Journal of Information Engineering and Applications www.iiste.org
ISSN 2224-5782 (print) ISSN 2225-0506 (online) DOI: 10.7176/JIEA
Vol.9, No.4, 2019

CryptoQuestion: The Solution of Question Leakage

Rejwana Haque
Computer Science and Engineering, Bangladesh University of Business and Technology, Dhaka, Bangladesh

Abstract
Question paper leakage is a severe problem, particularly in academic education. In Bangladesh, the catastrophe of question papers leak has taken an epidemic turn in recent few years. The tendency of question leakage is on the rise even after, a number of steps have been taken by the concerned authorities. Some solution has been proposed regarding the preventing of question leakage, but they do not address the confidentiality of question while storing in the server. In the research, we introduce a cryptography-based system for forming, warehousing and distributing question papers. As the proposed model requires no action for printing question and does not store the question undeviatingly, it supports full confidentiality of question paper in public examination. Theoretically the proposed system proves the ability to maintain confidentiality of question paper and to prevent question leakage.
Keywords: CryptoQuestion, Question Bank, Set Protocol, Question Combo.
DOI: 10.7176/JIEA/9-4-03
Publication date:June 30th 2019

1. Introduction

The phenomenon of circulation of question paper before examination is defined as question leakage. Question paper leakage has become a regular phenomenon in public examinations in recent years. It has placed the credibility and quality of exams, and reliability of the results under a question mark. Every time any public examination is held, there is allegation of question paper leakage. The leaked questions become available to many of the examinees through Facebook, WhatsApp and some other social media. Students become busy searching for the question rather than study. Leakage of the question of secondary school certificate and higher secondary certificate has become very common in recent years. Even the question of PSC, JSC and university admission exam is being leaked. According to a report (Transparency International Bangladesh [TIB], 2015), in 63 examinations between 2012 and 2015 the questions were leaked, of which all of PECE and JSC examination questions 2013 and 2014 were leaked.

A worldwide popular theory of the imperialists is – destroy the education system of a nation if you want to destroy them. Question paper leakage is one of the most impendent reasons for destroying the education system of our country. The social impact of question paper leakage is extremely alarming for the next generation. If students at such a tender age as class five get involved in a crime like passing with the help of leaked question papers and see that such crime can go unpunished, an attitude of callousness towards the law will develop in them. They will be encouraged to engage in criminal activities, rather than intellectual practice. Consequently, the nation will get a socially, culturally, morally and intellectually degraded future generation.

1.1 Reasons of Question Leak

There are various distinct steps now followed in the question preparation process. These include initial drafting of questions, reviewing the content and quality of the questions, selecting acceptable versions, choosing a final version out of two approved sets by lottery, printing the one final set, distribution of the question papers and storing them securely all over the country. On the examination day, the papers are transported to the centers and finally handed to the examinees in the examination halls (Ahmed, 2018).

The ministry of education has enlisted six reasons for leaking questions (Ittefaq, 2018). (i) The questions of public exams are printed in BJ press. Some dishonest officer and staff of the press may be involved in leaking question. ii) The Executive magistrate is responsible for distributing the question to the exam hall. But there is a shortage of people for this distribution. This creates a scope for question leak. iii) The distance of exam venues from the center is quite long. That's why the secretary of the center has to open the question 30 minutes before starting the exam. This creates an opportunity for the corrupted people to leak question. iv) It is very difficult to control the smartphone of the examinee and the staff involved in taking the exams. For some of those officers and staff, the question is leaked in social media. v) There is a shortage of skilled human resource for monitoring the Internet and finding those who are involved in this. The people responsible for the security should enhance their activity some days before the exam. vi) There is no strict rule of Bangladesh Telecommunication Regulatory Commission (BTRC) to control the users of social media. That's why it becomes very difficult to find out the people involved in leaking questions in social media.

1.2 Initiatives Taken

The government has taken some steps to stop question leaking. They make many sets of the question, print those

with great privacy. But still, questions are leaking. The ministry of education has set some hard rules which should be followed during exam including students must appear in the exam hall before 30 minutes of starting time. They slow down the internet for some particular hour before the exam. They also find the people who are involved in leaking question and handover them to police. Though the government is very concerned and maintaining zero tolerance in question leaking, it is still unstoppable.

1.3 Some Other Solutions

A number of scholars have proposed a number of solutions for the catastrophe of question leak. Using multiple sets of question papers for the same subject (Ahmed, 2018), non-printed question by displaying on the projector in the examination hall or giving tab to the students in the examination hall are some of the proposed solutions. All of the solutions address the leaking of printed questions but if the softcopy of a question leaks the proposed solutions cannot ensure the security and confidentiality of the question paper. Another solution for question leakage is Question Setter Software (Ahmed, 2017), that prepares the question from the database five minutes before the examination starts. But this needs a fast printer for printing the questions. Also, there is a probability of questions not to be uniformly distributed according to the syllabus.

1.4 Proposed Solution

The adverse impact of question leakage on society leads to the need for protection of question paper in public examinations for protecting the next generation to destroy. So maintaining the confidentiality of question paper is most important to guard the education system to be corrupted. To maintain the confidentiality of question paper we propose a cryptography-based system, CryptoQuestion forming, saving and broadcasting question paper in public examinations.

