Review on Cryptography in Network Security

MITESH SHARMA
M.E. Scholar, Department of Computer Science and Engineering
M.B.M. Engineering College
Jai NarainVyas University, Jodhpur

***Abstract*—With the explosive growth in the Internet, network security has become an inevitable concern for any organization whose internal private network is connected to the Internet. Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one who has the decipher key, and data cannot be changed means the original information would not be changed or modified; this is done when the sender includes a cryptographic operation called a hash function in the original message. A hash function is a mathematical representation of the information, when any information arrives at its receiver; the receiver calculates the value of this hash function. If the receiver's hash function value is equivalent to the sender's, the integrity of the message is assured. Network security is setup to guard against unauthorized access, alteration, or modification of information, and unauthorized denial of service. When a network is connected to the network that is vulnerable to potential intrusions and attacks. Security of data can be done by a technique called cryptography. So one can say that cryptography is an emerging technology, which is important for network security. This paper covers the various cipher generation algorithms of cryptography which are helpful in network security. Cryptography in the past was used in keeping military information, diplomatic correspondence secure and in protecting the national security. However, the use was limited. Nowadays, the range of cryptography applications have been expanded a lot in the modern area after the development of communication means; cryptography is essentially required to ensure that data are protected against penetrations and to prevent espionage. Also, cryptography is a powerful mean in securing e-commerce.**

*Keyword:***Plain Text, Cipher Text, Attacks, Cryptography, Symmetric Encryption, ASymmetricEncryption ,Hash Algorithm.**

I. INTRODUCTION

Nowadays, cryptography plays a major role in protecting the information of technology applications. Information security is an important issue, for some applications. Have the top priority such as ecommerce, e-banking, e-mail, medical databases, and so many more, all of them require the exchange of private information. Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. Cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing .

For example, let us consider a person named Alice a sender who wants to send adata message which has a length of characters to a receiver called Bob. Alice uses an unsecurecommunication channel. Which could be a telephone line , computer network, or any other channel. If themessage contains secret data, they could be intercepted and read by hackers. Also they may change ormodify the message during its transmission in such a way that Bob would not be able to discover thechange. In this survey a various ways of encryption is viewed and have been compared ,a lot ofexamples have been provided .

Network security is a new and fast moving technology and as such, is still being defined. When considering the desired learning outcomes of such a course, one could argue that a network security analyst must be capable of analyzing security from the business perspective in order to adhere to recent security legislation, and from the technical perspective in order to understand and select the most appropriate security solution. Network security originally focused on algorithmic aspects such as encryption and hashing techniques. While these concepts rarely change, these skills alone are insufficient to protect computer networks. As crackers hacked away at networks and systems,

courses arose that emphasized the latest attacks. Currently, many educators believe that to train people to secure networks, they must also learn to think like a cracker. The following background information in security helps in making correct decisions: Attack Recognition, Encryption techniques, Network Security Architecture, Protocol analysis, Access control list and vulnerability. For Network security cryptography is present. In cryptography data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. We use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plain text is called decryption. In cryptography three types of algorithms are present. Symmetric key algorithm, asymmetric key algorithm and hash function.

II. Cryptography Goals

By using cryptography many goals can be achieved, These goals can be either all achieved at the sametime in one application, or only one of them, These goals are:

a) **Confidentiality:**It is the most important goal, that ensures that nobody can understand thereceived message except the one who has the decipher key.
b) **Authentication:**It is the process of proving the identity, that assures the communicating entity isthe one that it claimed to be, This means that the user or the system can prove their ownidentities to other parties who don't have personal knowledge of their identities. (The primaryform of host to host authentication on the Internet today is name-based or address-based; andboth of them are notoriously weak).
c) **Data Integrity:**Its ensures that the received message has not been altered in any way from itsoriginal form, This can be achieved by using hashing at both sides the sender and the recipientin order to create a unique message digest and compare it with the one that received.
d) **Non-Repudiation:**It is mechanism used to prove that the sender really sent this message, ,andthe message was received by the specified party, so the recipient cannot claim that the messagewas not sent .
e) **Access Control:**It is the process of preventing an unauthorized use of resources. This goalcontrols who can have access to the resources, If one can access, under which restrictions andconditions the access can be occurred, and what is the permission level of a given access.

