International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

# Highly Secured Web Portal
# An Illustration of Enhanced Web Security

Swapnil B. Khalekar.
Department of Information Technology.
MIT College of Engineering.Pune, India.

Himesh Kishore
Department of Information Technology.
MIT College of Engineering.
Pune, India.

Aniruddha Desai
Department of Information Technology.
MIT College of Engineering.
Pune, India.

***Abstract*- Data security today is one of the most important things to be considered while designing web portal. Especially a portal where confidential data is being exchanged over client and server framework, data is exposed to unwanted intrusion. In such cases data is subjected to different types of attacks such as Man in the middle attack, eavesdropping, data modification etc. Many algorithms have been developed to tackle these serious issues for example RSA, AES, Diffie-Hellman, etc. All the algorithms developed are used to encrypt the data information being exchanged in cipher so that intruders don't get the meaning out of it. Some algorithms developed are regarding the keys being used in encryption process such as Diffie-Hellman. Even though these algorithms are widely used and accepted they are also subjected to attacks to break the encryption code.**

**Over all these attacks and drawbacks, web portal security is main issue. Any institution that uses web portal for data exchange needs to be very cautious about the portal security. An institution must ensure that no security wholes are present in the system.**

**For making this happen at user level on a portal we have come up with an idea about creating a secured portal. This paper we present is an illustration of a highly secured web portal which helps in exchanging data over a secured manner.**

## I. INTRODUCTION

This paper here presents and implements an idea of highly secured web portal for theuse at institutional level. University of Pune has question paper setting as one of its very important works to be managed every year with high confidentiality. Every year teacher and subject chief has to meet in person to decide about the question papers for upcoming examination.

They have to discuss the exam pattern, question paper quality and many things in a meeting held every time. This whole process takes big time. Teacher has to recompile the paper every time it is rejected by the subject chief. Subject chief has to create an authorized number of copies to be shared with authorized people, such as college authorities, printing authorities etc. All this work is done in hand to hand fashion. A tradition sealed envelope is used to ensure that the confidentiality is maintained.

This paper contains an illustrative example of a portal for question paper setting, which will be highly secured and exchanges data online so that confidentiality and data integrity is maintained and also the time and efforts consumed by the whole process are reduced.

This portal also known as Paper setter is basically a client server framework that will be managed by authorized entities at University level. Authorized entities at University will be Super Administrator, Administrator, and Teachers. Super administrator's job is to finalize the paper, administrator's job is to call the paper, and Teacher submits the paper.

Our portal here uses a hybrid algorithm to encrypt the question papers being exchanged. To make hybridization we use two well-known algorithms that are RSA and Diffie-Hellman. RSA is a well-known algorithm for encrypting the data. Diffie-Hellman is a well-known algorithm for exchanging keys over a session created by user. Hybridizing two different algorithms increases the complexity of the encryption process. We will discuss the reason behind the hybridization in coming sections.

## II. RSA ALGORITHM

A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978 that became a de facto standard. RSA formed the basis for a number of encryption programs, including Pretty Good Privacy (PGP). RSA is an algorithm for public key encryption. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key encryption. It involves three steps: key generation, encryption and decryption it is still widely used in electronic commerce protocols, and is believed security depends on the difficulty of decomposition of large numbers [2].

Steps of Algorithm for Key Generation: 1. Choose two distinct prime numbers P and Q. 2. Calculate N = P x Q. (n is used as mod for both the public and private keys) 3. Select the public key (i.e. encryption key) E such that it is not a factor of (P – 1) and (Q -1). 4. Select the private key (i.e. the decryption key) D such that the following equation is true (D x E) mod (P – 1) x (Q – 1) = 1. 5. For encryption, calculate the cipher text CT from the plain text PT as follows: CT = PTE mod N. 6. Then send CT as the cipher text to the receiver. 7. For decryption, calculate the plain text

PT from the cipher text CT as follows: PT = CTD mod N. This algorithm is based on the theory of Prime Numbers and the fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product. The private and public keys in RSA are based on very large (100 or more digits) prime numbers. Real challenge in the case of RSA is the selection and generation of public and private keys.

*Problems in RSA Algorithm*

"If any one of p, q, and e, d is known, then the other values can be calculated. So secrecy is important. "It is important to make sure that message length should be less then bit length otherwise the algorithm will fail." Due to the usage of public key RSA is much slower than any other symmetric cryptosystems. "The length of plain text that can be encrypted is limited to the size of n=p*q. "Each time RSA initialization process requires the random selection of two very large prime numbers (p and q).

