# Securing Online Paper Evaluation System Using Multi Prime RSA

Y.Yugesh Kumar Naidu[1], Dr.K.Venkataramana[2]
[1] *Y.Yugesh Kumar Naidu, Dept. of MCA, KMM Institute of Post Graduate Studies*
[2] *Dr.K.Venkataramana, Head of The Dept MCA, KMM Institute of Post Graduate Studies, Tirupati, A.P*

***Abstract*- This Online Examination System is a product arrangement, which enables any industry or establishment to organize, direct and oversee examinations by means of an online domain. It should be possible through the Internet/Intranet and/Local Area Network conditions. A portion of the issues looked amid manual examination frameworks are the deferrals happened in result handling, documenting represents an issue, sifting of records is troublesome. The possibility of loss of records is high additionally record seeking is troublesome. Upkeep of the framework is additionally exceptionally troublesome and takes part of time and exertion. Online examination is one of the significant parts for online training framework. It is proficient, sufficiently quick and decreases the huge measure of material asset. An examination framework is produced in view of the web. This paper portrays the guideline of the framework, shows the principle elements of the framework, dissects the auto-creating test paper calculation, and talks about the security of the framework.**

***Index Terms*- Encryption, Decryption, SeA encryption algorithm, Information Security**

## I. INTRODUCTION

The Online Examination System is an electronic application. This structure will help the school/Institution to evaluate the request have diverse option with one right answer. The school/Institution can coordinate the online examination and report the result in a couple time. The examination office is responsible for the making the request paper and it would be thoroughly secure. Online Examination structure give remotely access to understudies. It helps the monitor with diminishing crafted by driving exam, checking answer sheets and creating result. All these work is done by the machine. All the data is secured on the server. Likewise, clients can get to these databases and give exam. Here we use a client server show. Official offer access to educator and understudies. Understudies who have account on the system will have the ability to give exam. There are two sorts of exam portion Practice and Real test (1). Understudies can give the two tests. Right answer will be featured in different shading. Consequent to submitting test the result will be made and examinations are done on the start of result and send it to each and every understudy.

## II. RELATED FRAMEWORK

In standard system driving test is exceptionally redundant work for expert and expert individual as well. the total system of allotting test and evaluating their score once the investigate was done physically until date. Be that since it could, on-line examination structure is totally electronic system. The structure goes for diminishing costs associated with driving exams over a time period and achieving complete motorization of examination system associated assignments like visit, dissemination of results that prompts an abnormal state of system viability. Inside the wake of encountering huge quantities of reference papers finally, we tend to territory unit completed that we can processing plant made one goal structure that may offer easy to know access to determine for managing exam and examination of the outcome.

Network application development model is an important Browser-Server model. The special model as client server model that contained client side as web browser, and server side as web servers, for online network model. In case of LAN connectivity, the server node acts as the server side for handling and maintenance of the online network. The client nodes are the other computers connected in the local area network, which are able to gain the access to the question papers from the server for the specified

session. The main logic of the system is implemented on the server, later these copies of the main logic output are directly accessed on the client nodes. Such a web application has the good reusability and ease in maintainability. The entire system is developed in .Net Framework with use of C# (C Sharp) and JavaScript language and runs on the IIS (Internet Information Server) server. The whole system can be hosted on the network online, thus the name Online Examination System. JavaScript has become the technological need to be implemented in Web applications, because it is the easiest way in rapid development(3).

## III. LITERATURE SURVEY

exam bank developing This paper portrays the utilization of rearranging calculation in an Automatic Generator Question paper System (GQS) as a randomization method for arranging sets of exam paper(1). The outcomes shows the rearranging calculation could be utilized to beat randomization issue for GQS.

## IV. SCOPE

- Online Examination course of action is a Multiple Choice Questions based Examination structure. It gives a straightforward method to use nature for both test-conductors and understudies appearing for examination. Online Examination System is a web application that sets up a framework between the foundations and understudies. Foundations enter on the site the request they require in the exam. These request are appeared as a test to the qualified understudies. The appropriate responses enter by the understudies are then surveyed what's more; their score is registered and saved. This score at that point can be got to by the associations to center the passes understudies or to survey their execution(12). Online Examination System gives the stage yet does not particularly appreciate, nor is it incorporated into any tests drove. Request are posted not by the site, but instead customers of the site. The site requires an association to enroll before posting the request. The site has a supervisor who keeps an eye out for the general working of the structure.
- Online examination will lessen the hurried control of assessing the appropriate responses given by the candidates physically.
- Being an organized Online examination system it will diminish paper work.
- To allow workforce to give additional opportunity to understudies with handicaps.
- To allow workforce to make tests and answer key.
- To allow customized checking on and manual assessing which can be recorded per test(5).

