

DATA ENCRYPTION IN E-COUNSELLING SYSTEM (DEECS)

ATHIRAH FAYYADHAH OTHMAN

UNIVERSITI MALAYSIA PAHANG

BORANG PENGESAHAN STATUS TESIS

JUDUL : **DATA ENCRYPTION IN E-COUNSELLING SYSTEM**

SESI PENGAJIAN : 2009/2010

Saya : **ATHIRAH FAYYADHAH BINTI OTHMAN**
(HURUF BESAR)

mengaku membenarkan tesis (Projek Sarjana Muda/Sarjana/Doktor Falsafah)* ini disimpan di Perpustakaan Universiti Malaysia Pahang dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Malaysia Pahang
2. Perpustakaan Universiti Malaysia Pahang dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. **Sila tandakan (4)

☐

SULIT

(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

☐

TERHAD

(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

☐

TIDAK TERHAD

Disahkan oleh

(TANDATANGAN PENULIS)

(TANDATANGAN PENYELIA)

Alamat Tetap:
193, TAMAN SETONGKOL BARU
JALAN BUKIT SETONGKOL,
25200 KUANTAN,
PAHANG DARUL MAKMUR

Nama penyelia:
EN. ABDULLAH BIN MAT SAFRI

Tarikh :

Tarikh :

CATATAN: * Potong yang tidak berkenaan.

** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh tesis ini perlu dikelaskan sebagai SULIT atau TERHAD.

*** Tesis dimaksudkan sebagai tesis bagi Ijazah Doktor Falsafah dan Sarjana secara penyelidikan, atau disertasi bagi pengajian secara

“I hereby declare that I have read this thesis and in
my opinion this thesis is sufficient in terms of scope and
quality for the award of the degree of
Bachelor of Computer Science (Software Engineering)”

Signature :
Supervisor : Mr. Abdullah bin Mat Safri
Date :

DATA ENCRYPTION IN E-COUNSELLING SYSTEM (DEECS)

ATHIRAH FAYYADHAH OTHMAN

**A report submitted in partial fulfillment of the
requirements for the award of the degree of
Bachelor of Computer Science (Software Engineering)**

**Faculty of Computer Systems & Software Engineering
Universiti Malaysia Pahang**

NOVEMBER 2009

DECLARATION

I declare that this thesis entitled “Data Encryption in E-Counselling System” is the result of my own research except as cited in references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.”

Signature :

Name of Candidate : Athirah Fayyadhah binti Othman

Date : 24th November 2009

DEDICATION

To my beloved father and mother,
Mr. Othman bin Zainal Abidin and Mdm. Naziah binti Kamun,
who always give me a courage to finish this thesis.

To Mr. Abdullah bin Mat Safri thank you for the support, advices and helping hands
to finish this project.

To Norlia Che Saad, Nurul Hidayah Abd. Rahim,
Che Wan Nurul Fatihah Che Wan Fadzal, Siti Munirah Abdul Kudus,
Muhammad Khalis Yalah
my friends and all faculty members
thank you for your supporting teaching.

ACKNOWLEDGEMENT

Firstly, thanks to Allah for the idea, good health to complete this project. In preparing this thesis, I was contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my thesis supervisor Encik Abdullah bin Mat Safri and my mother for his encouragement, guidance, critics and friendship. Without their continued support and interest, this thesis would not have been the same as presented here.

I'm very thankful to Universiti Malaysia Pahang (UMP) for providing good facilities in the campus. Librarians at UMP also deserve special thanks for their assistance in supplying the relevant literatures and guiding me in using e-library to find resources to develop project.

My fellow postgraduate students should also be recognized for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance at various occasions. This views and tips are useful indeed. To all my friends thank you for your support, valuable opinion and sharing ideas during the progress of this project. Finally, special thank and

continuous love to my family for their understanding, encouragement and support, towards the completion of my project.

ABSTRACT

Communication has changed dramatically in recent years and many people now use the internet as the central role in their contact with friends, family and work colleagues. This social side to the web has been very successful and already been used at modern country like America. It is almost the expected way to do business. Previously, all the information of student was recorded manually by counsellor on paper. So, it have no guarantee of the security that the information would not be stolen or read by someone else and no security mechanism to ensure such data be read or handled in secure manner. The purpose of this project is to apply symmetric key (secret key) for encrypted memo in order to secure counselling session. This technique overcomes the problem of security in counseling session to ensure such data be read or handled in secure manner. Therefore, confidentiality can be achieve in this project.

ABSTRAK

Komunikasi telah berubah secara dramatikanya dalam kebelakangan tahun dan kini ramai menggunakan internet sebagai peranan utama dalam berhubung dengan kawan, keluarga dan rakan-rakan sekerja. Aspek sosial ini kepada web telah berjaya dan digunakan di negara moden. Ia hampir ke arah jangkaan untuk membuat perniagaan. Sebelum ini, segala maklumat pelajar direkodkan dalam kertas secara manual oleh kaunselor. Jadi, ianya tiada jaminan keselamatan bahawa maklumat tersebut tidak akan dicuri atau dibaca oleh orang lain dan tiada mekanisme keselamatan untuk memastikan data tersebut dibaca dan diuruskan dalam aspek keselamatan yang betul. Tujuan projek ini adalah untuk mengaplikasikan kekunci simetri (kekunci rahsia) dalam memo untuk menjamin sesi kaunseling yang selamat. Teknik ini mengatasi masalah aspek keselamatan dalam sesi kaunseling untuk memastikan data tersebut dibaca dan diuruskan dengan betul. Oleh itu, keyakinan boleh dicapai dalam projek ini.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENT	vii
	LIST OF TABLES	x
	LIST OF FIGURES	xi
	LIST OF ABBREVIATIONS	xiv
	LIST OF APPENDICES	xv
1	INTRODUCTION	
	1.1 Introduction	1
	1.2 Problem Statement	2
	1.3 Objective	4

	1.4 Scope	4
	1.5 Thesis Organization	5
2	LITERATURE REVIEW	
	2.1 Introduction	6
	2.2 Current Implementation of Counselling System	7
	2.3 Study on Related System	11
	2.3.1 Relationship Help Online	11
	2.3.2 Evaluation of Kooth.com	16
	2.4 Comparison between Two Related System	19
	2.5 Cryptography	20
	2.5.1 Symmetric Cryptography	20
	2.5.2 Asymmetric Cryptography	24
	2.5.3 Digest Message	26
3	METHODOLOGY	
	3.1 Introduction	27
	3.2 Project Methodology	28
	3.2.1 Planning	29
	3.2.2 Analysis	29
	3.2.2.1 Analysis on Questionnaire	30
	3.2.2.2 System Requirements	32
	3.2.3 Design	37
	3.2.3.1 Business Modeling Workflow	39
	3.2.3.2 Data Flow Diagram	40
	3.2.3.3 Database Design	40
	3.2.3.4 Interface Design	44
	3.2.3.5 System Design	44
	3.2.4 Implementation	45
	3.3 Hardware	46
	3.4 Software	47
	3.4.1 PHP	48

	3.4.2 MySQL Server	48
4	IMPLEMENTATION	
	4.1 Introduction	49
	4.2 MySQL Statement	49
	4.3 PHP Code	52
5	RESULT AND DISCUSSION	
	5.1 Introduction	68
	5.2 Student Module	69
	5.2.1 Homepage	69
	5.2.2 Sending Memo	70
	5.2.3 Sending Appointment Request	71
	5.2.4 View Appointment Status	72
	5.3 Staff Module	73
	5.3.1 Homepage	73
	5.3.2 View Inbox	74
	5.3.3 Reply Memo	75
	5.3.4 Reply Student Appointment Request	76
	5.3.5 View Appointment Schedule	77
	5.4 Constraint	78
	5.4.1 Development Constraint	78
	5.4.2 System Constraint	79
	5.5 Suggestions and Project Enhancements	80
6	CONCLUSION	81
	REFERENCES	83
	APPENDIX A – H	85 - 95

LIST OF TABLES

TABLE NO	TITLE	PAGE
2.1	Comparison between two related systems	19
3.1	Strengths and weaknesses of SDLC	28
3.2	Table of studinfo	42
3.3	Table of staffinfo	43
3.4	Table of compose	43
3.5	Table of request	43
3.6	Hardware specification	46
3.7	Software specification	46

LIST OF FIGURES

FIGURE NO	TITLE	PAGE
2.10	Flow process of apply an appointment	8
2.11	Flow process of counseling session for student who come willingness	9
2.12	Flow process of counseling session who is referred	10
2.13	Interface of Relationship Help Online	12
2.14	Interface of Kooth.com	16
2.15	Symmetric cryptography	21
2.16	Cryptography of symmetric key	21
2.17	Distribution key in private communication path	22
2.18	AES structure	23
2.19	Asymmetric cryptography	24
2.20	Encryption data by using public key	25
2.21	Encryption data by using private key	25
2.22	Digest message	26
3.10	The phase of SDLC	28
3.11	Survey analysis on question 1	30

