

MODEL BASED TESTING WITH TINY ALGORITHM

Paramjit Kaur *

Neeraj Raheja **

ABSTRACT

Software testing is a dynamic execution of the software in order to find out undiscovered error in the software. Role of software testing is not only to demonstrate the performance but also to take care of hidden defects since it is considered an ultimate barrier for release of software. Software testing is part of quality management. Quality management comprises of Quality assurance and quality control. Method applied to test the software is as follows:-

Functionality test is carried out manually or by applying automated testing Tools, such as Win runner, Quick test and latest tool Test Anywhere (tool).

Model based testing focus on the functional part that is at the front end (black box Testing) side when we look at its backend (white box Testing) for testing, that is taken care by the tester who prepare test cases manually and test them with automated Tools, In order to on form, whatever result we have obtained / achieved is as desired by tester as well as expectation of the customer. Whatever result obtained on testing need to be kept secret and if it is need to be transferred over a unsecured network, Tiny algorithm play a vital role since it not only encrypt the data that is to be kept secret (Results) but also provide security to the encrypted data being transmitted, in order to ensure that it reaches to desired destination's without any interruption.

Keywords: *Software Testing, Test cases generation, Tiny Algorithm, Encryption Decryption, Cryptography, Steganography.*

* Lecturer, Information Technology Department, Maharishi Markandeshwar University, Mullana, Ambala, Haryana.

** Assistant Professor, Information Technology Department, Maharishi Markandeshwar University, Mullana, Ambala, Haryana.

I. INTRODUCTION

Software testing is a dynamic execution of the software in order to find out undiscovered error in the software. Role of software testing is not only to demonstrate the performance but also to take care of hidden defects since it is considered an ultimate barrier for release of software. Software testing is part of quality management. Quality management comprises of Quality assurance and quality control. Method applied to test the software is as follows:-

Functionality test is carried out manually or by applying automated testing Tools, such as Win runner, Quick test and latest tool Test Anywhere (tool).

Model based testing focus on the functional part that is at the front end (black box Testing) side when we look at its backend (white box Testing) for testing, that is taken care by the tester who prepare test cases manually and test them with automated Tools, In order to on form, whatever result we have obtained / achieved is as desired by tester as well as expectation of the customer. Whatever result obtained on testing need to be kept secret and if it is need to be transferred over a unsecured network, Tiny algorithm play a vital role since it not only encrypt the data that is to be kept secret (Results) but also provide security to the encrypted data being transmitted, in order to ensure that it reaches to desired destination's without any interruption.

Section 2, Briefly discusses about Test Anywhere tool work. Section 3: Describe about test cases generations. Section 4, Describe how Tiny Algorithm can provide security to Test cases.

2. TEST ANYWHERE TOOLS:

Test anywhere is a intelligent and smart software that help us in creating a test cases at a faster speed and provide us the result rapidly, Create tests in minutes- record keyboard and mouse strokes, or use easy point, Easily manage automated tests across a single machine or multiple machines, Seamless information flow, is highly reliable and accurate, increase transaction speed and huge savings in time and costs. Use Testing Anywhere Client to automate data transfers, and import or export data between applications or from files. Automate routine backups and file management tests. Use Testing Anywhere Client to schedule tests using job scheduling. Automate software testing and routine Web development testing.

Automate FTP/SFTP, easily automated tests at any workstation, then upload or download it onto the server to share tests across users.

System requirements:

Requirements of Test Anywhere are windows -7, windows XP, vista, window 2008, windows 2003, and windows 2000.

3. TEST CASES BY ANYWHERE:

There are five ways in which test cases can be created using Test anywhere: And other features as Smart record, Object record, Web record test editor, image Reconization, report designer and many more

Example: - show how to use smart record

- a. Click on record button to start recording
- b. Then Click on smart record
- c. Type in note pad as my first record, save the text
- d. Click on checkpoint, window will appear
- e. Select window exit
- f. Save as, click on stop button to stop recording
- g. To see what is recorded click on run
- h. To edit in record line click on edit button.

4. TINY ALGORITHM:

“Secure Data Transmission through Network” is mainly designed for Providing security during transmission of data across the network. In this the Sender encrypts the data in to some form by using “Tiny Encryption Algorithm”. This algorithm has been used because it requires less memory. It Uses only simple operations, therefore it is easy to implement. The “Secure data transmission through network “is a web application Which deals with security during transmission of data across the network? Security for the data is required, as there is always a possibility for someone to Read those secret data. The system deals with implementing security using Steganography. Steganography is the art of hiding information in ways so as to Prevent detection of hidden messages.

