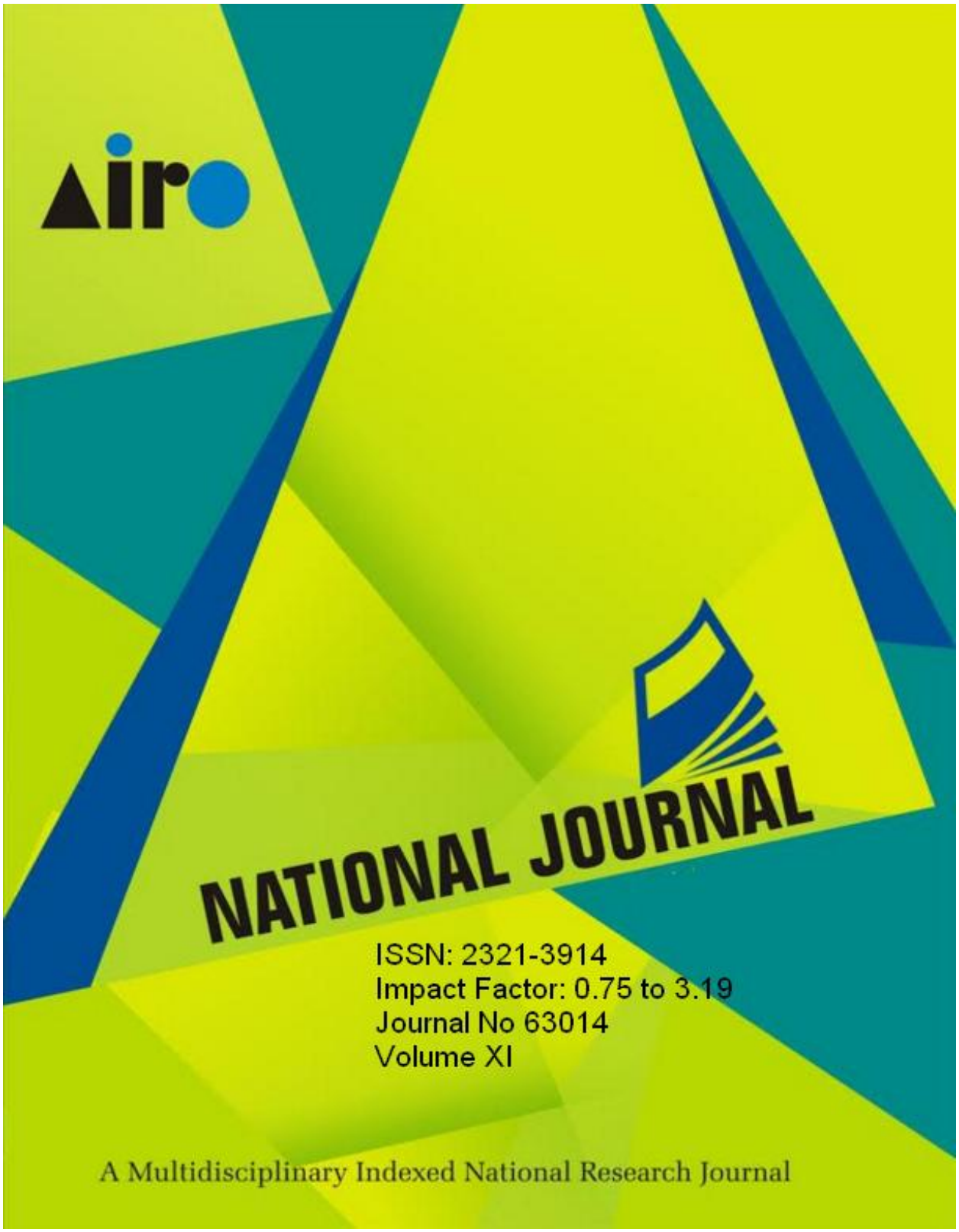
Airo
NATIONAL JOURNAL
ISSN: 2321-3914
Impact Factor: 0.75 to 3.19
Journal No 63014
Volume XI
A Multidisciplinary Indexed National Research Journal