3.12	Survey analysis on question 2	30
3.13	Survey analysis on question 3	31
3.14	Survey analysis on question 4	31
3.15	Survey analysis on student care of counseling services	32
3.16	Appointment form (in front side)	33
3.17	Appointment form (back side)	34
3.18	Student information form (page 1)	35
3.19	Student information form (page 2)	36
3.20	Flow of overall system in general	37
3.21	Typing message	38
3.22	Data encryption process in hybrid system	38
3.23	Secret key encryption process in hybrid system	39
3.24	Context diagram for DEECS	39
3.25	DFD for DEECS	40
3.26	ERD for DEECS	41
3.27	Prototype interface DEECS	44
4.10	MySQL query to create database	49
4.11	MySQL query to create 'studinfo' table	50
4.12	MySQL query to create 'staffinfo' table	51
4.13	MySQL query to create 'compose' table	51
4.14	MySQL query to create 'request' table	51
4.15	Variables declaration	51
4.16	Database connection query	53
4.17	Registration new student	53
4.18	Delete message	54
4.19	Edit existing student query	54
4.20	View existing data	55
4.21	Compose query	55
4.22	aes-lib.php	56
4.23	Encryption process	65
4.24	Decryption process	65

4.25	Request appointment process	66
4.26	Reply student appointment request	66
4.27	Login	67
4.28	Logout	68
5.10	Homepage for student module	70
5.11	Interface of sending memo	71
5.12	Database of 'compose' table	71
5.13	Interface of sending appointment request	72
5.14	Interface of view appointment status	73
5.15	Homepage for staff module	74
5.16	Interface of counsellor inbox	75
5.17	Interface of view message	75
5.18	Interface of reply memo	76
5.19	Interface of reply student appointment request	77
5.20	Interface of view appointment schedule	78

LIST OF ABBREVIATIONS

ECS	E-Counselling System
DEECS	Data Encryption in E-Counselling System
AES	Advances Encryption Standard
DES	Data Encryption Standard
SDLC	Software Development Life Cycle
DFD	Data Flow Diagram
PHP	Personal Home Page
IDE	Integrated Development Environment
RDBMS	Relational Database Management System
ERD	Entity Relationship Diagram
JHEPA	Jabatan Hal Ehwal Pelajar
UMP	University Malaysia Pahang
SQL	Structured Query language
PSM	Projek Sarjana Muda
SHA	Secure Hash Algorithm
HMAC	Authentication Code
NIST	National Institute of Standard and Technology
IDEA	International Data Encryption Algorithm

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Gantt Chart	86
B	Interview Question	88
C	Answer of interview session	89
D	Questionnaire	90
E	Sample answer of questionnaire	91
F	Flowchart of Counseling Session for student who come willingness	94
G	Flowchart of Counseling Session for student who is referred	95
H	User Manual	96

CHAPTER 1

INTRODUCTION

1.1 Introduction

The project name is Data Encryption in E-Counseling System. It is about online counselling that counselor communicate with user through internet, to give emotional support, mental health advice or some other counselling service. The user of this project are counsellor and student. Data Encryption in E-Counselling System (DEECS) is viable alternative source when user do not have enough time to go to the counselling unit to make an appointment or not comfortable to share problem face to face with counsellor. Online counselling can also be an effective source of help if you are unable to schedule an appointment for any reasons such as be experiencing an illness or disability that makes it difficult to attend the service in person or have hearing problems or other difficulties and would prefer to use text based communication. User can meet a counsellor for personal counselling or advice, from the privacy of their own computer over the internet.

No need to make an appointment and go to counsellor office. Just dial up anytime, day or night, at home or at hostel, counsellor can respond when ready to and can take time in processing any changes that are taking place, before next counselling session. It could be one or more question, it could be by email, but for this project it is over encrypted memo, more safety and privacy.

Memo are encrypted by using secret key. All the data transmission between student and counsellor are encrypted. So no one else can access or know the content of discussion. In detail why security are important in this system because to ensure the confidentiality of information that will be accepted by authentic user and cannot be read by other user.

1.2 Problem Statement

Current system for counselling unit, all the information of student was recorded manually by counsellor on paper and save it into file. Paper might be disappear or torn. So, it have no guarantee of the security that the information would not be stolen or read by someone else. No security mechanism to ensure such data be read or handled in secure manner and there is no confidentiality of counselling information.

Counsellor need to find manually one by one to get back or revise the information of some student or previous case. It is not a big problem if it only involved small number of students but the number of student will increase year by year and the record of student also increase significantly. It will take time to find information needed by counsellor. Counselling unit need to make preparation to cater this problem.

No online system for counselling unit give counsellor a big problem to face many students at one time. In addition, the number of student are too many for the counsellor to cater the student problem. By using online system, student

can share their problem and counsellor can cater the problem as many as possible they can any time, any where and any number of student at the same time.

Usually, student have a pack schedule and they do not have enough time to go to the counselling unit only to make an appointment with counsellor. In addition, student need to make an appointment again and again if counsellor are not around by that time. Because of that, it will make student get bored and no more feel to meet counsellor to share the problem.

Not all student are brave to meet counsellor face to face to share their problem. Some student need time to find someone that they are trust to share their problem and usually this type of person willing to share their problem without meet counsellor in person. They are more comfortable to share problem without face to face.

Other than that, not all students are perfect. There are some student that handicap. Some of them maybe have a sound trouble or not able to walk by their own and need to use wheel chair. It is more difficult for them to meet counsellor in person directly. Followings are the key points of problem statement that have been stated and elaborated above :

- i. Non confidential information
- ii. Information stored are not systematic
- iii. Student are too many for counselor to cater the problem
- iv. Time constrain to make an appointment
- v. Student not willing to meet counselor face to face
- vi. Handicap student

1.3 Objective

The objectives of the research are to:

- i. Apply secret key for encrypted memo in order to secure counselling session.
- ii. Develop database system for counselling unit to record information of student and counsellor.

1.4 Scope

Scope of this project are :

- i. Scope of Technique
 - Symmetric Cryptographic Technique (secret key) will be use in this project to apply encrypted memo and secure system.
- ii. Scope of User
 - User of this project are counsellor and student.
- iii. Scope of System
 - This system is an online web based system
- iv. Scope of Session
 - Only for individual counselling session available for this proposed system
- v. Scope of Data
 - Data are memo (plain text to cipher text), session information, secret key (Advance Encryption Standard, AES).

1.5 Thesis Organization

This thesis consists of three chapters. Chapter 1 will discuss on introduction to system. Chapter 2 will discuss on literature review. Chapter 3 will discuss on methodology. Chapter 4 will be discussing about the implementations of the system. Chapter 5 will discussed about the data analysis, constraints and recommendations for further study. Finally, Chapter 6 will state the conclusion that briefly describes the system.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In this chapter, it will show and discuss about the literature review, research about the system that has similar or related function with the E-Counseling. As an example, the system that similar to this project are online counseling, E-therapy and so on. In this chapter it will also describe about the technique and tools that are required and suitable to this project. All the information that required in this chapter can get from research on available similar project that have developed before this.

2.2 Current Implementation of Counselling System

Based on the study of the current system, there are weakness have been found about the manually system of counsellor unit. Normally in counselling session, long time are required to get information, to share and discuss a problem that student face it. During counselling session all the useful information are recorded manually by counsellor on paper. The paper might be disappear, torn or steal by someone. No security mechanism and there have no guarantee that the information are not steal or manipulate by someone. The information stored are not systematically. Counsellor need to find the information of certain student one by one if they want to revise the file again or to make the previous information as revision to new case. It will be a big problem and hard for counsellor if there have a large number of student record. After get all the useful information from the counselling session, counsellor make an analysis and come out with an early conclusion. Finally give the solution and motivation advised based on the problem occur. The flow process of the manual system for the evaluation method was shown in the Figure 2.10-2.12.

