ISSN: 2456-9348
Vol (02) _Issue (11) Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management

MODERN CRYPTOGRAPHY TECHNIQUES FOR INCREASE NETWORK SECURITY

Solmazsharifnia*
*Department of Mathematics, Shahed University, Tehran, Iran
s_sharifnia@yahoo.com

ABSTRACT
Network Security & Cryptography is a concept to protect network and data transmission over wireless network.Data Security is the main aspect of secure data transmission over unreliable network. Network security involves theauthorization of access to data in a network, which is controlled by the network administrator. Users choose or are assignedan ID and password or other authenticating information that allows them access to information and programs within theirauthority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobsconducting transactions and communications among businesses, government agencies and individuals. Networks can beprivate, such as within a company, and others which might be open to public access. Network security is involved inorganizations, enterprises, and other types of institutions. In this paper we also studied cryptography along with itsprinciples. Cryptographic systems with ciphers are described.The cryptographic models and algorithms are outlined.

Keywords:
Encryption, Decryption, Security,Cryptograghy,Cipher, Network Blocks

INTRODUCTION

Today's our entire globe is depending on internet and its application for their every part of life. Here comes the requirement of securing our data by ways of Cryptography. Cryptography plays a major role in a science of secret writing. It is the art of protecting information by transforming and technology application. The main reason for using email is probably the convenience and speed with which it can be transmitted, irrespective of geographical distance. Now a day's our entire globe is depending on internet and its application to protecting national security. Cryptography is used to ensure that the contents of a message are very confidentiality transmitted and would not be altered.

Cryptography provides number of security goals to ensure of privacy of data, on-alteration of data and so on. The idea of encryption and encryption algorithm by which we can encode our data in secret code and not to be able readable by hackers or unauthorized person even it is hacked. The main reason for not using encryption in email communications is that current email encryption solutions and hard key management.

Different encryption techniques for promoting the information security. The evolution of encryption is moving towards a future of endless form of possibilities. As it is impossible to stop hacking, we can secure our sensitive data even it is hacked using encryption techniques and which protecting the information security. In this paper we present a survey paper on cryptographic techniques based on some algorithm and which is suitable for many applications where security is main concern

II. LITERATURE REVIEW

Some of the concepts are used in Cryptography are mentioned here [1]:

2.1 Purpose of Cryptography

Authentication: Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified.

Confidentiality: The principle of confidentiality specifies that only the sender and the intended recipient should be able to process the contents of a message.

Availability: The principle of availability states that resources should be available to authorized parties all the times.

iJETRM
International Journal of Engineering Technology Research & Management

Integrity: The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.

Access Control: Access Control specifies and controls who can access the process.

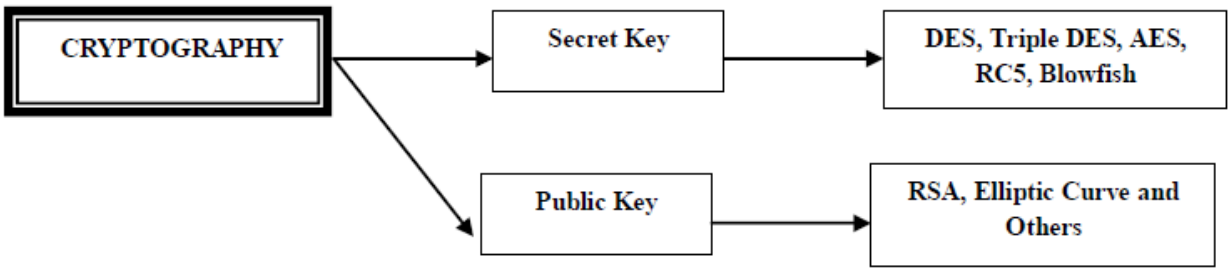

Fig.1. Classification of Cryptography

2.2 Types of Cryptography

Secret Key Cryptography: When the same key is used for both encryption and decryption, DES, Triple DES, AES, RC5 and etc., may be the examples of such encryption, then that mechanism is known as secret key cryptography.

Public Key Cryptography: When two different keys are used, that is one key for encryption and another key for decryption, RSA, Elliptic Curve and etc., may be the examples of such encryption, then that mechanism is known as public key cryptography.

