Volume 2, No. 6, June 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

A PROPORTIONAL ANALYSIS ON CRYPTOGRAPHY TECHNIQUES, FUNCTIONS AND RELATIVE PERFORMANCE ISSUES

Dr. S. N. Panda[1*], Gaurav Kumar[2]

[1]Professor, Regional Institute of Management and Technology [RIMT],Mandi Gobindgarh, Punjab, India
panda.india@gmail.com
[2]Research Scholar, Computer Science Manav Bharti University,Solan, Himachal Pradesh, India
kumargaurav.in@gmail.com

Abstract: Information is flowing in assorted network across the globe via copious channels. The commercial, personal as well defense communication is relying on different protocols for secured data transmission to provide the quality of service as well as confidentiality to the client. A significant research work is going on in the stream of cryptography and secured data transmission and a number of data encryption techniques have been devised to secure the network infrastructure and the trust on service. Cryptology refers to the execution as well as the study of hiding information from different eyes. Now days, cryptography is used in almost many disciplines including mathematics, computer science, and engineering. The applications of cryptography include Smart Cards, ATM Cards, computer passwords, defense communications and electronic commerce. This paper emphasizes on the proportional analysis on different cryptography techniques and their relative performance issues.

Keywords - Asymmetric Encryption, Cryptography, Comparison of Cryptographic Techniques, Data Communication, Hash Function, Network Architecture, Performance of Cryptography Methods, Symmetric Encryption,

INTRODUCTION

The concept of cryptography is not new to the world of information technology. All business establishments are sharing their confidential information through secured channel using encryption and effective cryptography techniques. Moreover, cyber terrorism has become very serious problem across the globe. Terrorism has become a serious problem across the globe. Terrorism is not only concerned with firing of metallic weapons only but also related to the digital threats. Now, new types of weapons are used by the terrorist organizations and these weapons are computer virus, Trojans or digital missiles which can damage the valuable and sensitive infrastructure of any country. Cyber warfare makes use of new type of armaments with various destructive effects on the target. Cyber weapons are usually programs with the objective to defend or attack a target. These e-weapons can be downloaded from the internet but some are kept private or are commercial. In Cyber warfare, there is no major difference between military and civilian infrastructure because non-military targets are also indirectly involved with military establishments. Disrupting the economy or damaging the public infrastructure can wield much larger effect as weapons of mass destruction and therefore it is necessary to build a strategy in order to get the global understanding of what attackers can do.

Since the advent of network applications and secured transactions, numbers of methods are in use to encrypt data streams. These can easily be executed using software applications, but not so simply decrypted in case the original or respective encrypted data stream are unavailable. The paramount encryption techniques have small effect on system performance, and have other benefits including data compression built in. One of the famous PKZIP service provides compression as well as data encryption for data. Moreover, a database management system package also makes use of some cryptography scheme so that a typical File Copy cannot be used to read sensitive information. It needs 'high performance' methods to encode and decode the data.

Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (e.g. RSA and ECC). Public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices. There are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key. DES uses one 64-bits key. Triple DES (3DES) uses three 64-bits keys while AES uses various (128, 192, 256) bits keys. Blowfish uses various (32-448); default 128bits while RC6 is used various (128, 192, 256) bits keys.

,

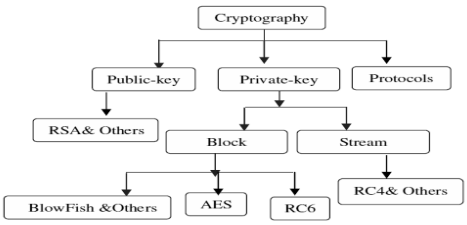

Figure 1: Cryptography Techniques

CRYPTOGRAPHIC ALGORITHMS IN PRACTICE

Copious cryptographic algorithms are used in the real world of financial, defense and personal transactions to transmit data across the network infrastructure without any risk.
Encryption is to reorganize the message into a different appearance so that the actual message is kept secret. The objective of encryption is to offer an easy means of encryption and decryption for all authorized users in possession of the appropriate key and difficult and expensive means to estimate the plain text without use of the key. Moreover, the encryption system must be applicable for different application areas and architectures.

