Journal of Computer and Mathematical Sciences, *Vol.6(3),159-170, March 2015* *ISSN 0976-5727 (Print)*
(An International Research Journal), *www.compmath-journal.org* *ISSN 2319-8133 (Online)*

Computer Code Algorithms and Encryption Laws for Security

Sanjay Jain and Vaibhav Jain

Department of Mathematical Sciences,
SPC Government College, Ajmer, INDIA.
drjainsanjay@gmail.com
Scholar, The Faculty of Law,
ICFAI University, Dehradun, INDIA.
jainvaibhav.jain004@gmail.com

(Received on: February 28, 2015)

ABSTRACT

Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. This is part of the reason why it's going to be so important for study security and laws to making sure that we do everything to harden sites and prevent those kinds of attacks from taking place. But even as we get better, the hackers are going to get better, too. In the present work, we try to correlate two branches namely mathematical computational codes and their related legal encryption laws for better security point of view.

Keywords: Code, Security, Encryption, Communication, Cryptography.

1. INTRODUCTION

Message transfer in coded form has played a key role in embarking the journey to achieve the goal of maximum securities from sender to the receiver. It has helped the sender to enhance the secrecy, increase transparency, and improve accessibility. With the advancement of coding technology, many sectors having confidential information has also expanded its horizons in the form of digital world, which is fast becoming the preferred mode of availing secure services. Many law councils suggested that monitoring security laws is necessary and effective.

Cyber attacks on law firms are growing and 46 states have enacted or are considering data breach notification legislation that can have costly consequences for law firms. Those are just few reasons why it is critical for law firms to stay current on info security threats and potential solutions. Northpage Research has published a report on the issue: "Why Information Security is now a Business-Critical Function for Law Firms." Key issues covered in the report: The unique role of information in law firms; the law firm information "gold mine;" IT systems as the lifeblood of law firms; and how compliance standards impact law firms.

Thus, ICT is going to be the propellant of the growth engine which has the potential to transform a country into a knowledge–led economy and society especially when we are fast adopting new paradigms such as Internet of Things, Smart Security etc. Today, country like India has emerged as a Global IT knowledge resource empowering the whole world. Spreading digital literacy to rural citizens across the country and generating employment opportunities in all ICT-enabled industries will be the next major leap to transform young India into a Digitally Empowered Society and a knowledge economy.

Subashini and Kavitha[10] work on security issues in service delivery models of cloud computing. A White Paper by Bloor Research[8] published on compliance and regulations for the IT security professional. Daouk, Charles, Lee and David[7] studied on security laws. Barker[2] provides a complete overview on counter-terrorism and national security legislation reviews. Blaze, Schneier, Shimomora, Thompson, and Weiner[3] studied for symmetric ciphers to provide adequate commercial security. Anderson[1], Dorothy[5], Coutinho[4] all provides a brief description on cryptography and data security. Some literature on encrypted communication and laws is also available online[9]. Flannery[6] works on Mathematical codes.

Shannon expanded the ideas of this article 'Mathematical Theory of Communication' in a 1949 book with Warren Weaver titled The Mathematical Theory of Communication (ISBN 0-252-72546-8). The book explains how the symbols of communication are transmitted, how the transmitted symbols convey meaning, and the effect of the received meaning. Many researchers also work on interdisciplinary field like data securities and legal aspect of related laws.

These things encourage us to combined different subjects like Computer (codes) and Law (Encrypted laws) and start some research work on it. In the next part of the paper we discuss about the basic idea of communication which is important factor to any type of message. After this some computer codes are introduce. Some idea of Cryptography is also provided to understand encryption. An example is also provided to explain how a coded message is decoded and vice-versa. Finally encryption/security laws are also listed.

2. COMMUNICATION

Communication is simply the act of transferring information from one place to another or exchange of thoughts and ideas in form of sentence / message etc. from one end to other end is basic definition of communication. The desired outcome or goal of any communication process is understanding. Communication theory is a field of

information and mathematics that studies the technical process of information and the human process of human communication.

