UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2016/2017

COURSE NAME	:	MULTIMEDIA SECURITY TECHNOLOGY
COURSE CODE	:	BIM 33403
PROGRAMME CODE	:	BIM
EXAMINATION DATE	:	JUNE 2017
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **SIX (6)** PAGES

Q1 Questions **Q1(a) – Q1(e)** are based on the following scenario.

The board of directors for Excellent Technology Sdn. Bhd. decided to develop a secure video transfer system between staff within the organization. It involves all branches located throughout Malaysia, using Internet. First, to use the in-house video transfer system, the staff must log in via a predetermined authentication method. Then, to enable secure video transfer between two staff, cryptography algorithm will be implemented for each session. Excellent Technology Sdn. Bhd. has 4 branches, each with 25 staff.

(a) Based on 'what you have' authentication approach, propose **TWO (2)** methods that can be used as the login mechanism for the system. For each method, provide **ONE (1)** suitable data type.

(6 marks)

(b) Suggest **TWO (2)** types of key if the asymmetric cryptography is used.

(4 marks)

(c) Calculate the number of keys required if the asymmetric cryptography is used.

(4 marks)

(d) List **TWO (2)** possible different attacks to the system. For each attack, provide **ONE (1)** possible source.

(6 marks)

(e) Propose the levels of security that will be implemented in the system.

(5 marks)

Q2 (a) Given the following scenario.

Movie Stream Bhd. is planning to develop a content delivery network that includes digital right management (DRM): a publisher, a server (streaming or Web), a client device (i.e., decoder box and smart card), and a financial clearing house. The communication between the server and the client is assumed to be unicast, i.e., point-to-point. The types of content include video (e.g., film, drama, documentary, and cartoon) and audio (i.e., radio channels). The authentication approach that will be used in this system is username and password.

Develop **ONE (1)** guideline to ensure the password being used is strong enough. The guideline should include what is required to make a strong password.

(8 marks)

(b) Given the text message below.

For things to change I must change first.

Suggest **TWO (2)** strategies to encrypt the text. For each strategy, provide **ONE (1)** example of the encrypted message.

(8 marks)

(c) Given the following scenario.

Maestro Movie is a content delivery company. They decided to encrypt the content during delivery so no one can view the content before it reaches the authorized decoder box. The main criteria for the encryption is that not a single movie part/segment can be viewed by unauthorized party.

Justify the suitable encryption scheme and discuss your answer.

(4 marks)

(d) Given the following scenario.

A graphical authentication scheme enforces the user to select 3 images. Each image must be selected from 10 given images. The 3 images must be selected in the right order.

Justify the strength of the scheme using the password complexity calculation.

(5 marks)

(b) Given the following **Figure Q4(b)**.

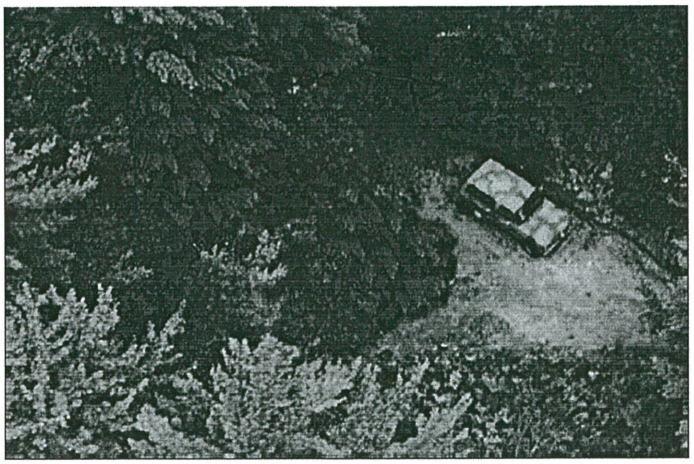

Figure Q4(b)

Assume image in **Figure Q4(b)** has been forged. Justify **ONE (1)** possible tampering method used to forge the image. Then, discuss **ONE (1)** method to detect it.

(4 marks)

(c) Given the following **Figure Q4(c)**.

Figure Q4(c)

Draw the watermarked image if the invisible watermarking technique is applied.

(4 marks)

Q3 (a) Justify why Content Scrambling System (CSS) used for solving broadcast encyrption is weak.

(5 marks)

(b) Given the following scenario.

```
Person A sends an attachment using an email to Person B.
```

Draw **ONE (1)** diagram to illustrate how to securely transmit the attachment via Internet from Person A's email account to Person B's email account.

(6 marks)

(c) Draw **ONE (1)** diagram to illustrate how 'what you are' approach can be integrated as the authentication and transaction access control mechanism for mobile banking system.

(6 marks)

(d) Given the text message below.

```
success successful fullhouse house successhouse full house
```

Suggest **TWO (2)** ways to combine encryption and compression processes during media streaming. For each way, provide **ONE (1)** example of the final output.

(8 marks)

Q4 (a) Given the following scenario.

```
Ramli used an online e-Locker to keep files containing
copyright pictures. The password of the e-Locker consists
of 5 characters. Each character must be selected from
number between 0 to 9.
```

Suggest **TWO (2)** Brute Force strategies to break the password.