In the First chapter we have mentioned some reasons of question paper leakage followed by initiatives taken by the government so far. Next chapter we will describe some hugely used Cryptographic techniques. In the last chapter we have focused on a few new terms of our proposed solution following the methodology of the proposed system with a suggestion of an encryption algorithm that can be used in CryptoQuestion. Than we evaluated the system theoretically in terms of maintaining the confidentiality of question paper. Finally we took a look to the infrastructural challenges for implementing the proposed system followed by the conclusions and future work of our research.

2. Cryptography

Cryptography is a science of mathematically writing in secret codes to maintain privacy and authentication. It encodes data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format to the authorized user. It ensures various data security such as confidentiality, integrity, authentication. The term is most often associated with encryption (scrambling plaintext into cipher text) and decryption (back to plaintext again). Generally, three types of schemas are used in cryptography:

I. Secret Key cryptography
II. Public Key cryptography
III. Hash Function

2.1 Secret Key Cryptography

In symmetric cryptography both sender and receiver share the same secret key and same encryption algorithm. As a single key is used in both encryption and decryption process the schema is called also symmetric cryptography. Its schema is generally categorized in two categories: stream ciphers and block ciphers.

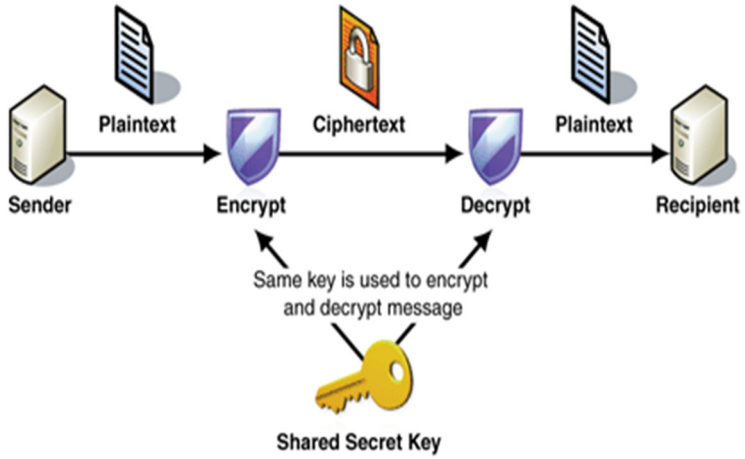

Fig 1: Secret Key Cryptography

Some common symmetric encryption algorithms used today include:

Data Encryption Standard (DES): DES (Davis,1978) is a block cipher algorithm having a block size 64bit and key size 56bits. It takes a fixed length string and transforms it to a fixed length ciphertext after a series of rounds. Triple DES is an enhancement of DES where the block size is the same as DES but key size is 192 bits. DES encrypts 32 bits in one round.

Advanced Encryption Standard (AES): The AES(Daemen & Rijmen,2001) is also a 128 bits block chipher which was designed to substitute DES in commercial uses. Here the key size may differ either 128 bits, 192 bits or 256 bits. The number of iteration depends upon the key length. AES encrypts 128 bits in one iteration.

Blowfish: The Blowfish is another block chipher used as a substitute for the DES algorithm. It is a 16 round Feisal cipher technique in which the key length may vary from 32 to 448 bits. It is optimized for 32 bit processors.

Twofish: (Schneier, 2005) A 128-bit block cipher using 128-bit, 192-bit, or 256-bit keys. Designed to be highly secure and highly flexible. The notable features of the algorithm are the use of pre-computed key-dependent S-boxes and a relatively complex key schedule.

2.2 Public Key Cryptography

In public key cryptography, different keys, one public key and one privet key are used for encryption and decryption process. As two different keys are used for encryption and decryption this is also called asymmetric encryption. Although these keys are mathematically related but knowledge of one key does not allow determining the other key easily. It can be used for confidentiality and authentication.

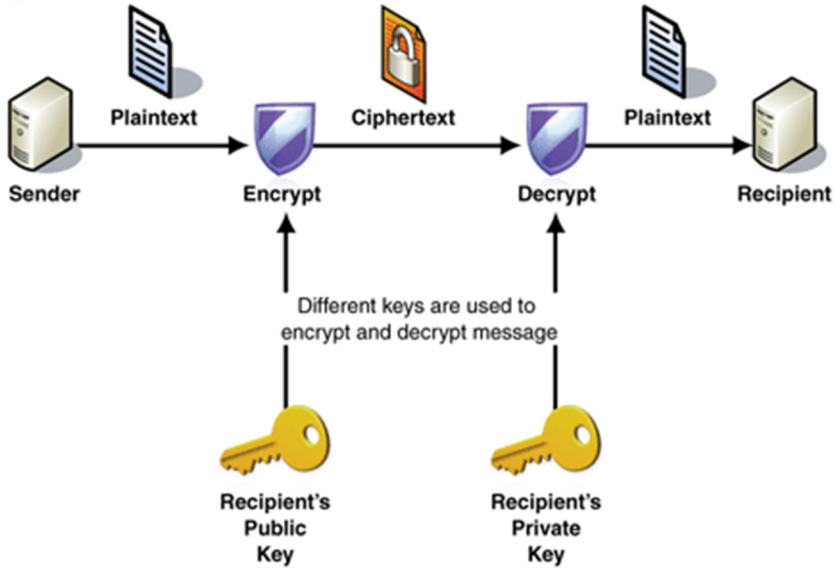

Fig 2: Public Key Cryptography

2.2.1 RSA Algorithm

The first, and still prevalent, public key cryptography is RSA (Rivest, Shamir et.al , 1978) algorithm. It is suitable for both confidentiality and authentication. RSA named after the developers of the algorithm three mathematicians Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA uses a variable size massage block and variable size key.

