Modern Cryptography: Approaches and Attacks

N. Gurutharsan, R. Hareesan, K. Kanarupan, R. Rajkumar, S. Sathiyavarthan
Department Of Computer Science & Engineering, University of Moratuwa

Abstract — *Information is in many forms and it is everywhere. Information is to be exchanged. At present communication systems are well developed and widely used. There arise the issues regarding the Security Measurements. The 'security impose' tends to trade off with communication speed. Cryptography is the main methodology used in security enforcement over information exchanges. With time the requirements change and so does the approaches for cryptography. With fresh approaches there emerge new attacks. This paper tends to analyze the generalized approaches and attacks over time and it is restricted (only) to the Computer Era (computer and internet related cryptography).*

Index Terms — Cryptography, Perspective, Security Pitfalls, Infrastructure

I. Introduction

At present, the computers and the internet are used in Commercial, Academic, knowledge, defensive (military) and medical requirements to exchange and share information. The value of information depends on the context (subjective) and it has no upper limit. Information can be considered as the most valuable thing on earth. Thus ensuring security elements like Confidentiality, integrity, authenticity and non-repudiation (only major elements are given) is essential to perform almost any task over this planet. Trust and Trustworthiness, the core of 'belief' can only be formed by asserting security on the information.

When we consider about cryptography, there are three types of views for a complete look up.

A. Users' perspective

This is the perspective of passive users who rely on the Cryptographic Services. Their view is limited only to high level of abstraction. The major requirements will be the general knowledge in the field (Cryptography, Security attacks and services) rather than the core implementing details.

B. Defenders' perspective

Defenders are interested in bit more specific details, comparisons of implementing methodologies, commercialization issues, Regulatory/ Legislative constraints, design pitfalls and modeling an optimized solution. The failure history and evolving trends are some of the other tracts that a designer should be interested in. There is another type of a group is pretty much interested in the above details. They are mentioned next.

C. Attackers' perspective

Attackers are the human beings (probably evil type ☺) who try to exploit the vulnerabilities of a system to breach security barriers to do undesirable things.

They are pretty much interested in tracing vulnerabilities, knowing attacking methodologies and learning techniques to implement their plan. Attacker is willing to know all the details that a designer does to improve their (attacker's) success.

These three perspectives are discussed to a reasonable extent in the paper.

A. From Users' Perspective

II. Cryptography

One of the generic definitions is "Cryptography is the study of 'mathematical' for solving two kinds of security problems: Privacy and Authentication" [1].

Cryptology is almost synonymous with encryption (not exactly), the process of converting ordinary information, plaintext into unintelligible information, cipher text, thus rendering it unreadable by interceptors or eavesdroppers. Decryption is the reverse, moving from the unintelligible cipher text back to plaintext [2].

A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a key [2].

A. Issues regarding Security

Security problems arise among other things to resource and workload sharing; complexity of interconnected networks; authentication of users; fast expandability of networks; threats to networks such as wiretapping and violations of the seven pillars of security: authentication, authorization, privacy, integrity, non-repudiation, availability and audit [2].

Secured Communication is a current issue in the Crypto systems. Contemporary Crypto Systems are improved in both logical and implementation aspects but the KEY exchange over communication channel facilitates many open problems Efficiency of Communication and Cryptography are in a trade-off. Other main problem is the Authentication. At present the techniques used to shift the physical Signature phenomena (Authentication tool) into the Digital world is not satisfying [1].

B. Cryptography: Core details

Cryptography is interrelated with other fields such as Communication and Computation. The 'Information theory' and the 'Computation theory' are offspring of the above

mentioned fields. Attribute of communication channels (private or public) depends on Users' point of view. "Any channel may be threatened with eavesdropping or injection or both, depending on its user" [1].

Cryptography can be categorized as "Computational secure" and "Condition less Secure". Computationally secure: this could succumb to an unlimited computation attack. It delays. Unconditionally secure: no matter how much computation is allowed, it will be secure [1].

