IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW ON SECURE DATA TRANSMISSION USING CRYPTOGRAPHIC TECHNIQUES

Er. Jyoti Sharma*, Prof. Jyoti Rani
Research Scholar, GZSCCET, Bathinda
Assistant Professor, GZSCCET, Bathinda

DOI: 10.5281/zenodo.61506

ABSTRACT

The ability to protect and secure information is vital to the growth of electronic commerce and to the growth of the Internet itself. Many people need or want to use communications and data security in different areas. Banks use encryption methods all around the world to process financial transactions. These involve transfer of huge amount of money from one bank to another. Banks also use encryption methods to protect their customers ID numbers at bank automated teller machines. So, this paper has reviewed various techniques to secure the data and then give the general comparison between these techniques.

KEYWORDS: Secure Data Transmission, Cryptography, Encryption Algorithms.

INTRODUCTION

Since, the growing demand for data safety, image encryption as well as decryption has turn out to be an essential research zone and also it has wide-ranging application visions. The arena of encryption is becoming quite significant in the current years. Image safekeeping is of extreme apprehension as various kinds of network attacks have turn out to be progressively more severe. Image encryption as well as decryption has apps in multimedia systems, telemedicine, internet communiqué, medical imaging, military communication, and so on [1].

Several image content encryption procedures have been recommended [1]. In the direction of making the information secure from numerous attacks as well as for the integrity of information we need to encode the information before it is conveyed or deposited. Government, hospitals, military, private business as well as financial institution, contracts with private images regarding their financial status, patient (in Hospitals), enemy positions (in defence),

geographical areas (in research), product, and so on. Maximum of this data is now composed together and stowed on electronic PCs as well as communicated across system to further computer. If these personal images regarding nemesis locations, patient as well as geographical regions drop into the incorrect hands, than such a type of breach of security could possibly lead to declaration of war, wrong treatment and so on. Guarding secret images is a virtuous as well as legitimate necessity.

Cryptography is actually participating in a major purpose throughout data protection throughout applications managing inside a network environment. The idea enables individuals to ply their trade in an electronic form without having problems associated with deceit and also lies besides guaranteeing this sincerity in the information and also authenticity in the sender. They have be a little more important to our day-to-day lifestyle simply because 1000s of folks have interaction in an electronic form every day; through e-mail, e-commerce, ATM equipment, cell phones, and so forth. This particular geometric increase associated with data carried in an electronic form has produced elevated reliability with cryptography and also authentication by consumers [2]. Although secured connection has been around since then, the key supervision issue has averted that coming from popular software. The actual development associated with public-key cryptography has allowed large-scale circle associated with network of users that may communicate safely with one another even when that they never communicated before [3].

Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography [4, 5].

- Confidentiality: Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.
- Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.
- Integrity: Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.
- Non Repudiation: Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.
- Access Control: Only the authorized parties are able to access the given information.

Applications of Cryptography

- Secret Communications, a trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.
- Feature Tagging Elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features
- Copyright Protection Copy protection mechanisms that prevent data, usually digital data, from being copied. The insertion and analysis of water- marks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding [6].
- Access control system for digital content distribution
- Media Database Systems
- To wrap up html pages
- Used in modern printers that contains serial numbers.
- Used by FBI, intelligence services.

RESEARCH METHODOLOGY

Blowfish Algorithm

Blowfish is really a symmetric key block cipher that may be properly used by encryption and also preserving associated with data. It will require the variable-length key, coming from 32 bits to 448 bits. Blowfish seemed to be developed throughout 1993 by Bruce Schneier like a quickly, cost-free alternative to present encryption algorithms. Blowfish Algorithm is a Feistel Network, iterating an effective encryption operate 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches [7].

Blowfish has a variable-length key and 64-bit block cipher. The algorithm consists of two parts: a key expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several sub-key arrays totalling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of permutation depending on key, and a data-dependent substitution. All operations are XORs and additions on 32- bit words. The only additional operations are four indexed array data lookups per round.

RSA Algorithm

RSA stands for in addition to Adelman, one more names on the designer. It turned out 1st for sale in 1978 among the 1st public key cryptographic programs. RSA can be used pertaining to key alternate along with digital camera signatures and also the encryption associated with tiny blocks associated with files. Currently, RSA is generally utilized to encrypt your procedure key useful for secret key encryption (message integrity) or perhaps your message's hash value (digital signature). RSA's statistical solidity emanates from your alleviate inside calculating good sized quantities and also the problem in finding your primary components of people good sized quantities. Although utilized together with quantities utilizing many digits, your instructional math powering RSA is reasonably straight-forward.

Any public key method suggests your algorithm [8] pertaining to encrypting a communication is widely acknowledged however the algorithm to be able to decrypt your concept is confidentially acknowledged.

Classification:

$a_1 \equiv b_1 \pmod{c_1} \Longleftarrow\!\!\Longrightarrow a_1 = b_1 + kc_1$ for some integer k.

Within cryptography, RSA is definitely an algorithm pertaining to public key cryptography. The particular RSA algorithms entail the application of two keys:

A public key, which is often well-known by everyone, in addition to enable you to encrypt statement.

A private key, acknowledged simply because of the receiver, in addition to utilize to decrypt communication.

