Symmetric Key Cryptosystem based on Randomized Block Cipher

S. Aruljothi
Research Scholar, Department of Computer Applications,
Kalasalingam University, Krishnankoil, Srivilliputtur (via),
Tamil Nadu, India, 626 190.
s.aruljothi.p@gmail.com

M. Venkatesulu
Professor & Head, Department of Computer Applications,
Kalasalingam University, Krishnankoil, Srivilliputtur (via),
Tamil Nadu, India, 626 190.
venkatesulu_m2000@yahoo.com

Abstract—**Multimedia data encryption attempts to prevent unauthorized disclosure of confidential multimedia information in transit or storage. Security of multimedia files attracts more and more attention and many encryption methods have been proposed in literature. If we call a multimedia data stream (message) plaintext , the process of transforming the plaintext into unintelligible data stream is referred to as multimedia encryption (MME) where the encrypted message (data stream) is often named ciphertext. The process of transforming the ciphertext back into plaintext is termed decryption. We propose a new block cipher based on randomized key of size n × n where n is the block size and the block undergoes n^2 iterations with the plaintext. Every iteration generates the pseudo cipher text. The encryption process generate the ciphertext C with the help of the randomized key. The decryption apply the key in reverse order on the cipher text, to get back the plain text. This work deals with the problem of efficient multimedia data encryption.**

Keywords- ciphertext, plaintext, encryption, decryption, randomize

I. INTRODUCTION

Everyone has secrets; some have more than others. When it becomes necessary to transmit those secrets from one point to another, it's important to protect the information while it's in transit. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography. In the past, cryptography is heavily used for military applications to keep sensitive information secret from enemies.

Cryptography [3] [10] presents various methods for taking legible, readable data, and transforming it into unreadable data for the purpose of secure transmission, and then using a key to transform it back into readable data when it reaches its destination. The most secure techniques use a mathematical algorithm and a variable value known as a 'key'. Cryptography uses a single key to encrypt i.e. changing data so that it is unrecognizable and useless to an unauthorized person and decrypt a message i.e. changing it back to its original form.

There are several ways of classifying cryptographic algorithms Secret Key Cryptography [1] [7], which uses a single key for both encryption and decryption. Public Key Cryptography, which uses one key for encryption and another for decryption. Hash Functions uses a mathematical transformation to irreversibly "encrypt" information. The goal of cryptography extends beyond merely making data unreadable; it also extends into user authentication, Privacy/confidentiality, Integrity, Non-repudiation.

Symmetric encryption techniques were used to secure information transmitted on public networks. Traditional symmetric cryptographic systems are based on the idea of a shared secret. In such a system, two parties that want to communicate securely first agree in advance on a single "secret key" that allows each party to both encrypt and decrypt messages.

A block cipher [13] [14] is a type of symmetric-key encryption algorithm that transforms a fixed-length block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length. This transformation takes place under the action of a user-provided secret key [13]. Decryption is performed by applying the reverse transformation to the ciphertext block using the same secret key. The fixed length is called the block size, and for many block ciphers, the block size is 64 bits. In this algorithm we use variable block size, the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.

In communications, a code is a rule for converting a piece of information (for example, a letter, word, or phrase) into another form or representation, not necessarily of the same sort. In communications and information processing, encoding is the process by which a source (object) performs this conversion of information into data, which is then sent to a receiver (observer), such as a data processing system. Decoding [2] [5] is the reverse process of converting data, which has been sent by a source, into information.

A key [12] is a piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of plaintext into ciphertext,. Keys are also used in other cryptographic algorithms, such as digital signature schemes and keyed-hash functions (also known as MACs), often used for authentication. For a well-designed algorithm, enciphering the same plaintext

978-1-4244-6949-9/10/$26.00 ©2010 IEEE

but with a different key should produce a totally different ciphertext. Similarly, decrypting should produce the same plaintext.

A random number generator (often abbreviated as RNG) is a computational or physical device designed to generate a sequence of numbers or symbols that lack any pattern, i.e. appear random [4]. Hardware-based systems for random number generation are widely used, but often fall short of this goal, though they may meet some of the statistical tests for randomness intended to ensure that they do not have any easily discernible patterns. The many applications of randomness have led to many different methods for generating random data. These methods may vary as to how unpredictable or statistically random they are, and how quickly they can generate random numbers.