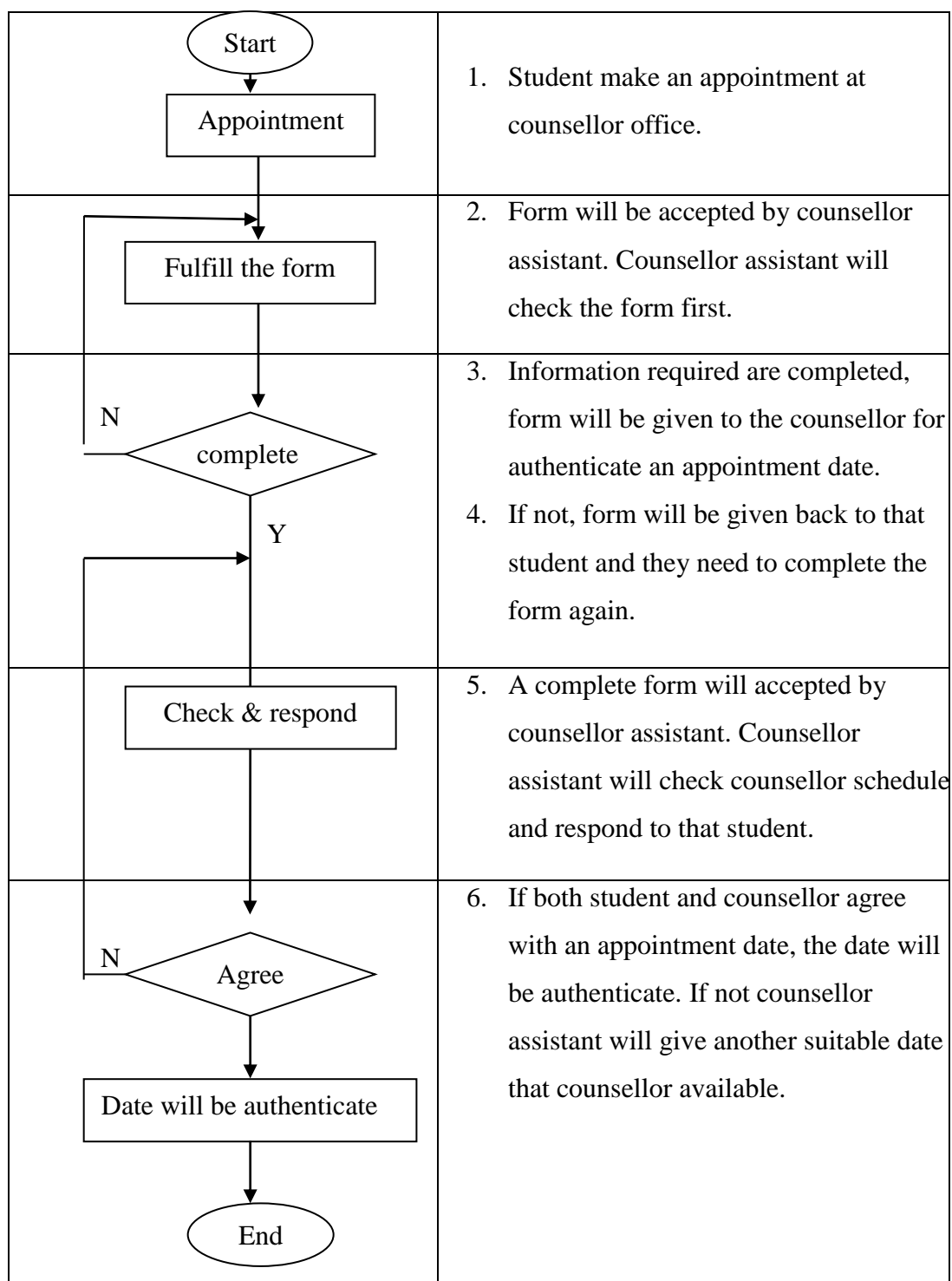


Figure 2.10 : Flow process of apply an appointment

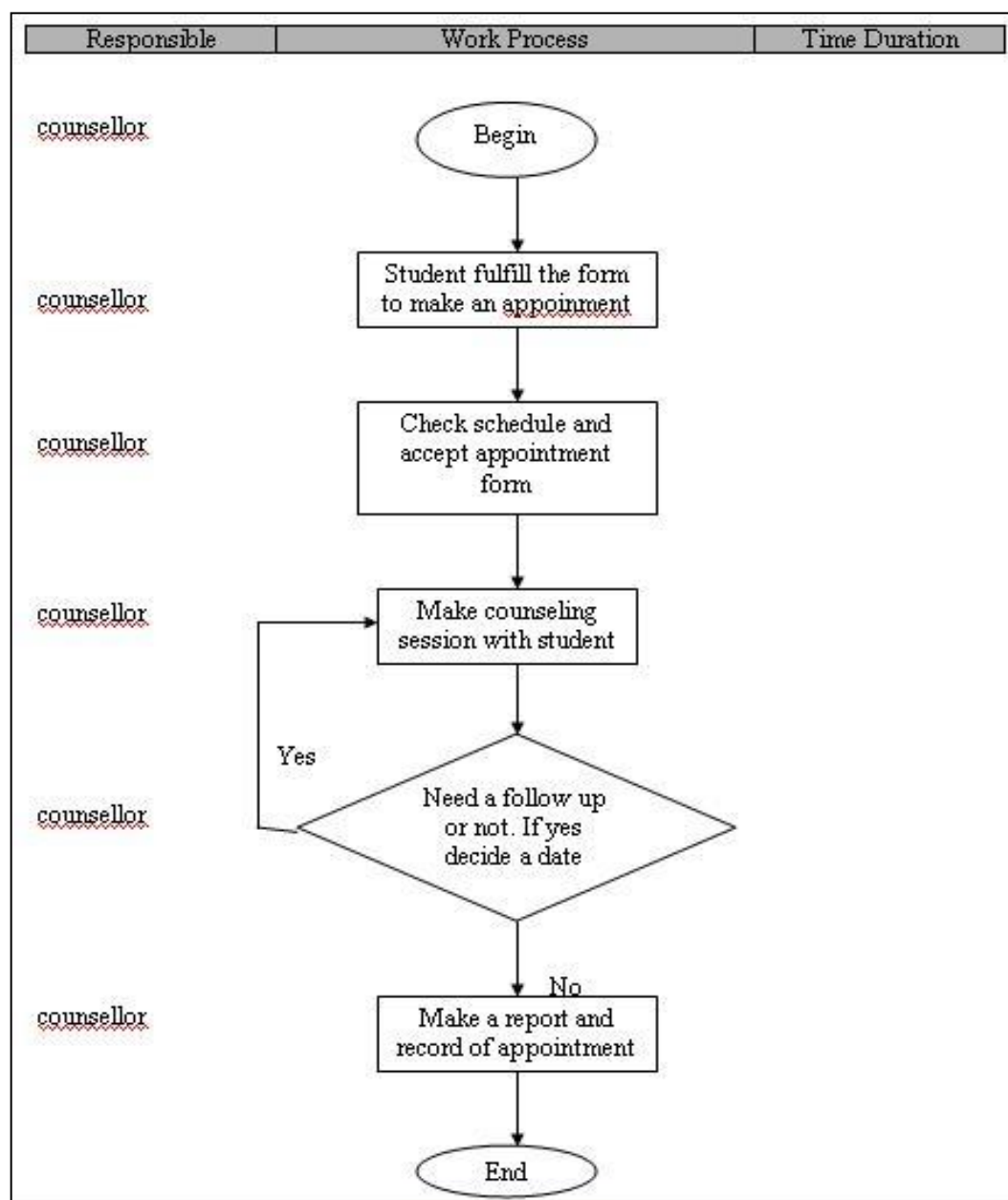


Figure 2.11 : Flow process of counseling session for student who come willingness

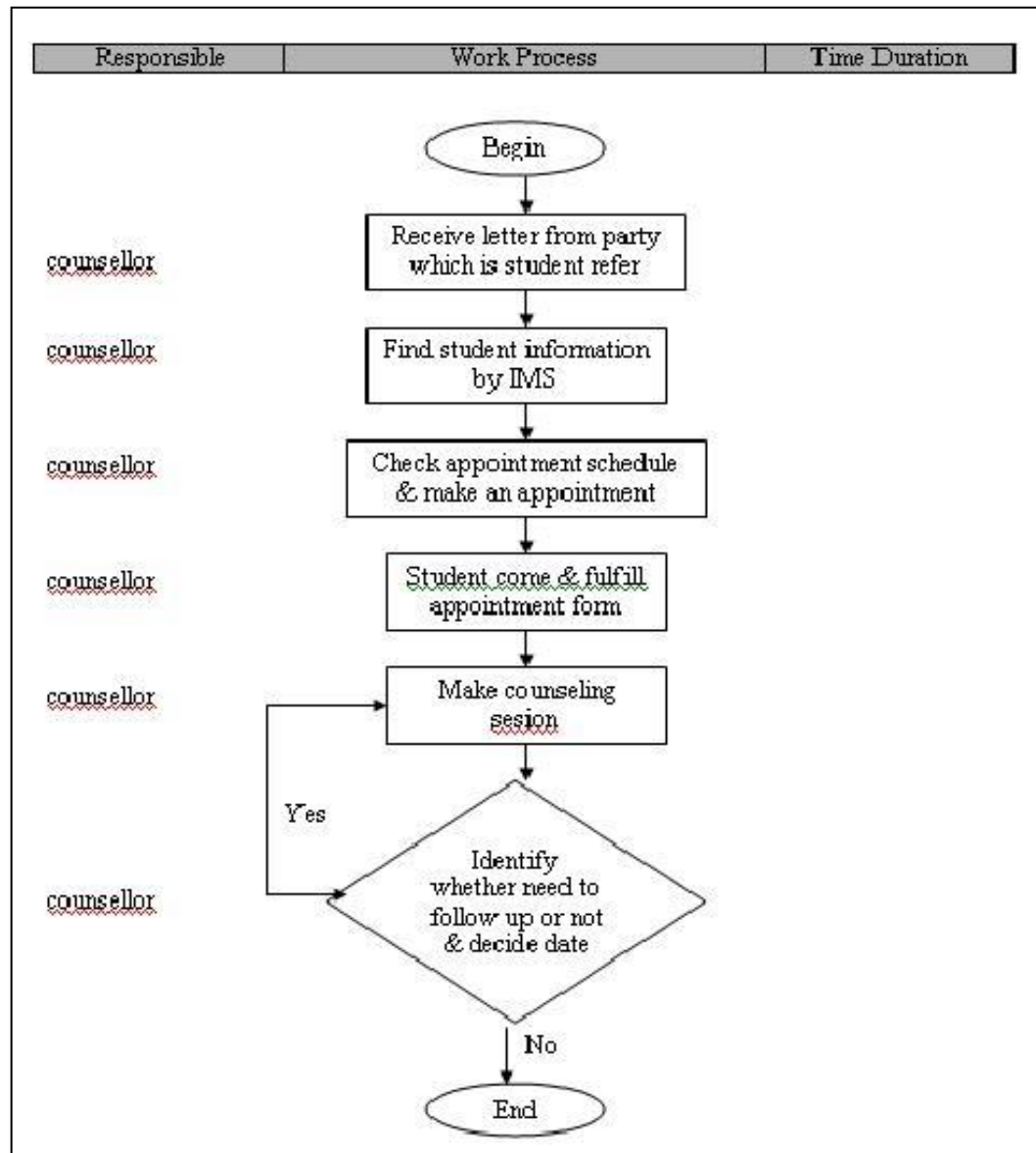


Figure 2.12 : Flow process of counseling session for student who is referred.

Figure 2.10 - 2.12 shows the overall process of current manual system from applying an appointment (Figure 2.10), then make a counseling session and follow up session based on how critical the case. For overall, the process between figure 2.11 and figure 2.12 are almost same, just only a little big different on a handling work based on student situation.

