FEASIBILITY ANALYSIS OF RSA ALGORITHM IN SECURITY OF LECTURER PERFORMANCE DATA

Muhammad Fikry[1], Bustami[2]
[1, 2] Department of Informatics. Faculty of Engineering, Universitas Malikussaleh
*Corresponding Author: muh.fikry@unimal.ac.id

ABSTRACT

Lecturer performance data is an important data that must be possessed by every lecturer and institution, therefore efforts are needed to ensure quality management of the university. For this reason, it is necessary to get the right algorithm to secure data. The RSA (Rivest-Shamir-Adleman) algorithm is one of the public key algorithms in the field of cryptography which is popular and widely used today. The number one factor that can be used to carry out prime numbers is a long time to do the factoring. Data that is encrypted with the RSA algorithm must be changed to universal code, namely ASCII (American Standard Code for Information Interchange) or the American Standard Code for information exchange are the International Standard in universal letters and symbol codes. Based on the Basic Tri Dharma of Higher Education, measurement of lecturer performance needs to be carried out in accordance with their original objectives. Data can be obtained from each lecturer up to date with good data security.

KEY WORDS: Lecturer Performance; Cryptography; RSA.

INTRODUCTION

The application of computer technology as a data processing tool at this time is increasing rapidly, accompanied by the presence of computer networks that allow us to connect and share data whenever and wherever we are without space and time. With this rapid progress, it will be easier for people to obtain data and information quickly and efficiently. The use of software plays a role in the development of all lines, be it educational institutions, the business environment, or the private sector. So, building a computer-based application can present data accurately with a very short time.

Therefore, a web-based information system is needed to process lecturer performance so that the data becomes more structured and efficient so that lecturers can more easily and effectively manage their profile and performance data. With the information system can also help lecturers publish scientific papers and teaching materials from each lecturer on an online so that data can be more easily accessed by students, and the recapitulation by the faculty is done easily.

Security issues in computer applications have become an important aspect in today's technological era. So maintaining the security of data from web-based information system using data encryption techniques. One encryption algorithm that is often used is the RSA (Rivest-Shamir-Adleman) algorithm. The RSA algorithm was created by 3 researchers from MIT (Massachusetts Institute of Technology) in 1976, namely: Ron (R)ivest, Adi (S)hamir, and Leonard (A)dleman. The security of the RSA algorithm lies in the difficulty of factoring large numbers into prime factors. Factoring is done to obtain private keys (Hersatoto Listiyono, 2009). As long as the factoring of large numbers into prime factors has not been found to be an efficient algorithm, then during that time, the security of the RSA algorithm is guaranteed. The problem in this study is how to analyze the feasibility of the RSA algorithm in securing lecturer data and the implementation of the lecturer performance system online.

Based on the introduction described above, the problem that the writer formulated is:

1. How do you analyze the RSA algorithm for a lecturer database on a web-based system?
2. How to build and implement a web-based lecturer profile and performance system?

LITERATURE REVIEW

Lecturer

A lecturer is a teacher at a university or college. At Malikussaleh University, most of the lecturers are civil servants.

According to Government Regulation of the Republic of Indonesia, Number 46 of 2011 in article 1 referred to as:

a. Civil Servants hereinafter referred to as PNS, are Civil Servants as referred to in the legislation.
b. PNS work performance appraisal is a systematic assessment process carried out by appraisal officials on employee work targets and PNS work behavior.
c. Work performance is the result of work achieved by each civil servant in the organizational unit in accordance with employee work objectives and work behavior.
d. Employee Work Target, hereinafter abbreviated as SKP, is a work plan and target to be achieved by a civil servant.
e. The target is the amount of workload that will be achieved from each job assignment.
f. Work behavior is every behavior, attitude or action taken by civil servants or not doing something that should be done in accordance with the provisions of the legislation.
g. The annual work plan is a plan that contains annual activities and targets to be achieved as a description of the targets and programs set by government agencies.
h. An appraisal official is a direct supervisor of a civil servant who is assessed, with the lowest provision of echelon V structural officials or other specified officials.
i. The supervisor of the appraisal office is the direct supervisor of the appraisal official.
j. The Personnel Supervisor Official is the Personnel Supervisor Official as referred to in the legislation governing the authority to appoint, transfer and terminate civil servants.

