TAYLOR'S UNIVERSITY
Wisdom · Integrity · Excellence

Bachelor of Computer Science (Hons)
Bachelor of Software Engineering (Hons)

ASSIGNMENT COVER SHEET

Module Code: **ITS64304**

Module Name: **Theory of Computation**

Students Name	**Students ID:**
1) Ishihara Satoaki	0354208
2) Basilia Sebastian	0353378
3) Syed Muhammad Taha Ali	0354100
4) Mohamed Fahad Farhan	0354487
5) Mohammad Sameed Khan	0353846
6)	

Assignment No. / Title	Assignment 3
Course Tutor/Lecturer	Assoc. Prof. Dr Raja

Declaration *(need to be signed by students. Otherwise, assignment will not be marked)*

We certify that this assignment is entirely our own work, except where we have given fully documented references to the work of others, and that the material contained in this assignment has not previously been submitted for assessment in any other formal course of study.

Signature of Students:

Marks:	**Evaluated by:**
Evaluator's Comments:	

Answer for Question 1

To find the decryption key d for RSA, we need to solve the equation:

$(d \times e)\ mod\ \varphi(n) = 1$

where φ(n) is the Euler totient function of n.

Given n = 221, we need to calculate φ(n) to proceed. In this case, φ(n) can be determined as follows:

φ(n) = φ(13 * 17) = φ(13) * φ(17) = (13 - 1) * (17 - 1) = 192

Now, we can find the decryption key d by calculating the modular multiplicative inverse of e (7) modulo φ(n) (192). In other words, we need to find a value for d such that $(d \times e)\ mod\ \varphi(n) = 1$.

Using the Extended Euclidean Algorithm, we find:

192 = 27 * 7 + 3
7 = 2 * 3 + 1

By working backward through the equations, we can express 1 in terms of 192 and 7:

1 = 7 - 2 * 3
1 = 7 - 2 * (192 - 27 * 7)
1 = 55 * 7 - 2 * 192

Comparing this to the equation $(d \times e)\ mod\ \varphi(n) = 1$, we can conclude that d = 55.

For large values of n, say of the order of 1024 bits, it is practically impossible to find the decryption key d using the same approach. The security of RSA relies on the difficulty of factoring large numbers into their prime factors. As the number of bits in n increases, it becomes exponentially harder to factor it into its primes, making it much harder to find the decryption key d. This is the basis for the security of RSA.

Answer for Question 2

To find the encryption key e for RSA, we need to calculate

$(d \times e) \, mod \, \varphi(n) = 1$

where φ(n) is the Euler totient function of n.

In this case, n = 187 and d = 67. We also need to calculate φ(n):

φ(n) = (p - 1)(q - 1) where n = pq

Since 187 is not a prime number, we need to factor it first. We can see that 187 = 11 * 17. So, we have:

φ(n) = (11 - 1)(17 - 1) = 160

We can now calculate e using the modular inverse of d:

$(67 \times e) \, mod \, 160 = 1$

Using the Extended Euclidean Algorithm, we find:

160 = 2 * 67 + 26
67 = 2 * 26 + 15
26 = 1 * 15 + 11
15 = 1 * 11 + 4
11 = 2 * 4 + 3
4 = 1 * 3 + 1

By working backward through the equations, we can express 1 in terms of 160 and 67:

1 = 4 - 1 * 3
1 = 4 - 1 * (11 - 2 * 4)
1 = 3 * 4 - 1 * 11
1 = 3 * (15 - 1 * 11) - 1 * 11
1 = 3 * 15 - 4 * 11
1 = 3 * 15 - 4 * (26 - 1 * 15)
1 = 7 * 15 - 4 * 26

1 = 7 * (67 - 2 * 26) - 4 * 26

1 = 7 * 67 - 18 * 26

1 = 7 * 67 - 18 * (160 - 2 * 67)

1 = 43 * 67 - 18 * 160

Therefore, e = 43.

For large values of n, say of the order of 1024 bits, it is practically impossible to find the encryption key e using the same approach. The security of RSA relies on the difficulty of factoring large numbers into their prime factors. As the number of bits in n increases, it becomes exponentially harder to factor it into its primes, making it much harder to find the encryption key e. This is the basis for the security of RSA.

