# ENCRYPTION TECHNIQUES: A TIMELINE APPROACH[†]

**Author and co-author**

**T Morkel [1], JHP Eloff [2]**

Information and Computer Security Architecture (ICSA) Research Group

Department of Computer Science

University of Pretoria, 0002, Pretoria, South Africa

Tel: +27 12 420-2361

Fax: +27 12 362-5188

[1] E-mail: tmorkel@cs.up.ac.za

[2] E-mail: eloff@cs.up.ac.za

[†] This material is based upon work supported by the National Research Foundation under Grant number 2054024 as well as by Telkom and IST through THRIP. Any opinion, findings and conclusions or recommendations expressed in this material are those of the authors and therefore the NRF, Telkom and IST do not accept any liability thereto.

**Abstract:** Encryption can be traced back for thousands of years. Since people first started to use encryption methods, the techniques that we know and use today have come a long way. The purpose of this paper is to construct a timeline of important encryption events that have occurred throughout the ages, and to discuss current and future encryption methods. Each event in the timeline is further researched and presented in more detail. Added attention is given to quantum encryption, the latest addition to encryption techniques. Businesses need more information about the difference between these techniques in order to make informed decisions. In this paper different encryption techniques are evaluated, especially from a business perspective, and compared according to a set of criteria.

**Keywords:** Encryption, Quantum Encryption, Evaluation

## 1. Introduction

Cryptography is the art of enciphering and deciphering of encoded messages [1]. It can be seen as an ancient art that has taken many forms over the years. Encryption started with simple pen-and-paper methods based on letter substitutions. From here it evolved into special machines that were built to encrypt messages. Today we have moved away from the more physical methods, and the focus is on digital encryption that can only be done using computers.

Cryptanalysis, on the other hand, is the art of "breaking" or "cracking" these encryption methods; i.e. the process of deducing the meaning of specially encoded messages without actually being the legitimate sender or receiver. The battle of codemakers versus codebreakers has been going on for quite some time. More than once a new "unbreakable" cipher has been developed by codemakers only to be "broken" by some codebreaker.

The remainder of this paper will focus on constructing a timeline for encryption events. Explanations of each of these events will follow. The timeline ends with quantum encryption – a new technology that is still in its embryonic phase. In the final section of the paper, different encryption techniques are evaluated according to certain criteria and compared.

## 2. The purpose of the timeline -approach

The purpose of the timeline of encryption events in this paper is to explore the history of encryption techniques from 1900 BC to the present. The events are listed in ascending order, and a short description of each of the inscriptions in the timeline is given later in the text.

There are various existing encryption timelines available on the Internet that were examined during the research for this paper. Two timelines stood out from the rest. One was the CME's Cryptography Timeline [a], which is a very extensive and detailed timeline of all events related to cryptography. It tended to be a little too extensive though, especially for a reader who is not familiar with encryption and who wants to acquire a holistic view of events. The other timeline examined was the Obiwan's Deathstar page [b], in the encryption section. This timeline included illustrations of the devices used, but unfortunately this only applies up to 1952.

It might therefore be more feasible to construct a timeline noting only the previous and current critical events in encryption. Thus this paper's timeline features only the encryption events that were felt to be more important and influential than others.

There are unresolved issues that exist with some of the dates listed in this timeline as sources differ on when actual events occurred. Some sources list the date that an idea was developed, and others list the date that the paper on that idea was first published. Furthermore, it is often not known which of these dates is stated. The dates on this timeline are thus just an estimation of the dates that encryption events occurred, and where known, emphasis is placed on whether it is the date of development or the date of publication.

Encryption techniques can be divided into two classes; traditional encryption techniques and modern encryption techniques. Traditional encryption techniques are pen-and-paper based techniques developed in an age when computers did not exist, although some of these ideas can be, and have been, transformed into computer-based algorithms.

With the start of the Computer Era, which can be marked with the appearance of the first computer, encryption techniques underwent a major change. Encryption techniques were being specifically designed for computer usage and used 'bits' instead of the alphabet. These encryption techniques are called modern encryption techniques.

Both of these encryption techniques will be discussed in detail further on in this paper.

