ISSN:0975-9646

A Study of Different Data Encryption Algorithms at Security Level: A Literature Review

Alongbar Daimary [#1], Prof. (Dr.) L. P. Saikia[*2]

[#]*Research Scholar, Assam down town University, Guwahati-26, India*
[*]*Professor & Head , Dept. of Computer Sc. & Engineering,*
Assam down town University,
Gandhi Nagar, Panikhaiti, Guwahati-26, India.

***Abstract*— In this paper, requirement and importance of data encryption algorithms is discussed with details review of literature. The main objective of this approach is awareness of security and its requirement to the common computer users, exploring different algorithms and their design, helping Software developers to use best encryption algorithm on their applications. The findings of the review provide insight for further studies.**

***Keywords*— Encryption, Decryption, Cryptography, Hacking, Computer Security, Securing Data, digital signature.**

I. INTRODUCTION

Now a day's our entire globe is depending on internet and its application for their every phase of life. Whether it is Banking (Online Banking), Marketing (Online Shopping), Entertainment, Education, Research Works, Messaging, Chatting, or any other area, it is being used as a tool. Even small children's know how to open social network (Facebook, twitter, etc.) using internet at their mobiles or laptops. But Question arises, how safe it is! Our common people believe that it is safe, whereas it is completely opposite. There lies the chance of being hacked our sensitive and valuable data or information by some ethical hackers.

Here comes the requirement of securing our data. The idea of encryption and encryption algorithms by which we can encode our data in some secret code that is not readable or usable or understandable by hackers or unauthorized persons even it is hacked. As it is impossible to stop hacking, we can secure our sensitive data even it is hacked using Encryption. That is the big headache for our software developers how to use encryption techniques and which algorithm to use. Other side many of our common computer users still requires awareness and knowledge of security encryption and its importance.

Data Encryption (Cryptographic) Algorithm may be of three types.

i) Symmetric or Secret Key Cryptography

In this kind of cryptography for both encryption and decryption a single key is used. And same key should be known to both sender who encrypts the message and the receiver who decrypts. DES, Triple DES, AES, RC5, etc may be the example of such encryption.

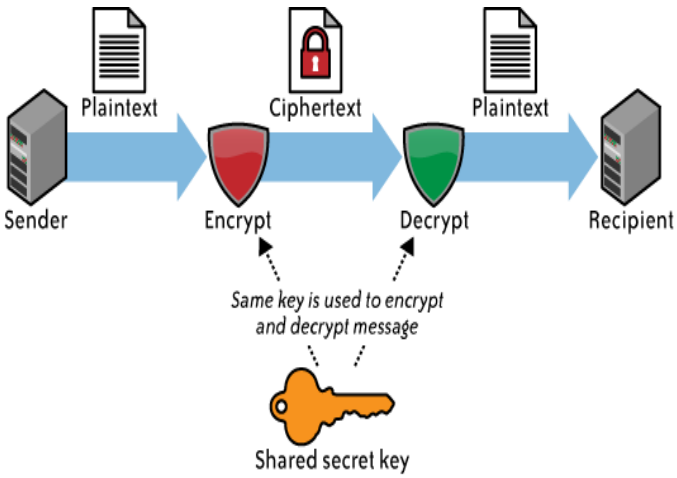

Fig. 1 Example of Symmetric Cryptography

ii) Asymmetric or Public Key Cryptography

Different key is used for both encryption and decryption in this cryptographic algorithm. Message sender encrypts the message or data using public key that may be known to all publicly. On the other side message receiver uses other secret key to decrypt the message. In this cryptography both public and private key can be used only for one purpose. RSA, Elliptic Curve, etc may be the examples of such Encryption.