Answer for Question 3

RSA Algorithm Digital Signature:

1. Calculate the digital signature:

   Digital Signature formula: $M^{d} \, mod \, n$

   Given: M = 27, d = 1019, n = 3337

   Plugging in the values:

   Signature = $27^{1019} \, mod \, 3337$

   Calculating the modular exponentiation: Signature = 2136

   ```
   pow(27, 1019) % 3337
   ```

   ```
   2136
   ```

   Therefore, the plain signature used by Robin is 2136.

2. Verification process by Ahana:

   To verify Robin's signature, Ahana needs Robin's public key (n, e) and the received message (M).

   Verification process formula: Recovered_M = $Plain\ Signature^{e} \, mod \, n$

   Given: Plain Signature = 2136, e = 79, n = 3337

   Plugging in the values: Recovered_M = $2136^{79} \, mod \, 3337$

   Calculating the modular exponentiation: Recovered_M = 27

   ```
   pow(2136, 79) % 3337
   ```

   ```
   27
   ```

   The recovered message, Recovered_M, is equal to the original message, M = 27.

The digital signature is authentic, and the message was not tampered with during transmission if the recovered message matches the original message. Ahana can trust that Robin sent the message intact.

Answer for Question 4

To encrypt the plaintext "STEPHEN KLEENE" using the RSA algorithm with prime numbers p = 11 and q = 17, we need to follow these steps:

Step 1: Calculate n and φ(n)
Calculate n = p * q:
n = 11 * 17 = 187

Calculate φ(n) = (p - 1) * (q - 1):
φ(n) = (11 - 1) * (17 - 1) = 160

Step 2: Choose e
Choose a value for e such that $1 < e < \varphi(n)$ and gcd(e, φ(n)) = 1 (e is coprime with φ(n)). Let's choose e = 7.

Step 3: Calculate d
Calculate d, the modular multiplicative inverse of e modulo φ(n). In other words, d is the number such that (d * e) % φ(n) = 1. We can use the Extended Euclidean Algorithm to find d.

Extended Euclidean Algorithm:
φ(n) = 160, e = 7

Divide φ(n) by e and get the quotient and remainder:

160 ÷ 7 = 22 remainder 6

Divide e by the remainder (6) and get the new quotient and remainder:

7 ÷ 6 = 1 remainder 1

Now, work backward substituting the remainders until you reach the coefficient of e:

1 = 7 - 1 * 6
1 = 7 - 1 * (160 - 7 * 22)
1 = 7 * 23 - 1 * 160

Since we are only interested in the coefficient of e (7), we can take its modulo φ(n):

d = 23 % 160 = 23

Step 4: Encrypt the plaintext

To encrypt each character of the plaintext, we convert it to ASCII value and raise it to the power of e (7) modulo n (187).

Plaintext: STEPHEN KLEENE

ASCII Value: 53, 54, 45, 50, 48, 45, 4E, 20, 4B, 4C, 45, 45, 4E, 45

Decimal Values converted from ASCII Values: 83 84 69 80 72 69 78 32 75 76 69 69 78 69

Now let's encrypt each value using the RSA algorithm and create a table:

Character	ASCII Value	Encrypted Value
S	53 (decimal value = 83)	8
T	54 (decimal value = 84)	50
E	45 (decimal value = 69)	86
P	50 (decimal value = 80)	75
H	48 (decimal value = 72)	30
E	45 (decimal value = 69)	86
N	4E (decimal value = 78)	56
(space)	20 (decimal value = 32)	76
K	4B (decimal value = 75)	114
L	4C (decimal value = 76)	167
E	45 (decimal value = 69)	86
E	45 (decimal value = 69)	86
N	4E (decimal value = 78)	56
E	45 (decimal value = 69)	86

```
print(pow(83, 7) % 187, pow(84, 7) % 187, pow(69, 7) % 187, pow(80, 7) % 187,
      pow(72, 7) % 187, pow(69, 7) % 187, pow(78, 7) % 187, pow(32, 7) % 187,
      pow(75, 7) % 187, pow(76, 7) % 187, pow(69, 7) % 187, pow(69, 7) % 187,
      pow(78, 7) % 187, pow(69, 7) % 187, sep = " ")
```

```
8 50 86 75 30 86 56 76 114 32 86 86 56 86
```

The encrypted text is: 8 50 86 75 30 86 56 76 114 32 86 86 56 86

Step 5: Decrypt the encrypted text

To decrypt each encrypted value, we raise it to the power of d (23) modulo n (187).