*Encryption Timeline*

| | | |
|---|---|---|
| **2003** | First commercial use of quantum encryption | Modern encryption techniques |
| **2000** | Advanced Encryption Standard (AES) developed | |
| **1991** | First quantum encryption system developed | |
| **1984** | BB84 protocol proposing quantum encryption published | |
| **1978** | RSA published | |
| **1977** | Data Encryption Standard (DES) created | |
| **1976** | Public key encryption proposed by Hellman and Diffie | |
| **1970** | Lucifer algorithm developed, later evolved into triple-DES | |
| **1943-1945** | First computer created | The Computer Era |
| **1942** | Navajo windtalkers used in World War II | Traditional encryption techniques |
| **1923** | Arthur Scerbius builds the German Enigma machine | |
| **1917** | Vernam cipher invented | |
| **1854** | Charles Babbage reinvents the wheel cipher | |
| **1790s** | Thomas Jefferson invents the wheel cipher | |
| **1585** | Blaise de Vigenére writes a book on ciphers | |
| **1553** | Password idea introduced by Giovan Belaso | |
| **.** | *THE DARK AGE OF ENCRYPTION* | |
| **.** | | |
| **50-60 BC** | Caesar Cipher introduced by Julius Caesar | |
| **486 BC** | Greek skytale presumably used | |
| **500 – 600 BC** | Hebrew ATBASH cipher used in writing the book of Jeremiah | |
| **1500 BC** | Mesopotamian tablet with encrypted recipe for pottery glaze | |
| **1900 BC** | First documented cryptography in Egypt | |

*Figure 1: Timeline of encryption events*

## 3. Traditional encryption techniques

Traditional encryption techniques are the earliest methods of encryption and have been around for centuries. They are pen-and-paper based techniques, although some rely on the spoken word. The main characteristic of traditional encryption techniques is that they were designed in an age when modern computers did not exist. Some of these traditional encryption techniques used physical objects, or mechanical machines, to conduct the encryption. Generally, traditional encryption techniques rely on the substitution of letters and the use of different symbols with the same meaning. The main component of any traditional encryption technique was the alphabet.

Historians believe that the first case of cryptography was in ancient China where the written language itself was used as an encryption technique [2]. Only upper-class citizens were allowed to learn how to read and write and could thus convey secret messages to each other, without peasants being able to decipher the messages. The first documented use of cryptography, however, dates back to 1900 BC in Egypt [2], where inscriptions were found that contained, not a different set of hieroglyphs, but a system of partial nonstandard hieroglyphs. The conclusion is that the scribe used some kind of encryption method to hide the true meaning of the hieroglyph.

In Mesopotamia, in 1500 BC, a tablet was found that contained an encrypted recipe for pottery glaze [2]. Between 500 and 600 BC, Hebrew scribes used the ATBASH cipher when writing the book of Jeremiah [c]. The ATBASH cipher was a reversed substitution cipher where the last letter of the alphabet was used as the first, and vice versa. This cipher was clearly a very simple cipher, since there was only one possible answer to break the code.

In 486 BC, an encryption method, called Greek Skytale, was developed as a military encryption technique [a]. Soldiers wrapped a strip of papyrus around a piece of wood. The message was written on the papyrus and when it was taken off the wood, different parts of the message was on different parts of the papyrus. Only when the papyrus was wrapped around a matching piece of wood, could the true meaning be deduced. There have, however, been allegations recently that the Greek Skytale is just a myth.

The most famous traditional encryption method is probably the Caesar Cipher, developed by Julius Caesar between 50 and 60 BC [1]. The Caesar Cipher worked on the principle of substitution, where each letter in the alphabet is substituted for another letter. In this case each letter was transposed with another three places after the original letter in the alphabet.

The Caesar cipher is quite a simple cipher, but was very effective and successful in the time of Julius Caesar because very few people could read and write. The Caesar Cipher's major disadvantage was the fact that a very obvious pattern arose from the coded message which could easily be deciphered with a little time and patience.

In Europe, the period between 500 and 1400 AC was known as the "dark age of encryption". A large amount of knowledge about encryption was lost because encryption was seen as a black magic [b] and consequently banned.

In 1553 Giovan Belaso first mentioned the idea of a password [b]. He suggested a type of encryption where the correct password was needed to decrypt the encrypted message. This password is the same as the 'secret key' used in encryption today.

