3rd International Conference on Recent Innovations in Science Engineering and Management
Sri Venkateswara College of Engineering and Technology,Srikakulam,Andhra Pradesh (ICRISEM-16)
27 February 2016, www.conferenceworld.in ISBN: 978-81-932074-1-3

ENCRYPTED EXAMINATION PAPER DISTRIBUTION SYSTEM FOR PREVENTING PAPER LEAKAGE

K Sujatha[1], P V Nageswara Rao[2], A Arjuna Rao[3], Ch Kusumanjali[4], T Manasa[5]

[1,2]CSE Department, GITAM University, Visakhapatnam, (India)

[3]Professor & Director, Miracle Educational Society Group of Institutions, Bhogapuram, Vizianagram, (India)

[4,5]B.Tech. Student, CSE Department, Miracle Educational Society Group of Institutions Bhogapuram, Vizianagram, (India)

ABSTRACT

An examination is an assessment intended to measure a test-taker's knowledge, skill, aptitude, fitness, or classification in distinguished areas. However many times news on question paper leakages are always sensational and sometimes even leakage is unknown to exam board. This leads to postponement or cancellation of exams which inturn has huge economic loss and psychological depression on students. Many times question papers leakage information will not be known to the universities itself. The use of strong encryption algorithms may solve the problem of securing files but they are time consuming both in encrypting and communicating the files. The Encrypted Examination Paper Distribution System involves distribution of paper by providing both authenticity and encryption. This uses the combination of two algorithms Digital Signature Algorithm for authentication and key generation and Blowfish Algorithm for encryption. This provides integrity, reliability, security with less computation power and high encryption speed.

Keywords : Question Paper leakages, Encrypted Examination Paper Distribution System(EEPDS), Authenticity, Encryption, Digital Signature Algorithm, Blowfish Algorithm

I. INTRODUCTION

Compared to other developing countries the percentage of literate people is very low in the country where we live, after obtaining a degree/certificate a large number of our dreams are getting a good job. This permits the undertaking of immoral and illegal ways to obtain the degree to ourselves. That is why the corrupt associations are able to take asset, by conducting their vested passion in leaking out question paper.

So, strict measures must be taken to stop this interruption by conducting cumulative operations from both private and government sectors. The operation must be started from grass root level, so that these insufferable activities can be stopped. Only then we can think of our present generation to be future leaders of the country. So for secure file storage and transfer we are using encryption.

ISBN: 978-81-932074-1-3

However the use of algorithms may solve the problem of securing a file properly in storage and in transit. The use of encryption algorithms itself does not imply complete security and confidence. There will always be some adjustments between security and usability. This will usually be resolute by user desires and risks. The main necessity for the management of keys used with public key algorithms is, the private key remains secret, the reliability of the public key is assured and that their use is controlled.

The manual paper distribution mechanism system is as shown in figure 1.