III. IMPORTANCE AND APPROACHES

The information that we need to hide, is called plaintext , It's the original text, It could be in a form ofcharacters, numerical data, executable programs, pictures, or any other kind of information, The plaintextfor example is the first draft of a message in the sender before encryption, or it is the text at the receiverafter decryption.The data that will be transmitted is called cipher text , it's a term refers to the string of "meaningless"data, or unclear text that nobody must understand, except the recipients. it is the data that will betransmitted Exactly through network, Many algorithms are used to transform plaintext into cipher texts

Cipher is the algorithm that is used to transform plaintext to cipher text, This method is called encryptionor enciphers (encode), in other words, it's a mechanism of converting readable and understandable datainto "meaningless" data, and it is represented as follows:

$$C = E_{(K)}(P) \quad (1)$$

Where is the encryption algorithm using key .

The opposite of cipher mechanism is called decipher (decode) that is the algorithm which recovers thecipher text, this method is called decryption, in other words it's the mechanism of converting"meaningless" data into readable data.

$$P = D_{(K-1)}(C) \quad (2)$$

The Key is an input to the encryption algorithm, and this value must be independent of the plaintext, Thisinput is used to transform the plaintext into cipher text, so different keys will yield different cipher text, Inthe decipher side, the inverse of the key will be used inside the algorithm instead of the key.

Computer security it's a generic term for a collection of tools designed to protect any data from hackers,theft, corruption, or natural disaster while allowing these data to be available to the users at the sametime. One example of these tools is the A-vast antivirus program .

Network security refers to any activity designed to protect the usability, integrity, reliability, and safety ofdata during their transmission on a network, Network security deals with hardware and software, Theactivity can be one of the following anti-virus and anti-spyware, firewall, Intrusion prevention systems, andVirtual Private Networks .

Internet Security is measures and procedures used to protect data during their transmission over acollection of interconnected networks .while information security is about how to prevent attacks, and todetect attacks on information-based systems.Cryptanalysis (code breaking) is the study of principles and methods of deciphering cipher text withoutknowing the key, typically this includes finding and guessing the secrete key, It's a complex processinvolving statistical analysis, analytical reasoning, math tools and pattern-finding, The field of bothcryptography and cryptanalysis is called cryptology .

Symmetric encryption refers to the process of converting plaintext into cipher text at the sender with thesame key that will be used to retrieve plaintext from cipher text at the recipient. while asymmetricencryption refers to the process of converting plaintext into cipher text at the sender with different keythat will be used to retrieve plaintext from cipher text at the recipient .

Passive attacks mean that the attackers or the unauthorized parties just monitoring on the traffic or onthe communication between the sender and the recipient, but not attempting to breach or shut down aservice, This kind of attacks is very hard to discover, since the unauthorized party doesn't leave anytraces. On the other hand active attacks mean that the attackers are actively attempting to cause harmto the network or the data. The attackers are not just monitoring on the traffic, but they also attempt tobreach or shut down the service .

Authentication is the process of determining whether someone is the same person who really is, such aslogin and password in login pages while authorization is the process of ensuring that this person has theability to do something. Brute force is the attacker who is trying all of the possible keys that may be used in either decrypt or encrypt information.

IV. TYPES OF CRYPTOGRAPHY

There are many types of cryptography, including codes, steganography (hidden orsecret writing), and ciphers. Codes rely on codebooks. Steganography relies on different ways tohide or disguise writing. Ciphers include both computer-generated ciphers and those created byencryption methods. The different types of ciphers depend on alphabetical, numerical, computerbased,or other scrambling methods.

a) Codes and Codebooks

A well-constructed code can represent phrases and entire sentences with symbols,such as five-letter groups, and is often used more for economy than for secrecy. A properlyconstructed code can give a high degree of security, but the difficulty of printing and distributingcodebooks—books of known codes—under conditions of absolute secrecy limits their use toplaces in which the books can be effectively guarded. In addition, the more a codebook is used,the less secure it becomes.

Imagine a codebook with two columns. In the first column is a list of all the wordsthat a military commander could possibly need to use to communicate. For example, it containsall the possible geographic areas in a region, all possible times, and all military terms. In theother column is a list of plain words. To create a coded message, the encoder writes down theactual message. He then substitutes words in the codebook by finding matches in the secondcolumn for the words in the message and using the new words instead. For example, suppose themessage is Attack the hill at dawn and the codebook contains the following word pairs: attack =bear, the = juice, hill = orange, at = calendar, and dawn = open. The encoded message wouldread Bear juice orange calendar open.

