A Secure License Key Generation using FBPS

Fatangare Sonal
Assistant Professor
JSPM's ICOER, Pune,
Maharashtra, India

Taksal Ashwini
Assistant Professor
JSPM's ICOER, Pune,
Maharashtra, India

Todmal Satish.R.
H.O.D.Computer Engg.
JSPM's ICOER, Pune,
Maharashtra, India

ABSTRACT
Secure message transmission is generally required for the system where transmitted message need to be verified at the receiver end. Fibonacci develops the reversible encryption algorithms as mentioned in below technique. The technique considers a message as binary string on which the Fibonacci Based Position Substitution (FBPS) method is applied. A block of n bits is taken as an input stream from a continuous stream of bits. The decimal equivalent value of a source block is obtain and finds its position on the Fibonacci series, on a number or in between two numbers. The source value is mapped on a previous number of the series called target number. For proper one-one mapping a scheme is applied on the target number. This target number is again projected on a previous number and so on until the target number reached in a 0 or 1. Each time of the projection a 0 or 1 is produced. Plain text is encrypted for different block sizes as per the specification of a session key of a session to generate the final encrypted stream. Comparison of the proposed technique with existing and industrially accepted RSA and Triple DES.

General Terms
Plug-in, FBPS algorithm, RSA, Session key.

Keywords
Fibonacci Based Position Substitution (FBPS) Technique, cipher bit, blocks cipher, Session Key, Plug-in, license key, algorithm.

1. INTRODUCTION
Now a day's more security applications are available for standalone systems. Antivirus are available for providing security to systems like operating systems, important data. Some application provided a key to install or run software successfully. But those keys are easily cracks by hackers, so hacker makes its copy and spread in market. This is affected to developers.

So to avoid this disadvantage, we implemented a new key concept that is Fibonacci based substitution method. In this technique we use the Fibonacci algorithm concepts, using this technique we secure the web base application. Fibonacci technique is more secure than other techniques and it is irreversible algorithm [1].

We have implemented one secure licensing system for web base application software. This licensing system is based on FBPS algorithm that is known as Fibonacci Based Position Substitution. In this system user downloads particular web base application software in secure manner by providing important information at that particular website from where user download the software. [1] Here our aim is to implement a secure system for web base application. These secure system is based on Fibonacci algorithm i.e. one of the secure algorithm. User goes to web site to download the web base application. At that time firstly user required to register and create own account on that website. User login into website then administrator provides rights to download the particular required web base software.

Users select the software that time he required some own known information. This information is nothing but IP address, Path, Domain Name, Validity, etc. Fibonacci class accepts this information and create the secured key i.e. license key. This license key is required to user to run the application on his website and without license key software don't work.

Important advantage of this system is providing more security means downloaded software work on only one website. Using this system we avoid duplication of software or piracy of the software.

1.1 Need
Software piracy refers to the unauthorized duplication and use of computer software. Developers work hard to develop solid software programs. If those applications are pirated and stolen, the software developers will often be unable to generate the revenue required to continue supporting and expanding those application. The effect of software piracy impact the entire global economy the reduced revenues often divert funding from product development and result in less research and less investment in marketing.

Software is intellectual property and is protected by copyright law in most country. Most software license grant user the permission to use the software, but license holders does not own the software they simply own license to use software.

Customers who use pirated software are not without risk. Pirated software may contain Trojans, Viruses and other form of Malware, because the pirated software will often modify the downloaded file with malicious code.

So to avoid this problem we have implemented this system i.e. FBPS. Using this system we have provide strong security for web base application.

1.2 Basic concept
- User will register for the license key with their details at which web application is going to execute. The details will contain mandatory information like IP address, domain name, path, expiry date.
- Fibonacci techniques are applied to generate license key message. Here message is nothing but license key.
- The encrypted license key will be available for user to download at their respective logins.
- The key decryption techniques is implemented at the end of third party application license check

1.3 Applications

The FBPS algorithm is applied to develop this system which is used to provide more security over internet for web base applications. So we use Fibonacci algorithm technique that is not easily cracks by any intruder.

The FBPS algorithm is implemented to make a secure system for web base application. These secure system is based on Fibonacci algorithm i.e. one of the secure algorithm. User goes to web site to download the web base application at that time firstly user required to register and create own account on that website. User login into website then administrator provides rights to download the particular required web base software [1].l.

2. LITERATURE SURVEY

Limitations or failure of existing systems or the awareness of technological advances relating to the particular are involved in particular systems which competitors are developing.