In assessing the performance of civil servants set in Ministerial Regulation No. 46 of 2011 which consists of SKP (*Sasaran Kerja Pegawai*), which is referred to in Article 5, namely:

a. Each PNS is obliged to compile the SKP as referred to in Article 4 letter a based on the agency's annual work plan.
b. SKP, as referred to in paragraph (1), contains job assignment activities and targets that must be achieved in the real and measurable assessment period.
c. The SKP that has been prepared as referred to in paragraph (1) must be approved and determined by the appraiser.
d. In the event that the SKP compiled by the PNS is not approved by the appraising official, the decision is submitted to the supervisor of the appraisal official and is final.
e. SKP, as referred to in paragraph (1), is determined every year in January.
f. f. In the event of a transfer of employees after January, the person concerned still prepares the SKP at the beginning of the month in accordance with the order to carry out the task or order to occupy the position.

Procedure for Assessment of SKP

1. SKP achievement scores are expressed in numbers and information as follows:
   91 – above: Very good
   76 – 90: Good
   61 – 75: Enough
   51 – 60: Less
   50 – down: bad
2. SKP assessment for each implementation of job assignment activities is measured by 4 aspects, namely: aspects of quantity, quality, time and costs as follows:
   a. Quantity aspect = $\frac{\text{Output Relazation (OR) x 100}}{\text{Output Target (OT)}}$
   b. Quality aspect = $\frac{\text{Quality Relazation (QR) x 100}}{\text{Output Target (OT)}}$
   To assess the quality of output, the following criteria are used:

Value Criteria	**Description**
91 – 100	Perfect work, no errors, no revisions, and services above the standards specified, etc.
76 – 90	The work has 1 or 2 minor mistakes, there are no major mistakes, revisions, and services according to predetermined standards, etc.
61 – 75	The work has 3 or 4 minor errors, and there are no major mistakes, revisions, and the service simply meets the specified standards.
51 – 60	The work has 5 minor errors and there are major mistakes, revisions, and the service does not adequately meet the standards specified, etc.
50 down	The work has more than 5 minor errors and there are major errors, unsatisfactory, revised, services under the standards specified, etc.

   c. Time aspect
      1. If the activity is not carried out then the realization time is 0 (zero):

$$\frac{1{,}76\ x\ Time\ Target\ (TT) - Time\ Realization\ (TR)}{Time\ Target\ (TW)}\ x\ 0\ x\ 100$$

      2. If the aspect of time of efficiency level ≤ 24% is given good grades up to very good:

$$\frac{1{,}76\ x\ Time\ Target\ (TT) - Time\ Realization\ (TR)}{Time\ Target\ (TW)} x100$$

3. If the aspect of time that has an efficiency level> 24% is given a pretty up to bad value:

$$76\left\{\left\{\left(\left[\frac{1{,}76\ x\ Time\ Target\ (TT) - Time\ Realization\ (TR)}{Time\ Target\ (TT)}\right] x100\right\} x100\right\}$$

4. To calculate the percentage of time efficiency levels from the target time:

$$100\% - \left[\frac{Time\ Realization\ (TR)}{Time\ Target\ (TT)} x\ 100\right]$$

d. Cost aspect

1. If the activity is not carried out, then the realization time is 0 (zero):

$$\frac{1{,}76\ x\ Cost\ Target\ (CT) - Cost\ Realization\ (CT)}{Cost\ Target\ (CT)} x\ 0\ x100$$

2. If the aspect of time of efficiency level ≤ 24% is given good grades up to very good:

$$\frac{1{,}76\ x\ Cost\ Target\ (CT) - Cost\ Realization\ (CT)}{Cost\ Target\ (CT)} x\ 100$$

3. If the aspect of time that has an efficiency level> 24% is given a pretty up to bad value:

$$76\left\{\left\{\left(\left|\frac{1{,}76\ x\ Cost\ Target\ (CT) - Cost\ Realization\ (CT)}{Cost\ Target\ (CT)}\right| x100\right\} x - 100\right\}$$

4. To calculate the percentage of time efficiency levels from the target time:

$$100\% \left[\frac{Cost\ Realization\ (CT)}{Cost\ Target\ (CT)} x\ 100\%\right]$$