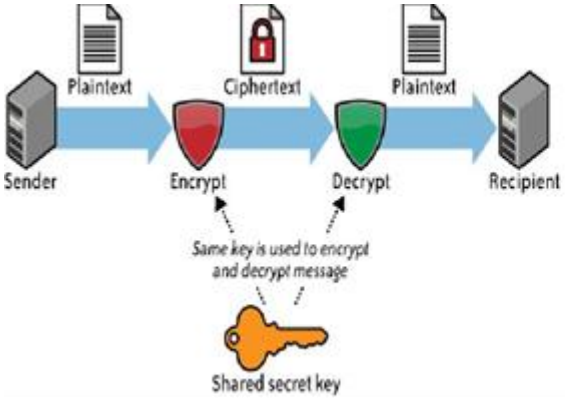

Fig.2. Secret Key Cryptography

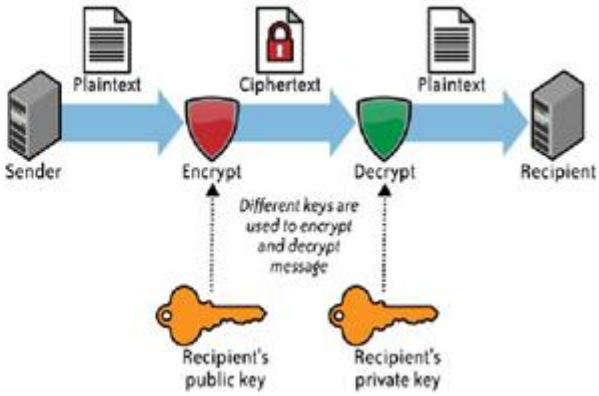

Fig.3. Public Key Cryptography

iJETRM
International Journal of Engineering Technology Research & Management

2.3 Cryptography

Plain Text: Any communication in the language that we use in the human language, takes the form of plain text. It is understood by the sender and the recipient and also by anyone who gets an access to that message.

Cipher Text: Cipher means a code or a secret message. When a plain text is codified using any suitable scheme the resulting message is called as cipher text.

Key: An important aspect of performing encryption and decryption is the key. It is the key used for encryption and decryption that makes the process of cryptography secure.

2.4Certificateless Public Key Cryptography

The concept of Certificate-less Public Key Cryptography (CL-PKC) is introduced by Al-Riyami and Paterson [1] in 2003, to overcome the key escrow problem of Identity Based Cryptography. In CL-PKC, a trusted third party, called the Key Generation Center (KGC), supplies a user with partial private key. While compared to identity based public key cryptography (IDPKC), the trust assumptions regarding the trusted third party in this scheme are significantly reduced. Using this scheme, the replacement of a public key of a user in the system by the KGC is equivalent to certificate by PKI system.

III. RELATED WORKS

3.1 DES

DES is a block cipher that uses shared secret key for encryption and decryption. DES algorithm as described by Davis R [2] takes a fixed length of string in plaintext bits and transforms it through a series of operations into cipher text bit sting of the same length and its each block is 64 bits.
There are 16 identical stages of processing, termed rounds. There is also an initial and final permutation which named as IP and FP

3.2 3DES

3DES is an enhancement of DES and it is 64 bit block size with 192 bits key size. In this standard the encryption of method is similar to the one in the original DES and increase the encryption level and the average safe time.
In 3DES is slower than other block cipher methods. It uses either two or three 56 bit keys in the sequence order of Encrypt-Decrypt-Encrypt.
TDES algorithm with three keys require 2^{168} chances of combinations and with two keys requires 2^{112} combinations; and the disadvantage of this algorithm is too time consuming problem.

3.3 AES

In AES [3] is the almost identical of block cipher Rijndael cipher developed by two Belgian cryptographers, Joan and Vincent Rijmen. The algorithm explains about by AES is a secret-key algorithm which means of the same key is used for both encrypting and decrypting the data.
AES on the other hand which encrypts all 128 bits in one iteration. This is one reason why it has a comparably small number of rounds. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices

3.4 GOST

The GOST block cipher (Magma), defined in the standard GOST 28147-89 (RFC 5830), is a Soviet and Russian government standard symmetric key block cipher with a block size of 64 bits. The original standard, published in 1989, did not give the cipher any name, but the most recent revision of the standard, GOST R 34.12-2015, specifies that it may be referred to as Magma. The GOST hash function is based on this cipher. The new standard also specifies a new 128-bit block cipher called Kuznyechik.