II. Related Studies

Cryptography [6] [17] probably began in or around 2000 B.C. in Egypt, where hieroglyphics were used to decorate the tombs of deceased rulers and kings. These hieroglyphics told the story of the life of the king and proclaimed the great acts of his life. They were purposefully cryptic, but not apparently intended to hide the text. Rather, they seem to have been intended to make the text seem more regal and important. As time went by, these writings became more and more complicated, and eventually the people lost interest in deciphering them.

Cryptanalysis [2] [21] is the practice of changing ciphertext into plaintext without complete knowledge of the cipher. The Arabs were the first to make significant advances in cryptanalysis. An Arabic author, Qalqashandi, wrote down a technique for solving ciphers which is still used today. The technique is to write down all the ciphertext letters and count the frequency of each symbol. Using the average frequency of each letter of the language, the plaintext can be written out. This technique is powerful enough to cryptanalyze any monoalphabetic substitution cipher if enough cyphertext is provided.

In 1628, a Frenchman named Antoine Rossignol helped his army defeat the Huguenots by decoding a captured message. After this victory, he was called upon many times to solve ciphers for the French government. He used two lists to solve his ciphers: "one in which the plain elements were in alphabetical order and the code elements randomized, and one to facilitate decoding in which the code elements stood in alphabetical or numerical order while their plain equivalents were disarranged." When Rossignol died in 1682, his son, and later his grandson, continued his work. By this time, there were many cryptographers employed by the French government.

In 1817, Colonel Decius Wadsworth developed a set of two disks, one inside the other, where the outer disk had the 26 letters of the alphabet, and the numbers 2-8, and the inner disk had only the 26 letters. The disks were geared together at a ratio of 26:33. To encipher a message, the inner disk is turned until the desired letter is at the top position, with the number of turn required for this result transmitted as ciphertext. Because of the gearing, a ciphertext substitution for a character will not repeat itself until all 33 characters for that plaintext letter have been used.

In 1844, the development of cryptography[3] [10] was dramatically altered by the invention of the telegraph. Communication with the telegraph was by no means secure, so ciphers were needed to transmit secret information. The public's interest in cryptography blossomed, and many individuals attempted to formulate their own cipher systems. The advent of the telegraph provided the first instance where a base commander could be in instant communication with his field commanders during battle. Thus, a field cipher was needed. At first, the military used a Vigenere cipher with a short repeating keyword, but in 1863, a solution was discovered by Friedrich W. Kasiski for all periodic polyalphabetic ciphers which upto this time were considered unbreakable, so the military had to search for a new cipher to replace the Vigenere.

In 1859, Pliny Earle Chase, developed what is known as the fractionating or tomographic cipher. A two digit number was assigned to each character of plaintext by means of a table. These numbers were written so that the first numbers formed a row on top of the second numbers. The bottom row was multiplied by nine, and the corresponding pairs are put back in the table to form the ciphertext.

In 1917, the Americans formed the cryptographic organization M I-8. It's director was Herbert Osborne Yardley. They analyzed all types of secret messages, including secret inks, encryptions, and codes. They continued with much success during and after WW1, but in 1929, Herbert Hoover decided to close them down because he thought it was improper to "read others' mail". Yardley was hard pressed to find work during the depression, so to feed his family, he wrote a book describing the workings of M I-8. It was titled "The American Black Chamber", and became a best seller. Many criticized him for divulging secrets and glorifying his own actions during the War. Another American, William Frederick Friedman, worked with his wife, Elizebeth Smith, to become "the most famous husband-and-wife team in the history of cryptology". He developed new ways to solve Vigenere-like ciphers using a method of frequency counts and superimposition to determine the key and plaintext.

In 1948, Shannon published "A Communications Theory of Secrecy Systems". Shannon was one of the first modern cryptographers to attribute advanced mathematical techniques to the science of ciphers. Although the use of frequency analysis for solving substitution ciphers was begun many years earlier, Shannon's analysis demonstrates several important features of the statistical nature of language that make the solution to nearly all previous ciphers very straight forward. Perhaps the most important result of Shannon's famous paper is the development of a measure of cryptographic strength called the 'unicity distance'.

