ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SURVEY OF CRYPTOGRAPHY IN NET SECURITY USED IN E-COMMERCE –A TOOL FOR SAFETY

Aamir Khan*, Akanksha Kesari, Aboli Sarode, Arti Dhanotiya, Arti Bansal, Apeksha Suryavanshi
Computer Science & Engineering, Acropolis Institute of Technology and Research, Indore (M.P.)-452001, India

DOI: 10.5281/zenodo.48392

ABSTRACT

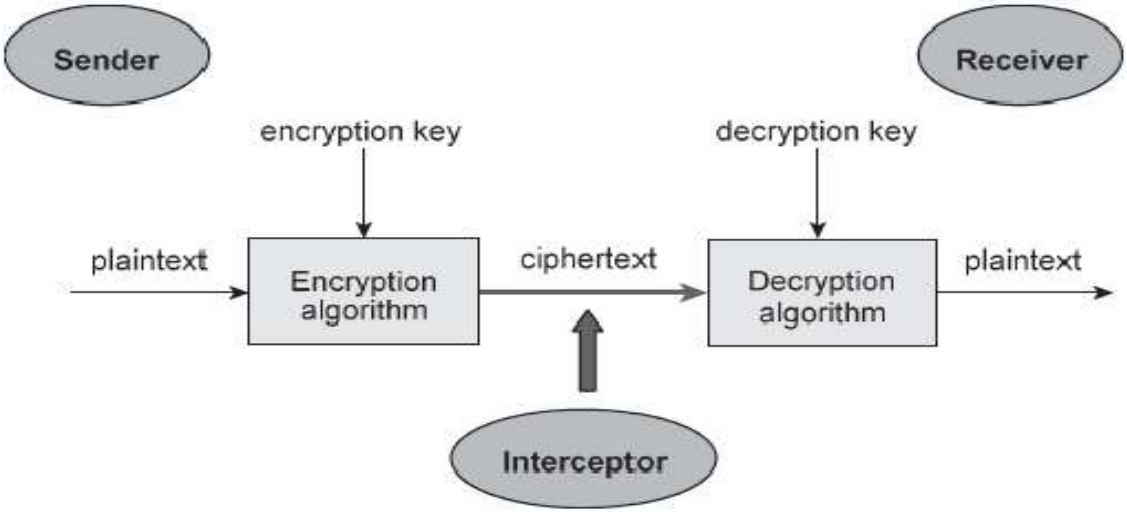
Today the use of computers in every one life is a common and easy way to improve day to day life and to lead the community at large to nurture the benefits of modern technologies, but this common path needs security, in its operations. In the early part of 21st Century computer networks were used as a daily tool for a human being for sending e-mails, making online transactions, sharing devices. The art of secret writing is 'CRYPTOGRAPHY', which enables a secured communication between two people over an insecure channel in such a way that the other opponents in the path cannot harm the communicators .This article throws light on process of sharing the information to a form that will be unintelligible to an unintended person by symmetric and asymmetric cryptography. It helps to understand the creation of basic 'CRYPTOSYSTEM', and also focus on the difficulties and challenges in use of cryptography in network security ,with a suggested solution on the problem .The sender and recipient may use same key and encryption /decryption algorithm to encrypt /decrypt given data or may use different key in public key cryptography. All secure data transactions including defence, net payment, access control, business and e-commerce apply cryptography in their operations to safeguard their interests. The use of cryptography technique is the reliable modern tool to build a fair system of confidentiality, integrity and control access, availability & authentication of data. The art and science of concealing the message to introduce secrecy in information security is Cryptography. As the cipher text is public and attackers can get the information and in asymmetric cryptography it require more processing power and computational time we present ECC and quantum computational algorithm.

KEYWORDS: Encryption, Decryption, Cryptanalysis, key.

INTRODUCTION

Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785



COMPONENTS OF A CRYPTOSYSTEM

The various components of a basic cryptosystem are as follows:

Plaintext: It is the data to be protected during transmission.

Encryption Algorithm: It is a mathematical process that produces a cipher text for any given plaintext and encryption key. It is a cryptographic Algorithm that takes plaintext and an encryption key as input and produces a cipher text.

Cipher text: It is the scrambled version of the plaintext produced by the encryption algorithm using a specific encryption key. The cipher text is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.