If the coded message fell into enemy hands, the enemy would know it was in code,but without the codebook the enemy would have no way to decrypt the message. Codebooks losesome of their value over time, however. For example, if the coded message fell into enemy

handsand the next day the hill was attacked at dawn, the enemy could link the event to the codedmessage. If another message containing the word orange were captured, and the following day,something else happened on the hill, the enemy could assume that orange = hill is in thecodebook. Over time, the enemy could put together more and more code word pairs, andeventually crack the code. For this reason, it is common to change codes often.

b) Steganography:

Steganography is a method of hiding the existence of a message using tools such asinvisible ink, microscopic writing, or hiding code words within sentences of a message (such asmaking every fifth word in a text part of the message). Cryptographers may apply steganographyto electronic communications. This application is called transmission security.Steganography, or secret writing, seems to have originated almost as early aswriting itself did. Even in ancient Egypt, where writing itself was a mystery to the averageperson, two distinct forms of writing were used. Hieratic or sacred writing was used for secretcommunication by the priests, and demotic writing was used by other literate people. The ancientGreeks and Romans, as well as other civilizations that flourished at around the same time, usedforms of steganography. The invention of the first shorthand system was presumably intended asa form of secret writing. Shorthand first came into wide use in ancient Rome, with notaeTironianae ('Tironian notes'), a system invented by Marcus TulliusTiro in 63 BC.

c) Ciphers

Ease of use makes ciphers popular. There are two general types of ciphers.

Substitution ciphers require a cipher alphabet to replace plaintext with other letters or symbols.Transposition ciphers use the shuffling of letters in a word to make the word incomprehensible.Ciphers are the secret codes used to encrypt plaintext messages. Ciphers of varioustypes have been devised, but all of them are either substitution or transposition ciphers.Computer ciphers are ciphers that are used for digital messages. Computer ciphers differ fromordinary substitution and transposition ciphers in that a computer application performs theencryption of data. The term cryptography is sometimes restricted to the use of ciphers or tomethods involving the substitution of other letters or symbols for the original letters of amessage.

d) Computer Ciphers & Encryption

Government agencies, banks, and many corporations now routinely send a great dealof confidential information from one computer to another. Such data are usually transmitted viatelephone lines or other nonprivate channels, such as the Internet. Continuing development ofsecure computer systems and networks will ensure that confidential information can be securelytransferred across computer networks.

e) Cryptanalysis

Cryptanalysis is the art of analyzing ciphertext to extract the plaintext or the key. Inother words, cryptanalysis is the opposite of cryptography. It is the breaking of ciphers.Understanding the process of code breaking is very important when designing any encryptionsystem. The science of cryptography has kept up with the technological explosion of the last halfof the 20th century. Current systems require very powerful computer systems to encrypt anddecrypt data. While cryptanalysis has improved as well, some systems may exist that areunbreakable by today's standards.

Today's cryptanalysis is measured by the number and speed of computers availableto the code breaker. Some cryptographers believe that the National Security Agency (NSA) ofthe United States has enormous, extremely powerful computers that are entirely devoted tocryptanalysis.The substitution ciphers described above are easy to break. Before computers wereavailable, expert cryptanalysts would look at ciphertext and make guesses as to which letterswere substituted for which other letters. Early cryptanalysis techniques included computing thefrequency with which letters occur in the language that is being intercepted. For example, in theEnglish language, the letters e, s, t, a, m, and n occur much more frequently than do q, z, x, y, andw. So, cryptanalysts look at the ciphertext for the most frequently occurring letters and assignthem as candidates to be e, s, t, a, m, and n. Cryptanalysts also know that certain combinations ofletters are more common in the English language than others are. For example, q and u occurtogether, and so do t and h. The more ciphertext that is available, the better the chances ofbreaking the code.

Security services

Security Requirements:
Confidentiality: Protection from disclosure to unauthorised persons,Integrity:Maintaining data consistency,**Authentication:** Assurance of identity of person or originator ofdata.Non-repudiation: Originator of communications can't deny it later,**Availability:** Legitimateusers have access when they need it,Access control: Unauthorised users are kept out.These are often combined: User authentication used for access control purposes, Non-repudiationcombined with authentication.

Security Threats
Information disclosure/information leakage,Integrity violation,Masquerading,Denialof service Illegitimate use,Generic threat: Backdoors, trojan horses, insider attacks,Most Internetsecurity problems are access control or authentication ones: Denial of service is also popular, butmostly an annoyance.

