons of the algorithms when the zoom in enabling us to deal with details of their settings. In Figure 3, the icons of DES and ADFGVX have options for the type of use (encryption - decryption), the channing mode associated with modes of algorithms parts (Electronic Code Book, Cipher Block Chaning, Cipher Feed Back, Output Feed Back and Counter) the padding mode (filling gaps), the keys used.

5.4 Display Connection

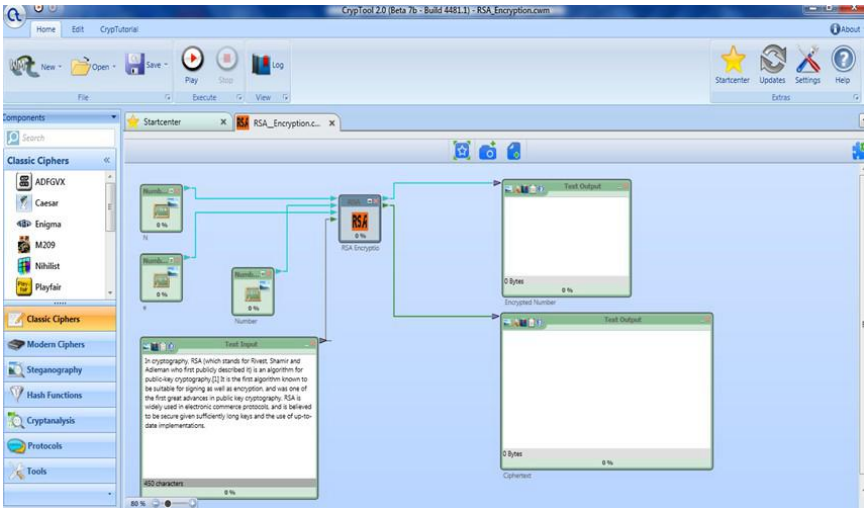

Figure 4

Then in Figure 4, it seems a case of how connected all the necessary elements to perform the operation. Appears RSA with which you encrypted a passage. Necessary figures in the left side are the public and private keys to encrypt data.

5.5 Operation

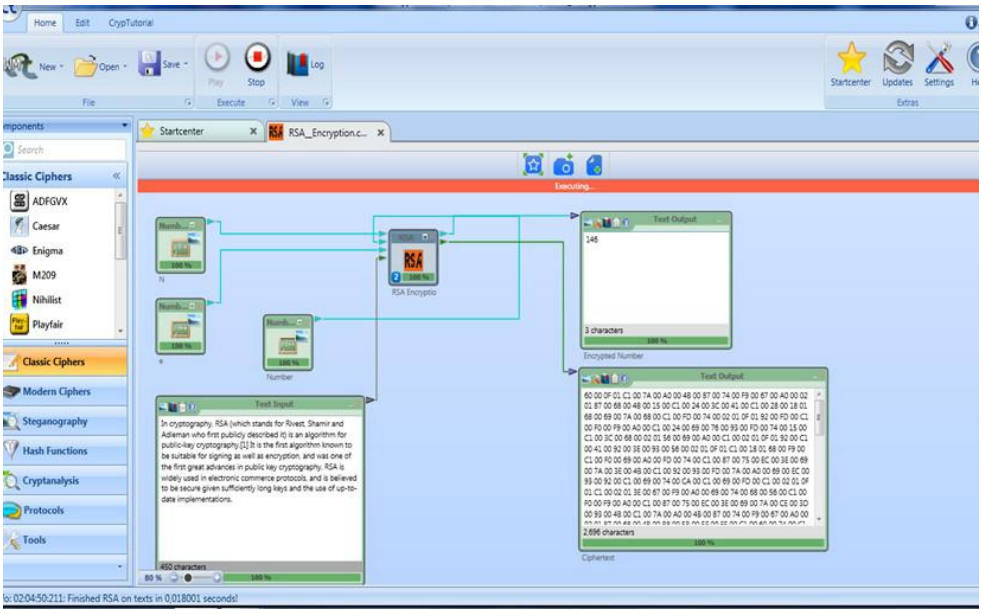

Figure 5

Figure 5 illustrates how becoming the "execution" of the program to export the result. Once you have given the 100% in the execution, we have completed, press the stop and we have the result.