RSA works in three stages: Key Generation, Encryption and Decryption. Padding is used in RSA to avoid attacks. For a padded massage M<n the RSA algorithm works as follows:

Key Generation:

The algorithm for public privet key pair generation is as follows:

1) Select p, q such that p and q both are prime, $p \neq q$
2) Calculate $n = p * q$
3) Calculate $f(n) = (p - 1)(q - 1)$
4) Select integer e such that $\gcd(f(n), e) = 1; 1 < e < f(n)$
5) Calculate d such that $d \equiv e^{-1} \pmod{f(n)}$
6) Public key $PU_k = (e, n)$
7) Private key $PR_k = (d, n)$

Encryption:

The sender encrypts message M with the public key of the receiver.

Cipher Text C is calculated as:

$C = M^e \bmod n$

Decryption:

The receiver encrypts message M with the privet key of the receiver.

Plain Text M is calculated as:

$M = C^d \bmod n$

2.2.2 Optimal Asymmetric Encryption Padding (OAEP)

To avoid attacks in RSA, practical implementation of RSA algorithm embed Optimal Asymmetric Encryption Padding (OAEP) into the value of M before encrypt it. For a massage m and n bit block for RSA module the OAEP is encoded as:

$m' = \text{OAEP}(m) = X||Y = (m00..0 \oplus G(r))||(r \oplus H(X))$

Here,

k_1 = number of 0's padded with m

r = randomly generated k_0-bit string

k_0 and k_1 are set by the protocol

m is the plaintext message, an $(n - k_0 - k_1)$-bit string

G and H are cryptographic hash functions

To decode,

1. Recover the random string as $r = Y \oplus H(X)$
2. Recover the message as $m00..0 = X \oplus G(r)$

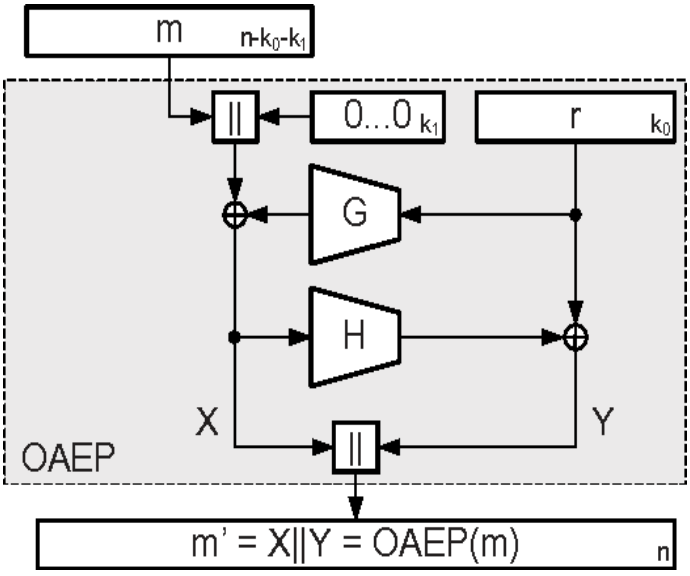

Fig 3: Optimal Asymmetric Encryption Padding

2.2.3 Diffie-Hellman Key Exchange

A simple public-key algorithm used for secret-key key exchange only, not for authentication. The protocol is secure only if the authenticity of the two participants can be established (Kumar, 2015). The algorithm is as follow:

1) Select two Global Public Elements: a prime number p and an integer α that is a primitive root of p.
2) Sender Key Generation: Sender selects a random integer $X_A < p$ which is private and computes $Y_A = \alpha X_A \bmod$

p, which is public.
3) Receiver Key Generation: Receiver selects a random integer $X_B < p$ which is private and computes $Y_B = \alpha X_B \mod p$, which is public.
4) The Sender calculates the secret key: $K = (Y_B) X_A \mod p$
5) The receiver calculates the secret key which is identical to the sender secret key. $K = (Y_A) X_B \mod p$.

2.3 Hash Function
Hash Function is also called one-way encryption. A hash function H accepts a variable-length block of data M as input and produces a fixed-size hash value h =H(M) (Kumar, 2015). The principal objective of a hash function is to ensure data integrity. A change in any bit in the message changes the hash code with a very high probability.