*Advantages of RSA Algorithm*

" it uses Public Key encryption which means that the text will be encrypted with someone's Public Key (which everyone knows about) but only the person intended for can read it, by using their private key (which only they know about). " Use of public key in RSA provides digital signatures that cannot be repudiated. "Ciphering & deciphering algorithm are same [2].

## III. DIFFIE – HELLMAN ALGORITHM

Whitfield Diffie and Martin Hellman discovered what is now known as the Diffie-Hellman (DH) algorithm in 1976. It is an amazing and ubiquitous algorithm found in many secure Connectivity protocols on the Internet [8, 1]. In an era when the lifetime of "old" technology can sometimes be measured in months, this algorithm is now celebrating its 25th anniversary while it is still playing an active role in important Internet protocols. DH is a method for securely exchanging a shared secret between two parties A and B over a public network and each holding public/private key to agree on a shared secret value. This shared secret is important between two parties who may not have ever communicated previously, so that they can encrypt their communications. As such, it is used by several protocols, including Secure Sockets Layer (SSL), Secure Shell (SSH), and Internet Protocol Security (IPsec). These protocols will be discussed in terms of the technical use of the DH algorithm and the status of the protocol standards established or still being defined. Diffie–Hellman establishes a shared secret key that can be used for secret communications by is called the base. 2. Picks a secret number "A" as first secret number = A, then picks another secret number "B" as second secret number = B. 3. Computes first public number X = GA mod P, and public number = X. Then computes second public number Y = GB mod P, and public number = Y. 4. Exchange their public numbers. 5. First knows P, G, A, X, Y, Second knows P, G, B, X, Y. 6. Computes First session key as KA = YA mod P OR KA = (GB mod P) A mod P OR KA = (GB) A mod P OR KA = GBA mod P. 7. Computes second session key as KB = XB mod P OR KB = (GA mod P) B mod P OR KB = (GA) B mod P OR KB = GAB mod P. 8. Fortunately for Both by the laws of algebra, First session key "KA" is the same as Second session key "KB", or KA = KB = K. 9. Know we have both the secret value as "K" [1].

*Advantages Of Diffie Hellmen Algorithm*

• No known successful attack strategies until now, so it is secure.
• Diffie-Hellman protocol generates a "shared secret"- an identical cryptographic key shared by each side of the communication.

*Problems in Diffie Hellmen Algorithm*

It is easily susceptible to man-in-the-middle attacks.
The algorithm cannot be used to encrypt messages.
There is also a lack of authentication.
The computational nature of the algorithm could be used in a denial-of-service attack very easily [1].

## IV. HYBRID ALGORITHM

RSA algorithm is used as Public key cryptography method. It is widely used in Electronic commerce protocol .It has a public key and private–key. Public key is known to everyone and used for encryption and Private Key is used for decryption. The RSA algorithm can be used for both public key encryption and digital signatures. It is based on the theory of Prime Numbers. Its security is based on the difficulty of factoring large integers. The amount of time it takes to factor a number of x bits is asymptotically the same as the time it takes to solve a discrete log over a field of size x bits. It is the world's most popular Asymmetric Key Encryption algorithm. Diffie Hellman algorithm is used as key exchange method that allows two parties that have no prior knowledge to each other to jointly share a secret key. DH is a method for securely exchanging a shared secret between two parties, in real-time, over an untrusted network. In our paper we use both RSA and Diffie- Hellman for providing more security.
Steps of this algorithm are as
1. Choose two large prime numbers P and Q.
a. Calculate N = P x Q.
b. Select public key (i.e. encryption key) E such that it is not a factor of (P – 1) and (Q -1).
c. Select the private key (i.e. the decryption key) D such that the following equation is true (D x E) mod (P – 1) x (Q – 1) = 1
d. Suppose R, S and G is automatic generated prime constants.
e. And put the value of E and D from above as secret number such that A=E and B=D.
2. Now calculate following as public number
X= GA mod R
Y= GB mod R
3. Calculate session key with formula

KA = YA mod R or KA = (GB mod R) A mod R or KA = (GB) A mod R or KA = GBA mod P.
KB = XB mod R or KB = (GA mod R) B mod R or KB = (GA) B mod R or KB = GAB mod R. Such that KA = KB = K.
4. For Encryption we use session key K with Plain text PT that will generate a new Cipher text CT. Then send CT as the cipher text to the receiver and for decryption, calculate the plain text PT from the cipher text CT. Firstly to use RSA each user must (privately) choose two large random numbers P and Q to create his own encryption and decryption keys. These numbers must be large so that it is not computationally feasible for anyone to factor N = P*Q. Next step (b & c) is to generate E and D. After this we put E and D as inputs A and B to Diffie- Hellman and compute XA and XB , through which we generate session key KA and KB such that KA = KB = K. Then we XOR our input Plain text with the session key (K) for Encryption or to produce Cipher text and for Decryption again XOR Cipher text with session key (K) to produce original Plain text.