2.3 Study on Related System

The research has been made to find out an example of the related system with e-Counselling. In this study, will be describe about Relationship Help Online System and Evaluation of Kooth.com : E-counselling and Early Intervention service. From both system, I am doing a study about chat software that are use to this system, equipment that need to be able to do e-counselling, scope of user, services, what circumstances might online counselling not be appropriate, chat protocols and others that related to my future system.

2.3.1 Relationship Help Online System

Relationship Help online is the online counselling service offered by Relationships Australia NSW. Online counselling has been developed in order to extend access to their counselling services - especially to people in rural and remote areas, who can't access face-to-face counselling. The Relationship Help Online counsellors are staff of Relationships Australia NSW. This means that they have gone through the Relationship Australia selection process, and have the necessary qualifications and experience in relationship counselling. All staff who do online counselling are also trained and supervised specifically in regard to providing counselling online. Counselling on this website is conducted via real-time secure chat. They take every precaution to protect confidentiality and security, however, communication over the Internet always carries a degree of risk [5].

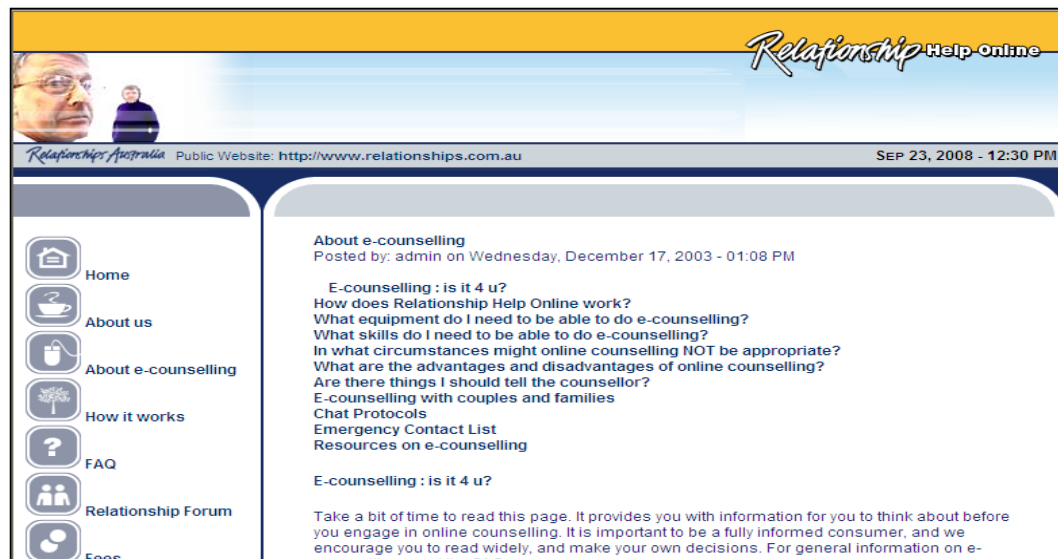


Figure 2.13 : Interface of Relationship Help Online System [5]

- i. Chat software that are use to this system.

This system use Relationship Help Online which is real-time chat services. This means that client make an appointment with a counsellor, and at appointed time, both client and counsellor communicate at the same time, by typing. This system use chat software, MSN. Counselling in this website is between one client and one counsellor [5].

- ii. Equipment do client need to be able to do e-counselling

The equipment required to do e-counselling for this available system is a computer or lap top with internet access and if have broadband or a fairly fast connection, that was more helpful. Client do not need to download any special software to use this system [5].

iii. What circumstances might online counseling NOT be appropriate

In this article, there have state that circumstances of clients which is might be online counselling are not appropriate to use. Clients and counsellor should aware of that circumstances below :

- If client are in a crisis situation, which case client had been advised to call one of the emergency numbers listed that had be given.
- If client personal safety is an issue that could include a domestic violence situation or suicidal feelings.
- If client need specialist medical treatment for a physical condition.
- If client suffer from a mental illness.

iv. Advantage of this available system

There have many advantages of e-counselling system that have been stated in this article :

- Anonymity which mean some people feel safer and are able to be more open to share problem with counsellor.
- Convenience which mean greater flexibility and options in appointments. Client can make an appointment any time and anywhere.
- Time efficiency which mean client do not need to take time off work or travel anywhere and time consuming will be reduced.
- Cost-effective which mean the cost for online system is less than face-to-face counselling such as travel cost, child-care cost and other cost can be eliminated.

v. Disadvantage of this available system

There have many advantages of e-counselling system that have been stated in this article :

- Text Based communications often 'truncate' the communication which may lead to misunderstandings. Client and counsellor would say more in a face to face situation better than typing with each others [5].
- Non-verbal cues normally present in a conversation are not accessible, increasing the risk of misinterpretation for both client and counsellor. Counsellors are trained in how to communicate tone, feeling, humour etc, but these can more easily be misinterpreted. Sometimes client have to say "out loud" what the counsellor would be able to deduce if they could see client [5].
- Sometimes situations are too complex to be adequately conveyed in text messages and therefore the online contact may need to be supplemented by telephone counseling [5].

vi. Chat protocols

Since there is no body language online, people often use smilies to show their emotions or actions. This article state some useful symbols that client or counsellor may use during a chat session [5].

- If there have more to say, but want to get part of thoughts on screen, end post with ..., press SEND, then continue with another post.
- WB = Welcome Back
- BTW = By The Way
- AFAIR = As Far as I Remember
- DK = Don't Know
- Most common smilies : :) = smile, :(= frown, :'(= crying

vii. Other services provided

This available system also offer some services that is set up individual counselling on relationship issues. This services can include client partner or a family member by arranging separate appointments [5]. There is some ways or options offer to client who want to use this services:

- Counselling options for an individual :
Face to face, telephone, email or e-counselling
- Counselling options for a couple :
Join session : Face to face or telephone
- Individual session : Email or e-counselling
- Counselling options for a family where all are in the same
location : Face to face, telephone, email or video conference.

2.3.2 Evaluation of Kooth.com : E-Counselling and Early Intervention Service

This evaluation was undertaken by Ms L Hale, Customer Care Manager (SMBC) due to external evaluator, identified early in the progress report to the ISB, failing to engage [7].

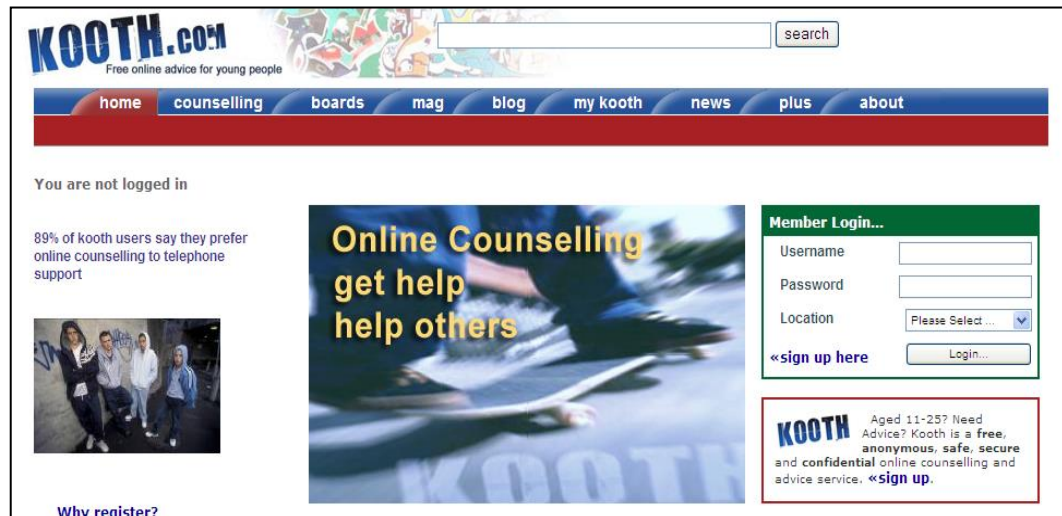


Figure 2.14 : Interface of Kooth.com [7]

i. Description of project

To establish an integrated confidential transactional online counselling and advice service available in the community through the internet accessible 24 hour a day and 7 days per week. The service to incorporate a new multi agency rapid response family support team based in the community, also operating 7 days per week and outside of traditional office hours. The 'Kooth' service, to be aimed at young people in need of support and particularly those more reluctant to access services in the traditional face to face manner [7].

ii. Description of Service

Kooth.com provides online access to counselling and support for young people in need. Kooth aims to work in partnership with both statutory and voluntary agencies in order to provide the most appropriate form of intervention at a stage that may prevent further more intensive support being required at a later date. 'www.kooth.com' is a website offering information, advice, support and counselling. The website is easy to use and self explanatory. The site has recently been hyperlinked to 'U R SORTED', another website designed by SMBC in partnership with Xenzone for young people, parents and practitioners. This site offers an A-Z of services and contains articles/publications relating to a range of issues relevant to young people (e.g. drugs, money, family relationships, housing, health, disabilities, education). A young person can also access the Kooth online magazine for information on various topical matters. Articles for inclusion in the magazine can be submitted [7].