In August 2002 researchers Fuller and Millar discovered a mathematical property of the cipher that, while not an attack, might be exploitable into an attack (the approach may actually has serious consequences for some other algorithms, too). Thus, it's worth staying tuned to future work. A good alternative to AES is the Serpent algorithm, which is slightly

slower but is very resistant to attack. For many applications triple-DES is a very good encryption algorithm; it has a reasonably lengthy key (112 bits), no patent issues, and a very long history of withstanding attacks (it's withstood attacks far longer than any other encryption algorithm with reasonable key length in the public literature, so it's probably the safest publicly-available symmetric encryption algorithm when properly implemented). However, triple-DES is very slow when implemented in software, so triple-DES can be considered ``safest but slowest.'' Twofish appears to be a good encryption algorithm, but there are some lingering questions - Sean Murphy and Fauzan Mirza showed that Twofish has properties that cause many academics to be concerned (though as of yet no one has managed to exploit these properties). MARS is highly resistent to ``new and novel'' attacks [8], but it's more complex and is impractical on small-ability smartcards. Don't use ``double DES'' (using DES twice) - that's subject to a ``man in the middle'' attack that triple-DES avoids. Your protocol should support multiple encryption algorithms, anyway; that way, when an encryption algorithm is broken, users can switch to another one.

For encrypting worthless data, the old DES algorithm has some value, but with modern hardware it's too easy to break DES's 56-bit key using brute force. If you're using DES, don't just use the ASCII text key [12] as the key - parity is in the least (not most) significant bit, so most DES algorithms will encrypt using a key value well-known to adversaries; instead, create a hash of the key and set the parity bits correctly (and pay attention to error reports from your encryption routine). So-called ``exportable'' encryption algorithms only have effective key lengths of 40 bits, and are essentially worthless; in 1996 an attacker could spend $10,000 to break such keys in twelve minutes or use idle computer time to break them in a few days, with the time-to-break halving every 18 months in either case.

Block encryption algorithms [11] [16] can be used in a number of different modes, such as ``electronic code book'' (ECB) and ``cipher block chaining'' (CBC) by H. Gilbert [11]. In nearly all cases, use CBC, and do not use ECB mode - in ECB mode, the same block of data always returns the same result inside a stream, and this is often enough to reveal what's encrypted. Many modes, including CBC mode, require an ``initialization vector'' (IV). The IV doesn't need to be secret, but it does need to be unpredictable by an attacker. Don't reuse IV's across sessions - use a new IV each time you start a session.

There are a number of different streaming encryption algorithms, but many of them have patent restrictions. RC4 was a trade secret of RSA Data Security Inc; it's been leaked since, and no real legal impediment to its use, but RSA Data Security has often threatened court action against users of it (it's not at all clear what RSA Data Security could do, but no doubt they could tie up users in worthless court cases). If you use RC4, use it as intended - in particular, always discard the first 256 bytes it generates, or you'll be vulnerable to attack [10] [15]. SEAL is patented by IBM - so don't use it. SOBER is patented; the patent owner has claimed that it will allow many uses for free if permission is requested, but this creates an impediment for later use. Even more interestingly, block encryption algorithms can be used in modes that turn them into stream ciphers, and users who want stream ciphers should consider this approach (you'll be able to choose between far more publicly-available algorithms).

The cracking of MD5 meant that forged digital certificates could be created to fool Website visitors into thinking a bogus Website was, in fact, legitimate an obvious potential boom for phishing sites. Shortly after the researchers' announcement, VeriSign moved to update all of the certificates it issued using MD5 to SHA-1 DES [18] [20](Data Encryption Standard) is a symmetric cipher defined in Federal Information Processing (FIPS) Standard Number 46 in 1977 as the federal government approved encryption algorithm for sensitive but non-classified information.

DES was developed by IBM and was based upon IBM's earlier Lucifer cipher.DES utilizes a 56-bit key. This key size is vulnerable to a brute force attack using current technology.