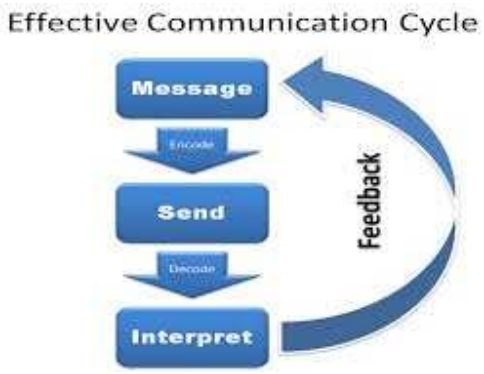
Communication requires a sender, a message, a medium and a recipient, although the receiver does not have to be present or aware of the sender's intent to communicate at the time of communication; thus communication can occur across vast distances in time and space. Communication requires that the communicating parties share an area of communicative commonality. The communication process is complete once the receiver understands the sender's message.

The characteristic of communication are

- Message delivered at right destination.
- Delivered in time.
- Message must not be tampered.

The components of communication are

- Sender
- Receiver
- Message
- Media
- Protocol



Encoding Messages

All messages must be encoded into a form that can be conveyed by the communication channel chosen for the message. We all do this every day when transferring abstract thoughts into spoken words or a written form. However, other communication channels require different forms of encoding, e.g. text written for a report will not work well if broadcast via a radio programme, and the short, abbreviated text used in text messages would be inappropriate if sent via a letter. Complex data may be best communicated using a graph or chart or other visualisation.

Effective communicators encode their messages with their intended audience in mind as well as the communication channel. This involves an appropriate use of language, conveying the information simply and clearly, anticipating and eliminating likely causes of confusion and misunderstanding, and knowing the receivers' experience in decoding other similar communications. Successful encoding of messages is a vital skill in effective communication.

Decoding Messages

Once received, the receivers need to decode the message, and successful decoding is also a vital skill. Individuals will decode and understand messages in different ways based

upon any barriers to communication which might be present, their experience and understanding of the context of the message, their psychological state, and the time and place of receipt as well as many other potential factors. Understanding how the message will be decoded, and anticipating as many of the potential sources of misunderstanding as possible, is the art of a successful communicator.

3. CODES

When, we want to communication/messages to be secret. Only one thing come to mind i.e., codes or secret codes. Code is a set of symbols for representing something. For example, most computers use ASCII codes to represent characters. Codes play a vital role in man/machine oriented secret message. Man/Machine oriented codes are a form of character representation. Computer codes help one to represent character for use by the machine. Code can appear in a variety of forms. The code that a programmer writes is called *source code*. After it has been compiled, it is called *object code*. Code that is ready to run is called *executable code* or *machine code*.

The main computer code's which are widely accepted:

Symbol representation:

It uses only two digits (0, 1). Sometime it is also called binary codes. There is large number of possible binary codes for representing information:

$10 = 8 + 0 + 2 + 0 = \mathbf{1} \text{ X } 2^3 + \mathbf{0} \text{ X } 2^2 + \mathbf{1} \text{ X } 2^1 + \mathbf{0} \text{ X } 2^0 = (1010)_2$

Mathematically, $N = 2^n$

Where N = Symbol, n = number of information bits available.

Number of bits required to represent N symbols is $\log_2 N$ rounded to the next integer.

For example:

There are 12 teams in cricket world cup. What is minimum number of bits required to represent each team with different binary code?