Blaise de Vigenère wrote a book in 1585 about ciphers which can be seen as a transition from traditional to modern encryption techniques [a]. In this book he explained the first encryption key system. To encrypt a message, one needs a key – a common characteristic of modern encryption techniques - as well as the Vigenère Square that uses the alphabet – a common characteristic of traditional encryption techniques.

To encrypt a message, the sender has to take the first (or nth) letter of the cleartext message and find the corresponding column in the Vigenère square. The corresponding first (or nth) letter of the key is then taken, and its place in the rows of the square must be found. The letter where this row and column overlap is the encrypted letter for that original character. This process is continued for all the letters of the cleartext message. Although Vigenère cipher was compromised in 1863 [b], it was seen as a very secure method of communication.

In the 1790s, Thomas Jefferson invented the wheel cipher [a]. Unfortunately his papers were lost and only rediscovered in 1922 [c]. Thus Charles Babbage re-invented the wheel cipher in 1854 without knowing that it has already been invented [a]. The wheel cipher consisted of a cylinder of wood with 26 disks that could rotate around a spindle. The letters of the alphabet were inscribed on each of the disks in a random order, and the disks could be turned to scramble and unscramble words. The disks were turned to depict a message, then that phrase's "ciphertext" was taken from another point on the wheel. To decrypt the message, the receiver had to have an identical wheel, with the disks arranged in the same manner. Similar devices were used by the US military in the First World War.

The oldest encryption algorithm still used today was developed in 1917 by Gilbert Vernam and is called the Vernam Cipher [d]. The Vernam Cipher is a version of a one-time pad – an algorithm that uses substitution where no pattern can arise. The sender encrypts a message using a randomly generated key and adds each bit of the key to the corresponding bit of the message. The receiver then decrypts the message by subtracting the same key. The Vernam Cipher is the only traditional encryption technique that provides perfect secrecy.

Unfortunately the system has some drawbacks. Due to the nature of the algorithm, an eavesdropper would be able to deduce some information from a pattern in the coded message if the same key had been used before. A further problem is that the key has to be exactly as long as the message, which makes it more difficult to distribute the key securely.

In 1923 Arthur Scerbius invented the Enigma machine [d]. Eventually the German government took over the patent and improved the machine to create the TYPEX machine used in the Second World War. The machine consisted of five rotors that changed the letters of the alphabet. Reversing the process could decrypt the message. The coding of the Enigma machine was broken in the 1930s by the Polish mathematician, Marian Rejewski [a]. The rotor-based Enigma was used as the basis for many encryption machines, but all of them have been compromised.

An example of where spoken – and written – language was used as an encryption device is the Navajo windtalkers used by the American military in the Second World War in 1942 [d]. These were Native American soldiers that communicated messages in their native language – a language so complex that the enemy could not understand the messages.

Between 1943 and 1945, the first general purpose electronic computer, the Electronic Numerical Integrator and Computer, referred to as ENIAC was built [e]. The people who designed this breakthrough technology were John Mauchly, J. Presper Eckert and Lieutenant Herman Goldstine [f]. ENIAC was originally designed to assist with complex mathematical functions in World War II and could perform calculations up to a thousand times faster than its predecessor, the mechanical calculator, and marks the start of the modern computer age. For the purpose of this paper, it is accepted that ENIAC was the first computer.

## 4. Modern encryption techniques

The invention of the first computer brought major changes to the existing methods of encryption. It was no longer feasible to develop pen and paper based traditional encryption algorithms as algorithms that

were once difficult to break could be solved within a short space of time using computers. The encryption field had to be re-invented. A new class of encryption techniques, from now on referred to as modern encryption techniques, were thus developed.

Modern encryption techniques are specifically designed for use on computers and no longer concern the written alphabet. The focus is on the use of binary bits.

One of the main problems of traditional encryption techniques was the fact that if you wanted to communicate secretly with more than one person, you would have to have a separate secret language for each person. This would not have been very practical, and scientists were forced to design a new type of algorithm.

The solution was standardised algorithms. The algorithm, and how it worked, would be publicly announced and the secrecy of the message would rely on another factor. Thus the cryptographic key was designed. Every message or transmission has a cryptographic key; sometimes shared by the sender and receiver. This key is used when encrypting and decrypting the message, and without the key no one can decipher the message. The cryptographic key is an important characteristic of modern encryption techniques.