## V. AREA OF THE PROJECT

- The main objective of this online exam system is to reduce the work of conducting the exam.
- The online examination framework is an electronic application which is valuable every where throughtout the instructive and corpotate sector(5).
- The online examination framework incorporates the engineering segments as Browser-Server design, Client-Server Architecture, Auto Question Generator System, Security, Randomization.
- The Random Number Generation Algorithm is utilizes for this framework. It is depicted forward.

## VI. RANDOM NUMBER GENERATOR

Random Number Generators i.e. RNG's utilized for uses of cryptography that for the most part creates an arrangement of zeros and one bits, that might be as one joined into the sub-successions or squares of arbitrary esteems. The two fundamental classes that are utilized for this calculation are as per the following:

1. Deterministic and
2. Non Deterministic.

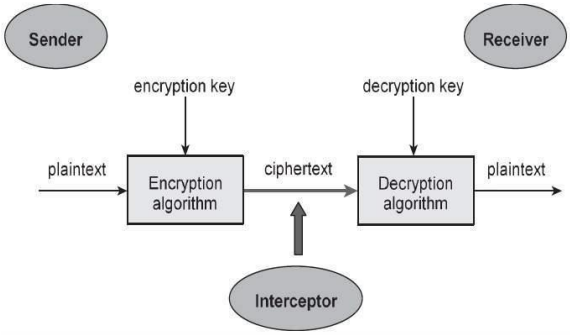
A Deterministic RNG comprises of calculation that delivers an arrangement of bits from an underlying worth called a seed.

A nondeterministic RNG produces the yield which is reliant on some eccentric physical source that is outside human control. No FIPS affirmed nondeterministic arbitrary number generators are there.

## VII. MULTI PRIME RSA ALGORITHM

We begin by describing a simplified (or textbook) version multi-prime RSA. For any integer r _ 2, r-prime RSA consists of the following three algorithms:

Key Generation: Let N be the product of r randomly chosen distinct primes p1, . . . , pr. Compute Euler's totient function of N : _(N) = Qr i=1(pi − 1). Choose an integer e, 1 < e < _(N), such that gcd(e, _(N)) = 1. The pair (N, e) is the public key. Compute the unique d 2 ZN such that ed _ 1 mod _(N) (i.e., compute d = e−1 mod _(N)). The private key is the pair (N, d).




*Encryption:* It is a scientific procedure that creates a ciphertext for any given plaintext and encryption key. It is a cryptographic calculation that takes plaintext and an encryption key as information and produces a ciphertext(13).

For any message m 2 ZN, the ciphertext is registered as c = me mod N.

*Decryption:* It is a scientific procedure, that creates a novel plaintext for any given ciphertext and decoding key. It is a cryptographic calculation that takes a ciphertext and an unscrambling key as info, and yields a plaintext. The unscrambling calculation basically switches the encryption calculation and is in this manner firmly identified with it(13).

For any ciphertext c 2 ZN, the plaintext is recovered by computing m = cd mod N. We call N the multi-prime RSA modulus, the RSA modulus (when r = 2), or simply the modulus. The integer e is called the public (or encrypting) exponent and d is called the private (or decrypting) exponent.

When r = 2 we have the original RSA encryption scheme. Superficially, the only difference between RSA and multi-prime RSA with r > 2 is the number of primes in the modulus. There are practical reasons for using more primes in the modulus, however, which can be found in the implementation details of the decryption algorithm. The first advantage is time; using the Chinese Remainder Theorem and performing calculations in parallel, the number of bit operations needed to decrypt a ciphertext is at most 3 2r3 (log2 N)3 (using standard arithmetic). So, the time needed for decryption decreases with each additional prime in the modulus. The second advantage is space; again, using the Chinese Remainder Theorem, the space needed for all decryption computations until the very last (recombining step) require only log2 pr space, where pr is the largest prime in the modulus. If all the primes are roughly (log2 N)/r-bits large (balanced primes), the space required decreases with each additional prime added to the modulus. As we shall see in Section 2, using too many primes in the modulus increases the risk of the modulus being factored. Thus, a trade-off is analyzed. We now give some notation and assumptions used in the rest of this work. First, we only consider r-prime RSA with balanced primes. That is, if we label the primes so that pi < pi+1 for i = 1, . . . , r − 1, then we assume that

$$|4 < \frac{1}{2}N^{1/r} < p_1 < N^{1/r} < p_r < 2N^{1/r}.$$

The modulus is given by N = Qr i=1 pi and Euler's totient function for N is simply _(N) = Qr i=1(pi − 1). The congruence ed _ 1 mod _(N) is called the public/ private key relation, or simply the key relation. Writing this congruence as an equation yields

$$ed - k\phi(N) = 1,$$

where k is some positive integer. We call this equation the public/private key equation, or simply the key equation. It is often convenient to express _(N) in terms of the modulus: _(N) = N − _. Defining the set Sr = {1, . . . , r} we see that _ can be expressed as

$$\Lambda = N - \phi(N) = \sum_{i \in S_r} N/p_i - \sum_{\substack{i,j \in S_r \\ i \neq j}} N/(p_i p_j) + \cdots + (-1)^r.$$