Encrypted text: 8 50 86 75 30 86 56 76 114 32 86 86 56 86

Now let's decrypt each value using the RSA algorithm and create a table:

Encrypted Value	Decrypted Value	Hex Value from Decrypted Value	Character
8	83	53	S
50	84	54	T
86	69	45	E
75	80	50	P
30	72	48	H
86	69	45	E
56	78	4E	N
76	32	20	(space)
114	75	4B	K
167	76	4C	L
86	69	45	E
86	69	45	E
56	78	4E	N
86	69	45	E

```
print(pow(8, 23) % 187, pow(50, 23) % 187, pow(86, 23) % 187, pow(75, 23) % 187,
    pow(30, 23) % 187, pow(86, 23) % 187, pow(56, 23) % 187, pow(76, 23) % 187,
    pow(114, 23) % 187, pow(32, 23) % 187, pow(86, 23) % 187, pow(86, 23) % 187,
    pow(56, 23) % 187, pow(86, 23) % 187, sep = " ")
```

```
83 84 69 80 72 69 78 32 75 76 69 69 78 69
```

The decrypted text is: STEPHEN KLEENE

Therefore, the original plaintext "STEPHEN KLEENE" was successfully encrypted and decrypted using the RSA algorithm with prime numbers p = 11 and q = 17.

Abstract

This study focuses on the users, who are frequently ignored in most research, to examine user acceptability of digital signature technology. The Unified Theory of Acceptance and Use of Technology (UTAUT), the theoretical framework used for this investigation, holds that users' behavioural intentions are influenced by their expectations for performance and effort.

Six important indications are used to gauge how well digital signatures are perceived by users: efficiency, information security, ease, comparative performance, scalability features, and other factors. On the other hand, contextual considerations, information accessibility, comparative easiness, and overall user experience are taken into account when evaluating user effort.

Although the UTAUT model forms the basis of the study, neither behaviour prediction nor model extension are its goals. Instead, it aims to comprehend how users view digital signatures. The study's limits, theoretical and practical repercussions, and suggestions for further investigation are presented in the end.

Face-to-face meetings have been prohibited as a result of the Covid-19 epidemic and the implementation of Movement Control Orders (MCO) and Enhanced Movement Control Orders (EMCO) in Malaysia, making it challenging to get conventional signatures. Digital signature use has increased as a result of this.

Handwritten signatures can be replaced with digital ones, which in nations like Finland are frequently combined with banking credentials and mobile ID technologies. Regardless of whether they are referred to as "digital signatures" or "electronic signatures," they are regarded by the law as having the same legal standing as handwritten signatures under EU regulation No. 910/2014.

In conclusion, this study examines how consumers see and interact with digital signatures, taking into account the impact of several variables on their adoption of this technology. It is especially essential in the current digital era, made more so by the recent rise in the usage of digital signatures as a result of pandemic-related constraints.

Introduction

The DSA, which regulates digital signatures, aimed to safeguard the security of legal concerns pertaining to electronic transactions, limit their usage in Malaysia, and verify their

use through certificates issued by accredited Certification Authorities [1].

What exactly are digital signatures?

In accord with the DSA, a digital signature is "a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and, if so, whether the message had been altered since the transformation was made."

According to Section 62 (1) of the DSA, the following circumstances give rise to the recognition of a digital signature:

1. The digital signature is checked against the public key mentioned in a current certificate issued by an authorised certification authority.

2. The signer attached the digital signature with the purpose to sign the communication and The digital signature is validated.

3. The private key used to create the digital signature is not legitimately held by the signer, or the receiver is unaware that the signer has violated their obligations as subscribers.

YES! A document with a digital signature that complies with the DSA has the same legal weight as one with a handwritten signature, an affixed thumbprint, or any other mark, according to Section 62 of the DSA.

As a digital substitute for handwritten signatures, digital signature technologies have evolved. Utilisation increased gradually but consistently until 2020, but the COVID-19 pandemic and the rapid shift to remote work and social

Distance considerably enhanced the digital signature. According to a press release from Visma Solutions, the technology firm that provides the service, the quantity of digital signatures through Visma Sign virtually quadrupled in just 10 weeks. The yearly growth had been in the tens of percent prior to the epidemic. (Visma Solutions, 2020)

Because digital signature services are becoming more and more common, it's important to understand the numerous factors that affect whether or not people embrace the technology. Previous studies on digital signatures focused mostly on technology and less on users'

perspectives. Technology hasn't advanced all that quickly until lately. Understanding the many forces that drive these forces and the ideas that support them is essential.