Modern encryption techniques can also be divided into two groups, asymmetrical encryption and symmetrical encryption. The following is a short description of each.

### *4.1 Symmetrical Encryption*

Also known as secret-key encryption, symmetrical cryptosystems require the sender and receiver to have the same secret key. This single key is required for both the encryption and decryption of the message.

A classic among the symmetric ciphers is the Data Encryption Standard known as DES. DES was developed in the 1970s and got the official approval of NIST (The United States National Institute of Standards and Technology) in 1977 [2]. DES uses substitution and permutation to scramble the bits of a message. Today DES is considered to be a weak encryption method since it was compromised by a machine built by the Electronic Frontier Foundation in 1998 [g]. The machine, Deep Crack, used 19-billion keys per second to try to guess the correct key, which was found in 4.5 days. In 1999 an Internet project was able to test 250-billion keys per second, which resulted in DES being cracked in a few hours [2].

Triple DES, also referred to as 3DES, was developed as an improvement to the DES algorithm. It uses up to three keys in succession, together with three different encryption operations and has not been compromised to date.

The successor of 3DES is the Advanced Encryption Standard (AES). AES is based on the Rijndael algorithm that was chosen from a list of contenders by NIST. AES is also bases on transposing the bits of a message in conjunction with the cryptographic key. While DES is still used frequently in governmental and military operations, it will soon be replaced with AES.

The main problem with symmetrical encryption is that if the key is lost, or stolen, the entire transmission can be compromised since the interceptors can immediately decrypt the message with the one key. This leads to another problem which is the distribution of keys. A key must either be communicated in a face-to-face manner, or must be delivered through a very trusted courier. Both methods are inconvenient to both parties as well as putting the method at risk.

### *4.2 Asymmetrical encryption*

Asymmetrical encryption methods, also referred to as Public Key encryption systems, were developed in 1976 by Whitefield Diffie and Martin Hellman [3]. The principle of public key encryption is that both parties, the sender as well as the receiver, have a pair of keys. The one key does not have to be kept secret and is called the public key. The two different keys held by the parties have different uses – one is used for encryption and the other for decryption. The encryption key is the public key, while the decryption key is the "private" key. The private key must be kept secret.

The public and the private key are mathematically related so that anything encrypted with the one can be decrypted with the other. The sender takes the receiver's key, which is publicly available on a website for instance, and encrypts a message. He then sends it to the receiver who will only be able to decrypt the message with his private key. The main advantage of this method is that the sender and receiver do not have to exchange keys at any time.

The first implementation of a public key cryptosystem was developed by Ronald Rivest, Adi Shamir and Leonard Adleman in 1978 and was called the RSA algorithm [1]. RSA uses a one-way function based on the multiplication of prime numbers to determine the key and relies on the fact that is it very difficult to factorise a large number into two prime numbers. The complexity of this mathematical problem increases exponentially the larger the numbers are, and for this reason the key-size of RSA is usually large and slow

to compute. Regardless, RSA is seen as a very secure system and is widely used today, especially for key distribution.

Public key encryption thus solves the key distribution problem of symmetric encryption, but unfortunately not without potential problems. The difficulty of the mathematical functions that public key encryption relies on can be seen as relative. At the moment there does not exist a mathematical algorithm that can factorise a number into prime numbers quickly. But if a mathematician were to develop such an algorithm, the RSA system will be compromised and many institutions that use the algorithm will be vulnerable.

Another issue with public key encryption is the fact that at the moment there does not exist a central certificate authority, only a decentralised model. This poses a problem in that if a sender wants to acquire and authenticate a receiver's public key, he has to do so at a certificate authority. A trust relationship is needed between certificate authorities, or alternately, only one certificate authority should exist.

## 5. Quantum Encryption

In 1984 Giles Brassard and Charles Bennett published a paper, the BB84 protocol, based on an idea of Stephen Weisner proposed in the 1970s, to use quantum mechanics to solve the key distribution problem. The first implementation of the BB84 protocol was developed in 1991, but only for a distance of 32 centimeters [7].