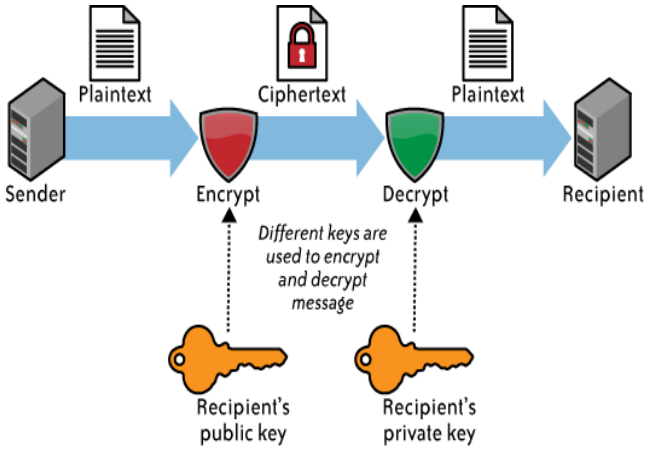

Fig. 2 Example of Asymmetric Cryptography

iii) Hash Function

In this cryptography no key is used and only some mathematical methods are used. Data cannot be decrypted back to plain text after encryption in this algorithm. So it also can be known as one-way encryption. MD5, SHA-1, etc may be such encryption.

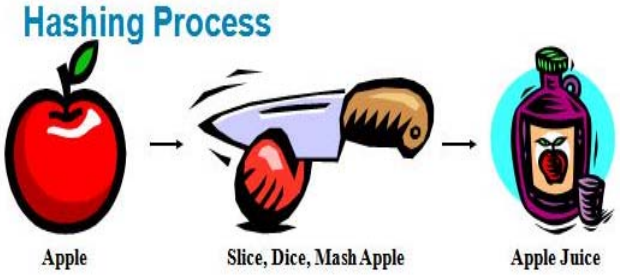

Fig. 3 Example of Hash Function

II. REVIEW OF LITERATURE

Ankit Fadia and Jaya Bhattacharjee [1] describe how to encrypt data in such a way so as to protect it from outsiders. It describes the definition of encryption and decryption and explanation of how encryption works with the growing need to safeguard one's privacy in communication and transaction. They explained the concept of developing a key details, cryptography, the most popular encryption algorithms, how encryption works, digital signature, digital certificates, and most importantly. Some real-life practical examples of where encryption can be put to use is explained in chapter 6 page 248-284. They supported a statement in chapter 5 page 238 *"….Encryption alone can be defeated is absolutely true*".

William Stallings [2] describes in different Part at his book: Part One: Provides a survey of symmetric encryption, including classical and modern algorithms at. The emphasis is on the two most important algorithms, the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). This part also covers the most important stream encryption algorithm, RC4, and the important topic of pseudorandom number generation. Part Two: Provides a survey of Asymmetric Ciphers including RSA (Rivest-Shamir-Adelman) and elliptic curve. Part Three: Begins with a survey of cryptographic hash functions. This part then covers two approaches to data integrity that rely on cryptographic hash functions: message authentication codes and digital signatures.

Mark Stamp[3] describes the information security into four major sections: i)*Cryptography:* Covers classic cryptosystems, symmetric key cryptography, public key cryptography, hash functions, random numbers and information hiding. Also, cryptanalytic techniques, including examples of attacks on cipher systems ; ii)*Access Control*: Focuses on authentication and authorization, password based security, ACLs and capabilities, multilevel and multilateral security, covert channels and inference control, coverage of security models such as BLP and Biba's Model, discussion of firewalls and intrusion detection systems (IDS); iii) *Protocols:* Focuses on generic authentication protocols and real world security protocols, such as SSL, IPSec, Kerberos and GSM; iv)*Software:* Discusses software flaws and malware, buffer overflows, viruses and worms, malware detection, software reverse engineering (SRE), digital rights management (DRM), secure software development and operating systems security functions, including discussion on Microsoft's "next generation secure computing base" or NGSCB.

Urs. E. Gattiker[4] provides complete and easy to read explanations of common security and infrastructure protection terms. Special attention is given to terms that most often prevent educated readers from understanding journal articles or books in cryptography, computer security, information systems, role-based access management and applied fields that build on those disciplines. Also included in the dictionary are terms that refer to computing forensics, malware attacks, privacy issues, system design, security auditing and vulnerability testing. This essential reference tool presents cutting-edge information on the most recent terms in use, in one concisely formatted volume. Similar to dictionaries for languages, statistics, epidemiology, and other disciplines, The Information Security Dictionary will be a valuable addition to the library of any IT professional and IT student. The Information Security Dictionary is designed for a professional audience, composed of researchers and practitioners in industry. This dictionary is also suitable for students in computer science, engineering, and information sciences.