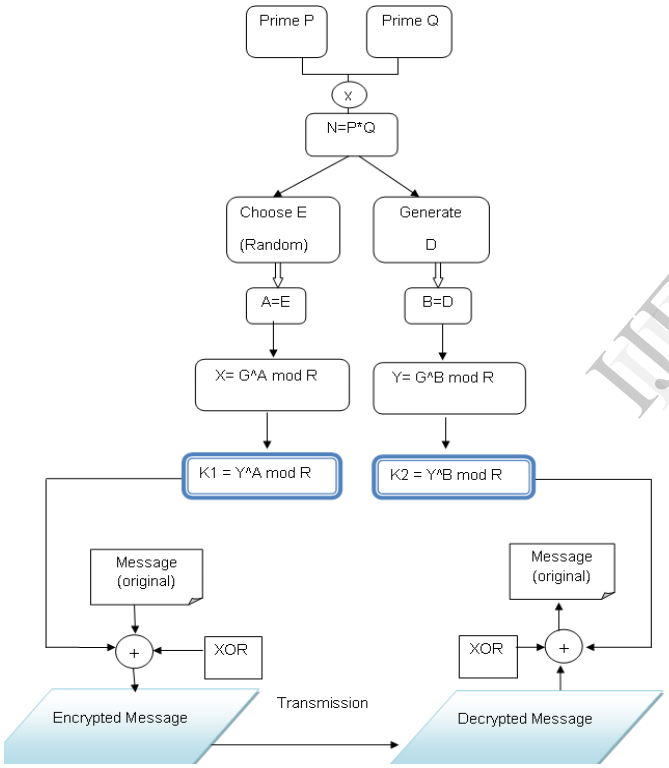



Fig. 1: Hybrid RSA Diffie-Hellman.

## V. Portal Flow.

University Paper Setter web portal, as mentioned above operates on client-server basis. It is divided mainly in three users Super Admin, admin and Teachers. Teachers first of all make registration university web portal by signing up with their information. Admin at university will verify that information, generate username and password for respective teacher and inform teachers with system generated email.

In the next step, Super admin will announce examination. Admin will set up a paper call, and respective teacher will receive a notification on his profile.

Next, Teacher will upload the question paper. System will calculate cipher text, and then put a digital signature for user authentication. This digitally signed data will be sent to the admin. Now, admin will calculate the digital signature message digest value and confirm the identity of teacher. Then he will enable the question paper for decryption process. After enabling the data for decryption process super admin will only decrypt the question paper to its plain text format and finalize it for printing process or else he will discard the paper and set up a recall in case of any mistakes in the question paper

## VI. Algorithm Implementation.

Above explained algorithm is used to encrypt the question papers. As the question paper's confidentiality is an important issue to be considered before conduction of the examination. Paper setter portal here accepts the paper from respective subject expert faculty and store it in an encrypted format. Session key K with Plain text PT will generate a Cipher text CT. Then CT is sent as the cipher text to the receiver admin and for decryption, PT is obtained from CT with key K.

Algorithm is implemented in JAVA. First we define three big numbers R, S, G as static final integers which will be constant through algorithm. Then an 'Array List<Long> list' is defined to store large prime numbers generated. Another class file 'Keys Generator' will generate a session key choosing from letters, numbers and special characters. All these are defined in an alphanumeric 'static final' string. For choosing a random character we use 'Math.random()' function which will return any value from 0.1 to 1.

Now once the Session key is generated we calculate Encryption key K using formulas given in the algorithm and XOR it with the plain text to obtain cipher and again XOR the cipher do decipher it to original plain text.

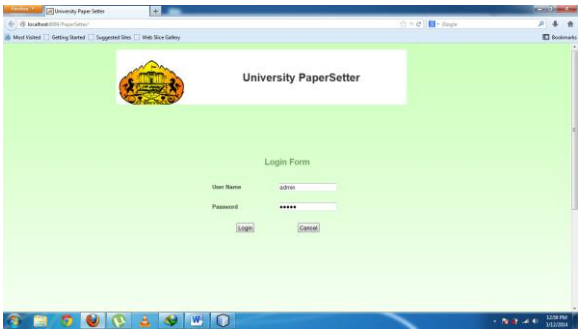
## VII. Digital Signature Calculation.

A digital signature is an electronically generated unique signature that will identify the user using it. Idea behind digital signature is a private key encryption concept. When a data is encrypted with a private key, any user can decrypt the data using first user's public key. This does not ensure data integrity but does ensure an identity of user who is encrypting it. Because when cipher is deciphered using a public key it confirms the private as an encryption key.