Minimum number of bits required $= \log_2 N$

$= \log_2 12 = \log_2 (4X3) = 2 \log_2 2 + \log_2 3 = 2 + 1.58$

$= 3.58 = 4$ (Next integer)

Team	Binary Code
1	0 0 0 0
2	0 0 0 1
3	0 0 1 0
4	0 0 1 1
5	0 1 0 0
6	0 1 0 1
7	0 1 1 0

8	0 1 1 1
9	1 0 0 0
10	1 0 0 1
11	1 0 1 0
12	1 0 1 1

ASCII code:

If we take 26 alphabet (Capital) + 26 alphabet (Lower) + (0-9) Number + all punctuation (34) = 96 symbols called alphanumeric character.
Number of minimum bits required for 96 symbol = $\log_2 96 = 7$ (Next integer)
American invented seven bit code and all standard code for information interchange in ASCII.

EBCDIC code: It is 8 bit code (2^8=256) containing extra graphic symbol with ASCII.

Excess 3-code: Take a secrete number and add 3 in each digit then convert into binary code digit wise, for example

Let the secrete number be 1 5

Add 3 3 in secrete number

1 5
3 3
4 8

Excess 3 code of 15 is (01001000).

Gray code: Main advantage of gray code is in the field of analog to digital conversion.
Convert 10111 to its Graycode.

Step I Record the M S B 1 0 1 1 1

↓

1

Step II Add this M S B to the next position i.e., 0, record the sum and neglect the carry if generated

1 0 1 1 1

↓↓

1 1

Step III Record the successive sums until completed

1 0 1 1 1

1 1 1 0 0

Hence Gray code of 10111 ⟶ 11100

Error Detection and Correcting codes (ED & CC):

Error detection defined as process of detecting errors and Error correction defined as process of correcting errors. In digital system information in binary format (1s and 0s) is passes from the sender to receiver; there is always chance of error. 1 can be interpreted as 0 or 0 taken to be 1. Three types of errors can arise here (1) Single bit error (2) Multiple bit error (3) Brust error.

Parity checking is the most common and inexpensive method for ED & CC. Here every piece of data, a parity bit is computed and sent along with data.

Step of parity computation:

Both the sender and the receiver initially agree to either even or odd parity

Sender		Receiver
1 1 0 1 …….	$\overset{\rightarrow}{\leftarrow}$	1 1 0 1 …1….
Parity	even	

Sender		Receiver
1 1 0 1 …….	$\overset{\rightarrow}{\leftarrow}$	1 1 0 1 …0….
Parity	odd	

Hamming code:

This code not only detects error but also correct the error. Assuming four data bits are to be transmitted, the word format Hamming gives

D_7 D_6 D_5 P_4 D_3 P_2 P_1

Where D_7 , D_6 , D_5 & D_3 are data bits and P_4 , P_2 & P_1 are parity bits.

P_1 is set which establishes even parity over bits P_1 , D_3 D_5 and D_7.
P_2 is set which establishes even parity over bits P_2 , D_3 D_6 and D_7.
P_4 is set which establishes even parity over bits P_4 , D_5 D_6 and D_7.
Ex. Write Hamming code for 1 0 1 0.

Here D_7 D_6 D_5 P_4 D_3 P_2 P_1
1 0 1 0

P_1 must be 0 in order to make bits 1, 3, 5 & 7 even.
P_2 must be 1 in order to make bits 2, 3, 6 & 7 even.
P_4 must be 0 in order to make bits 4, 5, 6 & 7 even.
So the Hamming code of 1 0 1 0 be 1 0 1 0 0 1 0.

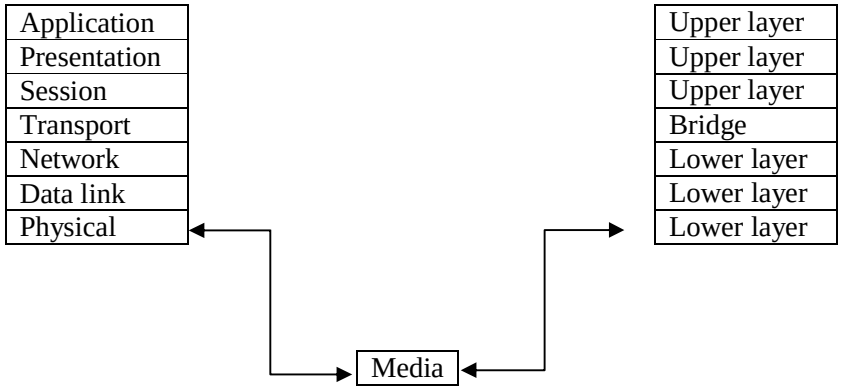
Open System Interconnection (OSI) Model:

For effective flow of information between computers it is necessary to establish rules for communication. These rules are termed as protocols. Every protocol has three components:

- Syntax (format of data),
- Semantics (meaning of various portions of data)

Timing (when data should be sent and how fast)

The ISO developed a seven layer model for computer network. This model is known as OSI model and its pictorial representation is as:



Upper layer is user oriented whereas lower layer is hardware oriented.
Here we consider only presentation layer and its main functions are:

- Data format conversion (to convert data in appropriate formats for machine to recognize)
- Encryption (in order to ensure privacy & authentication encryption is essential)
- Data compression (reduce the number of bits)
- Validating password

4. CRYPTOGRAPHY

It is the science of encrypting and decrypting written communication. Cryptography fundamentally deals with problem whose solution requires some secret knowledge like

decrypting an encrypted message/ signing some digital document etc. Historically four groups of people have used and contributed to the art of cryptography- The Military, The diplomatic corps, Diarists and Lovers. Out of these the military organization has had the most important role and has shaped the field.

Today, the term of Cryptography can be defined as the study of techniques and applications that depend on the existence of difficult problem.

The goal of Cryptographic systems:

- Privacy- information should restricted only to the two parties involve in communication.
- Authentication- recipient satisfy himself that the message he/she has received has originated only by the sender and not from an unauthorized person.
- Signature- Sender $\xrightarrow{\text{Message}}$ Receiver
  (Sign by receiver that message originated by sender)

Message and encryption:

Any message, which a human being understand is termed as plain text (clear text). Encryption is the process of converting the given plain text into a scrambled form. The encrypted message is called cipher text.

The process of turning cipher text back into plain text is called decryption.

A cryptographic algorithm is the mathematical function use for encryption and decryption purpose (easy to use but extremely difficult to crack), there are two function, one use for encryption and other for decryption.

- Symmetric key cryptography- using single key for both encryption and decryption.
- Asymmetric key cryptography- uses one key for encryption and another for decryption.

5. RSA ALGORITHM FOR PUBLIC KEY ENCRYPTION/DECRYPTION:

Public and private key are generated trough RSA algorithm easily, the steps of algorithm is as follows:

- Generate two large prime number, p & q.
- Let n = pq
- m = (p-1)(q-1)

- Choose a small number e which co prime to m.
- Find d (integer) such that d e % m =1
- Publish e and n as the public key; keep d and n as secret key.

Encryption $C = P^e \% n$, where C is coded text.
Decryption $P = C^d \% n$, where P is plain text.
Here we take an illustrated example based on RSA algorithm. For the sake of convenience, the value of p and q are taking very small.

Step	Action	Result
I	Two prime number	p = 7, q = 19
II	n = pq	n = 7 * 19 = 133
III	m = (p-1)(q-1)	m = (7-1)*(19-1) = 108
IV	Choose e, co prime to m So let e = 5	e = 2, gcd (2, 108) ≠ 1 e = 3, gcd (3, 108) ≠ 1 e = 4, gcd (4, 108) ≠ 1 e = 5, gcd (5, 108) = 1
V	Find d such that d e % m =1 Or d e = 1 + n m Or d = (1 + n m) / e d should be integer.	When n = 0, d is not integer. When n = 1, d is not integer. When n = 2, d is not integer. When n = 3, d = 65 (integer).
VI	For public key	n= pq= 133, e = 5
VII	For private key	n = 133, d = 65

Let use the message **P = 6** (less then p & q),

Encryption using RSA

$C = P^e \% n = 6^5 \% 133 = 7776 \% 133 = 62$
Hence coded text C = 62.