STEVEN FURNELL and PAUL DOWLAND[5] guides to Defend our business from attack , Use email clients to improve security, Preserve confidentiality, Protect our company's reputation The pocket guide provides a concise reference to the main security issues affecting those that deploy and use email to support their organizations, considering email in terms of its significance in a business context, and focusing upon why effective security policy and safeguards are crucial in ensuring the viability of business operations. For Our business or office relies on email for its everyday dealings with official staff, partners, suppliers and customers. While email is an invaluable form of communication, it also represents a potential threat to our information security. Email could become the means for criminals to install a virus or malicious software on our computer system and fraudsters will try to use emails to obtain sensitive information through phishing scams. If we want to safeguard our organization's ability to function, it is essential to have an effective email security policy in place, and to ensure our staff understand the risks associated with email. This pocket guide will help businesses or office to address the most important issues. Its comprehensive approach covers both the technical and the managerial aspects of the subject, offering valuable insights for IT professionals, managers and executives, as well as for individual users of email.

David Harley et. al.[6] guide to defending our system against the real threat of computer viruses. It presents a soup-to-nuts, full-bodied analysis on computer virus protection by offering: i) Current information on the expanding domain of computer viruses; ii) Real world case studies of virus infestations, solutions, and methods of

prevention; iii) Practical problem and solution analysis of the modern day virus threat.

Bradley Dunsmore et. al.[7] explores options for protecting computer network from attack across the Internet, emphasizing firewall solutions from Cisco, Symantec, Microsoft, and Check Point. It describes with general advice about how to set up a comprehensive system of defenses (comprising a firewall, an intrusion detection system, authentication and cryptography schemes, and protocols like IPsec). It concludes with information on the specifics of configuring several products.

Fauzan Mirza[8] gives a basic introduction to block cipher design and analysis. The concepts and design principles of block ciphers are explained, particularly the class of block ciphers known as Feistel ciphers. Some modern block cipher cryptanalysis methods are demonstrated by applying them to variants of a weak Feistel cipher called Simplified TEA (STEA), which is based on the Tiny Encryption Algorithm (TEA).

Paul C. Kocher[9] explains how attackers may be able to find fixed Diffe-Hellman exponents, factor RSA keys, and break other cryptosystems by carefully measuring the amount of time required to perform private key operations. And explained techniques for preventing the attack for RSA and Diffe-Hellman. He finally stated requirement of some cryptosystems to be revised to protect against the attack, and new protocols and algorithms to incorporate measures to prevent timing attacks.

III. CONCLUSION

In general, any channel which can carry information from a secure area to the outside should be studied as a potential risk. Implementation-specific timing characteristics provide one such channel and can sometimes be used to compromise secret keys. Vulnerable algorithms, protocols, and systems need to be revised to incorporate measures to resist timing cryptanalysis and related attacks.

REFERENCES

[1] Ankid Fadia, Jaya Bhattacharjee, *"Encryption, Protecting Your Data"*, Vikash Publishing House Pvt Ltd,2007, ISBN: 812592251-2

[2] William Stallings, *"Cryptography and Network Security"*, Fifth Edition, Person,2011, ISBN 978-81-317-6166-3

[3] Mark Stamp, *"INFORMATION SECURITY Principles and Practice"*, Second Edition, A JOHN WILEY & SONS INC. PUBLICATION,2011,

[4] Urs E. Gattiker, International School of New Media, *"THE INFORMATION SECURITY DICTIONARY"*, KLUWER ACADEMIC PUBLISHERS,ISBN: 1-4020-7889-7

[5] STEVEN FURNELL, PAUL DOWLAND, *"E-mail Security A Pocket Guide"*, IT Governance Publishing, 2010, ISBN 978-1-84928-097-6

[6] David Harley, Robert Slade, Urs Gattiker, *"Viruses Revealed"*, Osborne/McGraw-Hill

[7] Bradley Dunsmore, Jeffrey W. Brown, Michael Cross, *"MISSION CRITICAL! INTERNET SECURITY"*, Syngress Publishing Inc., 2001, ISBN: 1-928994-20-2

[8] Fauzan Mirza, "*Block Ciphers And Cryptanalysis*" PhD Thesis, Department of Mathematics, Royal Holloway University of London, 2001

[9] Paul C. Kocher, "*Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and Other Systems*", Cryptography Research Inc., San Francisco, USA.