III. SECURITY SERVICES AND ATTACKS

A. Security attacks: Attacks classified based on behavior

1) Passive attacks

Eavesdropping or monitoring of transmissions. This type of attacks doesn't affect the system operations. Two types of passive attacks are release of message contents and traffic analysis.

Release of message contents: learning sensitive information such as telephone conversations and emails.

Traffic analysis: observe pattern of massage being sent between two.

These passive attacks are very difficult to detect because they aren't changing anything but just observe.

2) Active attacks

Modifying contents or creating false stream. Thus this affects the system operations. It can be divided into four categories.

Masquerade: one entity pretends to be different entity.

Reply: capture massage from one and later reply massage to another.

Modification of messages: simply means that some portion of a legitimate message is altered.

Denial of service: prevents or inhibits the normal use or management of communications facilities.

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.

B. Security services (Based on [3])

1) Authentication

The service assures that the two entities are authentic, that is, that each is the entity that it claims to be and the service must assure that the connection is not interfered with in such a way that a third party can masquerade.

There are two types: peer entity authentication, data origin authentication.

2) Access control

Ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

3) Data confidentiality

Protection of transmitted data from passive attacks. The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

4) Data integrity

Assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service. On the other hand, a connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only.

5) Non repudiation

Non repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

6) Service availability

Property of a system or a system resource being accessible and usable upon demand by an authorized system entity.

C. Security mechanisms related to Cryptography

1) Encipherment

The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

2) Digital Signature

Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

There are other methods such as Access Control, Data Integrity, Authentication Exchange, Traffic padding, Routing, Notarization, Trusted Functionality, Security Label, Event Detection, Security Audit Trail and Security Recovery[3].

From here will shift the view to the Defenders' perspective.

B. From Defenders' Perspective

IV. CRYPTOGRAPHIC APPROACHES

Modern cryptography is based on a scientific approach and

cryptographic algorithms are around 'computational hardness'. Even though theoretically they are unbreakable it is not practical (it is quite possible to unbreakable, but legal and other practical issues will congest [4]).

A. Symmetric-key Cryptology

It is a system in which the sender and the receiver share the single, common key that is used to both encrypt and decrypt the message. So all the security if the system is based on this symmetric key. If some unauthorized parties get this key, they can read message. In order for an algorithm of this type to be considered as reliable, there is one requirement must be accomplished. That is, unauthorized users must not be allowed to get both cipher text and plain text, because knowing both of them is enough to discover the key. Main drawback is that the two parties must somehow exchange the symmetric key in a secure way [6].

B. Public-key Cryptography

Asymmetric encryption uses a pair of keys rather than one key as used in symmetric encryption. This single-key encryption between the two parties requires that each pair of party has its secret key, so that as the number of parties increases so does the number of keys. In addition to this, the distribution of the secret key gets unmanageable as the number of keys increases. Of course, a long-time use of the same secret key between any pair would make it more vulnerable to crypto analysis attack. So to deal with these inextricable problems, key distribution facility was born [2].

C. The Rijndael algorithm

It is a type of symmetric key algorithm. It is more computationally efficient and supports key length up to 256 bits which is very hard to discover by unauthorized users. It is also relatively easy to implement and requires very little memory [6].

D. The RSA algorithm

It is a type of an Asymmetric key algorithm. This is based on the fact that make impossible or make hard to discover the private key. Deducing an RSA key, therefore, requires an extraordinary amount of computer processing power and time. As RSA provides secure communication over distances, it has become a standard for industrial-strength encryption [6].

E. Visual Digital Signature Scheme

A digital signature can provide the functionality of a hand written signature. The concept of digital signature has been introduced by Diffie and Hellman in 1976 [5].

Most of the current digital signatures include more complex mathematical computations and algorithms. So the sender has to depend on his computer to make a digital signature and the receiver computer checks the validity of the signature.