Airo National Research Journal
Volume XI, ISSN: 2321-3914
August, 2017
Impact Factor 0.75 to 3.19
UGC Approval Number 63014

ANALYSIS OF CRYPTOGRAPHY-ALGORITHM AND SECURITY

Sumit Chauhan

Research Scholar, (Deptt. of Computer Science),Kalinga University, Raipur

Supervisor: Dr. Vivek Srivastava

ABSTRACT

A general human communication or human language which we speak is interpreted in the form of plain Text or clear Text. This encrypted message can be understood by knowing its language as long as the message is not confined in any manner. Thus, the information is now coded to protect it from accessing to non-permitted source. The report is covering both the state of cryptographic primitives and their application in higher-level protocols. In general, cryptographic primitives are rather well understood and studied objects. Compared to the frequency of protocol-level vulnerabilities, primitives are broken rather rarely. However, since many of the primitives are implemented in very low-level layers of communication infrastructure (often even in hardware), such a break may have far-reaching consequences. There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography.

Keywords: *symmetric encryption, algorithm*

INTRODUCTION

This report is collaborative effort of above 20 researchers & developers of Cybernatica in preparing various chapters or contributing their opinion after proofreading. Although

most of the conclusions drawn are not created by Cybernetica's team but has been concluded from many other teams from various countries. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. The concept of securing messages through cryptography has a long history. Indeed, Julius Caesar is credited with creating one of the earliest cryptographic systems to send military messages to his generals. "Cryptography" derives from the Greek word kruptos, meaning "hidden". The key to hiding data is to devise a hiding (encryption) mechanism that is very difficult to reverse (i.e., to find the original data) without using the decryption key. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem. In a typical situation where cryptography is used, two parties (X and Y) communicate over an insecure channel. X and Y want to ensure that their communication remains incomprehensible by anyone who might be listening. Furthermore, because X and Y are in remote locations, X must be sure that the information receives from Y has not been modified by anyone during transmission. In addition, she must be sure that the information really does originate from Y and not someone impersonating Y.

REVIEW OF LITERATURES

The NAV (Network Avanzato peril Vigneto – Advanced Vineyard Network) system was reported by A. Matese et al. The system was a wireless sensor network designed and developed with the aim of remote real-time monitoring and collecting of micro-meteorological parameters in a vineyard. "The system includes a base agrometeorological station (Master Unit) and a series of peripheral wireless nodes (Slave Units) located in the vineyard. The Master Unit is a typical single point monitoring station placed outside the vineyard in a representative site to collect agrometeorological data. It utilizes a wireless technology for data communication and transmission with the Slave Units and remote central server. The Slave Units are multiple stations placed in the vineyard and equipped with agrometeorological sensors for site-specific environmental monitoring, which store and transmit data to the Master Unit. Software was developed for setup and configuration functionality. A graphical user interface operating on the remote central server was implemented to collect and process data and provide real-time control. The devices were tested in a three-step process: hardware functionality and data acquisition, energy consumption and communication. The NAV system is a complete monitoring system that gave flexibility for planning and installation,

which fully responded to the objectives of the work in terms of energy efficiency and performance." "Phytophthora is a fungal disease which can enter a field because of a variety of sources. The climatological conditions within the field play a great part in the development and associated attack of the crop. Humidity is a crucial factor in the development of the disease as well as the temperature and whether the leaves are wet or not. [6]" For this reason, Baggio deployed a WSN to monitor humidity and temperature in order to better fight phytophthora in a potato field. However, only the pilot study was reported, and the full-size network has not been deployed yet. An in-fie1d soi1 moisture and temperature monitoring system was reported by Hui Liu et al. The system consisted of the soi1 monitoring wireless sensor network and remote data centre. The sensor node was developed using JN5121 modu1e and IEEE 802.15.4/ZigBee wire1ess microcontroller. The sink node for data aggregating was based on ARM7 p1atform to meet the requirements of high-performance. And a gateway was used for long distance data transmission. The alarm subsystem determines several alarm strategies in advance based on relevant production knowledge and experience. Alternatively, alarm thresholds are set up for several key parameters. Once the measured values of these parameters exceed the alarm thresholds, alarms in SMS format are automatically sent by the system to the designated mobile phones normally owned by farmers or relevant farming technicians.