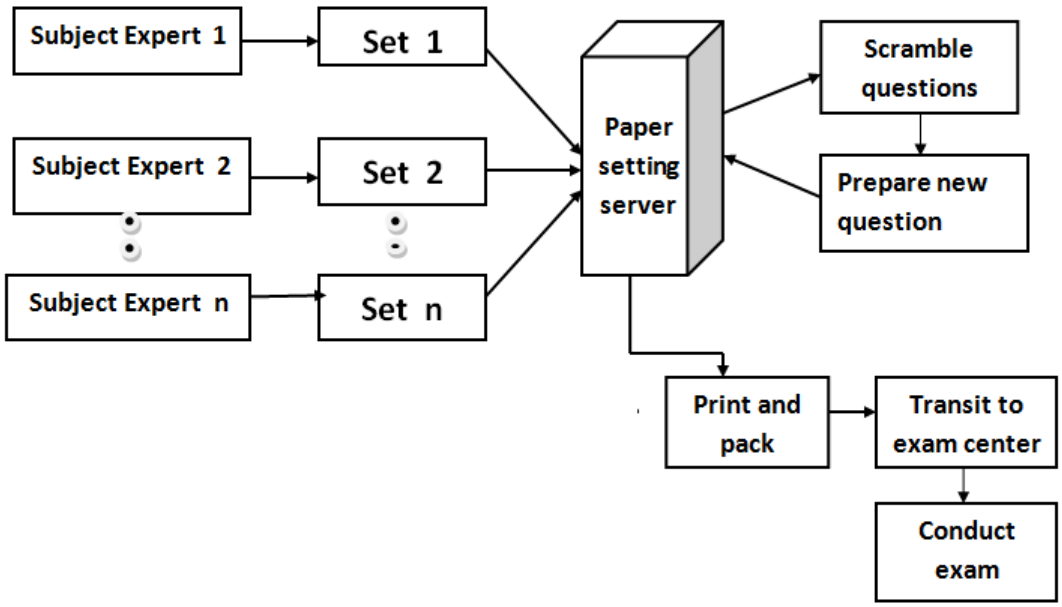

Figure.1 Architecture of exisiting voting system

There are many issues in this system as listed.

(a) This system is not economical

(b) Total system has many loop holes where paper leakage can happen at any stage.

(c) Reliability and security are major concern

(d) Examination Re-conduction is too expensive as this has to be done at no extra cost

(e) Well prepared Students enter into depression

(e) Paper leakage is difficult to be traced even in case it happens.

They are many side effects arising from these issues. Students are passing exams without studying and getting good results, where really talented students are facing real hardship which means a direct form of discrimination. Then they are getting jobs in important sectors, where there is a need for qualified personnel. Then they are getting jobs in sectors where there is a need for capable personnel. In calculation of human progression education plays a vital role and it is the backbone of a nation.

To lead the country towards successful educated people has a crucial performance. But when ones qualification is attained through illegal means, the total development process will be unskilled automatically. Due to this immoral way of getting a degree, the improficient work force in job sector may corrupt their jobs and willing to restore to any measure for their self-interest.

II ENCRYPTED EXAMINATION PAPER DISTRIBUTION SYSTEM (EEPDS)

2.1 Digital Signature Algorithm (DSA)

DSA is proposed by in August 1991 for digital signatures to employ in their Digital Signature Standard. The DSA can be used in situations wherever a digital signature is required and user authentication is required. This employs public key cryptography with two keys, private and public keys. The signature generation method uses private key and also signature verification method uses the public key's [1].

For signature generation and verification, the data that is taken as a message, M, is utilizes the Secure Hash algorithmic rule (SHA). However, by mistreatment the signatory's public key, anyone will verify a properly signed message [2]. Here, the generation of a new stored modulus is not done every time. The public key is has two parts where the first part is the public key (y) and next is the modulus data (p, q, and g). where modulus size is in between 512 and 2048 bits with 64 bits increment. [3].

DSA requires a means of associating public and private key pairs to the corresponding users. That is, there should be a binding of a user's identity and therefore the user's public key. This binding could also be certified by a reciprocally trustworthy party, for instance, a certifying authority might sign credentials containing a user's public key and identity to make a certificate. DSA is secured because of the difficulty of computing the discrete log. The purpose is to find the smallest natural number x as shown in equation (1), after choosing a prime p and α and β that are nonnegative integers mod p, t.

$$\beta \equiv \alpha x \pmod{p}. \qquad -(1)$$

The x is the number indicated by Lα(β), the discrete log of β with respect to α. Generally, α is considered to be a primitive root mod p. Also α is a primitive root mod p if and only if $\{i \bmod p \mid 0 \le i \le p-2\} = \{1, 2, \ldots, p-1\}$ [4].

2.1.1 DSA Advantages

1. Public Key Encryption requires no secret key communication.
2. Highly secured
3. Used in User Authentication

2.2 Blowfish Algorithm

In all security algorithms , Blowfish algorithm place a vital role in securing the data in storing and transferring. Bruce Scheier designed this algorithm in 1993 as alternative to existing encryption algorithm such as AES, DES. This is fast as it encrypts the data at a rate of 26 clock cycles per byte on large 32 bit micro processor. It is compact as it can run 5k of memory[5].

This uses addition, XOR look up tables with 32 bit operands. Blowfish is symmetric block cipher algorithm encrypts block data of 64 data at a time. This will follow feistel network and this algorithm is divided into two parts, Key Expansion and Data Encryption[6].