3. CryptoQuestion

In this section, we propose a cryptography-based method of setting question paper and taking exams. As the country is becoming digital day by day, it won't be difficult to set and distribute questions digitally. We propose a digital question setting method. There will be large number of question sets for examination. All of the question set will be encoded and stored in the database. The final question will be set five munities before exam. At the time of examination final question will be decoded in a computer of each exam center and it will be displayed on projector in each hall. In the proposed method, we use high level encoding and decoding algorithms that ensure the safety from digital attack. On the other hand, only 1 question will be set from the question of each question setter. So, if the any question is leaked, there will be a minimum probability of being that question in final question paper. The proposed method can play a huge role in stopping question leak.

3.1 Terminologies
We introduce a number of steps for generation and circulation of a secured platform of question papers in public examination. In the following we try to formalize some definitions involved in different steps for generating and circulating the questions of each subjects.
Set Protocol: The question of each subject must cover certain portion of syllabus. The constraints must include:

- A well-defined and unambiguous syllabus of each subject.
- Marks distribution of the question set.
- Clear guideline for what part of the syllabus will be addressed in which section of the question.
- Set Number mapped to the part of whole syllabus.

We define the above constraints as *Set Protocol*, which may be revised by the Education Ministry every year.
Moderator: Question moderators are the intellects, who are involved in moderation of submitted question for maintaining the standard of a question. For each subject there will be at least more than *Q* moderators, where *Q* is the number of Set in a question. The moderators have their own *Moderator ID* assigned by the Education Boards. Each *Moderator ID* is password protected using Hash (Schneier, 2015) so that no one else can access the ID of the Moderators. Each moderator will set one question set following the *Set Protocol* of the subject. A Moderator can edit and save the question by logging in to his *Moderator ID* before submitting the question.
Locking: We refer to the term *Locking* as no more modification can be made to the question. When a moderator completes a question he Locks the question by submitting it so that no further modification is made on the question. After *Locking* the question the Moderator himself view the question created by him. The *Locking* phase is necessary for maintaining confidentiality of question paper from the Moderator end. The encryption process takes place at the time of *Locking*.
Question Bank: The encrypted questions submitted by all the moderators are stored in a database table named *Question Bank*. The *Question Bank* stores the following fields:

- *Moderator ID*: It denotes the ID of the questioner.
- Set Number: This field denotes the question number for which section of the *Set Protocol* a question is given.
- Marks of Each Question: It denotes the marks assigned for each question set.
- The Encrypted Question: It contains the encrypted question. Only this part of the *Question Bank* is encrypted.

The *Moderator ID* and Set Number can uniquely identify each row in the *Question Bank*.
Question Combo: A number of different question combinations can be generated from the *Question Bank*. The combinations of the questions from the *Question Bank* can define the *Question Combo*. For generating the *Question Combo* the following rules must be maintained:

- No two questions in one Combo are from same Moderator.
- No two questions in one Combo have the same question number.
- The number of question set in a Combo must be the same as the number of question set defined by the

Set Protocol.

From the above criteria if:

M= number of moderator

Q= number of question set there will be

The total number of *Combo* Q_C of a subject is calculated by:

$Q_C = {}^{M}C_Q * Q! = {}^{M}P_Q$

We say each of the ${}^{M}P_Q$ question papers a *Combo*. All the *Combo*s will be saved in a database table called *Question Combo*. An auto increment primary key starting from 1, will uniquely identify each *Combo*.

Exam Timestamp: The examination of each subject has a predefined schedule. The education minister and controller of examination can set and update the schedule respectively only by using *Authorized Key*. According to the examination schedule the *Exam Timestamp* is generated. It is the count of second from setting the examination schedule to the starting time of the examination. The *Exam Timestamp* is downward counting timestamp.

Unlocking Key: This is a confidential key of a center for authenticating their Center ID (given by the education board). Only the head of the center knows the *Unlocking Key* of the center.

3.2 Methodology

In this section, we present the proposed system *CryptoQuestion* for public examination, which is intended for the prevention of question leakage. Firstly the traditional practice for taking public examination requires to be reformed so that no lettered questions are used in the examination so that no hard copy or a portrayal of the question paper is leaked. For preventing the leakage of soft copy of the question from the storage of the authority, we propose public key cryptography RSA algorithm for encrypting question paper and Hash function Secured Hash Algorithm (SHA-1) for verification of an authorized account.

For confidentiality and authentication the following schemas have been proposed:

1) For confidentiality of question RSA algorithm is proposed.
2) For integrity of question RSA is also proposed as digital signature.
3) For authenticate a user account hash function is proposed.

3.2.1 Define Set Protocol

For each subject of a public examination first of all the syllabus of must be well defined. The education board has the responsibility of a well defined Set Protocol. The Set Protocol ensures there is no repetition of any question in the final question paper. Table 1 is an example of Set Protocol. Here the chapter/topic section contains the list of topics associated with the question number.