TYPES OF CRYPTOGRAPHY

Cryptography is a process which is associated with scrambling plaintext into cipher text (a process called encryption), then back again (known as decryption). There are several ways to classify the various algorithms.

The most common type's are-

1. Secret Key Cryptography which is also known as Symmetric Key Cryptography and

2. Public Key Cryptography which is also known as Asymmetric Key Cryptography.

Secret key Cryptography

In secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plain text.

Encryption algorithm

Step 1: Generate the ASCII value of the letter

Step 2: Generate the corresponding binary value of it. [Binary value should be 8 digits e.g. for decimal 32 binary number should be 00100000]

Step 3: Reverse the 8 digit's binary number

Step 4: Take a 4 digits divisor (>=1000) as the Key

Step 5: Divide the reversed number with the divisor

Step 6: Store the remainder in first 3 digits & quotient in next 5digits (remainder and quotient wouldn't be more than 3 digits and 5 digits long respectively. If any of these are less then 3 and 5 digits respectively we need to add required number of 0s (zeros) in the left hand side. So, this would be the encrypted text. Now store the remainder in first 3 digits & quotient in next 5digits.

Public key Cryptography

Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised. Attacker may have

a) Collection of cipher texts

b) Collection of plaintext/cipher text pairs

c) Collection of plaintext/cipher text pairs for plaintexts selected by the attacker

d) Collection of plaintext/cipher text pairs for cipher texts selected by the attacker

Brute-Force Attack

- Try all possible keys K and determine if DK(C) is a likely plaintext – Requires some knowledge of the structure of the plaintext (e.g., PDF file or email message)
- Key should be a sufficiently long random value to make exhaustive search attacks unfeasible
- English text typically represented with 8-bit ASCII encoding
- A message with t characters corresponds to an n-bit array, with n = 8t
- Redundancy due to repeated words and patterns– E.g., "th", "ing"
- English plain texts are a very small subset of all n-bit arraysEntropy of Natural Language
- Information content (entropy) of English: 1.25 bits per character
- t-character arrays that are English text:(21.25)t = 21.25 t
- N-bit arrays that are English text:21.25 n/8 _ 20.16 n
- For a natural language, constant_1 such that there are 2_n messages among all n-bit arrays
- Fraction (probability) of valid messages 2_n / 2n = 1 / 2(1__)n

- Brute-force decryption– Try all possible 2k decryption keys– Stop when valid plain text recognized-
- Given a cipher text, there are 2kpossible plaintexts
- Expected number of valid plaintexts2k / 2(1__)n
- Expected unique valid plaintext, (no spurious keys) achieved at unicity distance n = k /(1__)
- For English text and 256-bit keys, unicity distance is 304 bits

Substitution Ciphers

- Information content (entropy) of English: 1.25 bits per character
- T-character arrays that are English text: (21.25)t = 21.25 t
- N-bit arrays that are English text: 21.25 n/8 _ 20.16 n
- For a natural language, constant_1 such that there are 2_nmessages among all n-bit arrays
- Fraction (probability) of valid messages2_n / 2n = 1 / 2(1__)n
- Brute-force decryption–Try all possible 2k decryption keys–Stop when valid plain text recognized.
- Given a cipher text, there are 2k possible plaintexts
- Expected number of valid plaintexts 2k / 2(1__)n
- Expected unique valid plain text, (no spurious keys) achieved at unicity distance n = k /(1__)
- For English text and 256-bit keys, unicity distance is 304 bits

Substitution Ciphers

– The **one-time pad** was invented in 1917 by Joseph Mauborgne and Gilbert Verna– We use a block of shift keys, (k1, k2, . .. , kn), to encrypt a plaintext, M, of length n, with each shift Key being chosen uniformly at random.