Digital signature is a verification method requires the signature holder to have two keys: the private-key (signature key) for signing a message and the public-key (verification key) for verification of authenticity of the message [5].

F. Identity-Based Encryption/ Decryption

1) Identity-Based Encryption

IBE is a type of Public Key Encryption (PKE), in contrast to PKE (Public Key Encryption), IBE does not have a distinct public key. Rather public key is created by some information about users, Email address for instance. So user's identity serves the public key's role. The user's private key is created by a trusted 3rd party.

2) Advantages of IBE over PKE

a) Less initialization

Private Key is issued by the trusted authority. So Alice can encrypt messages to Bob, even if Bob does not have the private key yet. That is to say, Bob does not have to be initialized into the system.

b) Less intercommunication

Bob's public key does not need to be communicated with Alice. So there is less communication than in PKE.

c) Less computational overhead in Encryption

PKE relies on Public Key Infrastructure (PKI) to authenticate public keys. PKI involves various validations those are not in the PKE.

3) Advantages of PKE over IBE

IBE has key escrow whereas PKE does not, Key escrow is the capability trusted authority to decipher Alice's cipher tests to Bob. In PKE, Alice can establish trust in Bob's public key. If Alice relies on the certification authority to trust the Bob's public key, then the Bob's public key can easily be faked out completely by some malicious entity.

4) Advantages of Identity-Based Decryption

IBD has most of the advantages mentioned above that IBE has over PKE: Less initialization, less communication, less computational overhead and escrow key. However some distinctions between IBE and IBD are,

a) In IBE, Bob has a private key which decrypts cipher texts. Bob only need to communicate with 3rd party once for each identity string. This is an advantage of IBE over IBD.

IBD can be easily realizable using any secure PKE, but IBE seems to require more specialized techniques. This is an advantage of IBD over IBE.

V. Commercialization of Cryptography

The methods being implemented in securing transaction is cryptography, more specifically public key encryption. In the early days, only the governments used cryptography. Then the

usage of cryptography became important to private sector with the growth of business competitions. Cryptography is a powerful tool used by governments in enforcement of law. Since some legitimate issues emerged.

An example scenario is described below.

The US government's reaction to the commercialization of cryptography within private sector was to legislate to prevent using the keys cannot be broken by them. If a stronger key has been used, that should be recoverable by the US government. With these all legislations, the companies wondered which technology to use and protect their information and intellectual assets as they try to deliver electronic commerce transactions through the Internet.

Then they come up with two different architectures.

A. Technologies supporting the government position that include the cryptography key management systems capable of key escrow.

B. Technologies that are flexible and can support either keying method but address commercial needs (rather than government needs), not necessarily providing key escrow.

The government was looking to enforce the law by accessing all data and the companies were looking to save their data with strong keys. Government came up with a choice for companies such as, either use a key pair that is low enough in strength that the government can break the cryptography, or use a higher strength key, but the key must be escrowed (or recoverable) to ensure the US government can gain access whenever they feel necessary for law enforcement purposes.

However large amount of companies do not wish to use low strength keys because, if the government can break the keys, that means, another company also can do so. So it makes data vulnerable to attack.

There are two keys of public key infrastructure. First one is key management, and second one is certificate management.

Companies that require security now should use the low cost security provided through third parties, unless their security needs are exclusively for internal use. If exclusively internal, then lowest-cost security should be used.

VI. Security of Modern Devices

At present embedded and hand held devices are widely used. Under this section we will discuss those security facilitations. As a narrowing down step, our discussion will be based on Java supported security methodologies.

For easy prototyping and to be platform independent, the security applications are first developed in Java. Two Java cryptographic libraries, the Bouncy Castle API and IAIK API are ported to a real embedded device for cost and performance evaluation.