Young people can access the Kooth website and just browse through the content. There is universal access to public message boards. These are moderated message boards where a young person can initiate a discussion topic by posting a message and waiting for replies to be posted to it from other Kooth users including the Kooth counsellors managing the site. The messages range from what may be deemed a simple expression of unhappiness to a detailed description of a problematic situation. The replies to the messages posted on the public boards are all moderated by the Kooth counsellors. A young person may access these boards merely to read the ongoing messaging discussion and in doing so may receive indirect advice/support regarding their own situation. Each young person registered with Kooth.com is allocated their own private message board. They can use this to post questions, problems or write messages to the counsellors who will aim to reply within 24 hours. This message board

can only be viewed by the individual user and the counsellors. Online live chats with individual counsellors can be booked in counsellor if the sessions become on going, this is to avoid conflicting advice being given and duplication of work [7].

iii. Coursework Management

The counsellors, who each have their own clinical supervisor (under BACP guidelines) work from home and meet fortnightly as a group to discuss their ongoing work. They will look at issues raised, action taken and outcomes. The case notes taken are confidential to each counsellor and permission is needed before a counsellor can access another's notes. The service manager can access all case notes. Cases are discussed in the fortnightly group forum and any ongoing concerns are fully explored. Problematic behavior on the website would be brought to the fortnightly forum or in an emergency directly to the service manager. Offensive/abusive messages are not published and the user is informed and provided with an explanation. Users can be removed from the site so that they cannot log in if their behavior is not acceptable. Due to the anonymity provided this does not however prevent them re-registering as with another name and continuing to use the site [7].

Conclusion that I can stated about Kooth.com system are they do not stated security value in detail in this system and they discuss more about target of user, their services, website linkage with their system and user expectation of user about their system. Advantage from this system is they make a relationship and cooperate with another agency to make their service more widely and include most type of problem such as counselling on drugs addict, social problem and others. They also give a training to their worker to be a good counsellor to make user satisfied with counsellor services.

2.4 Comparison between Two Related Systems

There are a numbers of available Online Counselling Systems on the market. Below is table consists the differences, similarities and also features that are available on selected Online Counselling system on market.

Table 2.1 Comparison between two related system

Name Of System	Relationship Help online	KOOTH.com
Type of System	Web-based System	Integrated Web-based System
Module	Consist of : i. User Registration ii. Real Time Chat Services iii. Forum	Consist of : i. User Registration ii. Forum iii. Online Chat
Scope	Focus on everyone	Focus on young people
Developer	Relationships Australia NSW	Xenxone
Origination	International Product	International Product

From the comparison table, every system that available on market nowadays does provide benefits to client. In term of features that they offer, most of the available system provides function that important and useful in order to help client build their trust before meet counsellor face to face and to help out counsellor manage and control workload.

2.5 Cryptography

Generally, cryptography mean secret writing. Cryptography are for :

- i. Keep secret. Avoid message from exposed to not authenticate user and covert the secret of message.
- ii. Complete. To ensure that sending message are not modify by other party.
- iii. Authenticate. Allowed receiver authenticate the original message.
- iv. Integrity. Sender cannot deny that they are not sending the message.

Cryptography are consist of two class such as classic cryptography and modern cryptography. For this sub topic, I will only discuss in detail about modern cryptography. It is use key system to provide security of message. The key cannot be exposed and only know by sender and receiver. This cryptography algorithm will be solve by computer software. Modern cryptography system can be categorize by two general category such as secret key system (symmetric cryptography system) and public key system (asymmetric cryptography system) [3].

2.5.1 Symmetric Cryptography

This method focus on uses of same key ($K=K'$), encrypt key K and decrypt key K' as shown in Figure 2.15 in order to encrypt message and to decrypt cipher text. This key are call as secret key. This key are use by both (sender and receiver) to encrypt and decrypt message which is send to them. For those who know this secret key, they can build cipher text that connected with original text and read its contain. By ensure the security of secret key communication, this secret key must be keep secret and only know by individual involved. Example of symmetry cryptography are Data Encryption Standard (DES) and International Data Encryption Algorithm (IDEA) and Advance Encryption Standard (AES) [3].

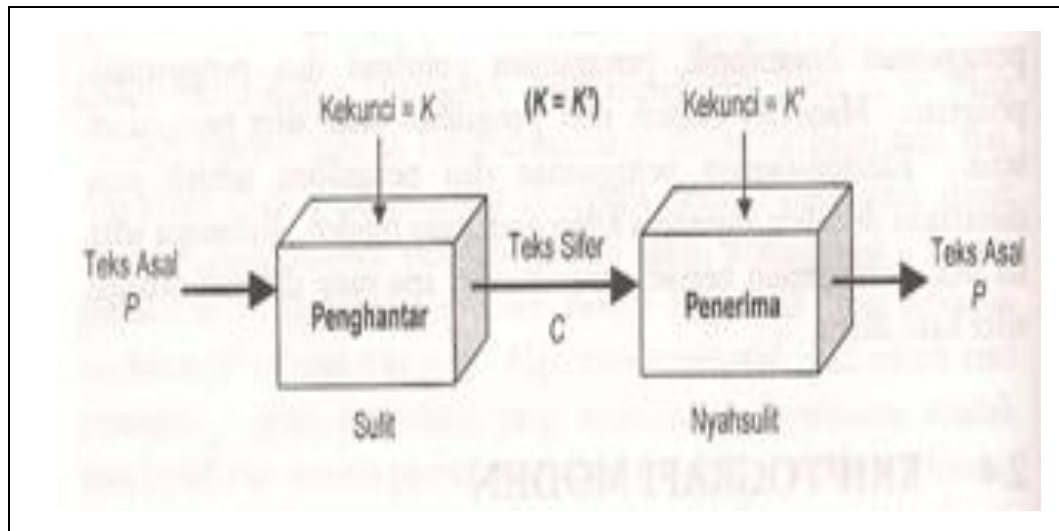


Figure 2.15 : Symmetric cryptography [3]

Message which is encrypt using key K, must be decrypt using the same key also. If Alia encrypt message using key K, so she must use the same key to get back original message. That is mean, if cipher text was send to Borhan, hence Borhan need use the same key also to get original message. This process called key share [3] .



Figure 2.16 : Cryptography of symmetric key [3]

For online counseling there have and may use large data transmission during conversation. Advantage of this key is its ability to encrypt large data faster than asymmetric cryptography [3]. The usage of one key can use in encryption and decryption process between two communicate entity. Other than that, there still have disadvantage in cryptography of symmetric key :

- i. if third party succeed get the key, hence message can encrypt again by third party.
- ii. problem during distribution key process. Encrypt and decrypt key are the same key and cannot exposed. Distribution of secret key process must be done in safety path to ensure key will be not stolen [3]. Management of encrypt key are complicated.
- iii. Only allowed communication between two entity over secret path. Each pair of entity need to have their own secret key for each communication path. Because of that, if more than one communication path from same or different entity occur, so more than one secret key are needed. Each communication path use one secret key to encrypt message and produce one communication path for two entity or certain message [3].

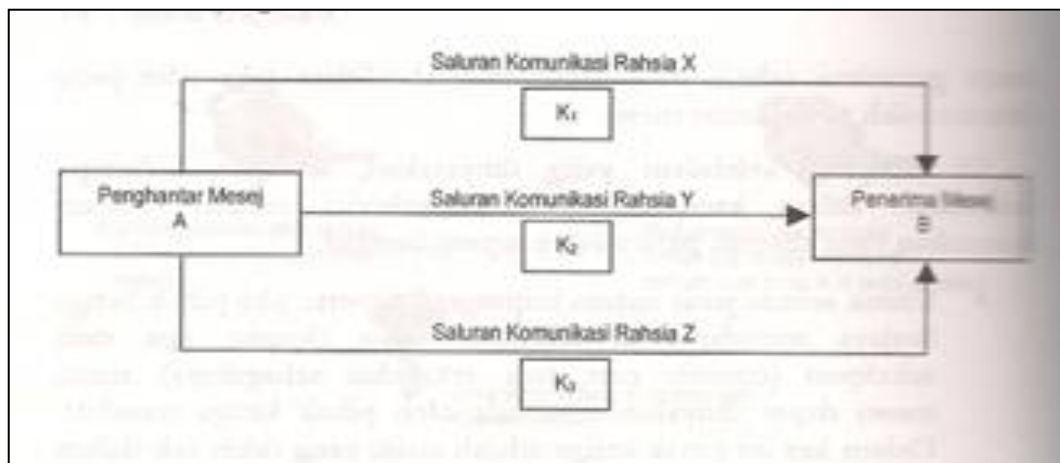


Figure 2.17 : Distribution key in private communication path [3]

AES is acronym for Advanced Encryption Standard. In 1997, National Institute of Standard and Technology (NIST) had start one process to choose encryption key symmetry algorithm which is can use to protect federation information. NIST had choose the best five algorithm from fifteen algorithm such as MARS, RC6™, Rijndael (AES), Serpent and Twofish which is proposed by variety cryptography group research after doing an analysis, discussion and research. Function of turning Rijndael have 4 layer. First layer S-box 8x8 will be used at each byte and called as *Byte Substitution*. Second layer, row will be to produce ambiguous message. This layer called *Shift Row*. Third layer column will mix and operate at level to produce ambiguous intra column and called as *Column Mixing*. Lastly, fourth layer, encryption process start and finish with increasing key [3].