Decryption Algorithm: It is a mathematical process, that produces a unique plaintext for any given cipher text and decryption key. It is a cryptographic algorithm that takes a cipher text and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.

Encryption Key: It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the cipher text.

Decryption Key: It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the cipher text in order to compute the plaintext.

TYPES OF CRYPTOSYSTEMS

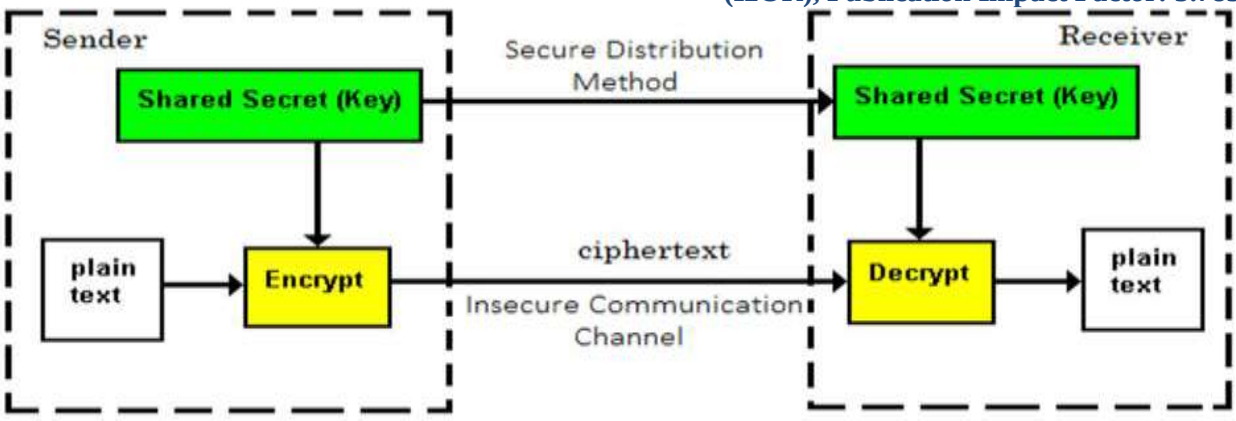
Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system:

A. Symmetric Key Encryption
B. Asymmetric Key Encryption

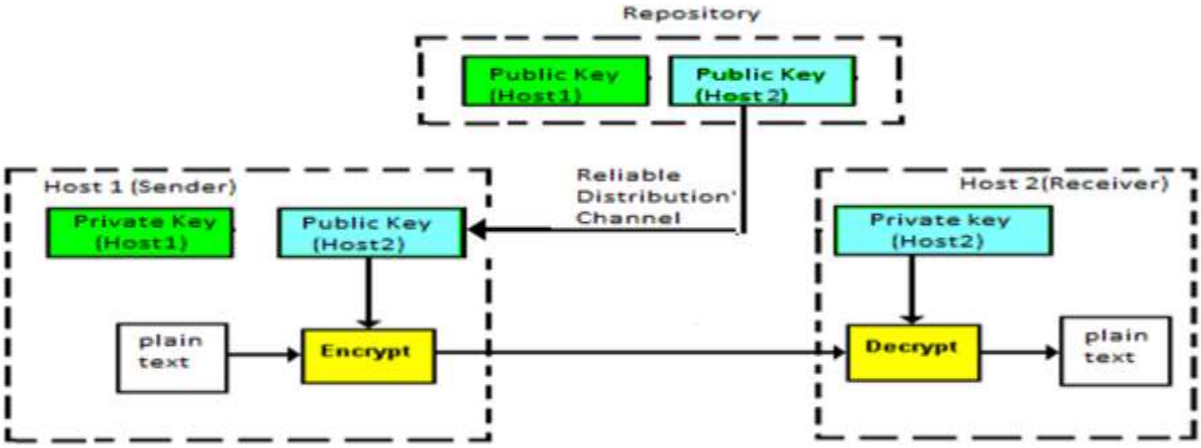
Symmetric Key Encryption:

The encryption process where **same keys are used for encrypting and decrypting** the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is referred to as **symmetric cryptography**. Symmetric cryptosystems are also sometimes referred to as **secret key cryptosystem.**



Asymmetric Key Encryption:
The encryption process where **different keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting cipher text is feasible.



SECURITY SERVICES OF CRYPTOGRAPHY

The primary objective of using cryptography is to provide the following four fundamental information security services. Goals intended to be fulfilled by cryptography.