AES Algorithm

It is a web instrument to scramble and decode content utilizing AES encryption calculation. You can choose 128, 192 or 256-bit long key size for encryption and unscrambling. The consequence of the procedure is downloadable in a content record. AES (acronym of Advanced Encryption Standard) is a symmetric encryption calculation. The calculation was produced by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES was intended to be proficient in both equipment and programming, and backings a square length of 128 bits and key lengths of 192, 128 as well as 256 bits [9].

DES Algorithm

The Data Encryption Standard algorithm (DES) is the most widely used symmetric encryption algorithm in the world so far. DES was quickly adopted for non-digital media. The banking industry, adopted DES as a finance criteria. Criteria's designed for the particularly banking commerce are fixed by means of the American National Standards Institute [10]. DES is a symmetric block cipher designed to encrypt and decrypt blocks of data consisting of 64 bits under control of sole 56 bit key. Every 8th bit of the particular 64-bit key is utilized on behalf of parity checking and if not then unnoticed. Decoding essentially be completed by utilizing the identical key as for encryption.

For example, if the plaintext message is "12345678ABCDEF12" and the key to encrypt the plaintext be "1234123412341234", then the cipher text will be "E112BE1DEFC7A367". Decoding of the above written cipher text utilizing the same key results in the plain text message "12345678ABCDEF12".

COMPARISON BETWEEN ALGORITHMS

FACTORS	**AES**	**DES**	**3DES**	**BLOWFISH**	**RSA**
KEY LENGTH	128, 192, OR 256 BITS	64 bits	(K1, K2 and K3) 168 bits (K1 and K2 is same) 112-bits	32-448 bits	Depends on number of bits in the modulus n where n=p*q
CIPHER TYPE	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Cipher Algorithm	Asymmetric Block Cipher Algorithm
BLOCK SIZE	128,192 or 265 bits	64 bits	64 bits	64bits	Minimum 512 bits
DEVELOPED	2000	1977	1978	1993	1978

CRYPTANALYSIS RESISTANCE	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable to differential and linear cryptanalysis: weak substitution tables	Vulnerable to differential brute force attacker could be analyse plain text using differential cryptanalysis	Vulnerable to differential, brute force attacker	Vulnerable to brute force attacker and Oracle attack
Structure	Substitutional Permutation	Festial	Festial	Festial	Public key algorithm
Ciphering and deciphering algorithm	Different	Different	Different	Same	Same
SECURITY	Replacement for DES, Excellent Security	Not secure enough	Adequate security	Excellent Security	Excellent Security
Flexible	Yes	No	Yes	Yes	No
ROUNDS	10(128-bits), 12(192-bits), 14(256-bits)	16	48	16	1
KEY(S)	Single key used for encrypt and decrypt	Single key used for encrypt and decrypt	Single key (later divide into 3 parts) used for encrypt and decrypt	Public key used for encrypt and decrypt	Two different Public and private key used for encrypt and decrypt

CONCLUSION AND FUTURE SCOPE

One of many major challenges associated with resource sharing with data communication network is actually their safety measures. That is premised with the belief that as soon as there's connection among personal computers sharing some resources, the problem associated with data security becomes important. The actual large progress within the networking technologies qualified prospects perhaps the most common culture intended for interchanging in the electronic digital photos really drastically. Hence it is a lot more prone associated with duplicating associated with electronic digital image and also redistributed by cyber-terrorist. Which means photos must be protected although transmitting it, vulnerable data such as credit cards, consumer banking purchases and also social safety numbers need to be protected. So, this paper has reviewed various encryption techniques like Blowfish, AES, RSA etc. It has been seen that all algorithms has its applications in various fields.

REFERENCES

[1] Kamal et al., 2014, “Enhancement Key Of Cryptography And Steganography Using RSA And Neural Network”, IJARCET, vol. 3, pp. 1707-1710.

[2] Akshay et al., 2013, “Steganography Technique using Neural Network”, International Journal of Computer Applications”, Vol. 82, pp. 39-42.

[3] Ell effly et al., 2013 “Detecting pixel-value differencing steganography using Levenberg-Marquardt neural network”, IEEE, Computational Intelligence and Data Mining (CIDM), pp. 160-165.

[4] Youssef, 2012, “A Generation-based Text Steganography Method using SQL Queries”, IJCA, Vol. 57, pp. 27-31.

[5] Babloo Sha et al, 2012, “Steganographic Techniques of Data Hiding using Digital Images”, DESIDOC, Vol. 62, pp. 11-18.

[6] Mohit Garg, 2011, “A Novel Text Steganography Technique Based on Html Documents”, JJAST, Vol. 35, pp.129-135.

[7] Jisna et al., 2011, “Audio Steganography in Wavelet Domain – A Survey, IJCA, Vol. 52, pp. 33-37.

[8] Bidyut Jyoti Saha, Kunal Kumar Kabi, Arun and Chittaranjan Pradhan, “A Robust Digital Watermarking algorithm using DES and ECC in DCT Domain for Color pictures” 2014 International Conference on Circuit, Power and Computing Technologies [ICCPCT]

[9] Makarand L. Mali “Implementation of Text 2013 International Conference on Communication Systems and Network Technologies Watermarking Technique Using Natural Language Watermarks.