Information systems projects originate from many reasons: To achieve greater speed in processing data, better accuracy and improved consistency, faster information retrieval, integration of business areas, reduced cost and better security. The sources also vary project proposals originate with department managers, senior executives and systems analysis. Sometimes the real origin is an outside source, such as a government agency, which stipulates systems requirements the organization must meet. When the request is made, the first systems activity, the preliminary investigation begins. The activity has three parts: request clarification, feasibility study and request approval.

The existing technology is also good and implemented but provides less security. Generating the encryption process from existing algorithm is easily track by intruder.

So we developed the system that provides the encrypted key i.e. license key using the Fibonacci algorithm. [1].

2.1 Related Work

Cryptography is notoriously the science of using mathematics to encrypt and decrypt data. It 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.

This system makes contributions to implement some of the cryptographic algorithms like DES [5], RSA [3,7] and FBPS [1] using J2SE, J2EE and Oracle technologies Aims is to reducing the brute force attacks on the FBPS algorithm and its quicker implementation plaintext and compressing a file before encryption reduces these redundancies.

Besides that encryption is time consuming; compressing a file before encryption speeds up the entire process.

The main purpose of development of this system is to provide more security over internet for web base applications. So we use Fibonacci algorithm technique that not easily cracks by any intruder. The Fibonacci Based Position Substitution (FBPS) method is applied. A block of n bits is taken as an input stream from a continuous stream of bits. The decimal equivalent value of a source block is obtain and finds its position on the Fibonacci series, on a number or in between two numbers. The source value is mapped on a previous number of the series called target number. For proper one-one mapping a scheme is applied on the target number. This target number is again projected on a previous number. To provide more security for web base application over the internet we required some type of information to generate the license key. This information is nothing but IP address, domain name, path, expiry date, etc. License is generated using this information and this license key is provide to web base application to run successfully on web.

2.2 Existing System

Cryptography is an essential aspect for secure communications to protect important data or messages from eavesdroppers. Since every algorithm available today for this purpose has merits and demerits, no single algorithms are sufficient. So there is need to develop algorithms in the field of cryptography to enhance the security further. This system have a new technique has been proposed where the source message is considered as a stream of binary bits. The technique transforms the document into an unintelligible form using FBPS from which the original message recovered using the reverse technique. A proposal for generalize key generation is described.

3. PROPOSED SYSTEM

The main purpose of development of this system is to provide more security over internet for web base applications. So we use Fibonacci algorithm technique that is not easily cracks by any intruder.

The Fibonacci Based Position Substitution (FBPS) method is applied. A block of n bits is taken as an input stream from a continuous stream of bits. The decimal equivalent value of a source block is obtain and finds its position on the Fibonacci series, on a number or in between two numbers. The source value is mapped on a previous number of the series called target number. For proper one-one mapping a scheme is applied on the target number. This target number is again projected on a previous number.

To provide more security for web base application over the internet we required some type of information to generate the license key. This information is nothing but path, IP address, domain name, expiry date, etc. License is generated using this information and this license key provide to web base application to run successfully on web.

To prepared a master plan for system which will guide at different time in different phases of software development.

3.1 Providing security to Web base application

To generate an encrypted key for web based application and it is provided to client when payment process is completed. Clients download particular software application and the encrypted key is available to clients. Many key generation software's are available but we are interested to providing security to web based application and providing security to web based application it's very difficult.

Because it's work on internet and huge number of peoples, Clients access this software and it's very difficult to maintain the security at that time. Here more chances are created to hack the particular software.