The bouncy castle API was developed by the Legion of the Bouncy Castle, and the package is organized so that it contains a light weight API suitable for use in any environment (including the newly released J2ME) with the additional infrastructure to conform the algorithms to the JCE framework. And the IAIK API architecture has been introduced by Java Cryptographic Architecture (JCA) making it possible for different cryptographic implantations to operate on common interfaces.

Nowadays applications for mobile devices become more usage and complex with new features and services over the network, such as online banking e-commerce, user and server authentication, and so on. At the same time, in mobile devices battery life is more essential thing over the applications. It is clear that these mobile devices require low power embedded security. So here new types of encrypt/decrypt technologies used to do more efficiently with low consumption of battery.

The KVM is part of the smallest runtime environment and included in the Java Platform, Micro Edition (Java ME, formerly J2ME platform) software for use in devices with limited memory and CPU power. Cell phones, pagers, and personal digital assistants (PDAs) frequently run a KVM to provide common computing features. KVM is used on cellphones and mobile devices whereas JVM is used on computers. For the performance optimization, we use the GEZEL design environment which allows us to move computational intensives modules to dedicated co-processors. To avoid bugs and potential security weaknesses, the GEZEL design environment allows co-simulation of the code running on the KVM and the cryptographic co-processors in a cycle-true manner.

We can use GEZEL design environment for modeling and simulating the hardware accelerator of cryptographic algorithms. It expresses the Finite State Machine and Data path (FSMD) and its simulation environment. For the performance optimization, we propose three methods of acceleration such as acceleration in C, acceleration in Assembly, acceleration in GEZEL. If the performance of the Java implementation of a cryptographic algorithm is not enough, the algorithm can be transferred from Java into C and executed via the K Native Interface (KNI) provided in J2ME/CLDC platform.

The SH3-DSP embedded processor core has been chosen as a target platform of the design. SH3-DSP is a 32bit RISC microprocessor core with a DSP unit, and is also known as the core of the SH-Mobile processor, it's the most popular one of the application processor specialized next generation cellular phone communication. Java has some built in security features with three different levels of security policies. The Java Cryptography Extension (JCE), the Java Secure Socket

Extension (JSSE), and the other Cryptographic extensions such as the Bouncy Castle Crypto API and IAIK API are provided to ensure the End-to-End security in Java.

VII. Security Pitfalls in Cryptographic Design

Even though stronger encryption algorithms are used, they can be circumvented by bypassing them (algorithms) altogether and exploiting their vulnerabilities. It will be important to prevent and detect the attacks. As any systems can be attacked it is important to take cautious actions to minimize the level of damage and keep track (the history) of the attacks for future purposes.

The strength of the cryptographic system is mainly depends on its encryption algorithm, digital signature algorithm, one-way half functions and message authentication codes it relies on. Improper implementation of any of the above will result in a weak cryptographic system [6].

Random-number generators (Cryptographic) are hard to design and build due to the constraints in both hardware and software level.

"The cryptography may be strong, but if the random-number generator produces weak keys, the system is much easier to break. Other products use secure random-number generators, but they do not use enough randomness to make the cryptography secure. Also those specific random-number generators may be secure for one purpose but insecure for another; generalizing security analyses is dangerous" [6].

"Detection and Prevention of the attack" is the main concern of the defenders. A design principle says that sooner or later any system will be successfully attacked. Thus detecting, planning for recovery and promulgate a new key pair is important.

"A good security product must defend against every possible attack, even attacks that have not been invented yet." Thus, actually it is very hard to ensure the absolute security. Any level of "BETA" testing can't reveal the vulnerabilities. Even theoretical implementation (Applied Cryptography) is not a panacea for the security problem [6].

In the coming sections we will view Cryptographic Systems in the Attackers perspective.

