

**Cryptography**

Year 1 Semester 2

## School of InfoComm Technology

Diploma in Information Security and Forensics

**Common Test**

**Practice Paper**

Date:

Time:

INSTRUCTIONS TO CANDIDATES:

1. Write your Student Number, Name, Module Group and Seat Number CLEARLY in the boxes provided above.
2. This paper consists of 11 pages including this cover page. Check carefully to make sure your set is complete.
3. There are FOUR questions. Answer **ALL** questions.
4. All questions carry equal marks.
5. Write your answers in the blank space provided for each question in this paper.

|  |  |
| --- | --- |
| **GRADE** |  |

There are FOUR questions. Answer **ALL** questions.

**QUESTION 1 (25 marks)**

1. Complete Table 1(a) by matching the appropriate given keywords with their respective descriptions. (9 marks)

Given keywords: Stream Cipher, Certificate Authority, Block Cipher, Data Encryption Standard, Triple Data Encryption Standard, Certificate Repository, Advanced Encryption Standard, Pretty Good Privacy, X.509 Standard, Public-Key Infrastructure.

|  |  |
| --- | --- |
| **Keyword** | **Description** |
| PGP | A popular email security system. |
| 3DES | Their effective key length can be 168bits |
| Block Cipher | Separate fixed length groups of bits are encrypted. |
| Public key infrastructure | Framework for all entities involved in digital certificates |
| DES | Was adopted as the standard by the US government with 56bits key. |
| Stream Cipher | Each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. |
| X.509 | Standard for most widely accepted format for digital certificates |
| Certificate Repository | Publicly accessible centralized directory of digital certificates and used to view certificate status |
| Certificate Authority | A trusted third party |

Table 1(a): Match the keywords with their respective descriptions

(b) A group of 20 people want to communicate securely among themselves. They want to select between symmetric key or asymmetric key cryptosystem for their communication.

1. Between the symmetric key cryptosystem and asymmetric key cryptosystem, which cryptosystem is scalable with respect to key management and why?

(5 marks)

|  |
| --- |
| Asymmetric.   1. Lesser number of keys than symmetric, more manageable as key formula is 2N compared to N(N-1)/2 |

Justify your answer to 2(b)(i) by stating the formula and calculating

1. The number of symmetric keys required for this group if they selected symmetric key cryptosystem.

(3 marks)

|  |
| --- |
| Formula:  Calculation: |

1. The number of asymmetric keys required for this group if they selected asymmetric key cryptosystem.

(3 marks)

|  |
| --- |
| Formula:  Calculation: |

(c) Complete Table 1(c) by matching the appropriate keywords with their respective descriptions. Given keywords: Confidentiality, Integrity, Authentication, Availability and Non-repudiation. (5 marks)

|  |  |
| --- | --- |
| **Keyword** | **Description** |
|  | Measures to ensure that one party of a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction. |
|  | Measures here include file permissions and user access controls. |
|  | Measures designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. |
|  | Measures to verify a claim of identity. |
|  | Measures to ensure that one rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. |

Table 1(c): Match the keywords with their respective descriptions

**QUESTION 2**

1. Utilize the Kid-RSA cryptosystem to answer the following questions. [Note that in this question, both the cipher text and the plain text is a number and not a readable text.]

|  |  |
| --- | --- |
| Given parameters: | a = 4, b = 10, a1 = 6, b1 = 9 |

1. Using the above parameters, calculate the following values:

(6 marks)

|  |  |  |
| --- | --- | --- |
| **Formulas** | **Substitute Values** | **Result** |
| M = (*a* x *b*) - 1 | 4 x 10 - 1 | 39 |
| e = (*a1* x *M*) + a | 6 x 39 + 4 | 238 |
| d = (*b1* x *M*) + b | 9 x 39 + 10 | 361 |
| n = ((*e* x *d*) - 1) / M | (238 x 361 -1) / 39 | 2203 |

1. Write the values that are used as the public key and private key. (2 marks)

|  |
| --- |
| Public = (2203,238)  Private = 361 |

1. State the encryption formula and encrypt the plain text (PT) = 750.

(2 marks)

|  |
| --- |
| Formula: CT = PT x e (mod n)  Calculation:750 x 238 (mod 2203) = 57 |

1. State the decryption formula and decrypt the cipher text (CT) = 270.

(2 marks)

|  |
| --- |
| Formula: PT = CT x d (mod n)  Calculation: 57 \* 361 (mod 2203) = 750 |

1. One such PGP’s secure email tool is known as the “Mailvelope”. Complete the table 2(b) below to provide the purposes of the given functionalities of Mailvelope. (6 marks)

|  |  |
| --- | --- |
| **Functionalities of Mailvelope** | **Purpose** |
| Generate Key | To generate user’s public-private key pair |
| Passphrase | Used to protect the private key in the user’s machine. |
| Import Keys | To import friend’s public keys |

Table 2(b): Functionalities of “Mailvelope”