Present day transactions are considered to be "un-trusted" in terms of security, i.e. they are relatively easy to be hacked. And also we have to consider the large amount of data through the network will give errors while transferring. Nevertheless, sensitive data transfer is to be carried out even if there is lack of an alternative. Network security in the existing system is the motivation factor for a new system with higher-level security standards for the information exchange.

Secure data transmission through network is software, which tries to alter to the originally of the data files in to some encrypted form by using " Tiny encryption Algorithm " encryption of data play very important role for providing data a security from intruder or stranger over unsecured network such that data is not altered, changed or deleted and reach destination in its original encrypted form. After data is being encrypted it can be transmitted over untrusted network with no fear. Main goal of research is to provide security to those test cases that need to be transmitted in some cases and it may possible the test cases that are generated by test anywhere need to kept confidential due to security purpose, so by using Tiny Algorithm these test cases that are needed to transmit and to keep the data confidential the original test cases can be converted into encrypted form by using Tiny Algorithm (figure 1.1).

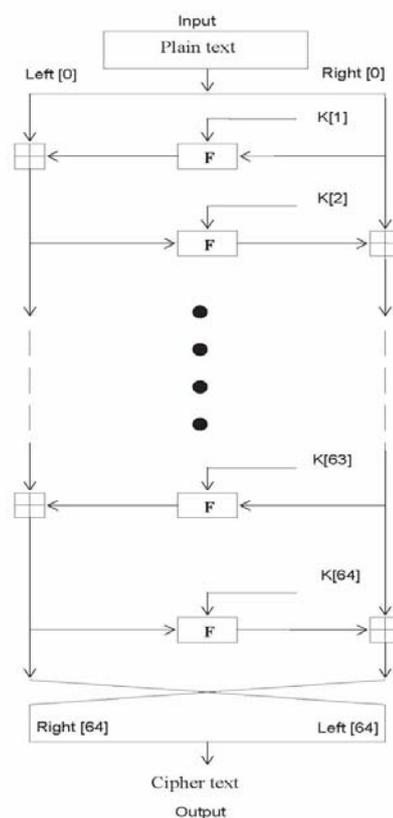


Figure 1.1: Diagram for encryption using tiny algorithm

Tiny Algorithm (TEA) is a cryptographic Algorithm designed to minimize memory and maximize speed. It is a feistel type cipher that uses operation from mixed algebraic groups. TEA seems to be highly resistant to differential cryptanalysis and achieves complete diffusion after only six rounds. Time performance on a modern desktop computer or workstation is very impressive.

Cryptographic Algorithm and protocols constitute the central components of system that protect network transmission and store data. The security of such system greatly depends on the methods used to manage, establish and distribute

The keys employed by the Cryptographic technique. Even if a Cryptographic Algorithm is deals in both theory and implementation, the strength of the Algorithm will be rendered useless if the relevant keys are poorly managed.

The Tiny Encryption Algorithm is a Feistel type cipher that uses operations from mixed (orthogonal) algebraic groups. A dual shift causes all bits of the data and key to be mixed repeatedly. The key schedule algorithm is simple; the 128-bit key K is split into four 32-bit blocks $K = (K [0], K [1], K [2], K [3])$. TEA seems to be highly resistant to differential cryptanalysis and achieves complete diffusion (where a one bit difference in the plaintext will cause approximately 32 bit differences in the cipher text). Time performance on a workstation is very impressive.

Block ciphers where the cipher text is calculated from the plain text by repeated application of the same transformation or round function. In a Feistel cipher, the text being encrypted is split into two halves. The round function, F , is applied to one half using a sub key and the output of F is (exclusive-or-ed (XORed)) with the other half. The two halves are then swapped. Each round follows the same pattern except for the last round where there is often no swap. The focus of this tiny algorithm is the TEA Festal Cipher

Decryption is to get the original data or information back these can be done with help of decryption diagram (Fig:1.2)