Confidentiality:
Confidentiality is the fundamental security service provided by cryptography. It is the security service that keeps the information confidential from an unauthorized person.

Data Integrity:
It is the security service that deals with identifying any alteration's made to the data. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user.

Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

Authentication:
Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.
Authentication service has two variants:

A. **Message authentication** identifies the originator of the message without any regard router or system that has sent the message.
B. **Entity authentication** is assurance that data has been received from a specific entity, say a particular website.

Non-repudiation:
It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party.

CRYPTOGRAPHY – DRAWBACKS

Apart from the four fundamental elements of information security, there are other issues that affect the effective use of information:

I. A strongly encrypted, authentic, and digitally signed information can be **Difficult to access even for a legitimate user** at a crucial time of Decision-making. The network or the computer system can be attacked and rendered non-functional by an intruder.
II. **High availability**, one of the fundamental aspects of information security, cannot be ensured through the use of cryptography. Other methods are needed to guard against the threats such as denial of service (Dos)or complete breakdown of information system.
III. Information security of **selective access control** also cannot be realized through the use of cryptography. Administrative controls and procedures are required to be exercised for the same.
IV. Cryptography does not guard against the vulnerabilities and **threats that emerge from the poor design of systems**, protocols, and procedures. This needs to be fixed through proper design and setting up of a defensive infrastructure.
V. Cryptography comes at cost. The cost is in terms of time and money:
VI. Addition of cryptographic techniques in the information processing leads to delay.
VII. The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome financial budget.
VIII. The security of cryptographic technique is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.

MODERN TRENDS IN THE WORLD OF CRYPTOGRAPHY

Developing perimeter security in networks helps to detect and prevent the attacks as early as possible, but the sheer volume of information in the age of Big Data often makes it difficult to detect anomalies that might indicate security issues.

Technological research challenges include binary hardening, network monitoring, IDS and IPS systems, and attack analysis. For instance, to detect and prevent attacks, we need techniques and tools to spot and remove vulnerabilities from software, and monitoring systems to raise an alarm when a system behaves in an anomalous manner.

In order to effectively detect such advanced malware – regardless of the attack methods being used, technology solutions are being developed which use a combination of sophisticated techniques to evaluate advance threats including checking real-time emerging campaigns and known new malicious websites that are being detected across organizations and static code analysis looking for suspicious behaviour, malicious code snippets, and redirects to other malicious sites. Solutions based on dynamic analysis by sandboxing the destination URL or attachments, to simulate a real user on a machine with a goal of observing any changes made to the system, are being worked on.

Command-and-Control Protection:
Any enterprise connected to the Internet can become a target of boot driven attack. Unlike widespread attacks, targeted boot net attacks are very stealthy in nature and are difficult to detect using traditional security solutions. However, despite their quiet nature, they can cause very expensive, sometimes irreparable damage to an organization.

By unique "fingerprint" detection of cloaked C&C traffic which can identify attackers' use of legitimate applications and websites as well as other advanced techniques, such as the use of internal C&C servers. Deep discovery custom sandbox analysis can also discover new C&C destinations of zero-day malware attacks and update the intelligent network and all customer security protection points.

Self-Defense Service
IT systems today are static and allow the adversary time to plan and launch attacks. As proposed by in latest research, layered and changing self-defense service prevents attackers from exploiting a target system by removing the static network & system attributes that simplify reconnaissance. Continuously refreshing the target system to a new virtual instance with a known trusted state and random service attributes, this limited-time-use virtual instance is comprised of a single application and OS combination and reduces system complexity.

Further development would proceed on a DNSSEC-aware application that will build on a successful the self-defence service prototype will focus on protecting web services, including web content delivery.

Cyber Security and Cryptography Focus Areas for Governments:
The governments around the world are eyeing continuous research in the field of cyber security to safeguard against the emerging and future threats. Some of the cyber security research areas that are in focus by various countries like Australia, Japan, Canada and USA are briefly mentioned below.