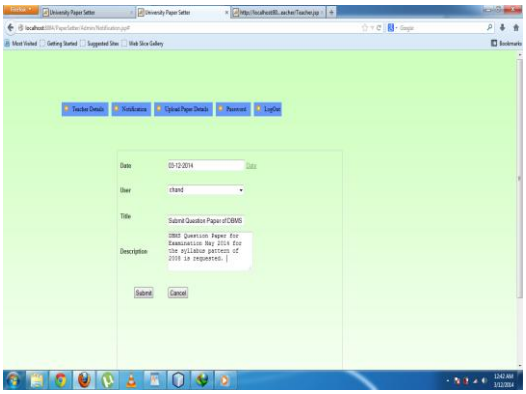
When the question paper is encrypted to cipher text, cipher text is given to a message digest algorithm to calculate a message digest value. This value is encrypted with private key of Teacher. Data is sent to Admin. Admin calculates the Message digest value by decrypting digital signature to message digest value and confirm the identity of Teacher [1].

## VIII. RESULTS.

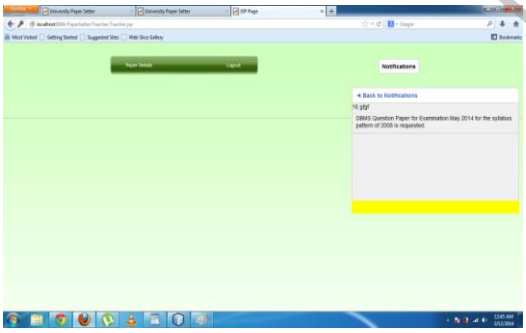
1. Login



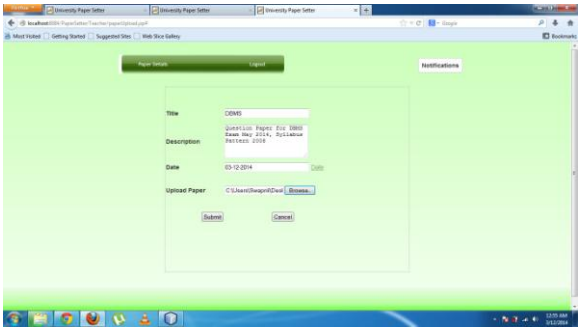

2. Generate notification.



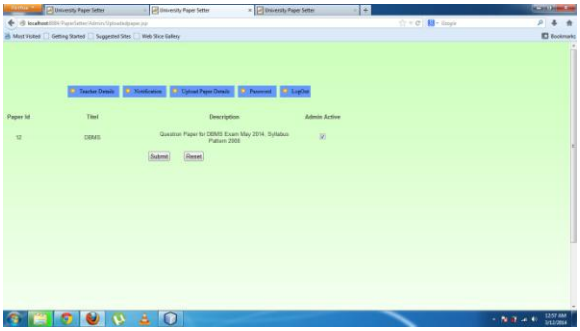
3. Receive notification.



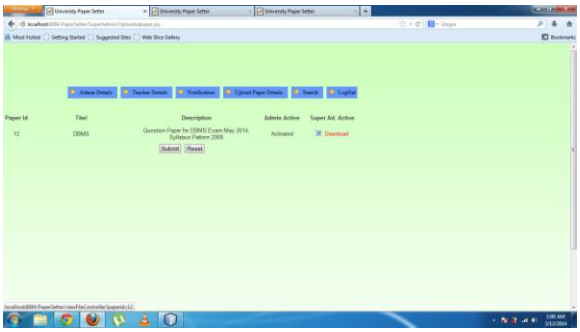
4. Upload Paper.



5. Admin active.



6. Super Admin Download.



## IX. REFERENCES

[1] Vishal Garg, Rishu, Improved Diffie e-Hellman Algorithm for Network Security Enhancement, J. Computer Technology & Applications, Vol 3 (4), 1327-1331

[2] William Stallings, Cryptography and Network Security Principles and Practice, fifthEdition Pearson publication.

[3] Atul Kahate, Cryptography and Network Security, fourth Edition, Tata McGraw-Hill.

[4] Emmanual Bresson, Dynamic group Diffi-hellman key exchange under standardassumption, Preceedings of EUROCRYPT, LNSC 2332, page no. 321-336, 2002

[5] A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman by Shilpi Gupta andJaya Sharma Department of Computer Science & Engineering Amity School of Engineering & Technology, Amity University, India . 978-1-4673-1344-5/12/$31.00 ©2012 IEEE