As per the public request for proposals for a standard cryptography algorithm issued by NBS in May 15, 1973 (as cited in Schneider, 1996), a series of design criteria are specified -

A) High level of security.
B) Completely specified and easy to understand.
C) The security of the algorithm must reside in the key; the security should not depend on the secrecy of the algorithm.
D) Available to all users.
E) Adaptable for use in diverse applications.
F) Economically applicable in electronic devices.
G) Efficient to use.
H) Able to be validated.
I) Exportable.

Broadly, we can classify the algorithms for cryptography in three categories -

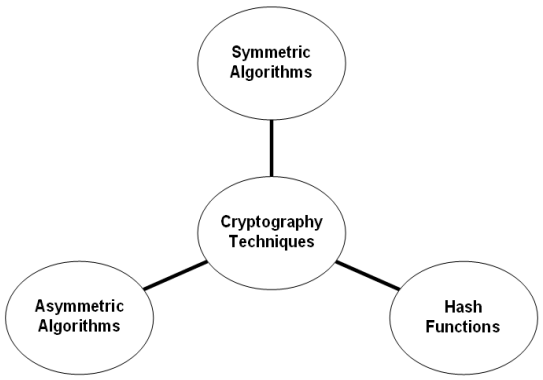

Figure 2: Cryptography Algorithms

SYMMETRIC ALGORITHMS (SECRET KEY CRYPTOGRAPHY)

This class of cryptography techniques uses a single key to implement encryption as well as decryption. This is also known as symmetric-key encryption, Single-key, shared-key, one-key and private-key encryption. Symmetric-key algorithms are further classified into stream ciphers and block ciphers whereby stream ciphers encrypt the message bytes one at a time while block ciphers receive a number of bytes and encrypt all as a single unit. The examples of accepted and well-fame symmetric algorithms include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, RC4, TDES, and IDEA. Symmetric ciphers have historically been susceptible to known-plaintext attacks, chosen plaintext attacks, differential cryptanalysis and linear cryptanalysis. Chary development of the functions for each step greatly helps in reducing the chances of attack.

	Symmetric Cryptography (Private Key)	Asymmetric Cryptography (Public Key)
Keys	One key is shared between two or more entities.	One entity has a public key and the other entity has a private key.
Key Exchange	Out-of-band	Symmetric key is encrypted with receiver's public key and sent with message; thus, the key is distributed by inbound means.
Speed	Algorithm is less complex and faster.	Algorithm is more complex and slower.
Key length	Fixed-key length	Variable-key length
Use	Bulk encryption, which means encrypting files and communication paths.	Key encryption and distributing keys.
Security service provided	Confidentiality and integrity	Confidentiality, integrity, authentication and nonrepudiation

When using symmetric algorithms, both parties share the same key for en- and decryption. To provide privacy, this key needs to be kept secret. Once somebody else gets to know the key, it is not safe any more. Symmetric algorithms have the advantage of not consuming too much computing power. A few well-known examples are: DES, Triple-DES (3DES), IDEA, CAST5, BLOWFISH, TWOFISH.

Asymmetric algorithms use pairs of keys. One is used for encryption and the other one for decryption. The decryption key is typically kept secretly, therefore called ``private key'' or ``secret key'', while the encryption key is spread to all who might want to send encrypted messages, therefore called ``public key''. Everybody having the public key is able to send encrypted messages to the owner of the secret key. The secret key can't be reconstructed from the public key. The idea of asymmetric algorithms was first published 1976 by Diffie and Hellmann.

Asymmetric algorithms seem to be ideally suited for real-world use: As the secret key does not have to be shared, the risk of getting known is much smaller. Every user only needs to keep one secret key in secrecy and a collection of public keys, that only need to be protected against being changed. With symmetric keys, every pair of users would need to have an own shared secret key. Well-known asymmetric algorithms are RSA, DSA, and ELGAMAL.

However, asymmetric algorithms are much slower than symmetric ones. Therefore, in many applications, a combination of both is being used. The asymmetric keys are used for authentication and after this have been successfully done, one or more symmetric keys are generated and exchanged using the asymmetric encryption. This way the

,

advantages of both algorithms can be used. Typical examples of this procedure are the RSA/IDEA combination of PGP2 or the DSA/BLOWFISH used by GnuPG.