VIII. Failure of Public Infrastructure

A. PKI- public key infrastructures

PKI is as an infrastructure that can be used to issue, validate, and revoke public keys and public key certificates.The widespread use of public key cryptography (in section 4.2) requires a public key infrastructure. The aim of a PKI is to make sure that a public key in use really belongs to the claimed entity. Without a PKI, public key cryptography would only be marginally more useful than traditional secret key cryptography. During boom time, the developers of PKIs expected not only to solve most problems concerning the security of transferred data, but also to provide general solutions for e-commerce. However, and in contrast to these relatively high expectations, PKIs have not really taken off.

B. Reason for the PKI failure

1) Technical reasons

a) Complexity

The complexity is due to the fact that X.509 certificates comprise many fields but moreover, comprise many (critical and/or non-critical) extension fields

b) Certificate management

Certificate management is a complex and very challenging task, and there are many things that can go wrong.

c) Global name space

The definition and maintenance of a global name space is not as simple in practice as theory suggests.

d) Cross certification

2) Economic reasons

a) Large investments

The establishment and operation of a PKI requires large investments. For example, the PKI must be established and operated in a physically secure environment.

b) Return on investment

If the establishment and operation of a PKI requires a large investment (as mentioned above), then the ROI is particularly important. Unfortunately, the ROI of a PKI is very difficult to determine and quantify.

3) Legal reasons

a) Non- repudiation

The owner of a public key certificate cannot repudiate a signature that is generated with the appropriate signing key.

b) Poor usability

The usage of public key cryptography in general, and public key certificates in particular, is less trivial than postulated by vendors.

c) Lack of awareness

The users of public key cryptography are often not aware of the vulnerabilities and pitfalls.

C. From attackers' perspective

IX. Attacks: Classified based on subjects (Based on [6])

A. Attacks against Implementations

The methodology of implementation can be prone to vulnerabilities. Memory transactions, usage and the exchange of master and session keys and other extreme cases the keys are vulnerable to the attackers.

B. Attacks against Passwords

Password selection (keeping it simpler) of users, number of character space given (varies with each interface) and weak recovery process are prone to disclose the password to the attackers.

C. Attacks against Hardware

Uses tamper-resisting hardware proof. The assumptions of terminal safety (e.g.:- dongles, electronic wallets etc.) are taken into the account.

D. Attacks against trust models

The systems depend on other systems and attacks on that that trusted models can weaken the overall system.

E. Attacks against users

This problem occurs due to the incautious actions by the users thus no system can solve the problem but can help to avoid those.

F. Attacks against failure recovery

Attackers can use the failure recovery procedure to penetrate into the system. Thus the system designers should be structure the system having these in mind.

G. Attacks against Cryptography

There were instances where wrong Cryptography is used or it faces conflicts during the implementation.

X. Cracking keys (An Interesting Example of a way of attack)

One of the most important mechanisms in cryptography is Random Number Generator which will generates a sequence of random numbers as the name suggests. What we basically mean by cryptography is alter the plain text (original message to me transmitted) into cipher text (encrypted message) which cannot be read without the key. The crypto system will change our original message into binary forms by applying some methods, applying A-01, B-02,…,Z-26 for example, then add the output numbers generated by the random number generator to get the cipher text. That's it. The cipher will be transmitted over line. Crypto system at the receiver site will generate the same random numbers using same generator and subtract these sequence of random numbers from cipher text to get the plain text.

Unless someone knows the key, it means unless someone knows the sequence of random numbers, the cipher text cannot be decrypted. If someone cracks the random number generator, he can read the whole message.

A scenario of a code break is stated below.

Let's say someone intercept the line and get the cipher text. Then this unauthorized person will try to discover the key. What he has to do is, he just has to guess a word in the original message (if this is the line between Pakistan and Israel, then one possible guess is "PAKISTAN").

Then he will place guessed word at one position in the cipher text, subtract those to get the key. After that he will decrypt the whole message using derived key. If it will be a meaningful text, that is the correct key. If it is not a meaningful message then the key he derived is wrong. So he tries to place this guessed word in another position and repeat the same thing until arrive a correct key: it means key repeats the same thing until the derived key will decrypt a meaningful message.