Quantum encryption uses light particles, called photons, to communicate instead of bits. A photon can have one of four orientations, either horizontal, vertical, 45° diagonal and -45° diagonal. Each of these represent a bit: - and / represents a 0; and | and \ represents a 1. Each bit in a message is randomly translated into one of the two orientations connected with that bit. The actual bits are then sent to the receiver via fiber optics. The receiver in turn has two filters: a + (rectilinear) and a x (diagonal) filter. If a vertical or horizontal photon moves through a rectilinear filter its stays the same, but when a diagonal photon moves through it, it will change. These filters are chosen randomly at the receiver end for each photon. Results are created which are kept secret by the receiver. The sequence of filters that were used is sent back to the sender where they are compared to the photons sent. Those locations where the correct filters were used are sent back to the receiver again and the resulting bits are used as the key. The bits that were changed are discarded

Quantum encryption is the first encryption method of its kind. The technology is still in its development phase, although one New York based company MagiQ Technologies claims to have developed the first commercially available quantum encryption system [j]. There are a couple of other companies that are promising working quantum encryption systems shortly.

## 6. Evaluation of encryption techniques

To effectively evaluate encryption techniques, the different encryption techniques must be examined and evaluated according to criteria, especially from a business perspective. Some of the evaluation criteria were taken from the list of specifications that NIST compiled when they evaluated the proposals for the Advanced Encryption Standard [i]. Further criteria were taken from a paper by Bruce Schneier, entitled "Security in the Real World: How to evaluate security technology" [9].

The criteria are as follows:

- **Robustness** – With the advances in technology it is of vital importance that any encryption system is robust enough to withstand the advances in technology. The more an encryption technique relies on mathematics, the less the robustness.
- **Availability** – Some of the encryption techniques discussed have been around for years, but not all are fully functional yet. Those that have been around for some time may have the advantage of being "tried-and-tested", while some organisations are not familiar with others.
- **Integration** [i] – The integration level of an encryption system will depend on how easily it can be integrated at the application level. The encryption technique must be able to be implemented on software and hardware.
- **Distribution** – With present day technology evolving around the Internet and networks, it is important that encryption techniques work on an entire network, not only on a point-to-point basis. When one broadcasts a message through a network all the intended recipients should get the same encrypted, secure message.
- **Time efficiency** [i] – Users expect encryption to be immediate, otherwise the process is cumbersome. The time efficiency of an encryption technique measures how long it takes to encrypt and decrypt information.
- **Flexibility** [i] – The flexibility issues of an encryption technique refer to the use of keys and whether the key lengths are set, or whether different key lengths can be used.
- **Reliance on users** [9] – In many systems, security is based on user-remembered secrets. When a user has to choose a key or a password, he/she usually chooses something that he/she will be able to remember. The issue is whether the encryption techniques will fail if a user has chosen a "bad" password or key.

- **Tested** [9] – Before an encryption technique can be made publicly available for purchasing it has to be tested thoroughly. The amount of testing done in a laboratory or in a public symposium may influence the security of an encryption technique.
- **Governmental support** [9] – In our society, businesses may be inclined to make use of an encryption technique if the government regards it as being secure. Some encryption algorithms have been approved by the government.
- **Security** [i] – The main, and most obvious, criterion for an encryption technique is the security of the algorithm. Has the algorithm been compromised? Is there any reason why the security of the algorithm is doubted? Most organisations invest in encryption techniques to ensure the confidentiality of their information, and this is the deciding factor.

This evaluation will not discuss all the encryption techniques mentioned in this paper, but will rather focus on those encryption techniques that are used at present, or may be used in the future. In Table 1 AES (Advanced Encryption Standard), the public-key system RSA and quantum encryption is compared.

| | **AES** | **RSA** | **Quantum Encryption** |
|---|---|---|---|
| **Robustness** | No | No | Yes |
| **Availability** | Yes | Yes | Somewhat |
| **Integration** | Yes | Yes | No |
| **Distribution** | Yes | Yes | No |
| **Computational efficiency** | Yes | No | Unknown |
| **Flexibility** | Somewhat | Yes | Yes |
| **Reliance on users** | Yes | Yes | No |
| **Tested** | Yes | Yes | Somewhat |
| **Governmental support** | Yes | No | Yes |
| **Security** | Somewhat | Yes | Yes |

*Table 1: Evaluation of encryption techniques*

In this paper, not all the criteria will be discussed in detail, but the following can be explained:

- **Robustness** – At the moment AES and RSA are still considered secure, but they are based on the vulnerability of mathematics. The more advanced technology becomes, the easier it becomes to

solve mathematical problems that were once thought of as unsolvable. Quantum encryption has got nothing to do with mathematics, thus it does not have that specific vulnerability.