RSA Algorithm

To date, the RSA algorithm is still the most popular and secure public-key cryptographic system. It was proposed by Rivest, Shamir and Adleman in 1977. Let p and q be two distinct large random primes. The core of RSA computations is modular exponentiation which can be realized by square and multiply algorithm, including "Left-to-Right" and "Right-to-Left" modular exponentiation algorithm, Chinese Remainder Theorem (CRT), SWE algorithm and so on. In the RSA encryption scheme the public key consists of n = pq, where p and q are primes, and an exponent e, where e is relatively prime to φ(n) = (p − 1)(q − 1). For security purposes, e should be chosen randomly. A message M is encrypted as M e (mod n). Theprivatekey d satisfies that ed ≡ 1 (mod φ(n)), and M e canbedecryptedby computing M = (M e) d (mod n). An additional assumption beyond the security of RSA is made in [8]: It is assumed that for a random number δ, it is hard to find (a, b) such that a e − b e = δ (mod n). Furthermore, it is assumed that given a set of such pairs {(a i , b i)} satisfying that a e i − b e i = δ (mod n), it is hard to generate such a new pair. Given d, it is easy to compute (a, b) by computing a = (a e) d (mod n) and b = (a e − δ) d (mod n). It should be noted that the assumption is not true for very small e (e.g. 2 or 3); the pairs (a i , b i) fall on a low degree curve, which can be used as a basis for an attack. However, a large e does not seem to be vulnerable to such an attack.

The RSA scheme itself adopts from the block cipher scheme, where before encryption, the existing plaintext is divided into blocks of the same length, where plaintext and ciphertext are integers (integers) between 1 and n, where n is usually 1024 the bit, and the block length itself is smaller or equal to log (n) +1 with base 2.

The level of security of the RSA encoding algorithm is very dependent on the size of the password key (in bits), because the greater the key size, the greater the possibility of a combination of keys that can be broken down with one by one check key combination method or better known as the brute force attack. If an RSA password is created with a 256-bit length, then the brute force attack method will be uneconomical and useless where hackers don't want to be able to break the password.

Generate Key

Generate Key Process is a process for generating keys that are used for encryption and decryption processes. Some quantities used to generate RSA keys are:

Tabel 2.3. Size of generating the key for RSA

LARGE	CHARACTER
p and q (primes)	Secret
n = p x q	Not secret
Totient(n) = (p - 1) (q - 1)	Secret
e (Encryption Key)	Not secret
d (Decryption Key)	Secret
m (Plaintext)	Secret
c (Ciphertext)	Not secret

The first thing to do in the process of generating keys is to enter two prime numbers namely p and q, then after inputting primes p and q, to calculate the public key (n), the encryption key (c) and decryption key (d).

This Generate key process is done using the following methods:

1. Select a prime number p (for example: p = 13) and choose a prime number q (for example: q = 17)
2. Calculate the value for public key n with the formula:
   n = p x q = 13 x 17 = 221
3. Calculate totient n with the formula:
   t(n)= (p-1)(q-1) = (13-1)(17-1) = 192
4. Select the e key which is a relatively prime number of t (n), for example, e = 5
5. Find the key d using the extended Euclidean algorithm, namely in the following ways:
   192 = 38 x 5 + 2
   5 = 2 x 2 + 1
   2 = 2 x 1 + 0
   n = 1, a1 = 5, q1 = 38
   n = 2, a2 = 2, q2 = 2
   n = 3, a3 = 1, q3 = 2
   t0 = 0;
   t1 = 1;

t2 = t0 – q1.t1 = 0 – 38 (1) = -38
t3 = t1 – q2.t2 = 1 – 2 (-38) = 77
obtained the key of d = 77

6. obtained the key
   n (public) = 221
   e (encryption) = 5
   d (decryption) = 77

The key generating process is the most important step in the encryption and decryption process by using the RSA algorithm because at this stage it is the stage to find keys that can be used for encryption and decryption. Based on the experiment if the numbers taken for p and q are not prime numbers, this will affect the peruses of decryption, ie the data that has been encrypted cannot be returned to plaintext, this is because when calculating the key is searched for using the Euclidean algorithm, there what is sought is the FPB number by dividing the number from totient n with the key number e until the remainder of the division is 0, the value of the FPB returns to the totient value n.

DISCUSSION

The Proposed Scheme

In this section, we explain the proposed scheme based on the performance requirements of the lecturer. The following is a general description of the scope of the system to be built.