Developed in the 1970s, the standard had been marked "Top Secret" and then downgraded to "Secret" in 1990. Shortly after the dissolution of the USSR, it was declassified and it was released to the public in 1994. GOST 28147 was a Soviet alternative to the United States standard algorithm, DES[4] Thus, the two are very similar in structure.

iJETRM
International Journal of Engineering Technology Research & Management

3.5 FEAL

In cryptography, FEAL (the Fast data EnciphermentALgorithm) is a block cipher proposed as an alternative to the Data Encryption Standard (DES), and designed to be much faster in software. The Feistel based algorithm was first published in 1987 by Akihiro Shimizu and Shoji Miyaguchi from NTT. The cipher is susceptible to various forms of cryptanalysis, and has acted as a catalyst in the discovery of differential and linear cryptanalysis.

There have been several different revisions of FEAL, though all are Feistel ciphers, and make use of the same basic round function and operate on a 64-bit block. One of the earliest designs is now termed FEAL-4, which has four rounds and a 64-bit key.

Problems were found with FEAL-4 from the start: Bert den Boer related a weakness in an unpublished rump session at the same conference where the cipher was first presented. A later paper (den Boer, 1988) describes an attack requiring 100–10000 chosen plaintexts, and Sean Murphy (1990) found an improvement that needs only 20 chosen plaintexts. Murphy and den Boer's methods contain elements similar to those used in differential cryptanalysis.

The designers countered by doubling the number of rounds, FEAL-8 (Shimizu and Miyaguchi, 1988). However, eight rounds also proved to be insufficient — in 1989, at the Securicom conference, Eli Biham and Adi Shamir described a differential attack on the cipher, mentioned in (Miyaguchi, 1989). Gilbert and Chassé (1990) subsequently published a statistical attack similar to differential cryptanalysis which requires 10000 pairs of chosen plaintexts.

In response, the designers introduced a variable-round cipher, FEAL-N (Miyaguchi, 1990), where "N" was chosen by the user, together with FEAL-NX, which had a larger 128-bit key. Biham and Shamir's differential cryptanalysis (1991) showed that both FEAL-N and FEAL-NX could be broken faster than exhaustive search for $N \leq 31$. Later attacks, precursors to linear cryptanalysis, could break versions under the known plaintext assumption, first (Tardy-Corfdir and Gilbert, 1991) and then (Matsui and Yamagishi, 1992), the latter breaking FEAL-4 with 5 known plaintexts, FEAL-6 with 100, and FEAL-8 with 2^{15}.

In 1994, Ohta and Aoki presented a linear cryptanalytic attack against FEAL-8 that required 2^{12} known plaintexts.

3.6 IDEA

In cryptography, the International Data Encryption Algorithm (IDEA), originally called Improved Proposed Encryption Standard (IPES), is a symmetric-key block cipher designed by James Massey of ETH Zurich and Xuejia Lai and was first described in 1991. The algorithm was intended as a replacement for the Data Encryption Standard (DES). IDEA is a minor revision of an earlier cipher Proposed Encryption Standard (PES).

The cipher was designed under a research contract with the Hasler Foundation, which became part of Ascom-Tech AG. The cipher was patented in a number of countries but was freely available for non-commercial use. The name "IDEA" is also a trademark. The last patents expired in 2012, and IDEA is now patent-free and thus completely free for all uses.[5][6]

IDEA was used in Pretty Good Privacy (PGP) v2.0 and was incorporated after the original cipher used in v1.0, BassOmatic, was found to be insecure.[7] IDEA is an optional algorithm in the OpenPGP standard.

3.7 Blowfish

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention, and Schneier recommends Twofish for modern applications.[8]

Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public

domain, and can be freely used by anyone."[9]

Notable features of the design include key-dependent S-boxes and a highly complex key schedule.

3.8 Twofish

In cryptography, Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Twofish is related to the earlier block cipher Blowfish.
Twofish's distinctive features are the use of pre-computed key-dependent S-boxes, and a relatively complex key schedule. One half of an n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent S-boxes). Twofish borrows some elements from other designs; for example, the pseudo-Hadamardtransform (PHT) from the SAFER family of ciphers. Twofish has a Feistel structure like DES. Twofish also employs a Maximum Distance Separable matrix.

Back in 2000, on most software platforms Twofish was slightly slower than Rijndael (the chosen algorithm for Advanced Encryption Standard) for 128-bit keys, but somewhat faster for 256-bit keys. But after Rijndael was chosen as the Advanced Encryption Standard, Twofish has become much slower than Rijndael on the CPUs that support the AES instruction set.[10]

Twofish was designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson; the "extended Twofish team" who met to perform further cryptanalysis of Twofish and other AES contest entrants included Stefan Lucks, Tadayoshi Kohno, and Mike Stay.