- **Distribution** – AES and RSA are used today in widely distributed networks all over the globe where one message can be encoded and simultaneously sent to more than one person. At the moment quantum encryption still only functions on a point-to-point principle where a message can only be sent to a computer directly connected to the sender within a certain distance.
- **Reliance on users** – With AES the user has to decide on a password to construct a key and with RSA there is still some responsibility resting with the user in selecting the public and private keys. In the case of quantum encryption though, the key is constructed entirely by the randomness of physics and the user is not involved in the creation of the key.
- **Governmental support** – AES is supported by the government of the United States as it is seen as the standard in the USA. The government of Great Britain recently declared that they fully support quantum encryption and the further research thereof.

## 8. Conclusion

As seen in the timeline, and in the explanations that followed, there have been many attempts at secure encryption, and most of them are no longer valid. Of those encryption techniques still being used today, the only way to really determine which one is superior is by evaluating and comparing the various methods.

Every encryption technique has its strong points and its vulnerabilities. Where one technique may be lacking in availability, another may be weak in distribution. For example, AES has governmental support, has been thoroughly tested, but may lack robustness in the future. Quantum encryption may solve this problem, as it is not reliant on users, but unfortunately a business will need a new infrastructure and hardware for implementation. This sort of comparison can be made regarding every aspect of the encryption techniques discussed.

Thus for a company to decide on which encryption technique to use, they would have to decide on what they want from the encryption, and if they are willing to compromise on some features to ensure the security of other features.

**List of references**

Listed in the order in which they were referenced:


[1] Whitman, M.E., Mattord, H.J., Principles of Information Security, Thomson Course Technology, 2003

[2] Schneier, B., Secrets & Lies: Digital Security in a Networked World, Wiley Computer Publishing, 1963

[3] Tudor, J.K., Information Security Architecture: An integrated approach to security in the organization, Auerbach Publications, 2000

[4] Gourley, B., Quantum Encryption vs. Quantum Computing: Will the Defense of the Offense Dominate?, SANS Security Essentials GSEC Practical Assignment Version 1.2e, 2001

[5] Atkins, D., Graff, M., Lenstra, A.K. & Leyland, P.C., Advances in Cryptology – ASIACRYPT '94, p. 263 – 277

[6] Shor, P.W., Algorithms for quantum computation: Discrete logarithms and factoring, Proceedings of the 35th Symposium on foundations of Computer Science, 1994, p. 124 – 134

[7] Bennet, C.H., Besette, F., Brassard, G., Salvail, L. & Smolin, J., Experimental quantum cryptography, September 1991

[8] Brylevski, A., Quantum key distribution: Real-time compensation of interferometer phase drift, NTNU, Department of Physical Electronics

[9] Schneier, B., Security in the Real World: How to Evaluate Security Technology, Computer Security Journal, Volume 15, Number 4, 1999


**List of WebPages**

Listed in the order in which they were referenced:


[a] CME's Cryptography Timeline, http://world.std.com/~cme, accessed on 2003-10-15

[b] Obiwan's Deathstar, http://www.deathstar.ch/security/encryption/history, accessed on 2003-10-15

[c] One Stop Information Center on Data Encryption, http://library.thinkquest.org/~27158/history.html, accessed on 2003-10-15

[d] Cryptographic Timeline, http://library.thinkquest.org/28005/flashed/timemachine/timeline.shtml, accessed on 2003-10-15

[e] A Science Odyssey: People and Discoveries: Eniac is Built, www.pbs.org/wgbh/aso/, accessed on 2003-10-22

[f] Eniac's 50th Anniversary: The Birth of the Information Age, http://www.upenn.edu/almanac/v42/n18/eniac.html, accessed on 2003-10-22

[g] Electronic Frontier Foundation, www.eff.org, accessed on 2003-10-03

[h] Quantum Cryptography Tutorial, www.cs.dartmouth.edu/~jford/crypto.html, accessed on 2003-09-17

[i] National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistbul/itl97-02.txt, accessed on 2004-02-23

[j] MagiQ Technologies Announces General Availability of World's First Commercial Quantum Cryptography System, 3 November 2003, http://www.magiqtech.com, accessed on 2004-01-11