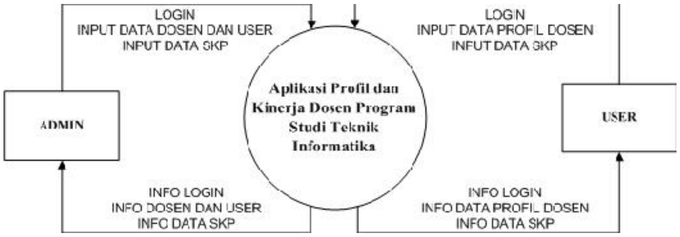


Figure 1 : Context Diagram

From the general description above will be made a diagram that illustrates the flow of data in the system. The description is as follows:

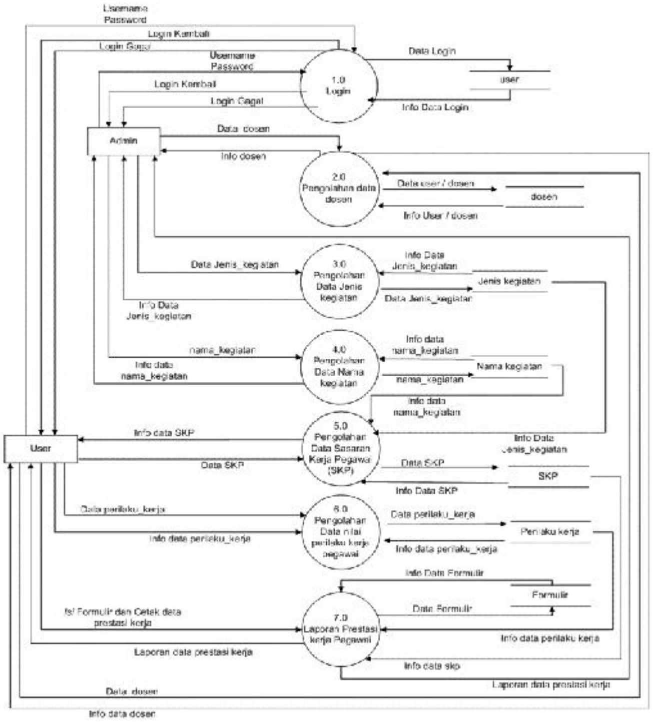


Figure 2 : Data Flow Diagram

In designing lecturer performance data applications, there are several tables that will be used to store data. The following is an overview of the database of lecturers performance in the faculty of engineering, malikussaleh university :

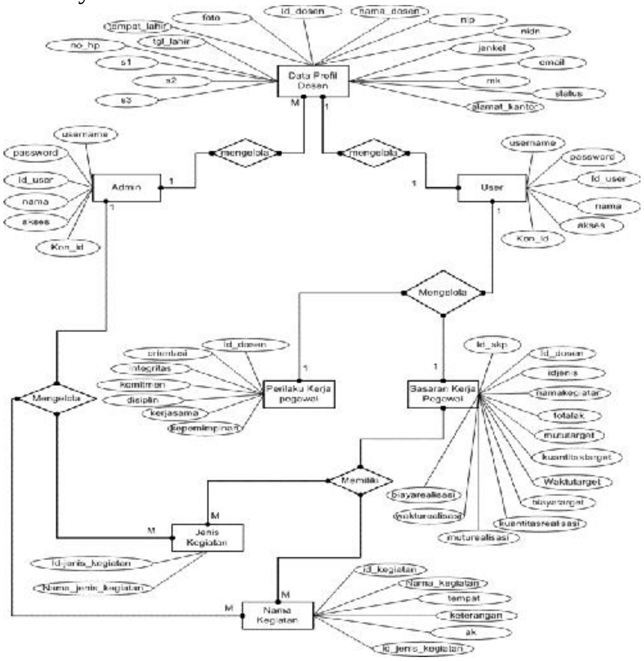
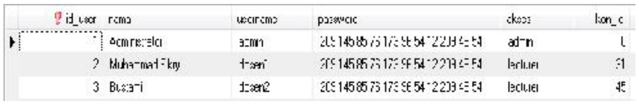


Figure 3 : Entity Relationship Diagram

To secure the database of lecturer performance, asymmetric key cryptography is applied, called RSA Algorithm, which is used to encrypt user and lecturer data in the database in the form of encoding. The strength of this algorithm lies in the exponential process and the factoring of numbers into 2 prime numbers which until now has taken a long time to do the factoring. The RSA scheme itself adopts the block cipher scheme, where before encryption, the existing plaintext is divided into blocks of the same length, where the plaintext and ciphertext are integers (integers) between 1 and n, where n is usually the size of 1024 bits, and the block length itself is smaller or equal to log (n) +1 with base 2.