The Twofish cipher has not been patented and the reference implementation has been placed in the public domain. As a result, the Twofish algorithm is free for anyone to use without any restrictions whatsoever. It is one of a few ciphers included in the OpenPGP standard (RFC 4880). However, Twofish has seen less widespread usage than Blowfish, which has been available longer.

3.9 Threefish

Threefish is a symmetric-key tweakable block cipher designed as part of the Skein hash function, an entry in the NIST hash function competition. Threefish uses no S-boxes or other table lookups in order to avoid cache timing attacks;[11] its nonlinearity comes from alternating additions with exclusive ORs. In that respect, it is similar to Salsa20, TEA, and the SHA-3 candidates CubeHash and BLAKE.
Threefish and the Skein hash function were designed by Bruce Schneier, Niels Ferguson, Stefan Lucks, Doug Whiting, MihirBellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker.

3.10 RC

The RC algorithms are a set of symmetric-key encryption algorithms invented by Ron Rivest. The "RC" may stand for either Rivest's cipher or, more informally, Ron's code. Despite the similarity in their names, the algorithms are for the most part unrelated. There have been six RC algorithms so far:
RC1 was never published.

RC2 was a 64-bit block cipher developed in 1987.

RC3 was broken before ever being used.

RC4 is the world's most widely used stream cipher.

RC5 is a 32/64/128-bit block cipher developed in 1994.

RC6, a 128-bit block cipher based heavily on RC5, was an AES finalist developed in 1997

3.11 RC5

In cryptography, RC5 is a symmetric-key block cipher notable for its simplicity. Designed by Ronald Rivest in 1994,[12] RC stands for "Rivest Cipher", or alternatively, "Ron's Code" (compare RC2 and RC4). The Advanced Encryption Standard (AES) candidate RC6 was based on RC5.
Unlike many schemes, RC5 has a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number

of rounds (0 to 255). The original suggested choice of parameters were a block size of 64 bits, a 128-bit key and 12 rounds.

3.12 RC6

In cryptography, RC6 (Rivest cipher 6) is a symmetric key block cipher derived from RC5. It was designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin to meet the requirements of the Advanced Encryption Standard (AES) competition. The algorithm was one of the five finalists, and also was submitted to the NESSIE and CRYPTREC projects. It was a proprietary algorithm, patented by RSA Security.
RC6 proper has a block size of 128 bits and supports key sizes of 128, 192, and 256 bits up to 2040-bits, but, like RC5, it may be parameterised to support a wide variety of word-lengths, key sizes, and number of rounds. RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition, and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes, although RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits

3.13 CAST-128

In cryptography, CAST-128 (alternatively CAST5) is a symmetric-key block cipher used in a number of products, notably as the default cipher in some versions of GPG and PGP. It has also been approved for Government of Canada use by the Communications Security Establishment. The algorithm was created in 1996 by Carlisle Adams and Stafford Tavares using the CAST design procedure.[13]
Another member of the CAST family of ciphers, CAST-256 (a former AES candidate) was derived from CAST-128. According to some sources, the CAST name is based on the initials of its inventors, though Bruce Schneier reports the authors' claim that "the name should conjure up images of randomness".[14]

CAST-128 is a 12- or 16-round Feistel network with a 64-bit block size and a key size of between 40 and 128 bits (but only in 8-bit increments). The full 16 rounds are used when the key size is longer than 80 bits.[15]

Components include large 8×32-bit S-boxes based on bent functions, key-dependent rotations, modular addition and subtraction, and XOR operations. There are three alternating types of round function, but they are similar in structure and differ only in the choice of the exact operation (addition, subtraction or XOR) at various points.

Although Entrust holds a patent on the CAST design procedure, CAST-128 is available worldwide on a royalty-free basis for commercial and non-commercial uses.

3.14 MARS

MARS is a block cipher that was IBM's submission to the Advanced Encryption Standard process. MARS was selected as an AES finalist in August 1999, after the AES2 conference in March 1999, where it was voted as the fifth and last finalist algorithm.
The MARS design team included Don Coppersmith, who had been involved in the creation of the previous Data Encryption Standard (DES) twenty years earlier. The project was specifically designed to resist future advances in cryptography by adopting a layered, compartmentalized approach.