SYMMETRIC VS ASYMMETRIC CRYPTOGRAPHY

Symmetric Cryptography

It is also referred as secret key cryptography and the most intuitive kind of cryptography involving the use of a secret key known only to the participants of the secure communication.

Strength

A) Faster than the asymmetric systems
B) Difficult to break if for large key size

Weaknesses

A) Needs the secured mechanism for delivery of key properly
B) Every pair of users requires unique pair of keys
C) Limited set of security is there
D) The key is sent via another channel than the message.

ASYMMETRIC CRYPTOGRAPHY

It is also known as public key cryptography and difference to symmetric cryptography is that this algorithm uses two different keys for encryption and corresponding decryption. Each end in a secure communication media has a unique pair of keys, called public key p and secret key s. These keys p and s are mathematically dependent on each other that is a requirement to the asymmetric algorithm being that, while p can be calculated easily from s, obtaining s from p is computationally unfeasible. This property allows making publicly known, while s must be kept secret by its owner. This asymmetry of the keys allows novel and very interesting uses of cryptography:

A) Secure transmission without requiring a shared secret
B) Digital signing of messages
C) Strong mutual authentication with flexibility of scalability
D) Secure storage on insecure media

ALGORITHMIC COMPLEXITY AND PERFORMANCE ISSUES

AES - Good performance (high speed and low RAM requirements) were an explicit goal of the AES selection process. Thus AES performs well on a wide variety of hardware, from 8-bit smartcards to high-performance computers. On a Pentium Pro, AES encryption requires 18 clock cycles / byte, equivalent to a throughput of about 11 MiB/s for a 200MHz processor. On a Pentium M 1.7GHz throughput is about 60 MiB/s.

TWOFISH

A) Twofish was designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson. They tried to implement in their design the following principles:
B) Simplicity – all the design elements of the algorithm have a clear reason or function
C) Performance – they compared all the different option on the basis of relative performance
D) Conservativeness - they left a margin for error and they provided more security than required while trying to design against attacks that are not yet known
E) Encrypt data in less than 500 clock cycles per block on an Intel Pentium, Pentium Pro, and Pentium II, for a fully optimized version of the algorithm.
F) Be capable of setting up a 128-bit key (for optimal encryption speed) in less than the time required to encrypt 32 blocks on a Pentium, Pentium Pro, and Pentium II.
G) Encrypt data in less than 5000 clock cycles per block on a Pentium, Pentium Pro, and Pentium II with no key setup time.
H) Able to accept key length up to 256 bits
I) Not contain any operations that make it inefficient on other 32-bit microprocessors.
J) Not contain any operations that make it inefficient on 8-bit and 16-bit microprocessors.
K) Not contain any operations that reduce its efficiency on proposed 64-bit microprocessors; e.g., Merced.
L) Not having any elements that make it inefficient in hardware.
M) Having a variety of performance tradeoffs with respect to the key schedule.
N) Encrypt data in less than 10 milliseconds on a commodity 8-bit microprocessor.
O) Implementable on a 8-bit microprocessor with only 64 bytes of RAM.
P) Implementable in hardware using less than 20,000 gates**.**

Asymmetric Algorithms (Public Key Cryptography)

Public key cryptography is one of the fundamental and extensively used technologies around the world for encryption and decryption of confidential messages. This class of cryptography algorithms uses one key for encryption and another for decryption of data packets in the network infrastructure. This cryptographic approach makes use of asymmetric key algorithms rather than or in addition to symmetric key algorithms. Dissimilar to symmetric key algorithms, it does not rely on a secure initial exchange of one or more secret keys to both sender and receiver. The public key cryptography algorithms create a mathematically related key pair of a secret private key and an open public key. Utilization of these keys allows protection of the authenticity of a message by creating a digital signature of the message using the private key, which is verified using the public key. Moreover, it allows the protection of confidentiality as well as integrity of message, by public key encryption, encrypting the message using the public key, which can only be decrypted using the private key. It is the approach which is employed by many cryptographic algorithms and cryptosystems. It underlies such Internet standards as Transport Layer Security (TLS) (successor to SSL), PGP, and GPG.