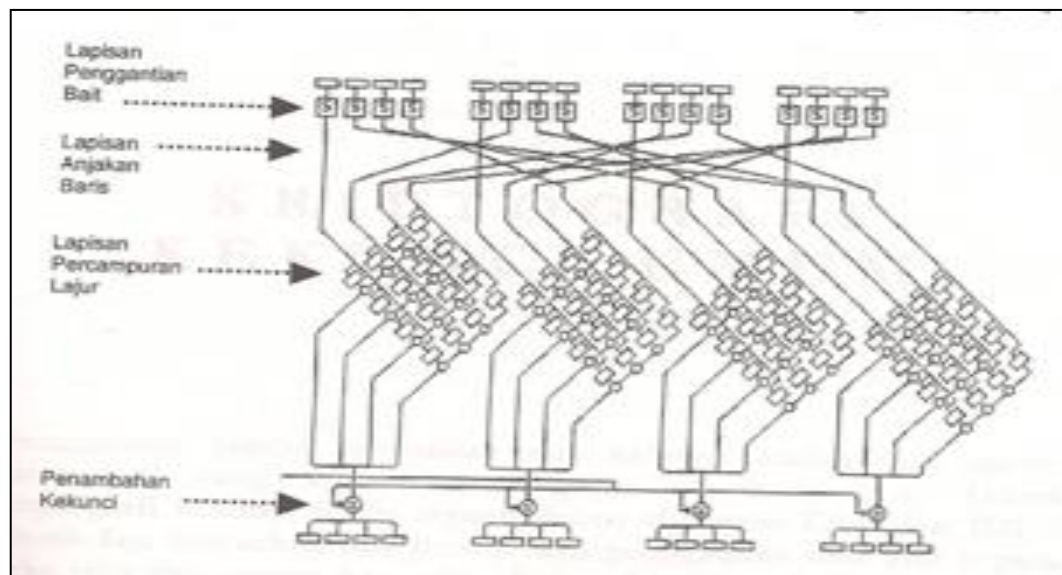


Figure 2.18 : AES structure [3]

Why I choose AES algorithm for implement in my system because of following advantages :

- i. Cipher AES is 3 times more faster than DES.
- ii. Small size of cipher and can apply in environment which is have limit size of RAM and ROM.
- iii. Can operate perfectly in variety platform include 8-byte platform, 64-byte and DSP
- iv. Short time of key production
- v. Give full support for block and key which is size 128 byte, 192 byte, and 256 byte in variety combination.
- vi. Support any block and key multiple of 32.

2.5.2 Asymmetric Cryptography

This method focus on uses of different key ($K \neq K'$), encrypt key K and decrypt key K' as shown in Figure 2.19 in order to encrypt message and to decrypt cipher text. This key are call as secret key. Both of different key are recognized as private key and public key. Private key will do encrypt process while decrypt process will do by public key [3]. Public key need not to be keep secret in order to allow someone encrypt message with that key but only the receiver (who has a private key) can decrypt that message.

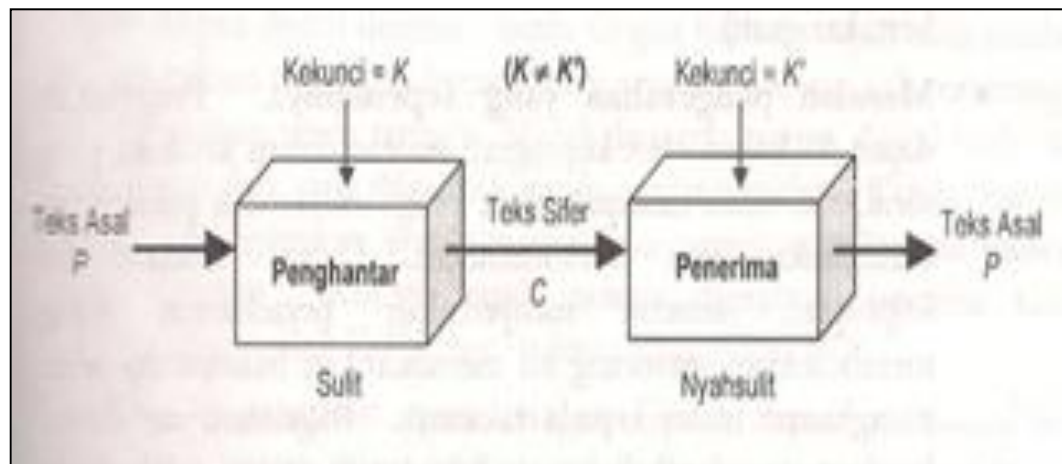
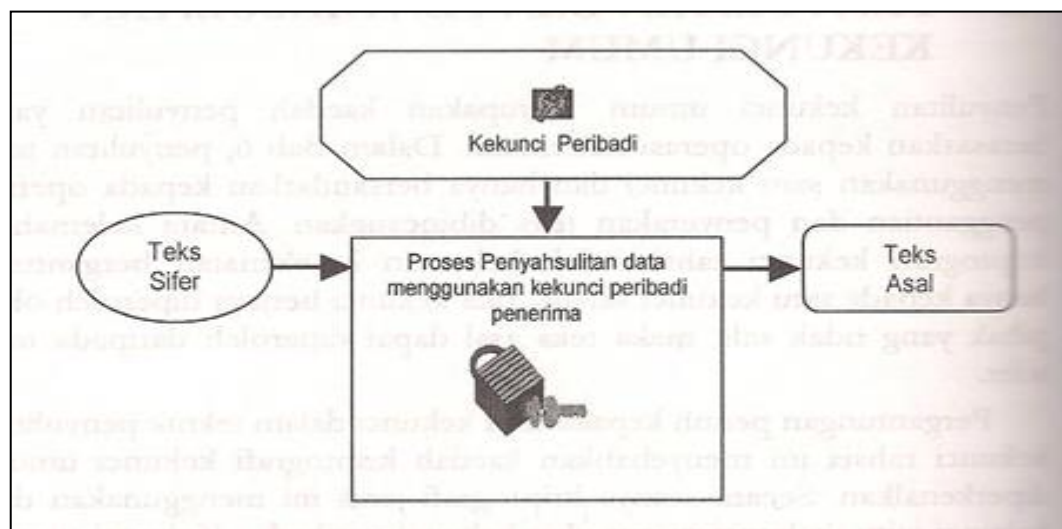
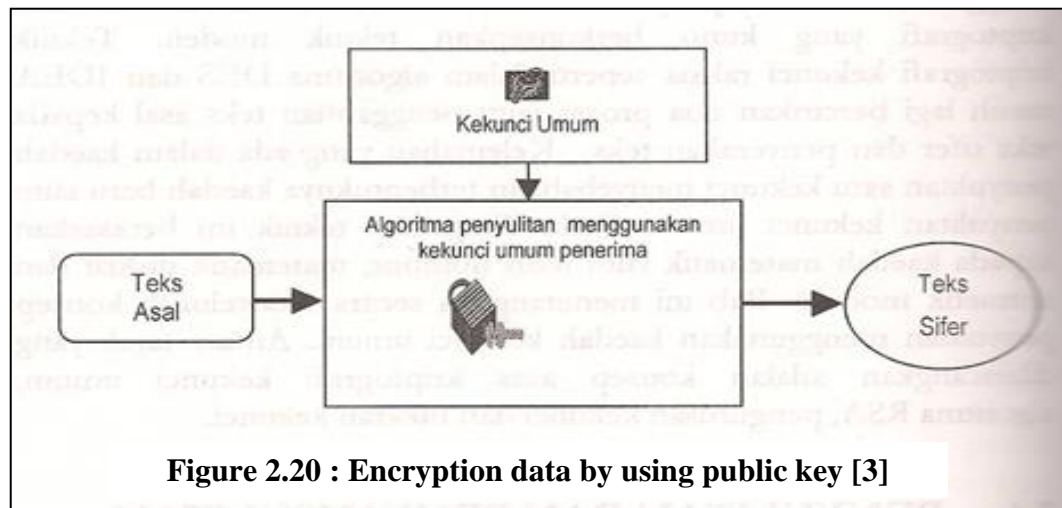


Figure 2.19 : Asymmetric cryptography [3]

Both following figure shown that origin text can encrypt using public key of text acceptor. For example, if text is for Ali, so public key of Ali that use to encrypt text and data will be sent to Ali in cipher text. Ali will use his remain private key for decrypted cipher text that he accepted by using encrypted algorithm. cipher text will be change to the origin text after decrypted [3].



2.5.3 Digest Message

The usage of digest message is for authenticate complete data. Large message will be mapped by hash function as input and produce large message that have permanent size as output. A generate digest message will be send with original data input to receiver. Receiver will generate new digest message by using arrival original data input. If that new generate digest message is same with arrival digest message, hence, receiver can prove that arrival data input are not modify by other party. Example of hash algorithm which is use for digest message are MD2, MD5, Secure Hash Algorithm (SHA) and Hash Message Authentication Code (HMAC) [3].

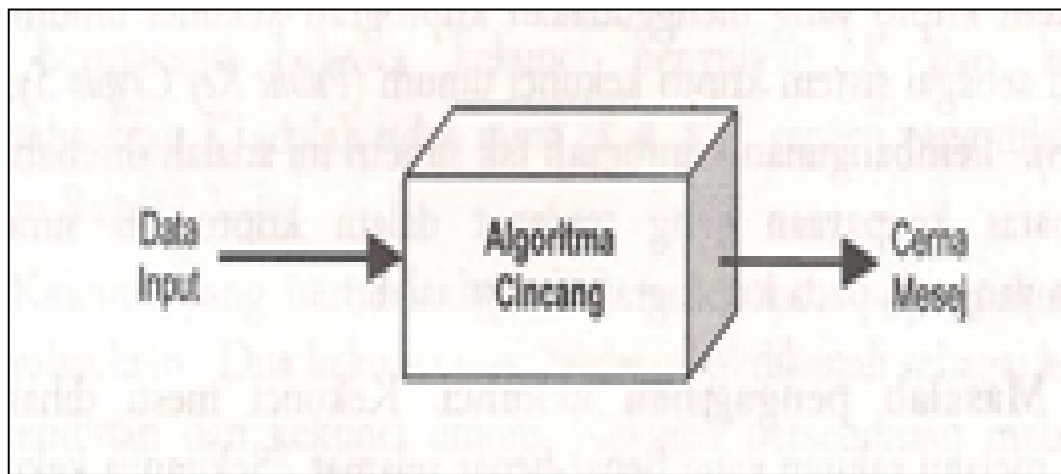


Figure 2.22 : Digest message [3]

CHAPTER 3

METHODOLOGY

3.1 Introduction

For overall, this chapter discussed about the methodology and techniques that will be used to develop this system and also discuss more detail of each phase of project methodology. This system used the Software Development Life Cycle (SDLC) as the methodology to develop the system. The aim of this chapter is to give clear about approach, framework for the project, method, technique, hardware and software necessity.