• Since each shift is random, every cipher text is equally likely for any plaintext.

Weaknesses of the One-Time Pad

• In spite of their perfect security, one-time pad shave some weaknesses

• The key has to be as long as the plaintext

• Keys can never be reused– Repeated use of one-time pads allowed the U.S. to break some of the communications of Soviet spies during the Cold War.);

Attacks against weaknesses in protocol logic

During the lifetime of the secure channel provided by TLS, maintained by running the record protocol, a renegotiation may be triggered by the parties. In this case, the handshake protocol is run again, and the keys of the channel are updated. The new handshake protocol may use different parameters than the original one; this is e.g. used to request the client to identify itself more strongly if it wants to access a more sensitive resource

Attacks against short keys

Certain cipher suites of TLS make use of short, so-called export strength keys, in particular 512-bit RSA or Diffie-Hellman keys. These suites are deprecated since the release of TLS v1.1, but support is still present in deployed clients and servers. They are a critical component of the FREAK attack, where bugs in client code make it accept a 512-bit RSA key from the server that still supports it and thinks the client was requesting an export strength cipher suite due to the adversary tampering with the first messages of the handshake protocol. If the server supports export strength Diffie-Hellman key exchange, then forcing the connection down to such cipher suite is again just a matter of tampering with the first handshake messages. After the server has sent the 512-bit group element in authenticated manner, the attacker can take over and complete the handshake with the client. At the end of the handshake protocol, the message authentication code has to be applied to the sequence of messages exchanged during the handshake protocol, but the attacker can do it because it knows the master secret at that time.

Security-

• **Security** of RSA based on difficulty of factoring

– Widely believed– Best known algorithm takes exponential time

• RSA Security factoring challenge (discontinued)

• In 1999, 512-bit challenge factored in 4 months using 35.7 CPU-years– 160 175-400 MHz SGI and Sun– 8 250 MHz SGI Origin – 120 300-450 MHz Pentium II– 4 500 MHz Digital/Compaq.

• In 2005, a team of researchers factored the RSA-640 challenge number using 30 2.2GHz CPU years.

The notions of hash function security-

Several different security properties of hash functions could be assumed based on applications.

Often in formal security proofs, hash functions are assumed to be random functions (the so-called random oracle model). Having such an assumption in mind, we may define an attack against a hash function as any method capable of finding input-output pairs for the hash function in a way that would be infeasible in the random oracle model.

The following three types of attacks against hash function h() are the most common:

• Pre-image attack: given an output y, find an input M for which h(M) = y.

• Second pre-image attack: given an input M, find a different input M0 so that h(M0) = h(M).

• Collision attack: find two different inputs M and M0 such that H(M) = H(M0).

Other security considerations-

While considered only the network security of the Mobile-ID protocol, there are other important technical and organisational details of the supporting infrastructure to consider.

A list of these details has been discussed in, mostly in the form of issues that should be more thoroughly considered. The next few paragraphs give an overview of those issues.

There are important technical aspects surrounding the SIM card and its keys, and the USIM application on it. The private keys on the card have to be generated securely. A good source of randomness must be employed for this generation, and the generation.

The organisational security methods around the Mobile-ID platform have to be carefully selected. The questions pertaining to the procurement of chips, the operating system and the application, as well as the personalisation and storage of the chips may be similar to the ID-card infrastructure or to the normal operations of a mobile telecommunications provider. Hence the same organizational methods may be applicable for securing all these processes. But the issue of managing secure channels between the Digi Doc Service and the mobile operators is unique to Mobile-ID.