Asymmetric Key Techniques

A) Diffie-Hellman key exchange protocol
B) DSS (Digital Signature Standard), which incorporates the Digital Signature Algorithm
C) ElGamal
D) Various elliptic curve techniques

,

E) Various password-authenticated key agreement techniques
F) Paillier cryptosystem
G) RSA encryption algorithm (PKCS#1)
H) Cramer–Shoup cryptosystem
I) NTRUEncrypt cryptosystem
J) McEliece cryptosystem
K) Merkle–Hellman knapsack cryptosystem

PROTOCOLS USING ASYMMETRIC KEY ALGORITHMS

A) GPG, an implementation of OpenPGP
B) Internet Key Exchange
C) PGP
D) ZRTP, a secure VoIP protocol
E) Secure Socket Layer, now implemented as an IETF standard TLS
F) SILC
G) SSH

Hash Functions Cryptography

Hash function is deterministic approach which makes use of mathematical transformation to encrypt the information permanently. It takes a capricious block of data and returns the fixed-size bit string, known as the cryptographic hash value. The data packet or simply message to be encoded is called the Message, and the Hash Value is called as the Message Digest or simply Digest.

Significant properties associated with the ideal cryptographic hash functions -

A) Simple in implementation and to compute the hash value for any given message
B) Infeasible to find a message that has a given hash
C) Infeasible to modify a message without altering its hash
D) Infeasible to find two different messages with the same hash

Most of the cryptographic hash functions are designed to accept a string of any length as input and produce a fixed-length hash value.

Input String → (Hash Function) → Message Digest

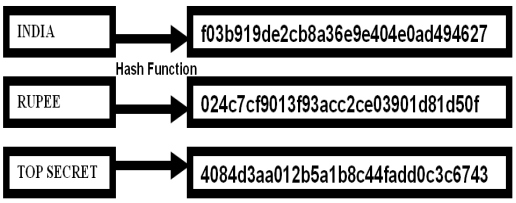

Figure 3: Message Digest for given Strings using MD5 Hash

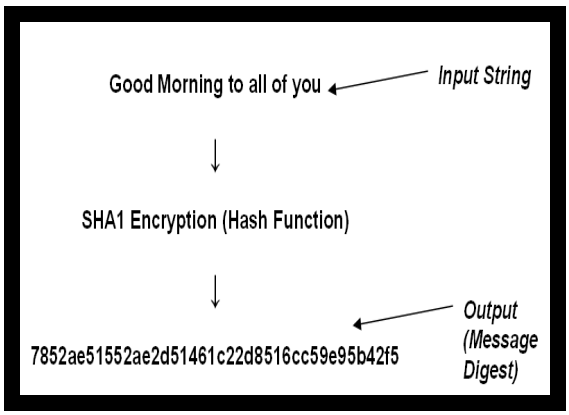

Figure 4:- Message Digest for given Strings using MD5 Hash

ALGORITHMS BASED ON HASH FUNCTIONS

GOST	HAVAL	MD2
MD4	MD5	PANAMA
RadioGatún	RIPEMD	RIPEMD-128/256
RIPEMD-160/320	SHA-0	SHA-1
Tiger(2)-192/160/128	WHIRLPOOL	

PERFORMANCE ANALYSIS AND PROPORTIONAL STUDY

Symmetric key encryption is the older method of encryption and asymmetric key encryption was developed to make up for its shortcomings. Yet, each of them still has advantages and disadvantages that make them appeal to different users and uses.

While each system has its proponents and opponents, both methods have advantages and disadvantages which are outlined below:

Symmetric encryption algorithms encrypt and decrypt with the same key. Main advantages of symmetric encryption algorithms are its security and high speed. Asymmetric encryption algorithms encrypt and decrypt with different keys. Data is encrypted with a public key, and decrypted with a private key. Asymmetric encryption algorithms (also known as public-key algorithms) need at least a 3,000-bit key to achieve the same level of security of a 128-bit symmetric algorithm. Asymmetric algorithms are incredibly slow and it is impractical to use them to encrypt large amounts of data. Generally, symmetric encryption algorithms are much faster to execute on a computer than asymmetric ones. In practice they are often used together, so that a public-key algorithm is used to encrypt a randomly generated encryption key, and the random key is used to encrypt the actual message using a symmetric algorithm. This is sometimes called hybrid encryption.