Table 1: Set Protocol Example

Set no	Subset no	Chapter/ Topics	Marks
1	a	Topic 1, Topic 2	5
	b	Topic 3, Topic 4	5
2	a	Topic 5, Topic 6	5
	b	Topic 7, Topic 8	5

3.2.2 Update Authorized key

Before the processing of a public examination starts, the Education Minister and the Controller of Examination have to set their *Authorized Key*. The algorithm of updating the *Authorized Key* is as follow:

Start
Step 1: Number of Attempt Count = 0;
Step 2: Enter previous *Authorized Key* AK_O;
Step 3: Compute the Hash Value of $AK_O = H(AK_O)$;
Step 4: Compare $H(AK_O)$ with stored H(AK);
Step 5: If ($H(AK_O) = H(AK)$)
{
Enter new *Authorized Key* AK_N;
Goto step 6;
}
Else {
If (Count++ = 3){
Send system generated random key AK_N through secured channel;
Go to step 6;
}
Goto step 2;
}
Step 6: $H(AK) = H(AK_N)$

End;
Automatic key generation for OAEP
The *Authorized* Key of education minister and exam controller are used generate k_0 and k_1 respectively. A cryptographic hash function generates k_0 and k_1 from the Authorized Keys.
$k_0 = H(AK_{EM})$ (1)
$k_1 = H(AK_{EC})$ (2)
Calculate number of bits in the RSA modulus
The number of bits in RSA module is calculated as:
$l = m+k_0+k_1$ (3)
Here,
m = number of bits of one character in the plaintext.
l = number of bits of one character after padding.
3.2.3 Key Generation
After calculating the module size for RSA algorithm, the public-privet key pair of education minister has to be generated following the RSA key generation phage.
Public key of Education minister PU_{EM}= (e, n)
Private key of Education minister PR_{EM}=(d, n)
This public-privet key pair is used for encryption of the questions. And also used to authenticate the displayed question in an exam center.
3.2.4 Set Exam Timestamp
Then the Education Minister will set the *Exam Timestamp* according to the examination routine. The Procedure to set Exam Timestamp is:
Let,
S = Total number of subjects
E= {e_1, e_2, …….. e_S} set of all subjects' examination
SC= Subject Code
$H(AK_{EM})$ = stored hash value of education minister's Authorized Key
$H(AK_{EC})$ = stored hash value of exam controller's Authorized Key
Set Exam Timestamp:
Step 1: Number of Attempt Count = 0;
Step 2: Enter Authorized Key AK_I
Step 3: Calculate hash value of education ministers Authorized Key $H(AK_I)$
Step 4: If $H(AK_{EM})= H(AK_I)${
For i=1 to S{
Enter Exam Schedule $S(E_i)$
Calculate Exam Timestamp $Ts(E_i) = (S(E_i) – Present Time)$ seconds
}
Goto End;
}
Else{
If Count++= 3
Notify Education Minister

Goto step 2;
}
End;
If the examination schedule is changed for some reason the controller of examination can update the update the *Exam Timestamp*. The update operation of an *Exam Timestamp* is as follows:
Update Exam Timestamp:
Step 1: Number of Attempt Count = 0;
Step 2: Enter Authorized Key AK_I
Step 3: Calculate hash value of education ministers Authorized Key $H(AK_I)$
Step 4: If $H(AK_{EC})= H(AK_I)${
Enter Subject Code SC_E
For i=1 to S{
If $SC_E = SC_i$
Enter Exam Schedule $S(E_i)$
Calculate Exam Timestamp $Ts(E_i) = (S(E_i) – Present Time)$ seconds
}

Goto step 5;
}
Else{
If Count+1= 3
Notify Exam Controller;
Goto step 2;
}
Step 6: Notify Education Minister;
End;

If an unauthorized user is trying to set or update exam time the controller and education minister will be notified. To accomplish this the 'Count' variable is used. Notification about updated routine to the education minister is needed so that both education minister and exam controller are aware of the update.

After scheduling the examinations Controller of the Examination will sent an official order to prepare question to the Moderators selected by the education board by sending them their *Moderator ID* and initial system generated password.

3.2.5 Change Moderator Password

After receiving the Email the Moderators have to acknowledge the email. For the security of *Moderator ID* and password Hash function can be used so that no one else can login to a *Moderator ID*. The Moderators must change the password before preparing the question.

3.2.6 Preparing Questions

The moderators will prepare the question of the subject following the *Set Protocol* before the deadline of question submission. The current status of the question prepared is automatically saved to moderator cookie when a moderator logs out from his ID so that he can edit it the next time he logs in to his ID. When the question is fully prepared the moderator will submit the question. After submitting the question the moderator can't edit the question farther. Fig 4 shows the flowchart of a Moderators question preparation process.