V. SYMMETRIC AND ASYMMETRIC ENCRYPTION

Encryption is the strongest and the safest way in securing data. Certainly, it is the most common one.Encryption systems are divided into two major types or forms, symmetric and asymmetric.

Symmetric encryption is known as secret key or single key, The receiver uses the same key which thesender uses to encrypt the data to decrypt the message,. This system was the only system used beforediscovering and developing the public key. A safe way of data transfer must be used to moving thesecret key between the sender and the receiver in symmetric encryption. Figure 4 shows how the systemworks. Symmetric encryption occurs either by substitution transposition technique, or by a mixture ofboth. Substitution maps each plaintext element into cipher text element, but transposition transposes thepositions of plaintext elements.

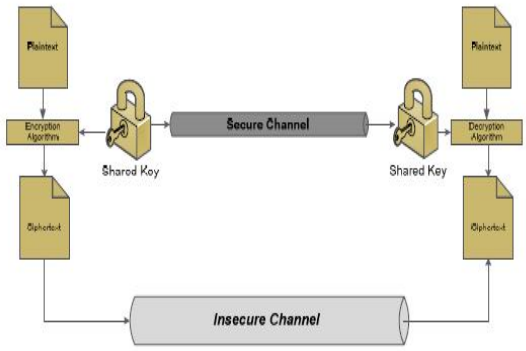


FIGURE .4 : Simplified model of conventional encryption

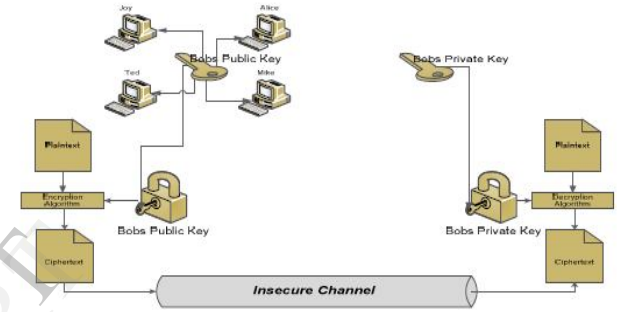
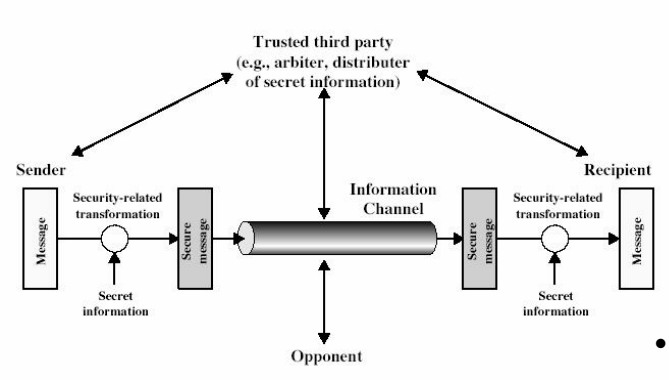


FIGURE 5 : Simplified model of asymmetric encryption

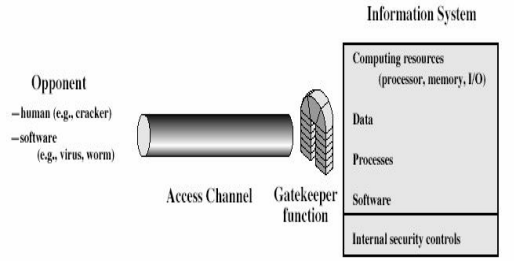
Asymmetric encryption is slower and very complicated in calculations than symmetric encryption .Therefore, asymmetric encryption deals with plaintext as a group of numbers which are manipulated inmathematics, while the plaintext in symmetric encryption deal as group of symbols and characters, theencryption process may permute these symbols, or may substitute one symbol by another.So the nature of the data determines the system of encryption type. And every system has its own uses.For example, asymmetric encryption may be used in authentication or in sending secret key fordecryption.

V. Model for Network Security

using this model requires us to:
– design a suitable algorithm for the security transformation
– generate the secret information (keys) used by the algorithm
– develop methods to distribute and share the secret information
– specify a protocol enabling the principals to use the transformation and secret information for a security service



Model for Network Access Security



VI. CRYPTOGRAPHY TECHNIQUES OF SECURED MANETS/WSNS DESIGN

Security is the combination of processes, procedures and systems used to ensure confidentiality,authentication, integrity, availability, access control, and non-repudiation.