Symmetric Key Encryption –

Symmetric key encryption is also known as shared-key, single-key, secret-key, and private-key or one-key encryption. In this type of message encryption, both sender

,

and receiver share the same key which is used to both encrypt and decrypt messages. Sender and receiver only have to specify the shared key in the beginning and then they can begin to encrypt and decrypt messages between them using that key. Examples include AES (Advanced Encryption Standard) and TripleDES (Data Encryption Standard).

ADVANTAGES

A) Simple: This type of encryption is easy to carry out. All users have to do is specify and share the secret key and then begin to encrypt and decrypt messages.
B) Encrypt and decrypt your own files: If you use encryption for messages or files which you alone intend to access, there is no need to create different keys. Single-key encryption is best for this.
C) Fast: Symmetric key encryption is much faster than asymmetric key encryption.
D) Uses less computer resources: Single-key encryption does not require a lot of computer resources when compared to public key encryption.
E) Prevents widespread message security compromise: A different secret key is used for communication with every different party. If a key is compromised, only the messages between a particular pair of sender and receiver are affected. Communications with other people are still secure.
F) Each trading partner can use the same publicly known encryption algorithm - no need to develop and exchange secret algorithms
G) Security is dependent on the length of the key

DRAWBACKS AND PROBLEMS IN THE MANAGEMENT OF SYMMETRIC KEY AND ENCRYPTION

A) A shared secret key must be agreed upon by both parties
B) If a user has n trading partners, then n secret keys must be maintained, one for each trading partner
C) Authenticity of origin or receipt cannot be proved because the secret key is shared
D) Management of the symmetric keys becomes problematic
E) Trading partners must always use the exact same key to decrypt the encrypted message
F) Key exchange is difficult because the exchange itself must be secure with no intervening compromise of the key
G) Management of keys is difficult as numbers of trading partners increases, especially when multiple keys exist for each trading partner
H) Need for secure channel for secret key exchange: Sharing the secret key in the beginning is a problem in symmetric key encryption. It has to be exchanged in a way that ensures it remains secret.
I) Too many keys: A new shared key has to be generated for communication with every different party. This creates a problem with managing and ensuring the security of all these keys.
J) Origin and authenticity of message cannot be guaranteed: Since both sender and receiver use the same key, messages cannot be verified to have come from a particular user. This may be a problem if there is a dispute.

PUBLIC KEY CRYPTOGRAPHY AS A SOLUTION FOR MANAGING SYMMETRIC KEYS

A) Public key cryptography simplifies the management of symmetric keys to the point whereby a symmetric key can be used not only for each trading partner, but for each exchange between trading partners
B) Additionally, public key cryptography can be used to unambiguously establish non-repudiation of origin and receiptn

Asymmetric/Public Key Encryption –

Also known as public key encryption, this method of encrypting messages makes use of two keys: a public key and a private key. The public key is made publicly available and is used to encrypt messages by anyone who wishes to send a message to the person that the key belongs to. The private key is kept secret and is used to decrypt received messages. An example of asymmetric key encryption system is RSA.

ADVANTAGES

A) Convenience: It solves the problem of distributing the key for encryption. Everyone publishes their public keys and private keys are kept secret.
B) Provides for message authentication: Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is truly from a particular sender.
C) Detection of tampering: The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature.
D) Provide for non-repudiation: Digitally signing a message is akin to physically signing a document. It is an acknowledgement of the message and thus, the sender cannot deny it.

DISADVANTAGES AND PROBLEMS ASSOCIATED

A) Public keys are required to be authenticated
B) No one can be absolutely sure that a public key belongs to the person it specifies and so everyone must verify that their public keys belong to them.
C) Slow: Public key encryption is slow compared to symmetric encryption. Not feasible for use in decrypting bulk messages.
D) Uses up more computer resources: It requires a lot more computer supplies compared to single-key encryption.
E) Widespread security compromise is possible: If an attacker determines a person's private key, his or her entire messages can be read.
F) Loss of the private key lead to irreparable which means that all received messages cannot be decrypted.