2.2.1 Key Expansion

It will convert a key of at most 448 bits into several sub key arrays totaling 4168 bytes. In general the key length is the range of 32 to 448 bits by default we are using 128 bit key length. These keys are generated to any encryption or decryption of data. The p array contain 18, 32 bit sub keys P1,P2,…P18. This contains four 32 S-boxes of 256 entries[7] :

S1,0, S1,1.....S1,255

S2,0, S2,1.....S2,255

S3,0, S3,1.....S3,255

S4,0, S4,1.....S4,255

By using blowfish algorithm the sub keys are calculated :

1.With a fixed string, initialize the P-array and the four S-boxes with a fixed string. String consists of the hexadecimal digits of pi(less the initial 3)

2. up to P14,XOR P1 with the first 32 bits of the key, XOR P2 with the second 32 bits of the key and so on repeated loop through the key bits until the entire P-array has been XORed.

3. using the sub keys described in step (1)and(2), encrypt all-zero string with the blowfish algorithm.

4. with the output of step(3) replace P1 and P2.

5. By using modified sub keys encrypt the output of step (3) using blowfish algorithm.

6. Replace P3 and P4 with the output of step (5).

7.Continuing this process replace all the entries of the P-array and then order all the four S-boxes with outputs of continuously changing the blowfish algorithm.

To generate all required subkeys 512 iterations are required in total. Rather than execute this derivation process multiple times applications can store the subkeys.

2.2.2 Data Encryption

Blowfish is a feistel network consisting of 16 rounds[8,9]. The inputs is a 64-bit data element, and the algorithm is as follows.

Algorithm : Blowfish encryption

Step 1 : Divide a into two 32-bit halves: aL,aR

Step 2 : For i=1to16:

Step 3 : aL=aL XOR Pi

Step 4 : xR=F(XL) XOR xR

Step 5 : Swap aL and aR

Step 6 : Swap aL and aR(undo the last swap)

Step 7 : aR=aR XOR P17

Step 8 : aL=aL XOR P18

Step 9 : Recombine aL and aR

The function F is as follows:

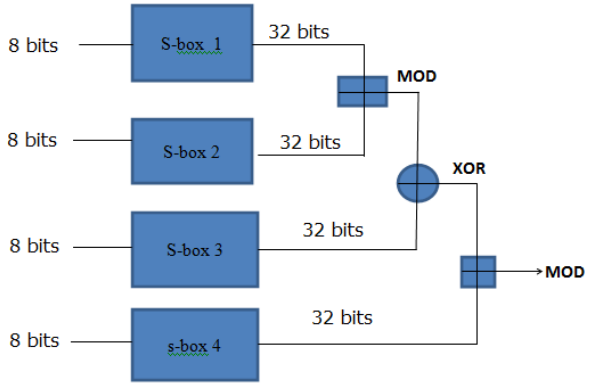

Figure.2 Architecture of exisiting voting system

2.2.3 Advantages of blowfish

1. Encryption Speed
2. Easy to Implement
3. Works on large amounts of Data

2.3 EEPDS

Here the user who can be the Subject Expert, Question Paper Setter, Exam coordinator, Examiners are all authenticated by using DSA. Then they are given the chance to accept the question paper. Then encryption or decryption is done by using blowfish algorithm. Though Blowfish is a symmetric algorithm, this is totally secure if key is transmitted securely. This can be generated by DSA and then transmitted using emails. Symmetric algorithms are fast compared to public key cryptographic encryption algorithms like RSA. Hence we are using Blowfish for encryption.

However symmetric algorithms do not provide Authentication. As this is one time process DSA is used for generating and verifying Signatures.