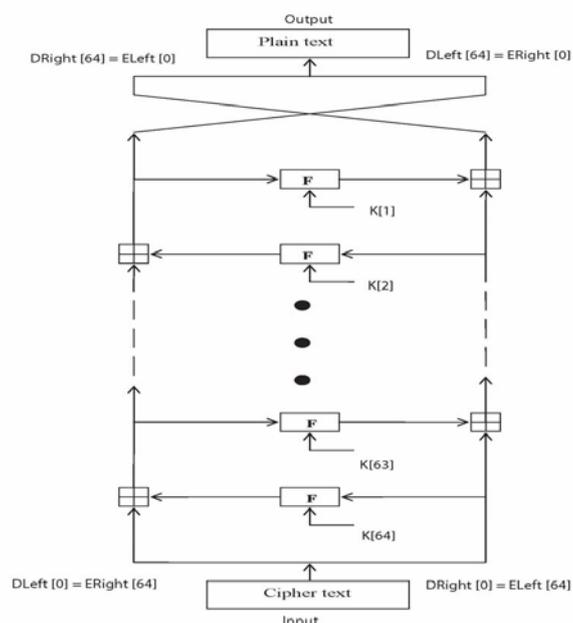


Figure1.2: Diagram for decryption using tiny algorithm

STEGANOGRAPHY:

Steganography is an art and science of hiding information within other information. These word has risen from Greek and it means hidden writings. In recent year's cryptography become popular in for the security of data or information. main difference between cryptography and Steganography, cryptography is about concealing of the message, and at the same time encrypted data package itself is a proof of existence of valuable data. And Steganography is one step ahead of Cryptography, Steganography it makes the cipher text invisible to unauthorized users, make the text appears as if it is of not much important as shown below (figure:1.3).

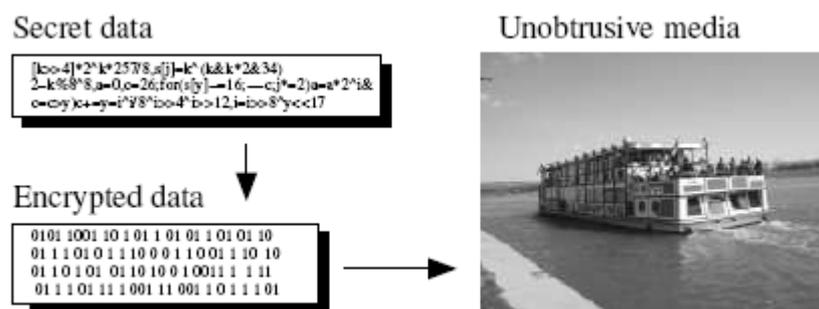


Figure 1.3: Steganography, make text invisible to unauthorized users

CONCLUSION:

In model based testing using tiny algorithm, we tried to generate test cases using test-anywhere automated testing tool and for security reason these test cases are converted to encrypted/decrypted using tiny algorithm before it is send over a unsecured network, so that the private data or information is protected from the intruder hence used these algorithm basically to provide security to data over network.

REFERENCES:

1. <http://www.google.com>
2. <http://www.wikipedia.com>
3. Andem, Vikram Reddy . “[A Cryptanalysis of the Tiny Encryption Algorithm](#)”,
4. Christian Cachin.” An information-theoretic model for steganography”. Lecture Notes in Computer Science, 1525:306.318, 1998.
5. Luis von Ahn and Nicholas J. Hopper. “Public-key steganography” In Lecture Notes in Computer Science, volume 3027,1995.
6. R. Anderson, R. Needham, and A. Shamir. “The steganographic file system”. In IWIH: International Workshop on Information Hiding, 1998.

7. M. Chapman and G. Davida. Hiding the hidden: A software system for concealing cipher text in innocuous text. In Information and Communications Security First International Conference, volume Lecture Notes in Computer Science 1334, Beijing, China, 11-14 1997.
8. Heehaws Pang, Kian-Lee Tan, and Xuan Zhou . “Steganographic schemes for file system”. IEEE Transactions on Knowledge and Data Engineering, 16(6):701.713, June 2004.
9. Kawaguchi, E; Eason RO . "[Principle and applications Steganography \(Original paper on Steganography\)](#)" sept 2008.
10. Hong, Seokhie; Hong, Deukjo; Ko, Youngdai; Chang, Donghoon; Lee, Wonil; Lee, Sangjin. "Differential cryptanalysis of TEA and XTEA". In Proceedings of ICISC , 2003.
11. Biham, E., & Shamir, “A Differential cryptanalysis of the data encryption Standard”. New York: Springer-Verlag, 1992.
12. Wheeler, D.J., & Needham, R.J. “TEA, a tiny encryption algorithm”. In Fast Software Encryption – Proceedings of the 2nd International Workshop, 1008, 1998.