Symmetric cryptography makes use of the same secret (private) key for encryption and decryption the data whereas asymmetric uses both a public and private key. Symmetric

,

requires that the secret key be known by the party encrypting the data and the party decrypting the data. Asymmetric allows for distribution of your public key to anyone with which they can encrypt the data they want to send securely and then it can only be decoded by the person having the private key. This eliminates the need of having to give someone the secret key (as with symmetric encryption) and risk having it compromised.

The issue with asymmetric is that it is about 1000 times slower than symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use strong a stronger key than symmetric.

a. Based on the concept of a key pair
b. Each half of the pair (one key) can encrypt information that only the other half (one key) can decrypt
c. The key pair is designated and associated to one, and only one, trading partner

REAL WORLD USAGE OF ASYMMETRIC ENCRYPTION

A) Public key encryption algorithms are considerably slower than symmetric key algorithms
B) Rarely used as encryption methodology for bulk messages or parts of messages
C) Normally used in conjunction with a Message Integrity Check (MIC) or to encrypt a symmetric key, where the MIC or symmetric key is what is encrypted using public key encryption algorithms

SPEED COMPARISON - SYMMETRIC VS. ASYMMETRIC

A) Software encryption using DES (symmetric key algorithm) is 100 times faster than software encryption using RSA (asymmetric key algorithm) - estimate provided by RSA Data Securities
B) Hardware encryption using DES (symmetric key algorithm) is anywhere from 1,000 to 10,000 times faster than hardware encryption using RSA (asymmetric key algorithm)

CONCLUSION AND SCOPE OF FUTURE WORK

A significant amount of research and development is going on in the stream of cryptography and cryptanalysis. Network scientists and engineers are executing the encryption techniques to make the data packets and messages secured from multiple interceptions so that the authenticity and integrity of the organization is not under threat. The development and execution of cryptography techniques is an ongoing process and still there is need to develop and implement a highly secured method which is able to detect and squash any attempt of interception on network establishment.

REFERENCES

[1] Gary C. Kessler (2010), An Overview of Cryptography URL : http://www.garykessler.net/library/crypto.html Last Accessed : 18 September 2010
[2] Bamford, J. (1983). The Puzzle Palace: Inside the National Security Agency, America's most secret intelligence organization. New York: Penguin Books.
[3] Bamford, J. (2001). Body of Secrets: Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of a New Century. New York: Doubleday.
[4] Barr, T.H. (2002). Invitation to Cryptology. Upper Saddle River, NJ: Prentice Hall.
[5] Bauer, F.L. (2002). Decrypted Secrets: Methods and Maxims of Cryptology, 2nd ed. New York: Springer Verlag.
[6] Denning, D.E. (1982). Cryptography and Data Security. Reading, MA: Addison-Wesley.
[7] Diffie, W., & Landau, S. (1998). Privacy on the Line. Boston: MIT Press.
[8] Electronic Frontier Foundation. (1998). Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design. Sebastopol, CA: O'Reilly & Associates.
[9] Federal Information Processing Standards (FIPS) 140-2. (2001, May 25). Security Requirements for Cryptographic Modules. Gaithersburg, MD: National Intitute of Standards and Technology (NIST). Retrieved from http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[10] Ferguson, N., & Schneier, B. (2003). Practical Cryptography. New York: John Wiley & Sons.
[11] Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. New York: John Wiley & Sons.
[12] Flannery, S. with Flannery, D. (2001). In Code: A Mathematical Journey. New York: Workman Publishing Company.
[13] Ford, W., & Baum, M.S. (2001). Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption, 2nd ed. Englewood Cliffs, NJ: Prentice Hall.
[14] Garfinkel, S. (1995). PGP: Pretty Good Privacy. Sebastopol, CA: O'Reilly & Associates.
[15] Grant, G.L. (1997). Understanding Digital Signatures: Establishing Trust over the Internet and Other Networks. New York: Computing McGraw-Hill.
[16] Grabbe, J.O. (1997, October 10). Cryptography and Number Theory for Digital Cash. Retrieved from http://www-swiss.ai.mit.edu/6.805/articles/money/cryptnum.htm
[17] Kahn, D. (1983). Kahn on Codes: Secrets of the New Cryptology. New York: Macmillan.
[18] Kahn, D. (1996). The Codebreakers: The Story of Secret Writing, revised ed. New York: Scribner.
[19] Kaufman, C., Perlman, R., & Speciner, M. (1995). Network Security: Private Communication in a Public World. Englewood Cliffs, NJ): Prentice Hall.
[20] Kessler, G.C. (1999, October). Basics of Cryptography and Applications for Windows NT. Windows NT Magazine.
[21] Kessler, G.C. (2000, February). Roaming PKI. Information Security Magazine.
[22] Kessler, G.C., & Pritsky, N.T. (2000, October). Internet Payment Systems: Status and Update on SSL/TLS, SET, and IOTP. Information Security Magazine.
[23] Koblitz, N. (1994). A Course in Number Theory and Cryptography, 2nd ed. New York: Springer-Verlag.