On this issue, some lecturers' data will be encrypted using RSA algorithms including passwords, lecturer NIP, lecturer NIDN, and Lecturer phone numbers. The following is how the RSA Algorithm works to encrypt the user's password into the database. For example, the password used by the user is "informatika" in the following database which has been encrypted into ciphertext:



id_user	nama	username	password	akses	kon_c
1	Administrator	admin	209 145 85 76 173 96 54 12 209 48 54	admin	1
2	Muhammad Fikry	dosen1	209 145 85 76 173 96 54 12 209 48 54	lectuer	31
3	Bustami	dosen2	209 145 85 76 173 96 54 12 209 48 54	lectuer	45

Figure 4 : The user table is encrypted

The Process of Encryption

In this case, encryption is carried out in the form of text data "informatika" in the password in the database. The encryption process is done using the formula:

$$c = m\text{^}e \bmod n$$

c = Ciphertext
m = Plaintext
e = encryption key
n = public key

An example of the encryption of the word "informatika" converted in plaintext using a decimal system (ASCII encoding) is "105 110 102 111 114 109 97 116 105 107 97":

i →c1 = 105^5 mod 221 = 209
n →c2 = 110^5 mod 221 = 145
f →c3 = 102^5 mod 221 = 85
o →c4 = 111^5 mod 221 = 76
r →c5 = 114^5 mod 221 = 173
m →c6 = 109^5 mod 221 = 96
a →c7 = 97^5 mod 221 = 54
t →c8 = 116^5 mod 221 = 12
i →c9 = 105^5 mod 221 = 209
k →c10 = 107^5 mod 221 = 48
a →11 = 97^5 mod 221 = 54
c = 209 145 85 76 173 96 54 12 209 48 54

From the results of the calculations above, the word "informatika" is encrypted into the ciphertext form to "209 145 85 76 173 96 54 12 209 48 54".

CONCLUSIONS

The RSA algorithm has reached the main goal of the system to secure the lecturer database by using data encryption techniques as described previously. The word "informatika" changed to a row of numbers "209 145 85 76 173 96 54 12 209 48 54" which is very different from the plaintext. With such security, the web-based lecturer performance system is ready to be implemented.

ACKNOWLEDGMENTS

Funding: This work is supported by the Faculty of Engineering, Malikussaleh University [Year of Grant 2018]; and research laboratory majoring in informatics, University of Malikussaleh.

REFERENCES

Chen, C., Wang, T., Kou, Y., Chen, X., & Li, X. (2013). Improvement of trace-driven I-Cache timing attack on the RSA algorithm. *Journal of Systems and Software*, *86*(1), 100-107.

Fikry, M. (2016). APLIKASI JAVA KRIPTOGRAFI MENGGUNAKAN ALGORITMA VIGENERE. *TECHSI-Jurnal Teknik Informatika*, *8*(1).

Fikry, M., Dinata, R. K (2016). Desain Web Dengan HTML dan CSS. *Unimal Press*.

Hsiao, F. H. (2018). Chaotic synchronization cryptosystems combined with RSA encryption algorithm. *Fuzzy Sets and Systems*, *342*, 109-137.

Listiyono, H. (2009). Implementasi Algoritma kunci public pada algoritma RSA. *Jurnal Dinamika Informatika*, *1*(2).

Lin, X. J., Sun, L., & Qu, H. (2018). An efficient RSA-based certificateless public key encryption scheme. *Discrete Applied Mathematics*, *241*, 39-47.

Nomor, P. P. R. I. (46). Tahun 2011 tentang Penilaian Prestasi Kerja Pegawai Negeri Sipil. *Peraturan Kepala Badan Kepegawaian Negara Nomor*, *1*.

Padmaja, C. J., Srinivas, B., & Bhagavan, V. (2018). On The Usage Of Aryabhatta Remainder Theorem For Improved Performance Of Rprime Rsa. *Journal of Theoretical & Applied Information Technology*, *96*(9).