- **Confidentiality:** The goal of confidentiality is to keep sent information from being read byunauthorized users or nodes. MANETs/WSNs use an open medium, so usually all nodes withinthe direct transmission range can obtain the data. One way to keep information confidential is toencrypt the data. In WSNs, confidentiality is achieved to protect information from disclosurewhen communication is between one sensor node and another sensor node or between the sensorsand the base station. Compromised nodes may be a threat to confidentiality if the cryptographickeys are not encrypted and stored in the node.
- **Authentication:** The goal of authentication is to be able to identify a node or a user and toprevent impersonation. In wired networks and infrastructure-based wireless networks, it ispossible to implement a central authority at a router, base station, or access point. However, thereis no central authority in MANETs/WSNs, and it is much more difficult to authenticate an entity.Confidentiality can be achieved via encryption. Authentication can be achieved by using amessage authentication code (MAC) (Menezes, Oorschot& Vanstone, 1996).
- **Integrity:** The goal of integrity is to keep a sent message from being illegally altered or destroyedduring transmission. When the data is sent through the wireless medium, the data can be modifiedor deleted by malicious attackers. The malicious attackers can also resend it, an action known as areplay attack. Integrity can be achieved through hash functions.
- **Non-repudiation:** The goal of non-repudiation is related to the fact that if an entity sends amessage, the entity cannot deny that it sent the message. By producing a signature for themessage, the entity cannot later deny having sent that message. In public key cryptography, anode, A, signs the message using its private key. All other nodes can verify the signed messageby using A's public key, and A cannot deny that its signature is attached to the message.
- **Availability:** The goal of availability is to keep the network service or resources available tolegitimate users. It ensures the survivability of the network despite malicious incidents. In a WSN,the examples of risk of loss of availability can be sensor node capturing and denial of serviceattacks. One solution could be to provide alternative routes in the protocols employed by theWSN to mitigate the effect of outages.
- **Access control:** The goal of access control is to prevent unauthorized use of network services andsystem resources. Obviously, access control is tied to authentication attributes. In general, accesscontrol is the most commonly needed service in both network communications and individualcomputer systems.

Cryptography is very strongly tied to mathematics and number theory. It is, therefore, difficult tocreate a new design using composite cryptographic techniques without the sound security analysis behindit, usually based on cryptographic reasoning. One way to reach this goal is to learn from others byreviewing the current MANET/WSN security schemes, and also to understand the network to furtherunderstand how cryptographic techniques combine with MANETs/WSNs to provide a security servicewith reasonable network performance, scalability, storage, and synchronization. Certainly the securitydesign can be evaluated using different techniques. Our goal is to provide perspective using cryptographictechniques and study basic cryptographic techniques (as seen in Figure 1) when applied to authentication,trust, and key management in MANETs/WSNs. Furthermore, we can study several of the mostcommonly-used cryptographic techniques and see how they are employed to deal with different tasks andbalance security and performance.

It is a common approach today to use software engineering design patterns to illustrate the design ofobject-oriented programming. Likewise, in security and performance of MANETs/WSNs, cryptographictechniques can successfully be used in different stages of network bootstrap, packet communication, andfactors to be evaluated. These techniques can certainly be reused after the analysis as known techniquesfrom the cryptography perspective. One of the approaches we take here is to break down the design usingcryptographic techniques and do some reverse engineering, then see how the new design is formed usingdifferent cryptographic techniques.

CONCLUSION

Cryptography is used to ensure that the contents of a message are confidentiality transmitted and wouldnot be altered. Confidentiality means nobody can understand the received message except the one thathas the decipher key, and "data cannot be changed" means the original information would not bechanged or modified; this is done when the sender includes a cryptographic operation called a hashfunction in the original message. A hash function is a mathematical representation of the information,when information arrives at its receiver; the receiver calculates the value of this hash function. If thereceiver's hash function value is equivalent to the sender's, the integrity of the message is assured. Inthis survey paper we describe and compare between symmetric and asymmetric encryption technique. Cryptology presents a difficulty not found in normal academic disciplines: the needfor the proper interaction of cryptography and cryptanalysis. This arises out of the fact that in theabsence of real communications requirements, it is easy to propose a system that appearsunbreakable. Many academic designs are so complex that the would–be cryptanalyst doesn'tknow where to start; exposing flaws in these designs is far harder than designing them in the firstplace. The result is that the competitive process, which is one strong motivation in academicresearch, cannot take hold.