CONCLUSION AND RECOMMENDATION

Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the send data now, in order to achieve these goals various cryptographic algorithms are developed by various people. For a very minimal amount of data those algorithms wouldn't be cost effective since those are not designed for small amount of data. The aim of this work was to design and implement a new algorithm to address this issue so that we don't have to apply those algorithms (which are not cost-effective) to encrypt a small amount of data. After publication of the previous, 2015 version of the report, no major cryptanalytic breakthroughs have occurred. This means that the recommendations given in are still valid. We will summarise them here as well-

• As the standard choice for symmetric encryption, AES block cipher is recommended.

In mid-term perspective (up to 10 years), all the standard key lengths (128, 192 and 256 bits) may be used. For long-term security (30-50 years), AES-256 is recommended.

Camellia cipher can also be considered secure. However, RC4, DES and 3DES are obsolete and their usage should be terminated.

• In case of RSA and discrete-logarithm-based systems (like Diffie-Hellman key exchange,

El Gamal and DSA), usage of 1024-bit keys should be stopped urgently. Existing deployments of 2048-bit keys may be continued for 5 years. New installations and installations requiring mid-term security should use at least 3072-bit keys.

• Usage of hash functions MD5 and SHA-1 should be discontinued as soon as possible.

• After the NSA announcement about Suite B recommendation updates, the situation with elliptic key cryptosystems is unclear. We estimate that implementation of a practical quantum computer capable of breaking current asymmetric encryption systems is still more than 5 years away. Hence, using standard elliptic curves (like P-256 andP-384) is fine for at least this time period. These recommendations should be taken into account when deciding upon the TLS cipher suite. Additionally, one has to select the key exchange algorithm and block cipher mode of operation. To provide forward security, ephemeral Diffie-Hellman key exchange should be used; the corresponding cipher suites have either DHE or EDH in their names take into account when building security-critical systems is modularity of the cryptographic primitives used. This is especially important in the light of the upcoming transition to post-quantum algorithms. Search for the next generation of cryptographic primitives has only started and no-one can really know how long they will last.

This means that the only way to ensure continuous security of the systems is to make the primitives easy to change. When planning for critical systems and infrastructure, security requirements must already be addressed in the public tender phase. Explicit security requirements should be stated in the call and the providers should open the technical specifications of their proposals to the extent that will allow for independent post-installation auditing.

REFFRENCES

[1] S. William, Cryptography and Network Security: Principles andPractice, 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50
[2] Computer and Network security by ATUL KAHATE
[3] Fundamentals of Computer Security, Springer publications “Basic Cryptographic Algorithms”, an article available at : -
[4] www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoIntro.htm#Algorithms
[5] S. Hebert, “A Brief History of Cryptography”, an article available at http://cybercrimes.net/aindex.html
[6] “Introduction to Public-Key Cryptography”, an article available at developer.netscape.com/docs/manuals/security/pkin.
[7] Muhammad Ali Mazidi, Janice Gillispie Mazidi, Rolin D.McKinlay, “The 8051 Micro controller and Embedded systems”
[8] Remote Sensing and Control of an Irrigation System Using a

Distributed Wireless Sensor Network Yunseop (James) Kim, Member, IEEE, Robert G. Evans, and William M. Iversen Remote Sensing and Control of an Irrigation System Using a Distributed Wireless Sensor Network Yunseop (James) Kim, Member, IEEE, Robert G. Evans, and William M. Iversen]

[9] S. Tanenbaum, C. Gamage, and C. Crispo, "Taking Sensor Networks from the Lab to the Jungle," IEEE Computer Society, Vol.39(8), pp 98-100, 2006.

[10] Alka Kalra, Rajiv Chechi, Dr. Rajesh Khanna," Role of Zigbee Technology in Agriculture Sector"in NCCI 2010 -National Conference on Computational Instrumentation,CSIO Chandigarh, INDIA, 19-20 March 2010,pp 51-52.