As shown in [18], a simple computation using the above expression for _ and (1) shows that _ satisfies

$$\Lambda = N - \phi(N) < (2r-1)N^{1-1/r}.$$

Thus, _(N) and N have roughly an (r − 1)/r fraction of their most significant bits in common. The public and private exponents will often be expressed as a fraction of the modulus. We use _ to denote the size of the public exponent (e = N_), and _ or _ to denote the size of the private exponent (d = N_ or d = N_) depending on the context. Also, we often use the acronyms MSB and LSB as shorthand for most significant bits and least significant bits, respectively.

## VIII. CONCLUSION

The main objective of this online exam system is to reduce the work of conducting the exam. • The online examination system is a web based application which is useful all over the educational and corporate sector.

In this task Client was Web Browser, which executed the structure's grandstand objective. The limit was to send a request to the web server through the web programs by the customers (teachers or understudies). While the Web Server restores the requested HTML pages or HTML pages intensely made by JSP page to the client, which were showed up in the Web program. Business justification level was expert principally by JSP and JavaBeans running the JSP Engine. It responded to client requests and achieved the business method of reasoning with the Web Server. Tomcat, an open source writing computer programs, was used as the JSP Engine and Web Server. Information level was recognized with database structure, used to store the business data, for instance, request and papers besides, control data, for instance, customer data. MS ACCESS was used to achieve the data level. The JSP change demonstrates in perspective of Model 1 is to a great degree reasonable for smart and little scale application headway.

## REFERENCES


[1] International Research Journal of Engineering and Technology (IRJET) ONLINE EXAMINATION SYSTEM Deepankar Vishwas Kotwal1, Shubham Rajendra Bhadke2, Aishwarya Sanjay Gunjal3, Puspendu Biswas4

[2] International Journal of Emerging Technology and Advanced Engineering, Website: www.ijetae.com ( ISSN 2250 - 2459, ISO 9001:2008 Certified Journal, Volume 4 , Issue 3 ,March 2014)660 Online Descriptive Examination and Assessment System Bhagyashri Kaiche 1, Samiksha Kalan 2, Sneha More 3 , Lekha Shelukar 4 1,2,3,4 KBT College of Engg Nashik, (India)

[3] Z. M. Yuan, L. Zhang, G. H. Zhan, A novel web-based online examination system for computer science education, In proceeding of the 33rd Annual Frontiers in Education, 2013, S3F7-10.

[4] WebBased online Secured Exam; B.Persis Urbana Ivy,A.shalini, A.Yamuna/International Journal of Engineering Research and Applications (IJERA) ISSN:2248-9622 www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012, pp.943-944943.

[5] Online Descriptive Examination and Assessment System.L. Zhang, et al., Development of Standard Examination System of Special Course for Remote Education, Journal of Donghua University (English Edition), 2013, Vol. 19, NO.1, 99-102.

[6] Challenges of Online Exam, Performances and problems for Online University Exam; IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013 ISSN (Print): 1694-0784 — ISSN (Online): 1694-0814. www.IJCSI.org

[7] Al-Mashaqbeh, I.F. Al Hamad, A.Student's Perception of an Online Exam within the Decision Support System Course at Al al Bayt University Conference publication Pages: 131135 7-10 May 2010.

[8] Design and Development of the Online Examination System based on B/S Structure.Hongmei Nie Math,Physics and Information Engineering College Zhejiang Normal University Jinhua,China E-mail: nhm@zjnu.cn

[9] Shuffling Algorithms for Automatic Generator Question Paper. Nor Shahida bt Mohd Jamail Abu Bakar Md Sultan Faculty of Computer Science and Information Technology Universiti Putra Malaysia, 43400 UPM SERDANG, Selangor, Malaysia. E-mail: shahidajamail@yahoo:com

[10] Hanxiao Shi, Guodong Zhou and Peide Qian (2010), An A ttribute - based Sentiment Analysis System, Information Technology Journal, pp 1607 - 1614.

[11] Papri Chakraborty (2012), Developing an Intelligent Tutoring System for Assessing Students Cognition and Evaluating Descriptive Type Answer, IJ MER, pp 985 - 990.

[12] J. Bl¨omer and A. May. Low secret exponent RSA revisited. In Cryptography and Lattices – Proceedings of CALC '01, volume 2146 of Lecture Notes in Computer Science, pages 4–19. Springer-Verlag, 2001.

**[13]** https://www.tutorialspoint.com/cryptography/cryptosystems.htm