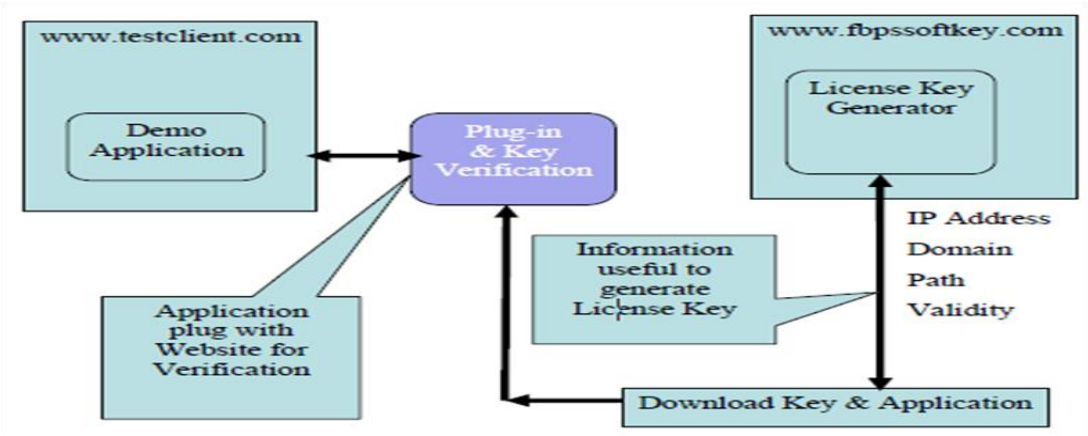

Fig 1: System Architecture

Working:
First step is simple both parties required to register into www.fbpssoftkey.com web site then login into their respective accounts. Client's checks software list and select software then new page open. Fill all the right information in form and submit the form. Choose payment type for purchasing the software. Administrator handles all function like monitoring software, checking requests, payment process. Payment process completed then admin provides software to client for downloads and key available for download.

Second step is uploading respective application into website and install encrypted key. If all provided information is right then application is registered successfully.

3.2 Client process

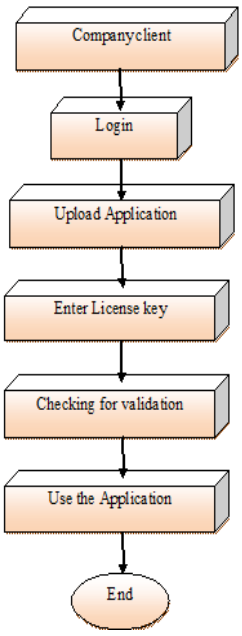

Fig 2: Client Process Flow diagram

User goes to web site to download the web base application. At that time firstly user required to register and create own account on that website. User login into website then administrator provides rights to download the particular required web base software.

3.3 Server Process

Users select the software that time he required some own known information. This information is nothing but IP address, Path, Domain Name, Validity, etc. Fibonacci class accepts this information and create the secured key i.e. license key. This license key is required to user to run the application on his website and without license key software don't work.

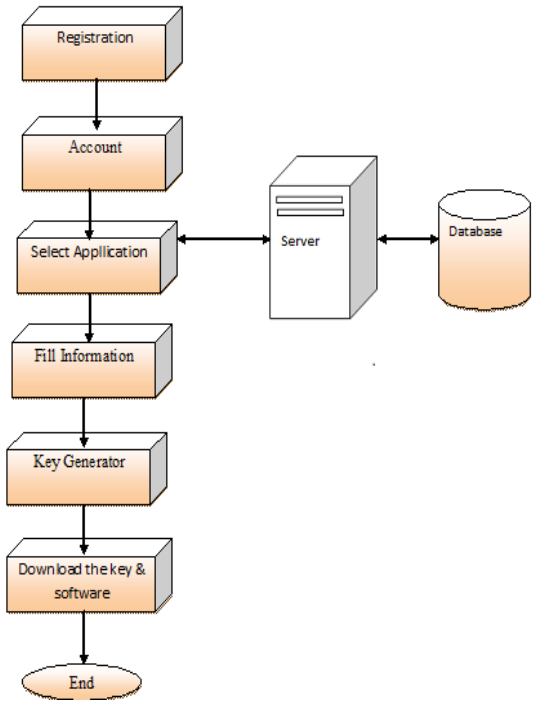

Fig 3: Client Process Flow diagram

3.4 Plug-in

A Plug-in is a software application. When an application supports plug-ins, it enables customization. The common examples are the plug-ins used in web browsers file type Adobe Flash Player, the QuickTime Player, and the Java plug-in, which can launch a user-activated Java applet Java virtual machine. software component that adds a specific feature to an existing to add new features such as search-engines, virus scanners, or the ability to utilize a newsuch as a new video format. Well-known browser plug-ins include the on a web page to its execution a local.

3.5 Mechanism

As shown in the figure, the host application provides services which the plug-in can use, including a way for plug-ins to register themselves with the host application and a protocol for the exchange of data with plug-ins. Plug-ins depend on the services provided by the host application and do not usually work by themselves. Conversely, the host application operates independently of the plug-ins, making it possible for end-users to add and update plug-ins dynamically without needing to make changes to the host application

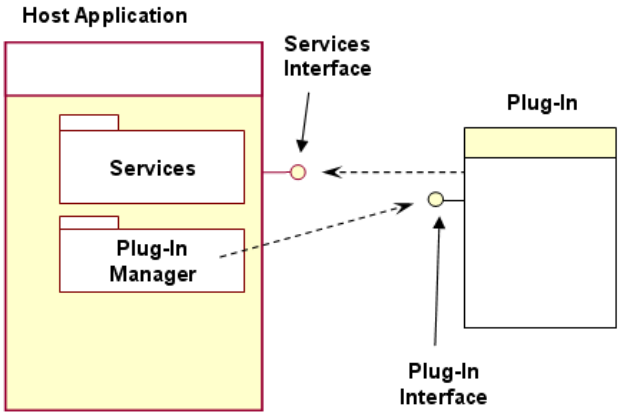

Fig 4. Plug-in working

4. RESULT

In this section proposed system implemented in java, PHP and ORACAL.The encryption and decryption average time for various files for proposed scheme are less than the RSA and Triple DES algorithm. The ten different sizes file taken for experiments. Following figure shows the comparative average time for proposed scheme and RSA Triple DES.