5.6 Input – Output of Algorithm

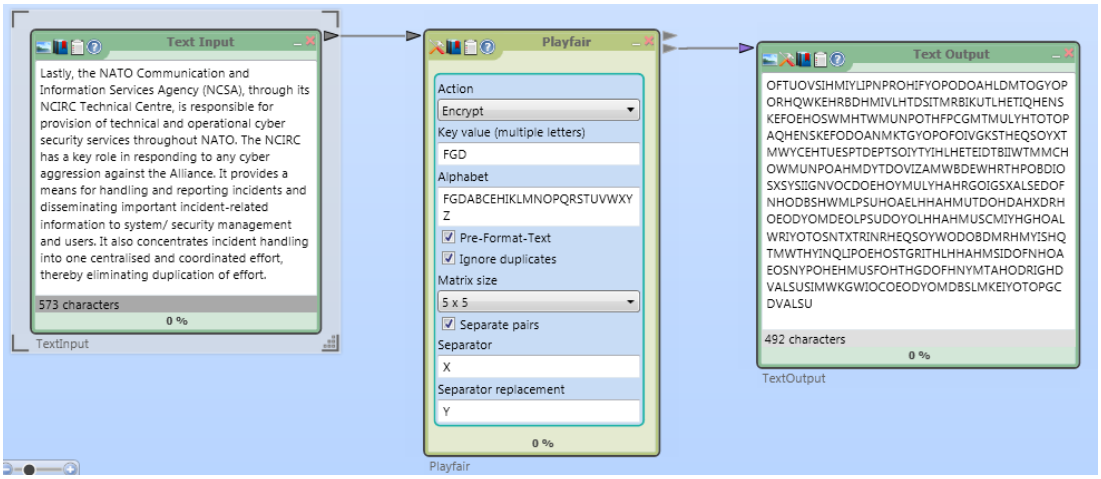

Figure 6

In Figure 6 we see what gives us a text from the PLAYFAIR. It is obvious that the result (out put) process can be used as input in a subsequent procedure.

5.7 Language Statistics

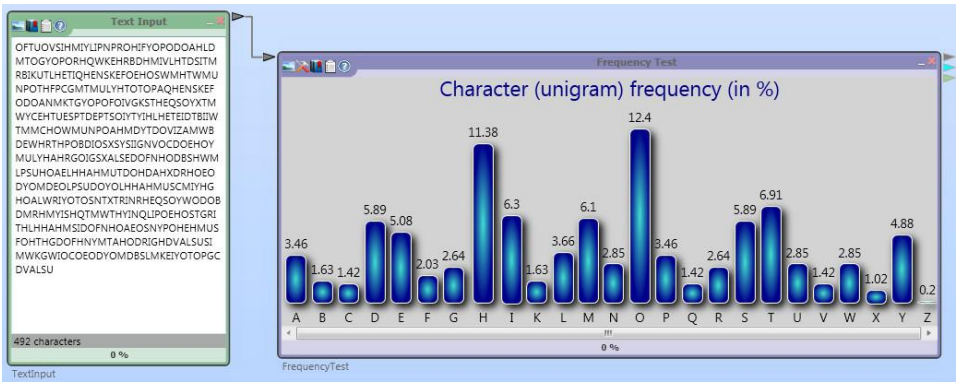

Figure 7

So if you use the exit of PLAYFAIR we can make use of another function is the statistics of the language (Figure 7). How often repeated that one letter. This is based on the specificity of each language is an element of cryptanalysis to extract the original message.

6 Cryptanalysis

Referring little earlier in language statistics and their usefulness should be noted that the potential of cryptool 2 are not limited to statistical incorporating other instruments (tests) cryptanalysis as the Friedman test (calculation process length possible keys to polyalphabetic substitution algorithm) and Kasinski test (is a process attack on polyalphabetic substitutions , based on an analysis of gaps in repeated sections ciphertext) . In Figure 9, we make use of the ENIGMA machine cryptanalysing the result by applying the tests mentioned above.