Public Awareness, Perception, and Acceptance of Digital Signatures in General

Digital signature adoption and use are greatly influenced by public perception, acceptance, and awareness. It is crucial for the successful application of this technology in numerous areas to comprehend how people view and accept it. The public's awareness, perception, and acceptance of digital signatures in general—and specifically in the context of Malaysia—will be examined in this section.

Below, we have some factors influencing public awareness and perception of Digital Signatures:

- Education and knowledge about the technology are two important aspects that affect public awareness of and perceptions of digital signatures. People are more likely to have a favourable opinion of digital signatures if they have a greater understanding of how they operate, their advantages, and their legal legitimacy. Public understanding and awareness can be increased by educational efforts, training programmes, and awareness campaigns.

- Trust and Security Issues: Trust and security issues have a significant impact on how the public views digital signatures. People must have confidence that their digital signatures are safe and cannot be altered or falsified. This trust is greatly influenced by the standing and dependability of Certification Authorities (CAs). Digital certificates that confirm the legitimacy of digital signatures are issued by CAs. So, to influence public image, their reputation and adherence to stringent security requirements are essential.

- Usability and Convenience: The usability and practicality of digital signatures are additional factors that influence public perception. People might be reluctant to adopt this technology if establishing and verifying digital signatures takes a lot of time and effort. The view of digital signatures as a practical and effective replacement for traditional signatures can be improved via user-friendly interfaces and simplified procedures.

Although there have been improvements in public acceptability of digital signatures in Malaysia, there are still several obstacles to their widespread use.

- The general public's lack of knowledge and comprehension of digital signatures continues to be a significant hurdle. To improve adoption, efforts must be made to inform people of the advantages, security attributes, and legal validity of digital signatures.

- Public acceptance is also influenced by issues of trust and security. To build confidence in the system, a strong structure for the accreditation and regulation of CAs must be established. These issues can be resolved and public confidence in digital signatures increased through ongoing work to strengthen cybersecurity safeguards, encryption systems, and audit mechanisms.

- Digital signature technologies' usability and accessibility are also important determinants of acceptability. Digital signatures can be more widely used if user-friendly platforms are developed, they are integrated with current digital systems, and interoperability is promoted across various industries.

Public Awareness, Perception, and Acceptance of Digital Signatures in Malaysia

In Malaysia, the Digital Signature Act (DSA) governs the use of digital signatures and gives documents that have been digitally signed legal standing. The Malaysian Communications and Multimedia Commission (MCMC) is in charge of the certified Certification Authorities (CAs) in Malaysia. The four authorised CAs now functioning in Malaysia are Pos Digicert Sdn Bhd, MSC Trustgate.Com Sdn Bhd, Telekom Applied Business Sdn Bhd, and Raffcomm Technologies Sdn Bhd.

Although there have been improvements in public acceptability of digital signatures in Malaysia, there are still several obstacles to their widespread use. The general public's lack of knowledge and comprehension of digital signatures continues to be a significant hurdle. To improve adoption, efforts must be made to inform people of the advantages, security attributes, and legal validity of digital signatures.

Public acceptance is also influenced by issues of trust and security. To build confidence in the system, a strong structure for the accreditation and regulation of CAs must be established. These issues can be resolved and public confidence in digital signatures increased through

ongoing work to strengthen cybersecurity safeguards, encryption systems, and audit mechanisms.

Digital signature technologies' usability and accessibility are also important determinants of acceptability. Digital signatures can be more widely used if user-friendly platforms are developed, they are integrated with current digital systems, and interoperability is promoted across various industries.

Certification Authorities (CAs) for Digital Signature in Malaysia

The Malaysian Communications and Multimedia Commission (MCMC) is responsible for regulating, enforcing, and supervising the activities of licensed Certification Authorities in accordance with the DSA's standards. Currently, there are only four Certification Authorities with licences, and they are as follows:

1. Pos Digicert Sdn Bhd (457608-K)
2. MSC Trustgate.Com Sdn Bhd (478231-X)
3. Telekom Applied Business Sdn Bhd (455343-U)
4. Raffcomm Technologies Sdn Bhd (1000449-W)