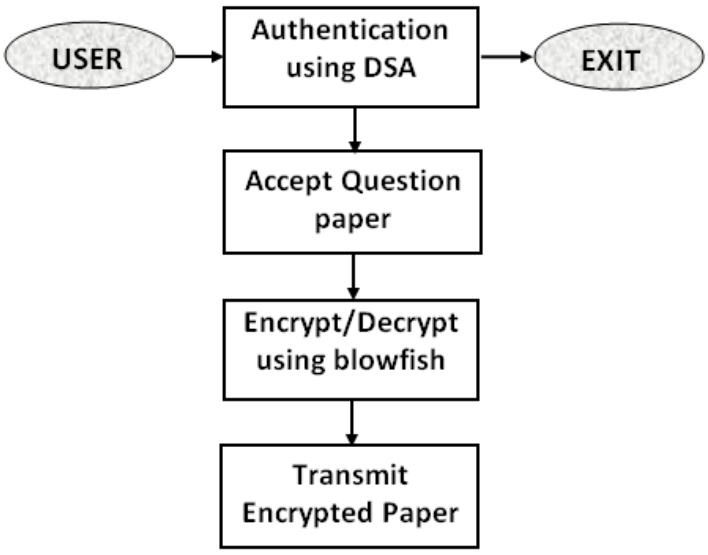

Figure.3 EEPDS Structural Diagram

The advantages of this system are

1. Provides user Authentication
2. Encryption is secure with blowfish algorithm
3. Exam Paper leakage is controlled at every stage

III RESULTS AND DISCUSSION

By implementing this EEPDS system, the examination process can be smoothened and secured. However this requires that the private key of DSA to be kept secured with user. The secret key must also be transmitted securely. The Blowfish algorithm is symmetric algorithm but provides equal security if the key is kept secure.

ISBN: 978-81-932074-1-3

However this takes comparatively less time and hence is preferable in encrypting huge amounts of data such as in examination system. Table 1 shows the comparative analysis of Blowfish with RSA.

Table 1 : Comparative Analysis Blowfish and RSA

Test Rounds	Size (KB)	Encryption/Decryption Time(ms)	
		Blowfish	RSA
1	100	40	202
2	250	66	370
3	65	34	155
4	780	180	600
5	356	93	409
6	30	22	102

Hence at times blowfish can be used with hybrid combination of DSA for increasing encryption speed where there is large amount of data to be encrypted.

IV. CONCLUSION

In any public examination, the question paper leakage has became a common phenomenon. Through their political and economic connections a group of people manage to leak these questions. Day by day this immoral practice is spreading out in to the society. Students are cheating themselves as well as the nation, who are passing their exams by help of leaked question papers. So this system solves all the issues arising from the leakage of the paper and provides tight security which is unbreakable.

V. ACKNOWLEDGEMENT

The authors would like to thank Prasad V Lokam, CEO of Miracle Software Systems for his encouragement and suggestions on working with advanced technologies. Useful discussions with Computer Science Faculty of Miracle Group on the present subject are gratefully acknowledged.

REFERENCES

[1] "Digital Signature Standard", NIST, U. S. Department of Commerce, FIPS PUB 186, May 1994.

[2] Ronald L. Rivest, "On NIST's Proposed Digital Signature Standard",ASIACRYPT '91, Proceedings of the International Conference on the Theory and Applications of Cryptology: Advances in Cryptology, pp 481-484, Lecture Notes in Computer Science, Springer-Verlag

[3] Kitsos P, Sklavos N., Koufopavlou O.," An efficient implementation of the digital signature algorithm", Electronics, Circuits and Systems, 2002. 9th International Conference, Vol 3, 2002 , pp 1151 – 1154, IEEE

ISBN: 978-81-932074-1-3

[4] Gilani J, Mir A.A.,"Using Digital Signature Standard Algorithm to Incorporate Non-invertibility in Private Digital Watermarking Techniques", Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing, 2009. SNPD '09. 10th ACIS International Conference, 27-29 May 2009, pp 399 – 404, IEEE.

[5] Bruce Schneier, "The Blowfish encryption algorithm", Dr. Dobb's Journal of Software Tools, 19(4), p. 38, 40, 98, 99, April 1994

[6] Tingyuan Nie, Teng Zhang, "A study of DES and Blowfish encryption algorithm", TENCON 2009 - 2009 IEEE Region 10 Conference, Jan. 2009, pp 1 – 4, IEEE

[7] Alabaichi, A. , Ahmad, F. ; Mahmod, R, "Security analysis of blowfish algorithm", Informatics and Applications (ICIA),2013 Second International Conference, Sept. 2013, pp 12 – 18, IEEE

[8] Meyers, R.K, Desoky, A.H., "An Implementation of the Blowfish Cryptosystem ", Signal Processing and Information Technology, 2008. ISSPIT 2008. IEEE International Symposium , Dec. 2008, pp 346 – 351, IEEE

[9] Mousa, A. , "Data encryption performance based on Blowfish", ELMAR, 2005. 47th International Symposium, June 2005, pp 131 – 134, IEEE