IBM's official report stated that MARS and Serpent were the only two finalists to implement any form of safety net with regard to would-be advances in cryptographic mathematics. The Twofish team made a similar statement about its cipher.[16]

MARS has a 128-bit block size and a variable key size of between 128 and 448 bits (in 32-bit increments). Unlike most block ciphers, MARS has a heterogeneous structure: several rounds of a cryptographic core are "jacketed" by unkeyed mixing rounds, together with key whitening

3.15 Serpent

Serpent is a symmetric key block cipher that was a finalist in the Advanced Encryption Standard (AES) contest, where it was ranked second to Rijndael. Serpent was designed by Ross Anderson, Eli Biham, and Lars Knudsen. Like other AES submissions, Serpent has a block size of 128 bits and supports a key size of 128, 192 or 256 bits.[17] The cipher is a 32-round substitution–permutation network operating on a block of four 32-bit words. Each round applies one of eight 4-bit to 4-bit S-boxes 32 times in parallel. Serpent was designed so that all operations can be executed in parallel, using 32 bit slices. This maximizes parallelism, but also allows use of the

extensive cryptanalysis work performed on DES.

Serpent took a conservative approach to security, opting for a large security margin: the designers deemed 16 rounds to be sufficient against known types of attack, but specified 32 rounds as insurance against future discoveries in cryptanalysis. The official NIST report on AES competition classified Serpent as having a high security margin along with MARS and Twofish, in contrast to the adequate security margin of RC6 and Rijndael (currently AES).[18] In final voting, Serpent had the least number of negative votes among the finalists, but scored second place overall because Rijndael had substantially more positive votes, the deciding factor being that Rijndael allowed for a far more efficient software implementation.

The Serpent cipher algorithm is in the public domain and has not been patented.[19] The reference code is public domain software and the optimized code is under GPL.[20] There are no restrictions or encumbrances whatsoever regarding its use. As a result, anyone is free to incorporate Serpent in their software (or hardware implementations) without paying license fees.

3.16 Camellia

In cryptography, Camellia is a symmetric key block cipher with a block size of 128 bits and key sizes of 128, 192 and 256 bits. It was jointly developed by Mitsubishi Electric and NTT of Japan. The cipher has been approved for use by the ISO/IEC, the European Union's NESSIE project and the Japanese CRYPTREC project. The cipher has security levels and processing abilities comparable to the Advanced Encryption Standard.[21]
The cipher was designed to be suitable for both software and hardware implementations, from low-cost smart cards to high-speed network systems. It is part of the Transport Layer Security (TLS),[22] cryptographic protocol designed to provide communications security over a computer network such as the Internet.

Camellia is a Feistel cipher with either 18 rounds (when using 128-bit keys) or 24 rounds (when using 192- or 256-bit keys). Every six rounds, a logical transformation layer is applied: the so-called "FL-function" or its inverse. Camellia uses four 8×8-bit S-boxes with input and output affine transformations and logical operations. The cipher also uses input and output key whitening.

3.17 RSA

RSA is a public key algorithm invented by Rivest, Shamir, Adleman [23]. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages.
Messages encrypted with the public key can only be decrypted using the private key. These keys for the RSA algorithm are generated in many ways.

iJETRM
International Journal of Engineering Technology Research & Management

Comparison of Cryptography Algorithms

Algorithm	Created by	Key size (in bits)	Blok size (in bits)
DES	IBM in year 1975	56	64
3 DES	IBM in year 1978	112 (or) 168	64
AES	Joan Daemen and Vincent Rijmen in year 1998	256	128
GOST	Ussr,KGB,8th Department in year 1994	256	64
FEAL	Akihiro shimizu and shoji miyaguchi(NTT) FEAL-4 in 1987, FEAL N/NX in 1990	64(FEAL),128(FEAL-NX)	64
IDEA	Xuejia lai and james masseg	128	64
BLOWFISH	Bruce schneier in year 1993	32 (or) 448	64
TOWFISH	Bruce schneier in year 1998	128,192, or 256	128
THREEFISH	Bruce Schneier,Niels Ferguson,Stefan Lucks,Doug whiting,Mihir Bellare,Tadagoshi Kohno,Jon callas,Tesse walker	256,512 or 1024	256,512 or 1024
RC	Ron Rivest	64 (RC2)	64 (RC2)
RC5	Ron Rivest in year 1994	0 to 2040(128suggested)	32,64 or 128(64suggested)
RC6	Ron Rivest,Matt Robshaw Ray Sidney,Yiqun lisa yin in year 1998	128,192 or 256	128
CAST-128	Carlisle Adams and Stafford Tavares in year 1996	40 to 128	64
MARO	IBM in year 1998	128,192 or 256	128
SERPENT	Ross Anderson,Eli Biham,Lars Knudsen in year 1998	128,192 or 256	128
CAMELLIA	Mitsubishi Electric,NTT in year 2000	128,192 or 256	128

Table1.Cryptograghy Algorithms – A Comparision

IV. CONCLUSION

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together. We have studied various cryptographic techniques to increase the security of network. Cryptography, together with suitable communication protocols, can provide a high degree of protection in digital communications against intruder attacks as far as the communication between two different computers is concerned.