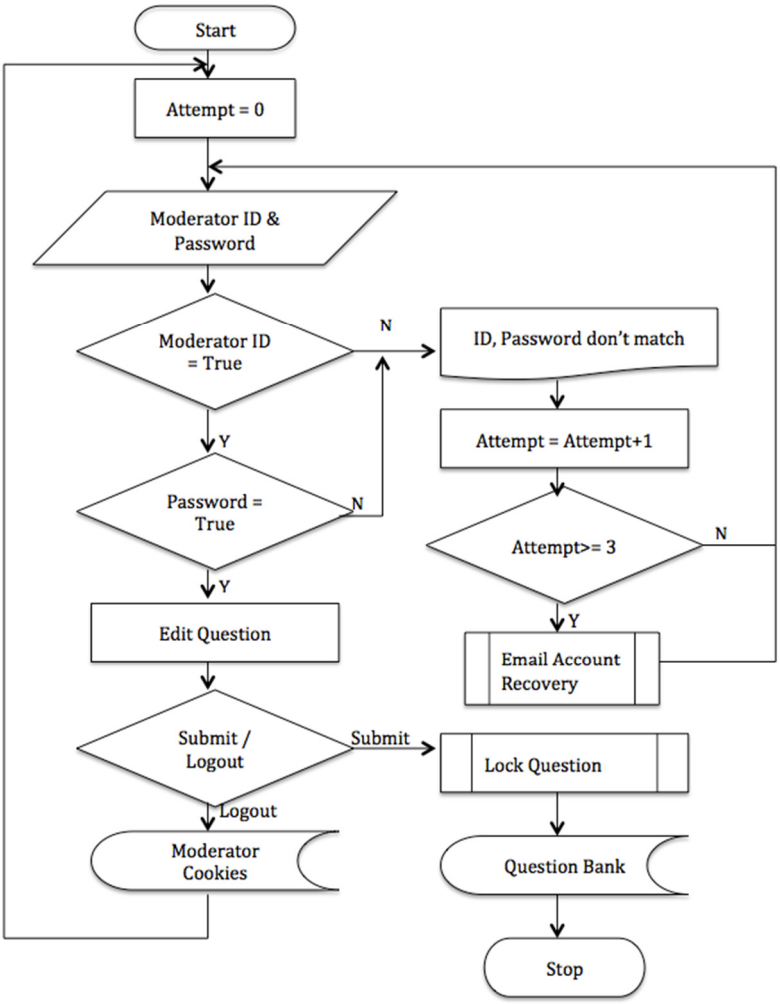

Fig 4: Flow Chart of Question Preparation

3.2.7 Lock Question

After submission the question is Locked and inserted into the corresponding subjects Question Bank. The encryption phase of RSA algorithm works in this locking stage. This encryption is for confidentiality of question paper. Only the Questions (neither set number nor marks assigned) are encrypted using public key of education minister (PU_{EM}). Before encryption the plaintext question (P_q) is padded using OAEP.

$P_q' = OAEP(P_q) = X||Y = (P_q00..0 \oplus G(r))||(r \oplus H(X))$ (4)

Here,

k_1, k_0 *are derived from equation (1) and (2)*

P_q is the plaintext qyestion, an $(n - k_0 - k_1)$-bit string

G ,H , r have the conventional meaning of OAEP

From padded question $M= P_q'$, using PU_{EM} = (e,n) cipher text question C is calculated as:

$C_q = M^e \bmod n$ (5)

Fig 5 shows a diagram of Locking phage.

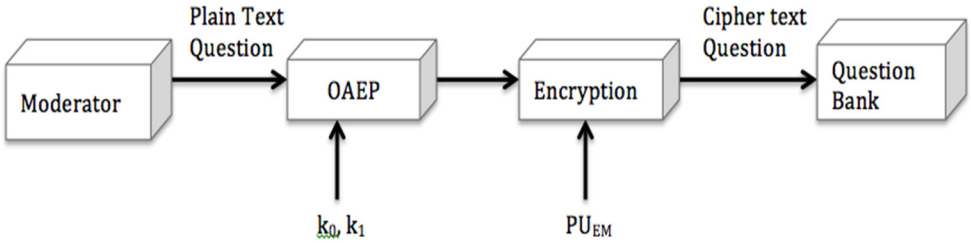

Fig 5: Block Diagram of Locking Phase

The cipher text questions from all moderators are stored in *Question Bank* table. The structure of Question Bank table is shown in Table 2.

Table 2: Structure of Question Bank

Field	Content	Data type
Moderator ID	Contains the ID of the Moderator who prepared the question	String
Set no.	Contains set number of the question. (e.g. 01, 02, 03 etc.)	Integer
Subset no.	Contains subset number of the question. (e.g. a, b, etc.)	Char
Question	Contains Encrypted Question	String
Marks	Marks assigned to the Question.	Number

Each row of the Question Bank has unique combination of Moderator ID, Question no. and Subset no. The cipher text question cannot be decrypted until the Exam Timestamp of the subject goes to zero. Which means the plaintext of the question can be revealed if and only if the following two conditions are satisfied:

- The correct Privet Key of education Minister is given.
- The *Exam Timestamp* is Zero.

3.2.8 Create Question Combo

After all of the questions of a subject are submitted to the *Questing Bank*, the *Question Combo* is generated for the subject following the rules stated in the definition section. *Authorized Key* the exam controller is needed to generate the Question Combo of each subject. So only the exam controller have the authority to generate the Question Combo of all the subjects. An enample structure of Question Combo is shown in Table.

Let, there are M numbers of moderator and Q question sets for a subject.

Moderator IDs = $\{MID_1, MID_2, \ldots\ldots\ldots MID_M\}$

Set no = {1, 2, ……., Q}

Table 3: Question Combo

Combo no.	Set 1	Set 2	…….	Set Q
01	MID_1	MID_3	…….	MID_M
02	MID_1	MID_2	…….	MID_M
03	MID_2	MID_1	…….	MID_{M-1}
:	:	:	::::::::::::::::::::	:
:	:	:	::::::::::::::::::::	:
:	:	:	::::::::::::::::::::	:
:	:	:	::::::::::::::::::::	:
$^{M}P_Q$	MID_3	MID_M	…….	MID_2

From the Table it is seen that Set# 01 of Combo# 01 in the *Question Combo* is the question selected by the Moderator having Moderator ID= MID_1. Similarly Set# 02 of the same *Question* Combo is the question selected by the Moderator having Moderator ID= MID_3. Thus a total of $^{M}P_Q$ combos are generated from the *Question Bank*.