A variant of DES [19], Triple DES, provides significantly enhanced security by executing the core DES algorithm three times in a row. The has the effect of making the DES encryption much more difficult to brute force. Triple-DES is estimated to be 2 to the 56th times more difficult to break than DES. Triple DES[18] can still be considered a secure encryption algorithm. Triple DES is also written as 3-DES or 3DES.

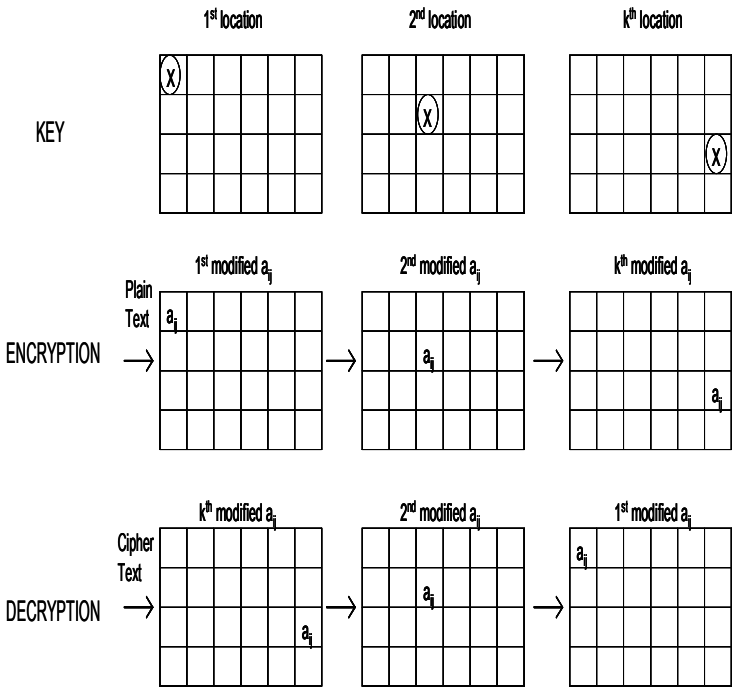
In cryptography [7] [10], RC2 is a block cipher designed by Ron Rivest in 1987. "RC" stands for "Ron's Code" or "Rivest Cipher"; other ciphers designed by Rivest include RC4, RC5 and RC6. RC2 is a 64-bit block cipher with a variable size key. Its 18 rounds are arranged as a source-heavy Feistel network, with 16 rounds of one type (MIXING) punctuated by two rounds of another type (MASHING). A MIXING round consists of four applications of the MIX transformation, as shown in the diagram.

The development of RC2 was sponsored by Lotus, who was seeking a custom cipher that, after evaluation by the NSA, could be exported as part of their Lotus Notes software. The NSA suggested a couple of changes, which Rivest incorporated. After further negotiations, the cipher was approved for export in 1989. Along with RC4, RC2 with a 40-bit key size was treated favourably under US export regulations for cryptography. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts by Y. Lu and S. Vaudenay [8].

III. Methodology

A novel methodology is proposed to achieve encryption by controlling certain operations in the data using a randomized key. The key is an $n \times n$ matrix positions generated with the help of randomize function without duplication. Every iteration generates a pseudo cipher text. The block size could be any value. The encryption process generates the ciphertext C the $m \times m$ matrix. The decryption process undergoes n^2 iterations using key and C to get the plaintext.

Figure 1. Block diagram



A. Algorithm

1) Step 1: Randomized key generation

Generate a pair of values (i,j) randomly, 1<=i<=m, 1<=j<=m, such that no pair (i,j) is repeated more than once.

Let K denote the collection of pairs (i,j) stored as per the order of generation.

2) Step 2: Encryption

Let p be a plaintext of size n.

Let a = n(mod m²).

If a = 0 set k = n/m² else set k = n/m² + 1.

The plaintext p is divided in to k blocks, say $p_1,p_2,---,p_k$, such that the first m entries of p form the first row of p_1, second m elements the second row of p_1 and so on.

Similarly we define $p_2,p_3,---,p_k$.

If a $\neq$ 0 then we add the require number of zeros at the end of the plaintext, so that the last block p_k is of order m $\times$ m.