3.2 Project Methodology

SDLC is Software Development Life Cycle that generally used by software developer as models or methodologies for the system that will be developed. SDLC is the basis of models or methodologies used to develop the systems. The systems development life cycle (SDLC) is a conceptual model used in project management that described the stages involves in the system development [2]. In SDLC, there are five phases, such as planning, analysis, design, implementation and maintenance.

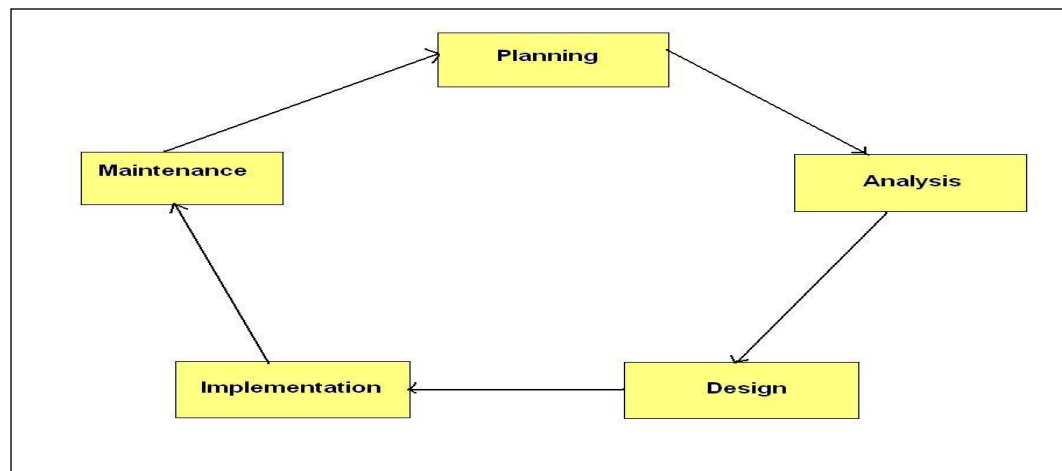


Figure 3.10 : The phase of SDLC [2]

There have some research about SDLC :

Table 3.1 : Strengths and weakness of SDLC.

Strengths	Weakness
Control.	Increased development time
Monitor Large projects.	Increased development cost.
Detailed steps.	Systems must be defined up front.
Documentation.	Hard to estimate costs, project overruns

3.2.1 Planning

Planning is the first phase in the SDLC. In this phase, system development team must know what they want to developed. They have to determine what are required requirement in the present market by doing a researches, surveys and project proposal. This phase is the most critical step in the system development. They have to make sure that the activities are coordinate efficiently and able to manage the project risks. The depth and formality of project plan should be equivalent with the characteristics and risks of the project [2]. I was planning my project schedule by doing a Gantt Chart which is divided into two as shown in Appendix A.

3.2.2 Analysis

The second phase in the SDLC is analysis which is system requirements are studied and structured [2]. Analysis has two sub phases. The first is requirements determination where the analyst works with users to determine what the users want from the proposed system. All requirements needed are gathered by conducting some interview with the counselor, Puan Paridah Mat Ali and some student of UMP. During this interview we have discuss about what problem counsellor and student face from the manual system, the improvement to counter the problem and expectation from my project. The list of interview question and answer with counsellor provided at Appendix B and C. Other than that I had made questionnaire in order to know the respond of user/student UMP. The number of respondent are 30 person, 15 male and 15 female which is come from different faculty. The result of survey analysis was shown at figure 3.11 – 3.15. The second is analyst study the requirements and structure them according to their inter-relationship and eliminate any redundancies. Some research of manual applications and collection of counseling appendices had been made at the JHEPA to get overview of the related process and to detail out the scope of this system.

3.2.2.1 Analysis on Questionnaire

Below are the result and analysis of questionnaire that I was made. The sample of questionnaire and the sample of questionnaire answered by respondent shown in Appendix D.

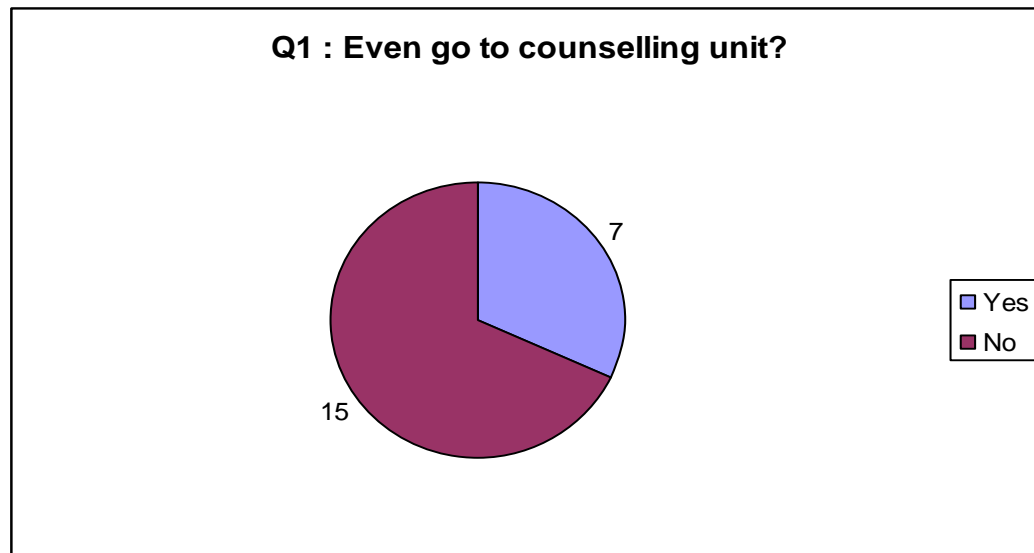


Figure 3.11 : Survey analysis on question 1

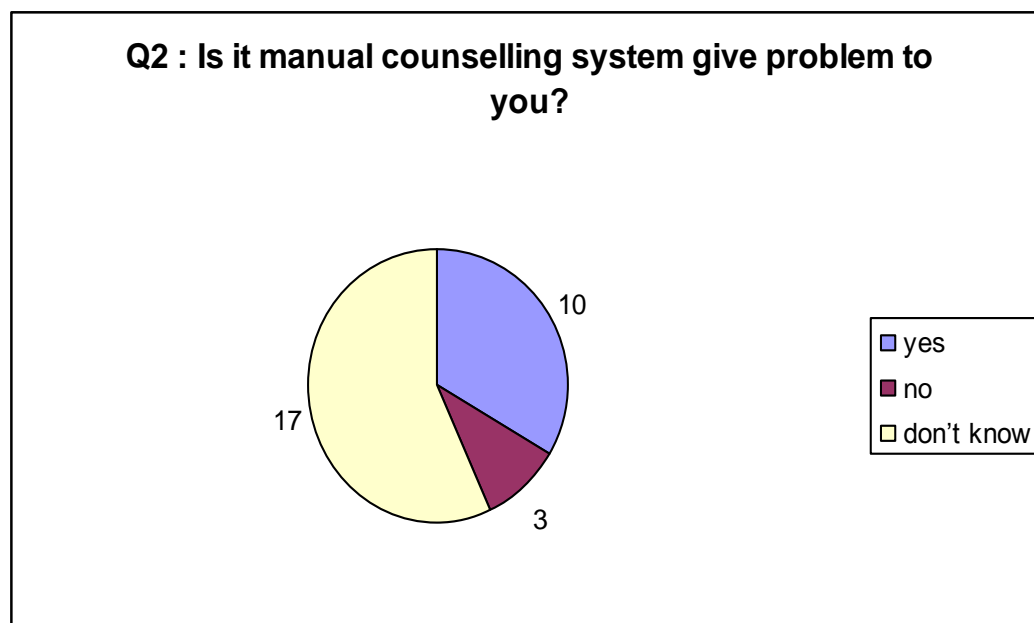


Figure 3.12 : Survey analysis on question 2

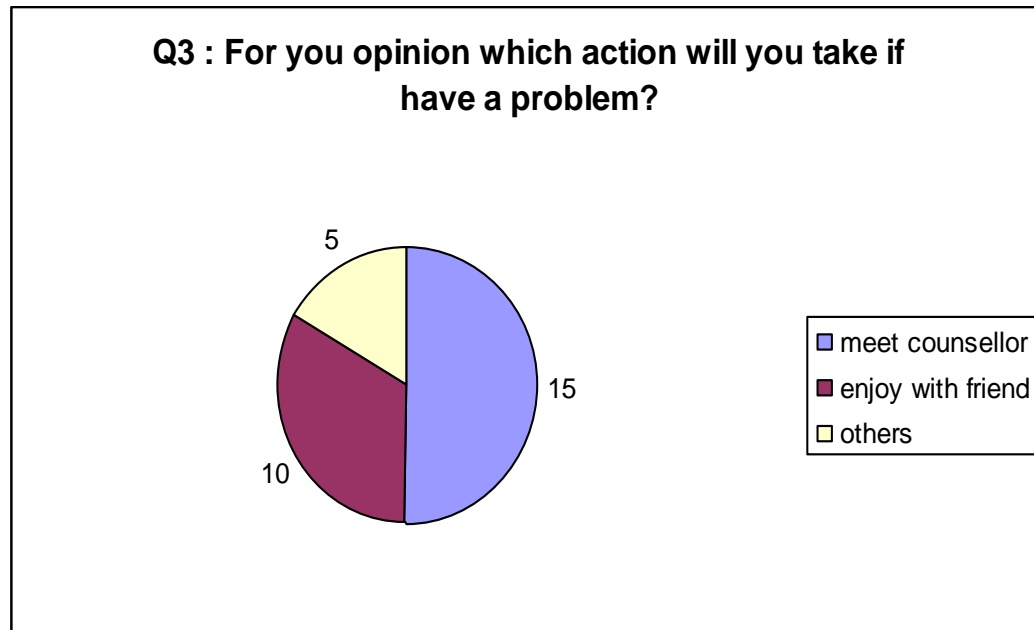


Figure 3.13 : Survey analysis on question 3

For question 3, respondents need to give answer based on 3 choices provided. If respondents choose 'others' answer, respondents must state the example. Mostly, they more prefer to settle down their problem individually without anyone know or share it with friend.