Eventually he can get the correct key and decrypt the message. He cracks a Random Number Generator!

XI. CONCLUSION

In this paper, we discussed about cryptography in different perspectives. The concept and core details of the Cryptography are been given. The anticipated security requirements and compromises regarding the speed and the type of communication are discussed. The modern approaches are described and the Design Impairments and failures are analyzed. Finally the current cryptographic model is analyzed from an attacker's point of view. Here we wish to highlight some major concerns in the Paper.

a) As techniques of Information security changes, so does the attacks technique.

b) There is no perfect solution. Even though theoretically proven, those methodologies are harder to abide practically. Thus we use methods that optimize.

c) There are legal concerns when dealing with cryptography.

REFERENCES

[1] WHITFIELD DIFFIE AND MARTIN E. HELLMAN, "New directions in Cryptography", MEMBER, IEEE, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976. http://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf

[2] Cryptography: A security pillar of privacy, integrity and authenticity of data communication, BhushanKapoor, (California State University, Fullerton, California, USA and Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, USA), PramodPandya, (California State University, Fullerton, California, USA and Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, USA), Joseph S. Sherif, (California State University, Fullerton, California, USA and Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, USA), http://www.emeraldinsight.com/journals.htm?articleid=17003516&show=html

[3] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall Pub, November 16, 2005. Source: http://www.filestube.com/bO1DqNe86Fzvq4had8Bzz2/Cryptography-and-Network-Security-Principles-and-Practices-4th-Ed-William-Stallings.html

[4] An overview of modern cryptography Ahmed Al-Vahed * Haddad Sahhavi, Mathematic School of Fada Mathematic School of Fada http://www.waprogramming.com/papers/vol1-no1/(03-08)%20An%20overview%20of%20modern%20cryptography.pdf
Judit Bar-Ilan, "Security issues on the Internet", Electronic Library, the, Vol. 14 Iss: 1, pp.37 – 42, 1996.Source: http://www.emeraldinsight.com/journals.htm?issn=0264-0473&volume=14&issue=1&articleid=1668182&show=html

[5] Cryptography, Tom Davis, tomrdavis@earthlink.net http://www.geometer.org/mathcircles, February 7, 2000 http://www.geometer.org/mathcircles/crypto.pdf

[6] Francisco A. Pujol, Higinio Mora, José Luis Sánchez, Antonio Jimeno, "A client/server implementation of an encryption system for fingerprint userauthentication", Kybernetes, Vol. 37 Iss: 8, pp.1111 – 1119, 2008 Source: http://www.emeraldinsight.com/journals.htm?issn=0368-492X&volume=37&issue=8&articleid=1741988&show=html

[7] Carrie Liddy, "Commercialization of cryptography", Information Management & Computer Security, Vol. 5 Iss: 3, pp.87 – 89, 1997 Source: http://www.emeraldinsight.com/journals.htm?issn=0968-5227&volume=5&issue=3&articleid=862688&show=html

[8] Junbaek Ki, Jung HeeCheon, Jeong-Uk Kang, Dogyun Kim, "Taxonomy of online game security", Electronic Library, the, Vol. 22 Iss: 1, pp.65 – 73, 2004.
Source:http://www.emeraldinsight.com/journals.htm?issn=0264-0473&volume=22&issue=1&articleid=862043&show=html

[9] Javier Lopez, Rolf Oppliger, GüntherPernul, "Why have public key infrastructures failed so far?", Internet Research, Vol. 15 Iss: 5, pp.544 – 556, 2005
Source:
http://www.emeraldinsight.com/journals.htm?issn=1066-2243&volume=15&issue=5&articleid=1528695&show=html
Bruce Schneier ,"Security pitfalls in cryptographic design", President,Counterpane Systems, Minneapolis, MI, USA,1998 (President, Counterpane Systems, Minneapolis, MI, USA)http://www.emeraldinsight.com/journals.htm?articleid=862716&show=pdf

[10] Ian Curry, "An Introduction to Cryptography and Digital Signature",March 2001

[11] John Loughran, and Tom Dowling, "A Java Implemented Key Collision Attack on the Data Encryption Standard (DES)" ACM Digital Library PPPJ '03 Proceedings of the 2nd International Conference on Principles and Practice of Programming in Java,
20 Oct. 2003.
Source: http://dl.acm.org/citation.cfm?id=957289.957335.