(c) Given the followings below, decrypt using statistical properties and show all your workings clearly. The value of the alphabets are as follows: A=0; B=1; C=2; etc. (7 marks)

|  |  |  |
| --- | --- | --- |
| **S.N.** | **Letters**  **(in the order of higher probability of occurrence)** | **Probability of Occurrence** |
| 1 | E | 0.120 |
| 2 | T, A, O, I, N, S, H, R | Between 0.09 ~ 0.06 |
| 3 | D, L | Around 0.04 |
| 4 | C, U, M, W, F, G, Y, P, B | Between 0.028 ~ 0.015 |
| 5 | V, K, J, X, Q, Z | Less than 0.01 |

Ciphertext: DOHDOWYTS

|  |
| --- |
| PT = CT-key mod 26  CT = PT + key mod 26  TEXTEMOJI |

**QUESTION 3 (25 marks)**

Alice wants to send a very large file to Bob. Bob requires Alice to send this file by combining both symmetric key and asymmetric key cryptosystems

(a) Draw well-labeled diagrams, show how Alice can perform secure key transfer and digital signature. (19 marks)

|  |
| --- |
|  |

(b) The above requirement from Bob is a valid requirement, due to the fact that symmetric key encryption is faster then the asymmetric key encryption. Complete the Reason 1 and 2 in table 3(a)(ii) below to explain as to why symmetric key encryption is faster and the asymmetric key encryption is slower in speed.

(6 marks)

|  |  |  |
| --- | --- | --- |
|  | **Reason 1** | **Reason 2** |
| Symmetric key encryption is faster because: |  | Simple -> subs/trans/mod |
| Asymmetric key encryption is slower because: |  | More complex -> mathematical formulation on individual characters needed since the two keys are mathematically related |

Table 3(a)(ii): symmetric key is faster than asymmetric key cryptosystem

**QUESTION 4 (25 marks)**

Figure 4 below is a screenshot of a typical digital certificate

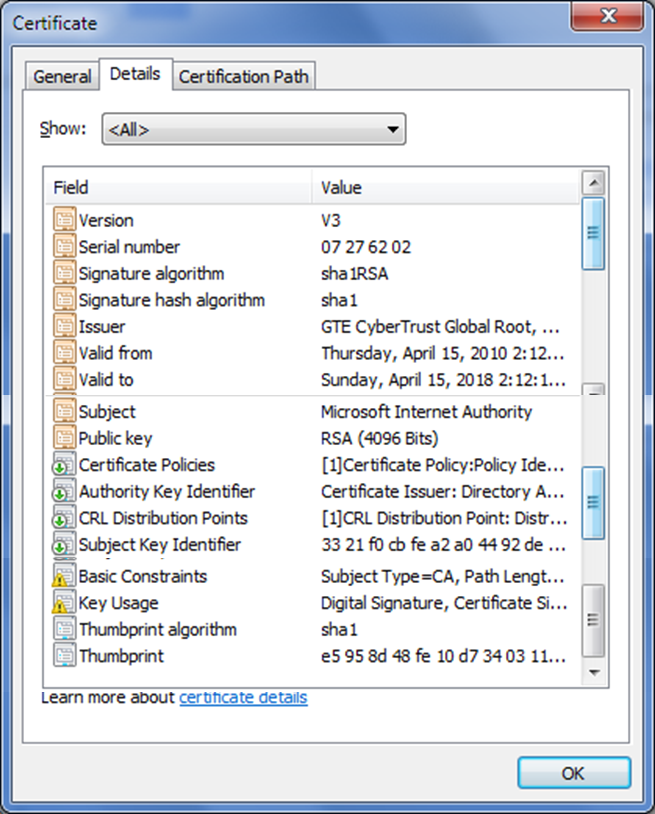


Figure 4: Digital Certificate

1. What is the main purpose of the digital certificate and why is there a need for such certificate? (4 marks)

|  |
| --- |
| It involves a trusted third party used to solve the problem of identity. It ensures that the owner name and public key really belongs to the authentic owner and helps prevent man in the middle attacks that impersonates the owner of the public key. |

1. In figure 4, who is the certificate authority? Briefly describe **two** roles play by the certificate authority? (6 marks)

|  |
| --- |
| GTE Cyber trust. The CA is responsible for generating issuing and distributing public key certificates as well as providing a means for subscribers to request certificate revocation. |

1. The CRL in the certificate shown in figure 4 is the Certification Revocation List. Briefly discuss **two** reasons why certificates are revoked?

(4 marks)

|  |
| --- |
| The certificate is no longer in use, and the private key of the certificate is exposed or suspected to be exposed / lost. |

1. Digital certificate has been used in code signing. What is code signing and state the two intended purposes of code signing?

(6 marks)

|  |
| --- |
| Code signing is the process software publishers use when they publish their code over the internet.  Purpose is to ensure to the users that the software publisher is authentic and to ensure to the users the integrity of the code after the code has been published |

(e) Why is there sometime a need for Registration Authority (RA) and discuss it role? (5 marks)

|  |
| --- |
| RA is a subordinate entity that is used to handles specific tasks of the CA.  It offloads registration functions and improves the workflow for CA. It receives, authenticates and processes certificate revocation request as well as identify and authenticate subscribers.  RA is used to authenticate and registers users and also used to authenticate certificate revocation request from users. It is there to help improve workflow for CA and act of behalf of CA. |

\*\* END OF PAPER \*\*