Decryption using RSA

$P = C^d \% n = 62^{65} \% 133 = 62 * (62^2)^{32} \% 133$ (using law of indices)
$= 62 * (3844\%133)^{32} \% 133$ (using Hash function)
$= 62 * 43 \% 133$ (on solving by using property of %)
$= 2666 \% 133$
$= 6$

So we can see that sender sends encrypted coded massage 62 and receiver decrypted it and find original message 6.

6. LEGISLATION AND REGULATIONS

What is legislation?

Legislation is the act of making or enacting laws. When people talk about 'the legislation', they mean a law or a body of laws. 'The private security legislation' in a state or territory is all the laws enacted specifically to control and administer the private security industry.

What are regulations?

Regulations are the way that the legislation is applied. They are generally very specific in nature, and are also referred to as 'rules' or 'administrative law'. Regulation of the private security industry is a state responsibility. Each state and territory has its own legislation and regulations listed below.

State/Territory Legislation and Regulations for the private security

ACT : Security Industry Act 2003, Security Industry Regulation 2003

NSW : Security Industry Act 1997 , Security Industry Regulation 2007

NT: Private Security Act, Private Security (Crowd Controllers) , Private Security (Miscellaneous Matters) Regulations , Private Security (Security Firms) Regulations, Private Security (Security Officers) Regulations

QLD : Security Providers Act 1993, Security Providers (Crowd Control Code of Practice) Regulation 2008, Security Providers Regulation 2008, Security Providers (Security Firm Code of Practice) Regulation 2008, Security Providers (Security Officer – Licensed Premises - Code of Practice) Regulation 2008

SA : Security and Investigations Industry Act 1995, Security and Investigations Industry Regulations 2011

TAS : Security and Investigations Act 2002, Security and Investigations Regulations 2005

VIC : Private Security Act 2004, Private Security Regulations 2005

WA : Security and Related Activities (Control) Act 1996, Security and Related Activities (Control) Act 1996.

Encryption Law or Cryptography Law deals with legislation ensuring that information is secure and transmitted confidentially, as well as policies designed to keep secure encryption schemes out of the hands of unauthorized individuals and foreign powers. The government has implemented several tools to transform data via encryption technology to prevent unauthorized access to or modification of sensitive governmental and public information.

Laws related to Encryption/Privacy in Indian scenario:

The privacy of communication is explicitly protected by Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights, and national law the government has not made any effort to define encryption in the Indian IT Act 2000, but technically it clearly says that it is not allowed.

The Department of Telecommunication ("DoT") controls all aspects regarding Telecommunications including encryption. Indian Information Technology Act 2000 would require all Internet Service Providers to monitor all traffic passing through their servers, making traffic, including the plain text of encrypted traffic, available to "properly constituted authorities" for "valid reasons of security." Properly constituted authorities include the

Central Bureau of Investigation (CBI), the Intelligence Bureau (IB) and the Research and Analysis Wing (RAW). Thus, there would be scope for such a right in Article 2128, in Article 19(1)(a)29 as well as in Article 19(1)(d)30. Since the exact position of the right to privacy with respect to enumerated rights appears to be somewhat vague.

It is evident that case law and judicial pronouncements play a significant role in determining the status of the right. The Constitutional position is that Article 19(2) imposes the restrictions upon the freedom of speech conferred by Article 19(1)(a) but since the right to privacy has been held to be largely under Article 21, it is subject only to ”procedure established by law”. This term may actually encompass more possibilities than have been intended by Article 19(2) but if one were to extend provisions such as those of the Telegraph Act to the Internet scenario it is clear that the effect would be to have restrictions similar to those imposed by Article 19(1(a).