Many applications are useful in real-time and daily life that areimplementd bycryptography through implicit or explicit concept of it.For example banking system,ATMcards, Smart cards, Magnetic strip technology,National Security Agency(NSA) to traceinformation through RADAR and with well equipped material,E-commerce,E-economics,business information,operating systems,databases and finally in System Protection.In this way Cryptography has many roles and many applicationprovide many example to show the differences.

REFERENCES:

- M. Bellare, V. T. Hoang and P. Rogaway.
  Adaptively Secure Garbling with Applications to One-Time Programs and Secure Outsourcing.
  Advances in Cryptology - Asiacrypt 2012 Proceedings, Lecture Notes in Computer Science Vol. 7658, X. Wang and K. Sakoeds, Springer-Verlag, 2012.
- M. Bellare, K. Paterson and S. Thomson.
  RKA Security beyond the Linear Barrier: IBE, Encryption and Signatures.
  Advances in Cryptology - Asiacrypt2012 Proceedings, Lecture

Notes in Computer Science Vol. 7658, X. Wang and K. Sakoeds, Springer-Verlag, 2012.

- Canetti, R., Krawczyk, H.: Universally composable notions of key exchange andsecure channels. In: Knudsen, L. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp.337–351. Springer, Heidelberg (2002)
- Cortier, V., Delaune, S.: Safely composing security protocols. Formal Methods inSystem Design 34(1), 1–36 (2009)
- Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions onInformation Theory 22, 644–654 (1976)
- Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactiveproof systems. SIAM J. Comput. 18(1), 186–208 (1989)
- Gross, T., M¨odersheim, S.: Vertical protocol composition. In: 24th IEEE ComputerSecurity Foundations Workshop (CSF 2011)
- Guttman, J.D., Thayer, F.J.: Protocol Independence through Disjoint Encryption.In: Computer Security Foundations Workshop, pp. 24–34 (2000)
- Maurer, U.: Secret key agreement by public discussion from common information.IEEE Transactions on Information Theory 39(3), 733–742 (1993)
- Maurer, U.: Indistinguishability of random systems. In: Knudsen, L.R. (ed.)EUROCRYPT 2002. LNCS, vol. 2332, pp. 110–132. Springer, Heidelberg (2002)
- Maurer, U.: Abstraction in cryptography. In: Halevi, S. (ed.) CRYPTO 2009.LNCS, vol. 5677, p. 465. Springer, Heidelberg (2009)
- Publication 197 - Announcing the Advanced Encryption Standard (AES). FederalInformation Processing Standards, 26 Nov. 2001.
- Ralston, Anthony, Edwin D. Reilly, and David Hemmendinger. Encyclopedia ofComputer Science. Fourth ed. London, England: Nature Publishing Group, 2000
- Rosen, Kenneth H. Elementary Number Theory and Its Applications. Boston:Pearson/Addison Wesley, 2005.
- Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. New York: Wiley, 1996.
- Trappe, Wade, and Lawrence C. Washington. Introduction to Cryptography: withCoding Theory. Upper Saddle River, NJ: Prentice Hall, 2002.
- Stinson, Douglas R. Cryptography: Theory and Practice. Boca Raton: Chapman & Hall/CRC, 2002.
- Wolfram, Stephen. A New Kind of Science. Champaign, IL: Wolfram Media, 2002.
- Michel Abdalla, Emmanuel Bresson, Olivier Chevassut and David Pointcheval,
  Password-based Group Key Exchange in a Constant Number of Rounds, Public Key Cryptography - PKC 2006, Moti Yung, YevgeniyDodis, AggelosKiayias, and Tal Malkin (Eds.), LNCS 3958, pp. 427-442, Springer-Verlag, April 2006.
- Michel Abdalla, MalikaIzabachène, and David Pointcheval,
  Anonymous and Transparent Gateway-based Password-Authenticated Key Exchange,
  7th International Conference on Cryptology and Network Security - CANS 2008, LNCS 5339, pp. 133--148, © Springer, Matthew Franklin, Lucas Hui, and Duncan Wong (Eds.), December 2008.
- Novak, R.: SPA-Based Adaptive Chose n-Ciphertext Attack on RSA Implement ation. In Naccache, D., ed: Public Key Crytography 2002. Volume 2274 of LN CS., Springer, 2002, pages 252-262.