For l = 1,…,k.

Let a_{ij} be the (i,j)th element of p_l.

Change a_{ij} as per the generation order of the pair(i,j) as follows,

$$\hat{a}_{ij} = \left(\sum_{r=1}^{n} a_{rj} + \sum_{s=1}^{n} a_{is} - a_{ij} \right)$$

If $\hat{a}_{ij}$ (mod 2) = 0, set a_{ij}= 1 else set a_{ij} = 0.

Let cl be the m × m matrix with the modified a_{ij}.

c1 is the ciphertext corresponding to p_1.

3) Step 3: Decryption

For l = 1,---,k.

Let a_{ij} be the (ij)th element of cl.

Change aij as per the reverse order of generation of the pair (i,j) as follows,

$$\hat{a}_{ij} = \left(\sum_{r=1}^{n} a_{rj} + \sum_{s=1}^{n} a_{is} - a_{ij} \right)$$

If $\hat{a}_{ij}$ (mod 2) = 0, set a_{ij} = 1 else set a_{ij} = 0.

The (a_{ij}) = pl, the original plaintext block.

The plaintext p = $p_1,p_2,---,p_k$.

IV. Experimental Results

As a result of the widespread use of image, audio, and video data, protecting media content is becoming increasingly necessary. The algorithm uses the experimental environment, CPU: Intel(R) core(TM)2 DVOE7200 @ 2.53GHz, 0.99 GB of RAM; Operating System: Windows XP Professional.

A. Results: Block size : 8 bits

TABLE I. COMPARISON OF DIFFERENT FILE FORMATS

FILE TYPE & SIZE	TIME FOR ENCRYPTION	TIME FOR DECRYPTION
Txt,1kb	78ms	63ms
Doc,551kb	1secs 360 ms	1secs 47 ms
Bmp,14.3kb	141 ms	143 ms
Jpeg,1.69mb	3 secs 469 ms	3 secs 266ms
Pdf,245kb	562 ms	531 ms
Xls,29kb	141 ms	125 ms
Mp3,50.3kb	171 ms	128 ms
Wav,45.3mb	36 secs	35 secs
Vob,62.8mb	47 secs	46 secs

A VOB file (Video Object) is a container format in DVD-Video media [9]. VOB can contain video, audio, subtitle and menu contents multiplexed together into a stream form. VOB is based on MPEG-2 Program stream format, but with additional limitations and specifications in the private streams.The MPEG-2 Program stream has provisions for non-standard data (as used in VOB files) in the form of so-called private streams. VOB files are a very strict subset of the MPEG-2 Program stream standard. While all VOB files are MPEG-2 Program streams, not all MPEG-2 Program streams comply with the definition for a VOB file.

File format: video file
File size:62.8mb
Play time: 3mts

TABLE II. COMPARISON OF DIFFERENT FILE FORMATS

BLOCK SIZE ***(BITS)***	**TIME FOR ENCRYPTION**	**TIME FOR DECRYPTION**
8	47 secs	46 secs
16	1 min 10 secs	1 min 9 secs
32	1 min 31 secs	1 min 30 secs
64	2 min 35 secs	2 min 34 secs

V. CONCLUSION

The traditional approaches which encrypt the general data directly are not suitable for the special nature of multimedia data. The multimedia data requires the application of security in order to protect the privacy of its contents. The encryption of files is among the simplest ways employed in protecting the contents of a document from being accessed without authorization. So many new encryption approaches have merged to overcome shortcomings and provide confidentiality. In this paper we developed a novel dynamic cryptographic key generation scheme for multimedia data encryption..

REFERENCES

[1] M. Bellare and P. Rogaway, “Robust computational secret sharing and a unified account of classical secret-sharing goals”, Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS), ACM, 2007.

[2] J. Zhou, Z. Liang, Y. Chen, and O. C. Au, “Security analysis of multimedia encryption schemes based on multiple Huffman table”, IEEE Signal Processing Letters, vol. 14, no. 3, pp. 201– 204, 2007.

[3] M. Bellare, A. Boldyreva and A. O'Neill, “Deterministic and efficiently searchable encryption”, Advances in Cryptology - Crypto 2007 Proceedings, Lecture Notes in Computer Science Vol. 4622, A. Menezes ed, Springer-Verlag, 2007.