3.2.9 Selection of Final Question

When the Exam Timestamp goes to zero the education minister will be notified to input a number ranges from 01 to $^{M}P_{Q}$, to select the *Combo* for the subject before examination. The Education Minister will submit the number by using his *Authorized Key*. After selecting the Combo the cipher text questions will be retrieved from the Question Bank according to the Combo's Set no. and MID. Which means, the final copy of question paper will be created in cipher text just before the exam starts. Meanwhile the examination centers will send request to Key Distribution Center (KDC) for public key (PU_{EM}) by entering Center ID and Unlocking Key. If valid *Center ID* and *Unlocking Key* are given the KDC sends PU_{EM} to the Center. Fig 6 shows a flowchart for selecting final question.

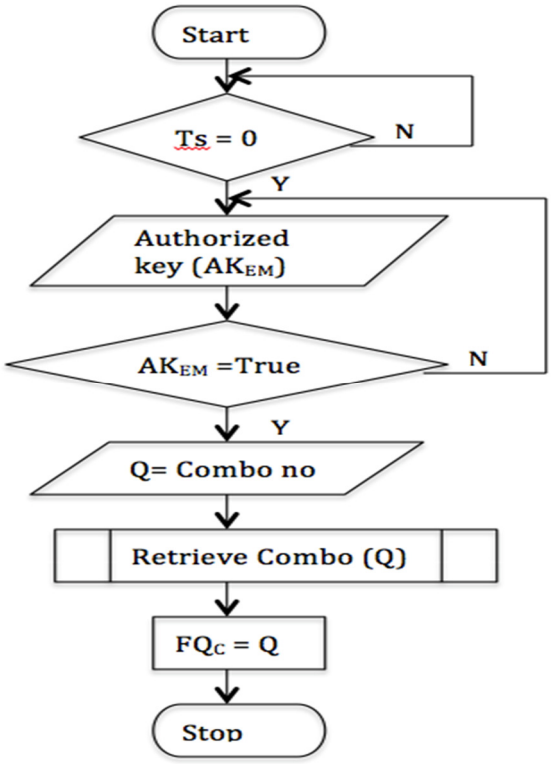

Fig 6: Flow chart for selecting Final Question in cipher text (FQ_C)

3.2.10 Unlocking and Broadcasting Final Question

Unlocking the final question works in following steps:

Step 1: Decrypt the cipher text of the question with Privet Key of education minister (PR_{EM} = d,n);
Step 2: Decode the massage using OAEP decoding to get Final Question FQ;
Step 3: Encrypt the plaintext question with Privet Key of education minister E[FQ ,PR_{EM}];
Step 4: If (Center ID& Unlocking Key) = True
Send E[FQ, PR_{EM}];
Step 5: Centers decrypt encrypted question E[FQ,PR_{EM}] with Public Key of the education minister;
D[(E[FQ,PR_{EM}]), PU_{EM}] = FQ;
Step 6: Display the FQ on projector;
END

The fourth and fifth step of the above algorithm is needed to authenticate the Final Question paper. A block diagram of unlocking and broadcasting the final question is given in Fig 7.

