**Assignment/Tutorial/Practical Report Cover Sheet**

|  |  |
| --- | --- |
| Assignment Number of Title: | **Group Assignment** |
| Subject Code: **TME 4433** | Subject Name: **Computer Security** |

|  |  |
| --- | --- |
| **Name** | **Matric No** |
| Abdul Muqtasid bin Rushdi | 64575 |
| Fikri Hazmie bin Norhamzah | 64746 |
| Karisma Diana binti Ismail | 66338 |
| Mohd Nur Haziq Irsyamudiin bin Junaidi | 66722 |
| Nurul Sakinah bt Mohd Heree | 65155 |

|  |  |
| --- | --- |
| Name of Lecturer: | **Dr Adnan Shahid Khan** |
| Due Date: **29th April 2022, 23:59 hours** | **Date received and approved**  **(For office use only)** |

|  |
| --- |
| ***Plagiarism and Collusion are methods of cheating that falls under PeraturanAkademikUniversiti Malaysia Sarawak para 11: EtikaAkademik***  **Plagiarism**  Plagiarism is the presentation of work which has been copied in whole or in part from another person’s work, or from any other source such as the internet, published books or periodicals without due acknowledgement given in the text.  **Collusion**  Collusion is the presentation of work that is the result in whole or in part of unauthorized collaboration with another person or persons.  Where there are reasonable grounds for believing that cheating has occurred, the only action that may be taken when plagiarism or collusion is detected is for the staff member not to mark the item of work and to report or refer the matter to the Dean. This may result in work being disallowed and given a fail grade or if the circumstances warrant, the matter may be referred to a Committee of inquiry for investigation. Such investigation may result in the matter being referred to the University Discipline Committee, **which** has the power to exclude a student. |
| **Note:** Assignments are returned after being assessed by lecturer and to be collected from the lecturer’s office. Students should endeavour to collect their assignments prior to commencement of next semester. All unclaimed assignments become the property of the faculty and will become subject to destruction. |
| **Student’s Statement :**  I certify that I have not plagiarized the work of others or participated in unauthorized collusion when preparing this assignment.I also certify that I have taken proper case in safeguarding my work and have made all reasonable efforts to ensure that may work not be able to be copied.  Signature(s) : …………………………………… |

|  |  |
| --- | --- |
| **MARK:** | Comments: |

This cover sheet must be completed, signed and firmly attached to the front of the submission. All work must be submitted by the due date. If an extension of work is granted, an assignment extension acknowledgement slip must be signed by the lecturer/tutor and attached to the assignment.

Please note that it is the student’s responsibility to retain a copy of his/her own assignment.

Table of Contents

[1. ELGAMAL and RSA Cryptographic Algorithms Differentiation 2](#_Toc101371406)

[1.1 Key Generation Time 2](#_Toc101371407)

[1.2 Encryption and Decryption Time 3](#_Toc101371408)

[2 Details Working of ElGamal and RSA Algorithms 6](#_Toc101371409)

[2.1 Encryption / Decryption (confidentially) 6](#_Toc101371410)

[2.2 Signature (non-repudiation) 6](#_Toc101371411)

[2.3 Key Exchange (secure communication) 6](#_Toc101371412)

[3 References 7](#_Toc101371413)

# ELGAMAL and RSA Cryptographic Algorithms Differentiation

**ElGamal Cryptograhic Algorithm**

According to Nalwaya et al. (2014), in 1985, Taher ElGamal invented the ElGamal cryptographic algorithm. ElGamal is a key encryption algorithm that is an asymmetric which uses the Diffie-Helman key exchange as a public key encryption alternative to RSA cryptographic algorithm. ElGamal is also utilised in the ElGamal signature algorithm, according to Sukhija (2014), which is a digital signature generating process. For semantic security a homomorphic method dubbed paillier was applied (Farah et al., 2012).

**RSA Cryptographic Algorithms**

According to Rivest et al. (1983), in 1977, RSA Cryptographic Algorithm (Rivest, Shamir, and Adleman) were the first to introduce the algorithm. RSA is an algorithm which is asymmetric that is used for decryption and encryption for message (Hasib & Haque, 2008). RSA algorithm is commonly utilised when keys will be sent through channel that is insecure. Because of its nature as asymmetric algorithm, RSA uses two keys. The first is the public key, while the second is the private key. In the cryptosystem, an authorised person will keep the private key hidden although the accessibility for key which is public can be access by anybody. Integrity, data confidentiality, authenticity, and nonrepudiation are all provided by RSA (Alanazi et al., 2010). RSA algorithm is more widely used and utilised for online money transfer in the electronic business and in the future, may be utilised (Alanaza et al., 2010).