[4] Elaine Barker and John Kelsey, “Recommendation for Random Number Generation Using Deterministic Random Bit Generators”, NIST Special Publication 800-90. Revised March 2007.

[5] M. Grangetto, E. Magli and G. Olmo, “Multimedia selective encryption by means of randomized arithmetic coding”, IEEE Transactions on Multimedia, vol. 8, no. 5, 2006.

[6] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier and H. Shi, “Searchable Encryption Revisited: Consistency Properties”, Relation to Anonymous IBE, and Extensions. Advances in Cryptology - Crypto 2005 Proceedings, Lecture Notes in Computer Science Vol. 3621, V. Shoup ed, Springer-Verlag, 2005.

[7] K. Pietrzak, M. Bellare and P. Rogaway, “Improved Security Analyses for CBC MACs”, Advances in Cryptology - Crypto 2005 Proceedings, Lecture Notes in Computer Science Vol. 3621, Springer-Verlag, 2005.

[8] Y. Lu and S. Vaudenay, “Faster correlation attack on Bluetooth keystream generator E0. In M. Franklin, editor, Advances in Cryptology - Crypto 2004, 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004. Proceedings, volume 3152 of Lecture Notes in Computer Science, pages 407 - 425. Springer-Verlag, 2004.

[9] L. S. Choon, A. Samsudin, and R. Budiarto, “Lightweight and cost-effective MPEG video encryption, in Proc. of Information and Communication Technologies”, From Theory to Applications, 2004, pp. 525–526.

[10] B. Canvel, A. Hiltgen, S. Vaudenay, and M. Vuagnoux,”Password interception in a SSL/TLS channel”, In D. Boneh, editor, Advances in Cryptology - Crypto 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, volume 2729 of Lecture Notes in Computer Science, pages 583-599. Springer-Verlag, 2003.

[11] H. Gilbert, “The Security of One-Block-to-Many Modes of Operation”, In Thomas Johansson (Ed.) Fast Software Encryption - FSE 2003, Lecture Notes in Computer Science, Springer-Verlag, 2003.

[12] M. Bellare and B. Yee, “Forward-Security in Private-Key Cryptography”, Topics in Cryptology - CT-RSA 03, Lecture Notes in Computer Science Vol. 2612, M. Joye ed, Springer-Verlag, 2003.

[13] H. Gilbert and M. Minier, “New results on the pseudorandomness of some block cipher constructions”, In M. Matsui (Ed.) Fast Software Encryption - FSE 2001, Lecture Notes in Computer Science 2355, Springer-Verlag, 2002, 248–266.

[14] P. Rogaway, M. Bellare, J. Black and T. Krovetz, “OCB: A block-cipher mode of operation for efficient authenticated encryption”, Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS), ACM, 2001.

[15] J. Kelsey, Bruce Schneier, David Wagner, and C. Hall, “Cryptanalytic Attacks on Pseudorandom Number Generators, Fast Software Encryption”, Fifth International Workshop Proceedings (March 1998), Springer-Verlag, 1998, pp. 168-188.

[16] Mitsuru Matsui, “The First Experimental Cryptanalysis of the Data Encryption Standard”. In Advances in Cryptology Proceedings of CRYPTO ’94, Lecture Notes in Computer Science 839, Springer-Verlag, 1994.

[17] Alfred J.Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

[18] Christof Paar and Jan Pelzl, "The Advanced Encryption Standard", Chapter 4 of "Understanding Cryptography, A Textbook for Students and Practitioners". Springer, 2009.

[19] Diffie, Whitfield and Martin Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard" IEEE Computer 10(6), June 1977, pp74–84.

[20] John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, and Doug Whiting, “Improved Cryptanalysis of Rijndael”, Fast Software Encryption, 2000 pp213–230.

[21]] M. Hellman, R.Merkle, R. Schroeppel, L.Washington, W. Diffie, S. Pohlig, and P. Schweitzer, “Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard”. Technical Report SEL 76-042, Department of Electrical Engineering, Stanford University, 1976.