(6 marks)

(d) Given the following scenario.

With the aid of audio watermarking technology, it is possible to embed additional information in an audio track. To achieve this, the audio signal of a music recording is slightly modified in a defined manner.

Justify **TWO (2)** reasons why audio watermarking is very reliable to avoid human detection and/or unauthorized extraction.

(6 marks)

(e) List **THREE (3)** attributes of the pyramid of an effective enforcement for Digital Right Management (DRM).

(3 marks)

(f) State the standard name for International Standards Organization (ISO) 27001:2013.

(2 marks)

- END OF QUESTION -

A climate of innovation.

NAUTICA®
DEHUMIDIFIERS

NAUTICA DEHUMIDIFIERS, INC.
www.NauticaDehumid.com
1.866.628.8424

TERBUKA

PSYCHROMETRIC CHART

Normal Temperature

SI Units

SEA LEVEL

BAROMETRIC PRESSURE: 101.325 kPa

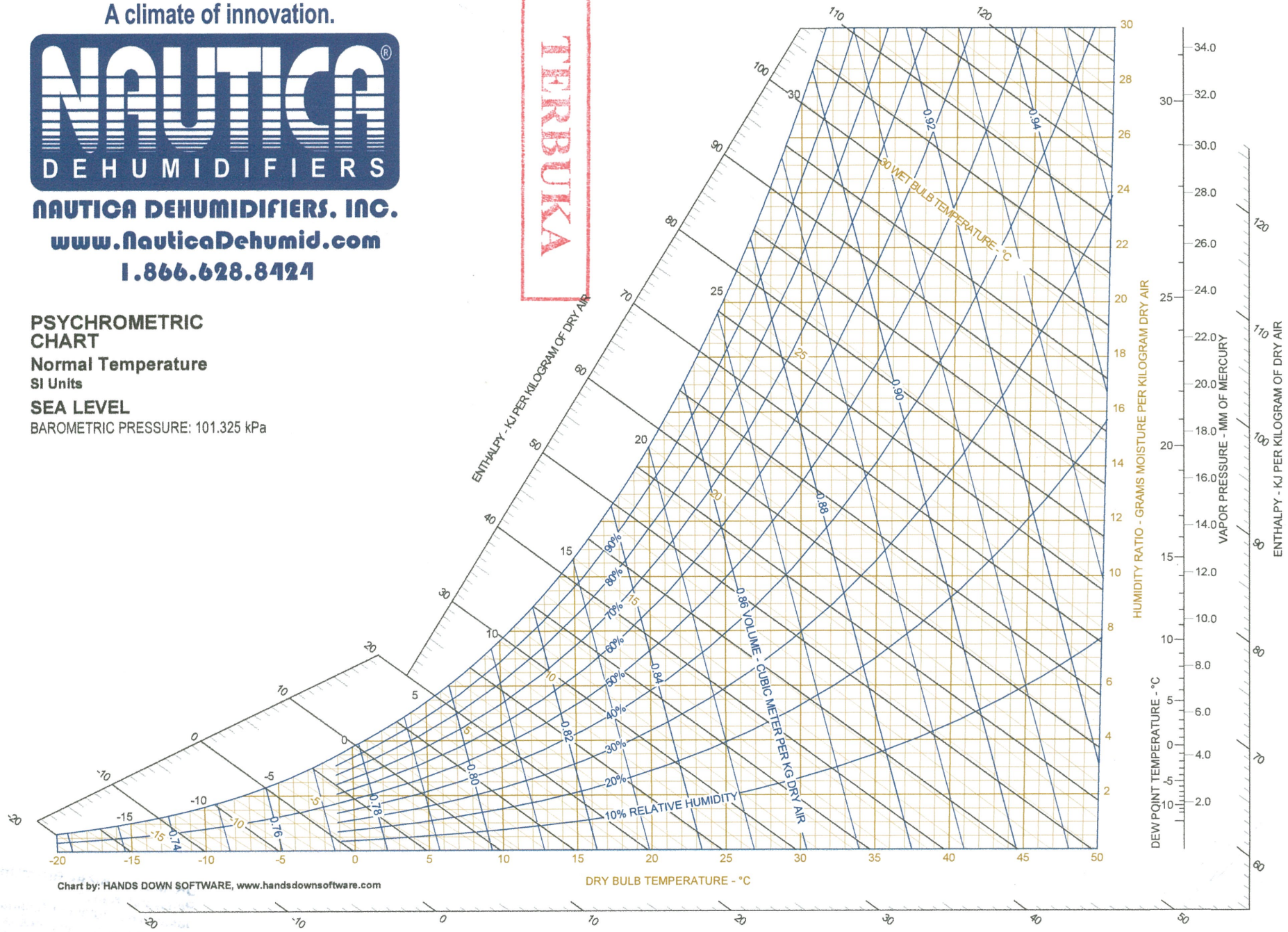

Chart by: HANDS DOWN SOFTWARE, www.handsdownsoftware.com