MSC Trustgate is one of the reputable and important Certification Authority (CA) in Malaysia. The business, which was established in 1999, has led the way in the nation in terms of offering digital certification services, including digital signatures. MSC Trustgate issues digital certificates as a licenced CA under the Malaysia Digital Signature Act 1997 for the purpose of generating and authenticating digital signatures. Their services are essential for assuring the legitimacy and integrity of digital transactions in Malaysia's diverse industries. For instance, MSC Trustgate's digital signatures are extensively used to verify digital documents and protect online transactions in industries including government, healthcare, banking, and education. To further assure secure online interactions, MSC Trustgate also offers Public Key Infrastructure (PKI) solutions, Secure Email Certificates, and Secure Socket Layer (SSL) certificates. Due to its status as a local provider of digital certificates and its adherence to Malaysian regulatory requirements, MSC Trustgate is a significant participant in the country's digital signature market. The credibility and acceptability of digital signatures in Malaysia are increased by their digital signature solutions, which are supported by legally enforceable security standards.

Conclusion

The successful adoption of digital signatures in Malaysia and around the world depends on public perception, acceptability, and public understanding of them. Public perception and adoption are greatly influenced by elements like education and information, trust and security concerns, and simplicity of use and convenience.

It is crucial to make efforts to increase public knowledge through educational programmes and awareness campaigns. To increase public confidence, it is crucial to strengthen the security and trust mechanisms related to digital signatures, including the control of Certification Authorities.

Digital signatures may also be more widely accepted if user experience is enhanced by creating user-friendly interfaces and encouraging interoperability between industries. Digital signatures will become more widely used and their advantages will become apparent in Malaysia and other countries as a result of continued technological breakthroughs and initiatives to satisfy user needs and concerns.

References

[1] Geng Yong , T. and Kai Di, H. (2021). *Electronic & Digital Signatures in Malaysia – Tuang, Chu & Co – Advocates & Solicitors*. [online] Tuang, Chu & Co Advocates & Solicitors. Available at: https://tcclaw.com.my/electronic-digital-signatures-in-malaysia/#:~:text=Digital%20signatures%20are%20governed%20by. [Accessed 25 June. 2023].

[2] Adobe.com. (2022). *Electronic Signature Laws & Regulations - Malaysia*. [online] Available at: https://helpx.adobe.com/legal/esignatures/regulations/malaysia.html. [Accessed 25 June. 2023].

[3] Paul, E. (2017). *What is Digital Signature: How it works, Benefits, Objectives, Concept*. [online] EMP Trust HR. Available at: https://www.emptrust.com/blog/benefits-of-using-digital-signatures/. [Accessed 27 June. 2023].

[4] Economic Planning Unit, Prime Minister's Department (n.d.). *MALAYSIA DIGITAL ECONOMY BLUEPRINT*. [online] Ministry of Economy, Malaysia. Available at: https://www.ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf. [Accessed 29 June. 2023].

[5] MSC Trustgate.com Sdn Bhd (n.d.). *Digital Signature – Trustgate*. [online] Trustgate. Available at: https://www.msctrustgate.com/digital-signature. [Accessed 29 June. 2023].

[6] Lääveri, L. (2021). *CONSUMER ACCEPTANCE AND USAGE OF DIGITAL SIGNATURE TECHNOLOGIES*. [online] Available at: https://jyx.jyu.fi/bitstream/handle/123456789/76881/1/URN%3ANBN%3Afi%3Ajyu-202106284071.pdf. [Accessed 27 June. 2023].

[7] Khye Yen, L. (2021). *Digital Signatures & Its Functionality in Malaysia | Publication by HHQ | Law Firm in KL Malaysia*. [online] HHQ | Law Firm in KL Malaysia. Available at: https://hhq.com.my/publications/digital-signatures-its-functionality-in-malaysia/ [Accessed 30 June. 2023].

Personal Contributions

Student Name	Contribution made:
1) Satoaki Ishihara	● Question 1 ● Question 2 ● Question 5 (References) ● Overall Formatting documents
2) Basilia Sebastian	● Question 5 (Public Awareness, Perception, and Acceptance of Digital Signatures in General) ● Question 5 (Public Awareness, Perception, and Acceptance of Digital Signatures in Malaysia) ● Question 5 (Conclusion)
3) Syed Muhammad Taha Ali	● Question 5 (Abstract) ● Question 5 (Introduction) ● Question 5 (Certification Authorities (CAs) for Digital Signature in Malaysia)
4) Mohamed Fahad Farhan	● Question 3 (Co-work with Sameed Khan) ● Question 4 (Co-work with Sameed Khan)
5) Mohammed Sameed Khan	● Question 3 (Co-work with Fahad) ● Question 4 (Co-work with Fahad)