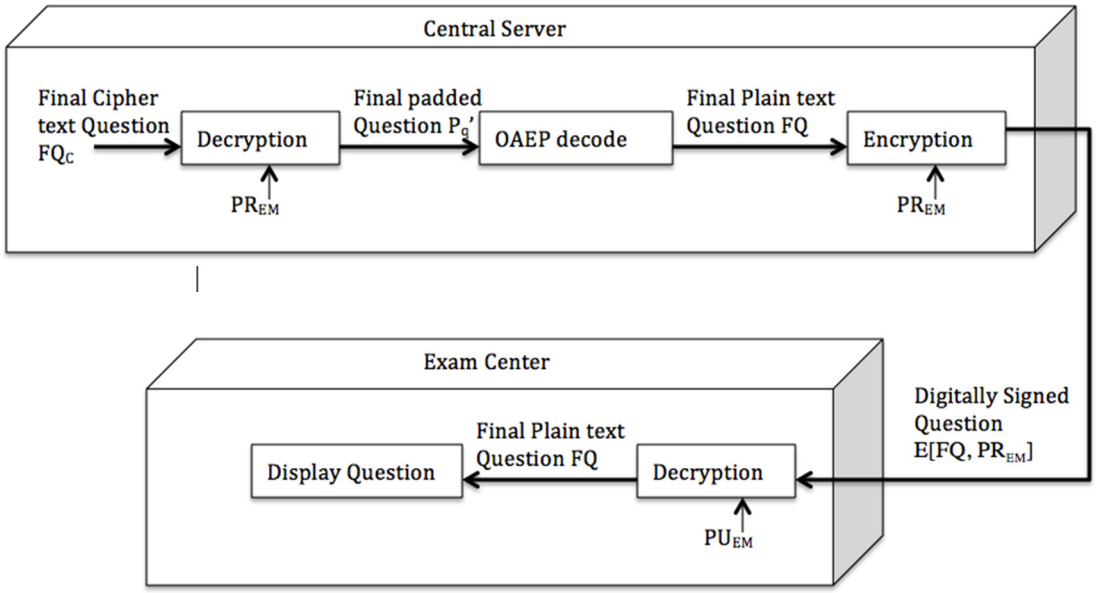

Fig 7: Unlocking and Broadcasting Final Question

4. System Evaluation

In this section we evaluate the performance of *CryptoQuestion* in terms of security and confidentiality of question paper in the public examination. In this paper we proposed a platform that can be a solution of the leakage of question paper. To evaluate the security of the proposed system we focus of the probability of the question leakage using the system.

- As the examination is not taken with a printed version of question, so there is no chance of a question paper to be leaked before the examination.
- If a moderator leaks the full question he prepared, the question of the examination will not be leaked. Because multiple moderator prepares a number of questions and one *Combo* is does not contain the entire question set from one moderator.
- If an unauthorized access takes place to the *Question Bank*, than only the encrypted versions of questions will be seen. For a key size of 128 bits it will take $5*10^{21}$ years to decrypt the *Question Bank*, if 50 billion keys are checked per second, which is not feasible time for revealing the question. (Alanazi, 2011)
- If the *Authorized Key* of the education minister is somehow compromised it will be not possible to see the plain text of the question in the *Question Bank*. Because the *Exam Timestamp* will not be zero before examination.
- If both *Authorized key* of the education minister and exam controller are compromised by known attack or any side channel attack, then an attacker will get Q_c number of question among them which question will be given in the examination is undecided. If we take the parameters 10 moderators and 05 question set per subject:

  $M = 10$
  $Q = 05$
  $Q_c = {}^{10}P_5 = 30240$

  So there will be 30240 *Combo*s will be available from only 10 moderators in each subject. It is unfeasible to predict the exact question paper from the huge number of *Combo*s. More over the decryption will be notified to the education minister and the further steps will be taken to deal with the attack.
- In any time before and after the examination the question paper leakage got caught it will be easier to identify the responsible person, if for the security of the question there are involvement of only two people (The Education Minister and The Exam Controller).

5. Challenges

Our proposed *CryptoQuestion* system is based on cryptography for taking public examination. But several challenges may arise to implement the *CryptoQuestion*. The traditional examination system has to be reformed, which involves the change to some educational policy made by the government. From question preparation to question circulation the system is fully dependent on Internet and the server. So the *CryptoQuestion* needs a very strong and robust network infrastructure throughout the country. Moreover, the teachers and students are used to

the traditional examination system. To change the examination system huge training must be needed for both the teachers and the students allover the country. Finally, the security of the whole system entirely depends on the *Authorized Key* of only two persons (the education minister and the exam controller).

6. Conclusion & Future Scope

The solutions of question leakage so far provided by digital means do not address the problem of leaking the softcopy of the question paper. Here we address the problem and also provide a solution for maintaining the confidentiality of the softcopy of large set of the question paper. In this paper we just proposed a system that can be implemented to provide confidentiality of question paper in public examination. In future we platform will be implemented to test the actual performance of the proposed system using different types of encryption algorithms. The proposed solution is for the subjective section of question. For objective section also a different *Set Protocol* and *Combo* system can be developed. Here only the algorithms that can be implemented for encrypting and hashing are addressed. In future the actual process of encryption and hashing can be discussed and implemented. Though there are a number of challenges regarding the implementation of the system in our country, we believe that, the implementation of *CryptoQuestion* will solve the digester in a wide extant.

References

Davis, R. (1978), The Data Encryption Standard in Perspective. Proceeding of Communication Society magazine, IEEE.

Daemen, J., Rijmen, V. (2001), Rijndael: AES-The Advanced Encryption Standard, Springer, Heidelberg.

Schneier, B. (2005-11-23). Cryptanalysis Rumors".Schneier on Security blog. Retrieved 2013-01-14.

Kumar, S.N., (2015), Review on Network Security and Cryptography. International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3, No. 1, 1-11

Rivest, R.L., Shamir, A., Adleman, L. (1978), A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communication of the ACM.

Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., & Al-Nabhani, Y. (2010). New comparative study between DES, 3DES and AES within nine factors. arXiv preprint arXiv:1003.4085.

Daemen, J., & Rijmen, V. (2013). The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media.

Ahmed, M. (2018, February 17), Plugging question leaks: A technical solution. The Daily Star, Retrieved from https://www.thedailystar.net

The Daily Ittefaq. (2018, February 20). Six Reasons marked for Question Leakage, Retrieved from http://www.ittefaq.com.bd

Ahamed, A.(2017). Akash Ahamed : Digital World [Question Setter Software]. Dhaka, Bangladesh: BICC

Schneier, B. (2015). One-Way Hash Functions. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C, 429-459.

Transparency International Bangladesh. (2015). Question Leakage in Public Examinations: Process, Reason and Way Forward [Executive Summary].