## Key Generation Time

How long it took for any encryption to produce ciphertext from a plaintext is called encryption time (Vijayalakshmi, 2012). The duration it takes for encrypted text to decrypt back again to plain text is called decryption time. Key creation time on the other hand, is the time it takes the key generation function to generate keys. These programmes create various durations in any algorithm based on the key length and number of text files. According to Maqsood et al. (2017), the generation times of ElGamal and RSA cryptographic algorithm are shown in the Table 1.1 below.

Table 1.1 Key Sizes with Their Generating Time (Maqsood et al., 2017)

|  |  |  |  |
| --- | --- | --- | --- |
| **Cryptographic Algorithms** | | **Key Size (bits)** | **Generation Time (milliseconds)** |
| Asymmetric | RSA | 1024 | 287ms |
| ElGamal | 160 | 86ms |

Cryptographic algorithm, RSA and ElGamal, key generation time, is shown in Figure 1.1 below. The length of a key determines how long to produce a key. The longer something is then the longer it takes. The RSA algorithm takes longer to produce a key since the key is 1024 bits long compares to ElGamal algorithm that takes less time because the key is 160 bits long.

Figure 1.1 Key Generation Time of RSA and ElGamal (Maqsood et al., 2017)

## Decryption and Encryption Time

According to Maqsood et al. (2017) in their research paper, they looked at the performance of asymmetric algorithms, RSA and ElGamal cryptographic in terms of decryption time, encryption time. Table 1.2 listed the decryption, encryption timing concerning to cryptographic methods which is asymmetric that has varying sizes of file. The findings show that as text file sizes increase, the time required to encrypt and decode the text will also increase.

Table 1.2 Decryption, Encryption Timings according to the File Size (Maqsood et al., 2017)

|  |  |  |  |
| --- | --- | --- | --- |
| **Asymmetric Cryptography Algorithms** | **File size (kb)** | **Decryption Timing (s)** | **Encryption Timing (s )** |
| RSA | 32 | 0.15 | 0.13 |
| 126 | 0.43 | 0.52 |
| 200 | 0.66 | 0.74 |
| 246 | 0.93 | 1.11 |
| 280 | 1.23 | 1.39 |
| ElGamal | 32 | 0.43 | 0.45 |
| 126 | 0.85 | 1.03 |
| 200 | 1.13 | 1.41 |
| 246 | 1.30 | 1.75 |
| 280 | 1.64 | 1.83 |

Time took to encrypt for both algorithms over multiple file sizes are depicted in Figure 1.2. As seen in Figure 1.2, RSA cryptographic requires less time for encryption than ElGamal technique. According to the results in Figure 1.3, the RSA decryption time also indeed quicker compared to ElGamal time taken to decrypt. Thus conclude, RSA cryptographic algorithm outperforms ElGamal cryptographic algorithm in terms of encryption and decryption time.

Figure 1.2 Encryption Time of RSA and ElGamal (Maqsood et al., 2017)

Figure 1.3 Decryption Time of RSA and ElGamal (Maqsood et al., 2017)

# Details Working of ElGamal and RSA Algorithms

## Encryption / Decryption (confidentially)

## Signature (non-repudiation)

## Key Exchange (secure communication)

# References

A. Al Hasib and A. A. M. M. Haque, “A comparative study of the performance and security issues of AES and RSA cryptography,” Proc. - 3rd Int. Conf. Converg. Hybrid Inf. Technol. ICCIT 2008, vol. 2, no. November 2001, pp. 505–510, 2008

D. Sukhija, “Performance Evaluation of Cryptographic Algorithms: AES and DES,” vol. 3, no. 9, pp. 582–585, 2014.

H. O. Alanazi, B. B. Zaidan, a. a. Zaidan, H. a. Jalab, M. Shabbir, and Y. Al-Nabhani, “New Comparative Study Between DES, 3DES and AES within Nine Factors,” J. Comput., vol. 2, no. 3, pp. 2151–9617, 2010.

K. B. R. P.R.Vijayalakshmi, “Performance analysis of rsa and ecc in identity-based authenticated new multiparty key agreement protocol,” International Conference on Computing, Communication and Applications (ICCCA), 2012.

Maqsood, F., Ahmed, M., Mumtaz, M., & Ali, M. (2017). Cryptography: a comparative analysis for modern techniques. *International Journal of Advanced Computer Science and Applications*, *8*(6), 442-448.

P. Nalwaya, V. P. Saxena, and P. Nalwaya, “A cryptographic approach based on integrating running key in feedback mode of elgamal system,” Proc. - 2014 6th Int. Conf. Comput. Intell. Commun. Networks, CICN 2014, pp. 719–724, 2014.

R. L. Rivest, A. Shamir, and L. Adleman “A Method for Obtaining Digital Signatures and Public- Key Cryptosystems.” Communications of the ACM, vol. 26, no. 1, pp. 96–99, 1983

S. Farah, M. Y. Javed, A. Shamim, and T. Nawaz, “An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms,” Recent advaces Inf. Sci., vol. 8, pp. 121–124, 2012.