Privacy under the Indian Information Technology Act, 2000 Section 72 of the Act, establishing an Information Technology Offence of “Breach of Confidentiality and Privacy” Restrictions on Cryptography in India and Information Technology Act, 2000 The Act takes into consideration the system of ‘key-pair encryption’ for the recording and authentication of digital signatures. The Act provides specifically, that the public key is to be deposited with a certifying authority. Section 69 reads as under. “69.

Directions of Controller to a subscriber to extend facilities to decrypt information.-(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. It may be concluded that the procedure is not adequate as it leaves complete discretion in the hands of the controller.

CONCLUSION

Any solution to the encryption issue will upset those on both sides of the issue. The challenge is to find a solution that protects society, yet allows the greatest amount of privacy protection for individuals and commercial enterprise. Allowing economic interests alone to drive such a sensitive policy is problematic. It appears as though that what is essentially driving the proposed legislation. Even privacy issues seem to take the back seat when statements like "Encryption is good for American business and good business for Americans," is the norm.

By far the most disturbing thing is the perception that the government and law enforcement organizations cannot be trusted not to abuse their power excessively. While this does happen, the Clipper failure illustrates the paranoia that has set in with regard to government power. While it might be foolish to have every decryption key in one place, guarded by one agency, seeking a way to ensure the police can still do their job doesn't seem like a horribly oppressive perspective.

The proposals above are not bullet proof, there are still loop-holes. However, their purpose is not to provide an ultimate answer, rather, it is to provide an example of how the interests of all parties can be negotiated to an imperfect but livable solution that protects privacy, while ensuring the continued viability of our judicial system. If everyone were to use unbreakable cryptography, and not even a subpoena could force decryption, the effectiveness of the judicial system, and the gathering of evidence would be hampered. It is up to all of us to make sure this does not happen, while we still ensure our basic constitutional freedoms are intact. Not an easy chore from any perspective, but one we must undertake together.

This paper is not designed to be an exhaustive review of every law and directive applicable across the world and is not to be construed as legal advice. By reading this paper, IT security practitioners, IT managers and others will gain an awareness of legal factors that affect them today. It is strongly advised that any organization requiring further explanations or details of appropriate legislation consult qualified legal practitioners.

REFERENCES

1. Anderson, R.: Why Cryptography fails, In the Proceedings of the Ist ACM conference on Computer and Communication Security, 215-227, (1993).
2. Barker, C,: Counter-terrorism and national security legislation reviews: a comparative overview, Foreign Affairs, Defence and Security, RESEARCH PAPER SERIES, 2014–15, (2014).
3. Blaze, S, Thompson, S, Weiner: Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security, (1996).
   Available Online URL http://www.bsa.org/bsa/cryptologists.html.
4. Coutinho, S. C.: The Mathematics of Ciphers: Number Theory and RSA Cryptography. Wellesley, MA: A K Peters, (1999).
5. Dorothy, D: *The Future of Cryptography*. *Available Online* URL http://www.eff.org/pub/Crypto/ITAR_export/Key_escrow/denning_02".
6. Flannery, S. and Flannery, D.: In Code: A Mathematical Journey. Profile Books, (2000).
7. Hazem, D, Charles M. C., Lee and David, T.: How Do Security Laws Affect Market Performance?
   http://www.aem.cornell.edu/research/researchpdf/wp/2005/Cornell_Dyson_wp0508.pdf
8. Stanley, N.: EU compliance and regulations for the IT security professional, A White Paper by Bloor Research, (2009).
9. Statement of Senator Leahy on Introduction of Encrypted Communications Privacy Act of 1996, (1996).
   Available Online URLhttp://www.cdt.org/crypto/leahy_stment.html.
10. Subashini, S, Kavitha, V,: A survey on security issues in service delivery models of cloud computing, *Journal of Network and Computer Applications*, 34, 1–11, (2011).