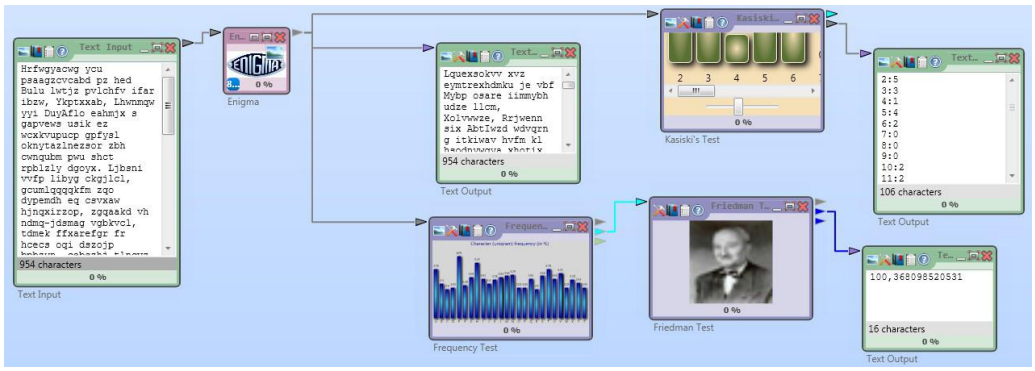

Figure 9.

7 Advantages

After all the above, which gave an overview of the content and the way the program works is essential to locate somebody advantages - disadvantages to install the program and move into a grueling use in all fields of interest.

We would like to point out some advantages are obvious:

1. It is a free version available to anyone on the internet which is constantly reviewed and updated.
2. It is very easy to install and has no requirements for the use of specialized equipment, we need a simple PC.
3. It is very simple to use and provides a lot of information and sources of information for which the user does not know to approach it and understand it . The environment is windows and intimate in the vast majority of users.
4. Broad in scope and covers all genres and ways of cryptography.

8 Conclusions-Suggestions

Given the advantages we conclude that displayed some reasons why the use of this program can be systematically exploited

1. For experimentation in cryptography and cryptanalysis to consolidate the theoretical knowledge but also solve queries.
2. It’s a potential tool for teaching staff needed to increase their knowledge and training in cryptography. The simplicity and strength that characterize contribute to use by people who have no special knowledge of computers and cryptography and can thus understand and learn more.
3. Our focus on military personnel does not know about cryptography and should shortly be updated and exercised. More specifically in schools or courses of short duration would be desirable to standardize the use and combine objects IT security and proper use of Information and Communication Systems.

Our main aim will be to obtain in a short time the most fundamental issues, their strengthening and tracking daily developments especially in security issues.

References

[1] B. A. Forouzan; TCP / IP Protocol Chap 28 Network Security, PUBLICATIONS GKIOURDAS, 3rd 2006

[2] J. F. Kurose and K. W. Ross: Networking Computer Chap 8 Security in Computer Networks, PUBLICATIONS GKIOURDAS 4th 2009

[3] B. H. Thomas: An invitation to cryptology, Aug 2001

[4] W. Diffie and M. Hellman: New directions in cryptography, Nov 1976

[5] S. Nigel: Cryptography: an introduction, Sep 2002

[6] E. Rescorla: SSL And TLS designing and building secure systems, Nov 2000

[7] P. Kotzanikolaou and Ch Douligeris: "Network Security. Introduction and conceptual foundations ' notes for the " Network Security: Introduction and conceptual foundations", October 2009

[8] K. Patsakis: Cryptanalysis algorithms and applications of cryptography to malware, PhD Thesis, University of Piraeus, 2008

[9] Vas. Liagos: Secure and reliable communication protocols using cryptography and cryptanalysis, PhD Thesis, University of Patras, 2008

[10] D. Lekkas: Security of information and communication systems using services trusted third entity: functional, architectural and organizational issues, Ph.D. Thesis, University of the Aegean, 2002

[11] N. Moschopoulos: Cryptography Public and private key: effective implementation of algorithms in VLSI, PhD Thesis, National Technical University of Athens (NTUA), 2001.

[12] Th. Tsiakos: Applied cryptography standard method and model for security of electronic transactions, PhD Thesis, University of Macedonia, 2005

[13] A. Fournaris: Designing a Public Key Cryptosystems, PhD Thesis, University of Patras, 2008

[14] G. Selimis: Design cryptosystems with special-purpose hardware, PhD Thesis, University of Patras, 2008

[15] Ch. P. Masone: Attribute-Based, Usefully Secure Email, PhD Thesis, DARTMOUTH COLLEGE Hanover, New Hampshire August, 2008

WEBSITES

[16] www.cryptool.org

[17] www.wikipedia.org