The Cyber Security Research Roadmap released by the Department of Homeland Security (DHS) in the US, identifies the following eleven hard problems that require R&D efforts:
a. Scalable trustworthy systems
b. Combating insider threats
c. Combating malware and botnets
d. Global-scale identity management
e. Survivability of time-critical systems
f. Situational understanding and attack attribution
g. Provenance (relating to information, systems, and hardware)
h. Privacy-aware security
I. Usable security

Cyber Technology Evaluation and Transition (CTET) — provides a coordinated process of assessments, evaluations, and operational experiments and pilots to transition the fruits of research into practice. - Cyber Security Assessment and Evaluation - Cyber Security Experiments and Pilots - Transition to Practice

The National Strategy for Trusted Identities in Cyberspace (NSTIC) in the US intends to create an 'Identity Ecosystem' wherein individuals and organizations will be able to trust each other as they follow agreed upon standards to obtain, authenticate and maintain their digital identities, and also of devices.

Cyber Security Research Developments - Global and Indian Context
Cyber Security Research – Indian Perspective
Over the past few years, India has witnessed massive adoption of cyber technologies in all the facets of life. This adoption on one hand is enabling nation to attain high economic growth, welfare, empowerment and active participation of people in policy matters, but on the other it is raising concerns and challenges from cyber security and privacy view point. These challenges become more severe when affecting the national security and economic

prospects of the country. Moreover, India being a preferred outsourcing destination for IT and BPM services requires a focused and continued attention on security and privacy.

Cyber security capability building is a rising phenomenon globally and India is no exception in this and in the recent past country has witnessed significant improvement in this domain. R&D activities in cyber domain are gaining traction in private sector and academia in India, with the support of and encouragement by the government. In recent past country has witnessed numerous successful research outcomes and many of them have been translated into businesses, through the emergence of indigenous cyber security companies. Academia is playing a crucial role in India to build a healthy ecosystem for the cyber security research, which is evident from rising of indigenous cyber security companies emerging out from the incubation centres of these academic institutions.

The global acceptance for the wide range of indigenous products & services offered by these companies has also been seen in recent past, validating indigenous competence. Traditional IT services providers are also giving due prominence to cyber security domain and some of the players have expanded their research activities in cyber security. In this paper, some of the ongoing research activities in the country have been discussed and this paper should not be considered as a credible source for all the ongoing research activities in the country. Some of the research areas are highlighted below.

Quantum Cryptography & Secure Multiparty Computation

R&D activities in India are focused both on the contemporary requirements and high-tech and futuristic need of security in cyberspace. Research in futuristic area such as Quantum Cryptography which allows conducting various cryptographic tasks that are proven to be impossible with classical processing is being undertaken by the researchers. This results in a highly secured communications (such as sharing of keys or sharing of information which is accessible to the receiver only at a specific location) among the parties, and allows detection and elimination of eavesdropping during the transit.

Inherent concerns around privacy and security in such analysis (as in case of medical records processing), this research area is gaining significant traction and already being undertaken by researchers in the country.

Next Generation Firewall

Research organizations are also working in future-ready security solutions and Multi identity based technology such as Next Generation Firewall, that offer security intelligence to enterprises and enable them to apply required and best suited security controls at the network perimeter. Integration of aforesaid technology with other security solutions such as threat intelligence and management systems, Web Application Firewall, Web filtering, Anti-Virus, Anti- Spam , etc. , will help in creating more efficient and secure ecosystem.

HISTORY

Today, there are much fewer limitations on developing and releasing cryptographic materials than there were in the past. In the year 2000, the **Department of Commerce Bureau of Export Administration** relaxed the restrictions on exporting cryptography. Publicly available encryption source code is now freely exportable everywhere. Any cryptographic algorithms developed by an individual or company are also exportable, but they still require export licenses from the government and that is necessary. Export of cryptography to terrorist organizations is still strictly prohibited.The struggle between the government and everyone else developing cryptography still continues to this day. From last 50 years, the NSA had a monopoly on cryptography development and strictly limited public access and research into cryptographic algorithms. The government labelled cryptography as a type of munitions, and thus enforced strict laws governing the export of cryptography. Starting in the 1990s, the control the government had over cryptography began to break down as the Internet allowed for the near instantaneous spread of information with millions of people around the world. Today, the government has relaxed the restraints over the distribution of cryptography, and publishing a paper on cryptography or starting an open source project to create a new encryption algorithm are much easier to do than they were in the past.