REFERENCES

[1] A. R. Sattam and P. Kenneth, “Certificateless public key cryptography a full version”, in Asiacrypt’03, LNCS 2894, Springer, 20, 452-473, 2003.
[2] Davis.R, “The Data Encryption Standard in Perspective”, Proceeding of Communication Society magazine, IEEE, Vol 16, Nov 1978.
[3] Daemen.J and Rijmen, The Advanced Encryption Standard, Dr. Dobb’s Journal, March 2001.
[4] Fleischmann, Ewan; Gorski, Michael; Hühne, Jan-Hendrik; Lucks, Stefan (2009)."Key Recovery Attack on Full GOST Block Cipher with Zero Time and Memory".Published as ISO/IEC JTC.1.
[5] "Espacenet - BibliografischeDaten" (in German). Worldwide.espacenet.com. Retrieved 2013-06-15.

[6] "Espacenet - BibliografischeDaten" (in German). Worldwide.espacenet.com. Retrieved 2013-06-15.
[7] Garfinkel, Simson (December 1, 1994), PGP: Pretty Good Privacy, O'Reilly Media, pp. 101–102, ISBN 978-1-56592-098-9.
[8] Dahna, McConnachie (2007-12-27). "Bruce Almighty: Schneier preaches security to Linux faithful". Computerworld.p. 3.Archived from the original on 2016-12-02.Retrieved 2018-01-26. At this point, though, I'm amazed it's still being used. If people ask, I recommend Twofishinstead.
[9] Bruce Schneier (1993)."Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)". Fast Software Encryption, Cambridge Security Workshop Proceedings.Springer-Verlag: 191–204. Archived from the original on 2014-01-26.ad.
[10] Bruce Schneier; Doug Whiting (2000-04-07)."A Performance Comparison of the Five AES Finalists" (PDF/PostScript).Retrieved 2013-01-14.
[11] Ferguson; et al. (2010-10-01)."The Skein Hash Function Family" (PDF).The paper in which Threefish was introduced.
[12] Rivest, R. L. (1994). "The RC5 Encryption Algorithm" (pdf).Proceedings of the Second International Workshop on Fast Software Encryption (FSE) 1994e. pp. 86–96.
[13] Carlisle M. Adams (1997)."Constructing Symmetric Ciphers Using the CAST Design Procedure" (PDF). Designs, Codes, and Cryptography (12): 283–316.
[14] Bruce Schneier (1996). Applied Cryptography, (2nd ed.). John Wiley & Sons. pp. 334–335. ISBN 0-471-11709-9.
[15] Carlisle M. Adams (1997-05-12)."CAST Design Procedure Addendum" (PDF). Entrust.
[16] NIST (2000), Report on the Development of the Advanced Encryption Standard (AES) (PDF), NIST.
[17] Ross J. Anderson (2006-10-23)."Serpent: A Candidate Block Cipher for the Advanced Encryption Standard". University of Cambridge Computer Laboratory.Retrieved 2013-01-14.
[18] NIST (2000), Report on the Development of the Advanced Encryption Standard (AES) (PDF), NIST.
[19] Serpent Holds the Key to Internet Security – Finalists in world-wide encryption competition announced (1999).
[20] SERPENT – A Candidate Block Cipher for the Advanced Encryption Standard "Serpent is now completely in the public domain, and we impose no restrictions on its use. This was announced on the 21st August at the First AES Candidate Conference. The optimised implementations in the submission package are now under the General Public License (GPL), although some comments in the code still say otherwise. You are welcome to use Serpent for any application. If you do use it, we would appreciate it if you would let us know!" (1999).
[21] "News Release 050710: Japan's First 128-bit Block Cipher "Camellia" Approved as a New Standard Encryption Algorithm in the Internet". NTT. July 20, 2005.
[22] RFC 4132 Addition of Camellia Cipher Suites to Transport Layer Security (TLS).
[23] R.L.Rivest, A.Shamir, L.Adleman, "A Method for obtaining Digital Signatures and Public-Key Cryptosystem", Communication of the ACM, Vol 21, Feb 1978.