,

[24] Levy, S. (1999, April). The Open Secret. WIRED Magazine, 7(4). Retrieved from http://www.wired.com/wired/archive/7.04/crypto.html
[25] Levy, S. (2001). Crypto: When the Code Rebels Beat the Government — Saving Privacy in the Digital Age. New York: Viking Press.
[26] Mao, W. (2004). Modern Cryptography: Theory & Practice. Upper Saddle River, NJ: Prentice Hall Professional Technical Reference.
[27] Marks, L. (1998). Between Silk and Cyanide: A Codemaker's War, 1941-1945. New York: The Free Press (Simon & Schuster).
[28] Schneier, B. (1996). Applied Cryptography, 2nd ed. New York: John Wiley & Sons.
[29] Schneier, B. (2000). Secrets & Lies: Digital Security in a Networked World. New York: John Wiley & Sons.
[30] Singh, S. (1999). The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography. New York: Doubleday.
[31] Smith, L.D. (1943). Cryptography: The Science of Secret Writing. New York: Dover Publications.
[32] Spillman, R.J. (2005). Classical and Contemporary Cryptology. Upper Saddle River, NJ: Pearson Prentice-Hall.
[33] Stallings, W. (2006). Cryptography and Network Security: Principles and Practice, 4th ed. Englewood Cliffs, NJ: Prentice Hall.
[34] Trappe, W., & Washington, L.C. (2006). Introduction to Cryptography with Codin Theory, 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall.
[35] Young, A., & Yung, M. (2004). Malicious Cryptography: Exposing Cryptovirology. New York: John Wiley & Sons.
[36] Deni Connor is principal analyst for Storage Strategies Now, a research firm in Austin, Texas. http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1294607,00.html
[37] Chaotic Encryption Techniques http://www.hkstar.com/~hmk409/research/ces/research/200107/project.htm
[38] http://en.wikipedia.org/wiki/Cryptographic_hash_function
[39] Antoine Joux. Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions. LNCS 3152/2004, pages 306-316 Full text.
[40] Jonathan J. Hoch and Adi Shamir (2008-02-20). On the Strength of the Concatenated Hash Combiner when All the Hash Functions are Weak. http://eprint.iacr.org/2008/075.pdf.
[41] URL: http://www.encryptionanddecryption.com/encryption
[42] Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger, MD5 considered harmful today: Creating a rogue CA certificate, accessed March 29, 2009
[43] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, Finding Collisions in the Full SHA-1
[44] Bruce Schneier, Cryptanalysis of SHA-1 (summarizes Wang et al. results and their implications)
[45] Shai Halevi, Hugo Krawczyk, Update on Randomized Hashing
[46] Shai Halevi and Hugo Krawczyk, Randomized Hashing and Digital Signatures
[47] NIST.gov - Computer Security Division - Computer Security Resource Center
[48] Evaluating The Performance of Symmetric Encryption Algorithms, Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud, International Journal of Network Security, Vol.10, No.3, PP.213-219, May 2010
[49] "Performance Comparisons of the AES submissions" (PDF). 1999-02-01. http://www.schneier.com/paper-aes-performance.pdf. Retrieved 2010-12-28.
[50] http://www1.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.html#Crypto++
[51] http://www.securityarena.com/cissp-domain-summary/63-cbk-cryptography.html?start=3