The Way Forward for India:

For strengthening the cyber ecosystem, a focused attention and adequate investment of efforts & resources would be required for cyber security. Investment in the R&D activities in cyber security domain could result in high returns

such as opportunities for entrepreneurs leading to expansion of businesses which in turn could result in more jobs in the market, increased trust & credibility and self-reliance of the nation. Though R&D activities pertaining to cyber security being undertaken in India have risen lately, a lot more needs to be done, specially to match the level of technological advancements happening globally. By virtue of its dynamic nature, cyber security requires continuous tracking of evolving technologies globally and its alignment with a country's R&D objectives and agenda. Increasing role of cyberspace puts in place a high demand of extensive R&D activities to be carried out in the nation, with a set agenda. This

Demand is re-enforced in the light of huge opportunities that exists in the global and domestic market.
Contribution would be required from all the stakeholders - government, Industry and academia - requiring that they come together and define a cyber security R&D roadmap for the country. Public Private Partnership (PPP) is the way forward, as it would help in combining best of both worlds and complement capabilities to develop a securer cyber ecosystem. Arrangements also need to be put in place for retaining the talent in the country and providing appropriate protection to the IPRs developed by the indigenous cyber security research organizations. The government should fund research in academia and also in the industry, and provide incentives to the businesses for investing in R&D activities. The research should be market driven, and deliver solutions for the real world.

The emergence of cyberspace as fifth domain requires attention, and enhancement of R&D capabilities stands as an important component. There is growing focus on developing R&D capabilities in India. Enormous opportunities exist and sustained efforts need to be undertaken.

CONCLUSION

Cryptography clearly defines it's boundaries when the fundamental need for an end user is **SECURITY**, Although it is widely used in main aspects for transmitting information and data among various organisations. After discussing all the above information which is connected with cyber security in its broad aspects there is still a room for further research and advancements in the field of Cryptography which will be well sustained with increasing times. **Elliptic**

Curve Cryptography (ECC) has already been invented but its advantages and disadvantages are not yet fully understood. ECC allows to perform encryption and decryption in a drastically lesser time, thus allowing a higher amount of data to be passed with equal security. However, as other methods of encryption, ECC must also be tested and proven secure before it is accepted for governmental, commercial, and private use.

Quantum computation is the new phenomenon. While modern computers store data using a binary format called a "bit" in which a "1" or a "0" can be stored; a quantum computer stores data using a quantum superposition of multiple states. These multiple valued states are stored in "quantum bits" or "qubits". This allows the computation of numbers to be several orders of magnitude faster than traditional transistor processors.

The need of an hour in this modern era is secure, authentic, viable, environment for all operations carried out through computers, which can be easily achieved by use of cryptography But as "Nothing is Perfect" so as is the case with Cryptography, so a consistent effort from organisations and researchers is needed towards improving the current art of cryptography which will surely help each and every end user to securely convey his message or information to the other end user without any obstacles provided by any unauthorized intruder.

Finally over the ages the techniques used in cryptography will be improved and generalisation in this field will be taken whole upto a new level which will be proved beneficial to the layman.

REFERENCES

[1] http://searchsoftwarequality.techtarget.com/definition/cryptography
[2] Hinsley, Harry. "The Enigma of Ultra." History Today 43 (1993). EBSCOHost. Georgia Tech Library, Metz. 16 July 2006. Keyword: Cryptography.
[3] Kartalopoulos, Stamatios V. "A Primer on Cryptography in Communications." IEEE Communications Magazine (2006): 146-151. EBSCOHost. Georgia Tech Library, Metz. 16 July 2006. Keyword: Cryptography.

[4] www.cs.iit.edu/~cs549/lectures/CNS-1.pdf
[5] https://www.shoretel.in/web-communication-cryptography-and-network-security
[6] nptel.ac.in/courses/106105031/
[7] williamstallings.com/**Cryptography**/
[8] http://www.pearsonhighered.com/educator/product/Cryptography-and-Network-Security-Principles-and-Practice/9780133354690.page
[9] http://technav.ieee.org/tag/477/cryptography
[10] https://en.wikipedia.org/wiki/Cryptography
[11] cryptography and network security by atul kahate pdf
[12] Cryptography & Network Security Book by Behrouz A. Forouzan
[13] http://www.webopedia.com/TERM/C/cryptography.html
[14] http://www.laits.utexas.edu/~norman/BUS.FOR/course.mat/SSim/history.html
[15] http://www.businessdictionary.com/definition/cryptography.html