Parameters	Schemes	Encyption	Decryption
Avg time (s)	Proposed Scheme	8.3	9.1
	RSA	20	21.8
	Triple DES	50	54

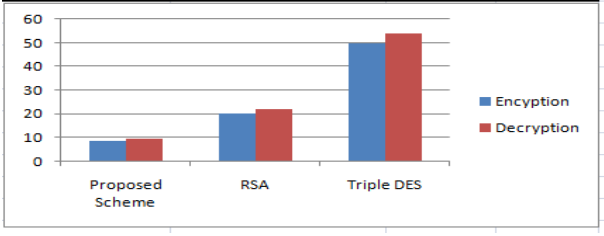

Fig 5. Comparison of average encryption and decryption time for proposed scheme and RSA and Triple DES

The following figure shows secure license keys generated by RSA, Triple DES and FBPS algorithms. Here FBPS generate more secure and longer Secure key than RSA and Triple DES.

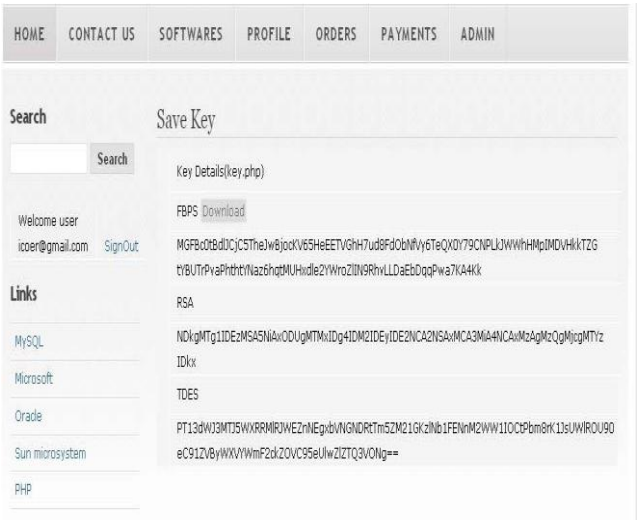

Fig 6 License Key generation using FBPS

5. CONCLUSION

The FBPS technique proposed here is a mapping technique which has a very small space overhead. Moderate percentage of bit flips reveals that a good diffusion occurs among bits. Parametric tests also show comparable results. Cascading same principle as round may enhance the security but in principle as round may enhance the security but in same encryption and decryption algorithm can be designed for K^n-1 <=V < Ki for some base K that may be either 2 or 3 or any other integer acting as the base.Also we can change K in different sessions to increase the security. It can be easily implemented in any high level language for practical application purpose to provide security in message transmission and the encryption time can be made comparable with decryption time by choose a suitable search techniques.In future scope the various other tests may be performed for operability of proposed scheme.

6. ACKNOWLEDGMENTS

Foremost; I would like to express my sincere gratitude to our principal Dr. S.V. Admane for his continuous support, patience, motivation, enthusiasm, and immense knowledge. His guidance helped us in all the time of research and preparing of this paper.

7. REFERENCES

[1] J. K. Mandal, Mangalmay Das, 2009 "Fibonacci Based Position Substitution (FBPS) Encoder for Secured Message Transmission" Proceedings of IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009.

[2] B Mandal, J. K. Paul, M., 08th 09th February 2008 "A Permutative Cipher Technique (PCT) to Enhance the Security of Network Based Transmission", Procedings of 2nd National Conference on Computing for Nation Development, Bharati Vidyapeeth's Institute of

Computer Applications and Management, New Delhi,, pp. 197-202,.

[3] D. Welsh, 1988 "Codes and Cryptography", Oxford; Claredon Press.

[4] RSA Vulnerabilities", Journal of Cryptology, vol 10, pp 233-260, 1997.

[5] DES:http://en.wikipedia.org/wiki/Data_Encryption_Standard.

[6] TDES: http://en.wikipedia.org/wiki/Triple_DES

[7] RSA:http://en.wikipedia.org/wiki/Rsa_algorithm