[12] D.M. Hutton ,"Java Cryptography (J2ME)" Emerald Group Publishing Limited,July 1, 2001
Source: http://www.emeraldinsight.com/journals.htm?articleid=1472147

[13] Yusuke Matsuoka, and Patrick Schaumont, "Java Cryptography on KVM and Its Performance and Security Optimization Using HW/SW Co-design Techniques."ACM Digital Library. CASES '04 Proceedings of the 2004 International Conference on Compilers, Architecture, and Synthesis for Embedded Systems,
16 Sept. 2004.
Source: http://dl.acm.org/citation.cfm?id=1023833.1023874

[14] Johnny Li-Chang Lo, and Judith Bishop, "Component-based Interchangeable Cryptographic Architecture for Securing Wireless Connectivity in JavaTM Applications ", ACM Digital Library SAICSIT '03 Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology,
12 Nov. 2003
Source: http://dl.acm.org/citation.cfm?id=954014.954047

[15] SomeswarKesh, Sam Ramanujan, Sridhar Nerur, "A framework for analyzing e-commerce security", Information Management & Computer Security, Vol. 10 Iss: 4, pp.149 – 158, 2002
Source: http://www.emeraldinsight.com/journals.htm?issn=0968-5227&volume=10&issue=4&articleid=862824&show=html

[16] Billy B.L. Lim, Yan Sun, Joaquin Vila, "Incorporating WS-Security into a Web services-based portal", Information Management & Computer Security, Vol. 12 Iss: 3, pp.206 – 217, 2004
Source: http://www.emeraldinsight.com/journals.htm?issn=0968-5227&volume=12&issue=3&articleid=862874&show=html

[17] David C. Chou, David C. Yen, BinshanLin, Philip Hong-Lam Cheng, "Cyberspace security management", Industrial Management & Data Systems, Vol. 99 Iss: 8, pp.353 – 361, 1999
Source: http://www.emeraldinsight.com/journals.htm?issn=0263-5577&volume=99&issue=8&articleid=849966&show=html
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, "New directions in Cryptography", MEMBER, IEEE, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976.

[18] Tom Davis, "Cryptography", February 7, 2000.
Source: http://www.geometer.org/mathcircles

[19] James Reed ,"Cracking a Random Number Generator", January 1977, Volume 1, Number 1, issue of Cryptologia (pp. 20-26)
Source: http://www.dean.usma.edu/math/pubs/cryptologia/

[20] Thomas Jacobsen, "A fast method for crytanalysis of substitution ciphers."
Source: http://www.dean.usma.edu/math/pubs/cryptologia/

[21] AJ. Menezes and P. C. van Oorschot and S. A. Vanstone,"Handbook of Applied Cryptography", CRC Press, 1996
Source: http://www.cacr.math.uwaterloo.ca/hac/

[22] D. Stinson, "Cryptography Theory and Practice", CRC Press, February 2002.
Source: http://bitsnoop.com/cryptography-theory-and-practice-th-q32066908.html

[23] Cryptography ,Tom Davis ,tomrdavis@earthlink.net http://www.geometer.org/mathcirclesFebruary7,2000 http://www.geometer.org/mathcircles/crypto.pdf

[24] Visual Digital Signature Scheme http://www.iaeng.org/IJCS/issues_v37/issue_4/IJCS_37_4_04.pdf

[25] Identity-Based DecryptionDaniel R. L. Brown May 30, 2011 http://eprint.iacr.org/2011/266.pdf