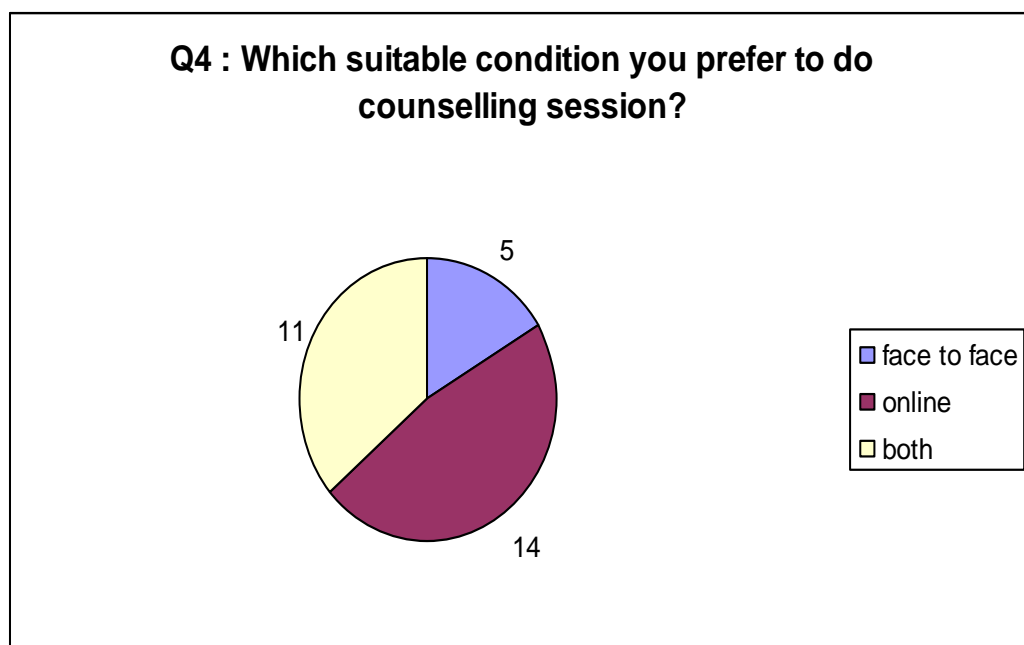


Figure 3.14 : Survey analysis on question 4

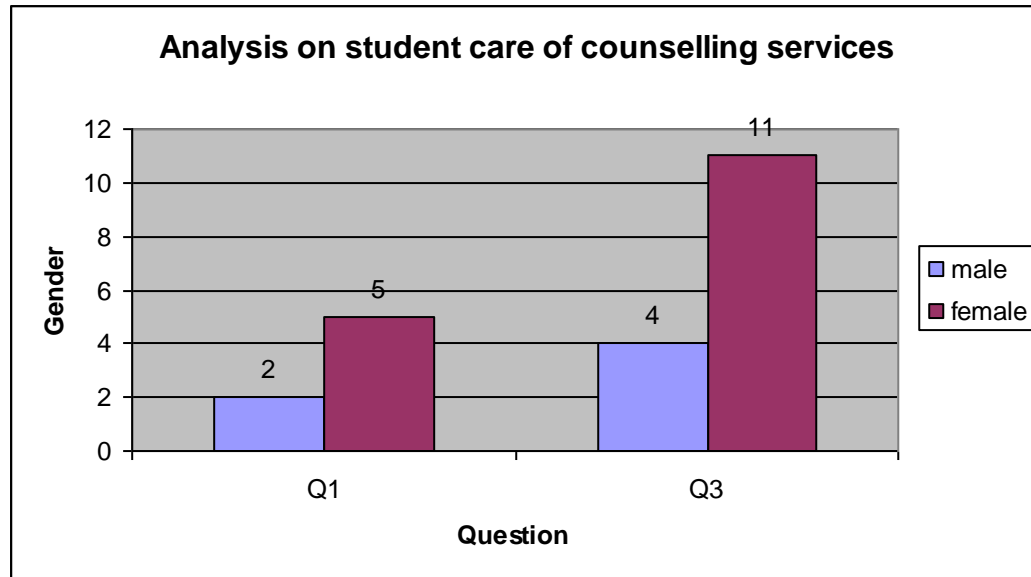



Figure 3.15 : Survey analysis on student care of counseling services

The result of analysis of figure 3.15 was taken from survey analysis on question 1 and question 3 which is I divide respondents by gender. From the analysis result, it shown that male student lack of interest with counseling than female student. I made this survey because according to an interview session with counsellor before this, student are seldom come to counselling unit to meet counsellor or share problem especially male student. So from my proposed system

3.2.2.2 System Requirements

Figure 3.16 shows the requirement information needed during counseling session. This form have two side page, in front side which is fulfill by student and back side which is fulfill by counsellor. But this form is to simple and counsellor more prefer to use another one form which is more detail shown at figure 3.18 - 3.19.



BORANG PERTEMUAN
UNIT KAUNSELING, KERJAYA & ALUMNI
JABATAN HAL EHWAL PELAJAR & ALUMNI

NAMA PELAJAR :
 NO MATRIK :
 NAMA KAUNSELOR :
 MASA :
 TARIKH :

Sila tandakan (✓) di dalam petak berkenaa
 Saya bertemu kaunseling kerana:

☐ Sesi kaunseling ☐ Dirujuk Sukarela
☐ Pengesahan sijil/pengesahan aktiviti/pengesahan pelajar
☐ Perbincangan persatuan/kertas kerja/aktiviti
☐ Lain-lain : Sila nyatakan

Tandatangan Pelajar

Figure 3.16 : Appointment form (in front side)

Untuk diisi oleh kaunselor

Catatan Kaunselor

.....

.....

.....

.....

Tindakan Kaunselor

.....

.....

.....

.....

Perlu Sesi Pemantauan? ☐ Ya ☐ Tidak

Catatan :

Perlu Dirujuk? ☐ Ya ☐ Tidak

Catatan :

Figure 3.17 : Appointment form (back side)

UNIT KAUNSELING, KERJAYA & ALUMNI
JHEPA, UMP

BORANG MAKLUMAT KLIEN

NO. RUJUKAN : **TARIKH :**

Nama :

Umur :

Jantina :

Bangsa :

Agama :

Pendidikan :

Pekerjaan :

Alamat surat-menyurat :

Alamat tempat tinggal :

No. Telefon : (R) (P) (H/P)

E-mail :

Status perkahwinan :

Latar belakang keluarga :

Ibu (termasuk umur/dll) :

Bapa (termasuk umur/dll) :

Masalah fisiologikal/psikologikal :

Adik beradik (termasuk status perkahwinan/umur/dll) :

Masalah fisiologikal/psikologikal :

1

Figure 3.18 : Student information form (page 1)

UNIT KAUNSELING, KERJAYA & ALUMNI
JHEPA, UMP

Isu yang dikongsikan :

Sejarah kesihatan (Fisiologikal & Psikologikal) :

Pengambilan dadah / alkohol / dll :

Pengalaman diinstitusikan / rawatan psikiatri :

Sejarah kemalangan & kecederaan :

Ubat-ubatan (Dengan preskripsi doktor) :

Pengalaman kaunseling :

Kaunselor yang dipilih : 1. Lelaki 2. Perempuan

Catatan / Penilaian Kaunselor :

T/Tangan : No. Pendaftaran :

Nama Kaunselor : Tarikh :

2

Figure 3.19 : Student information form (page 2)

Requirement information of appointment form and student information form above, guide me to create and build student module (registration and online appointment request) and others. I also use this information to create a database table. Flowchart of counseling session that I got from counsellor, shown at Appendix F - G, was made as a reference to build system workflow, system design such as module would implement in the proposed system.

3.2.3 Design

Next phase in SDLC is design. After determined cost project and approved planning, the developing of architecture of the system can be start. The design phase involves converting the informational, functional and network requirements identified during the initiation and analysis phases into unified design specification [2]. Functions and operations are described in detail, including screen layouts, business rules, process diagrams and other documentation within data flow diagram (DFD), system design and database design. The output of this stage will be to describe the new system as a collection of modules or subsystems. The following figures below, show the flow of how each users of this system collaborate.

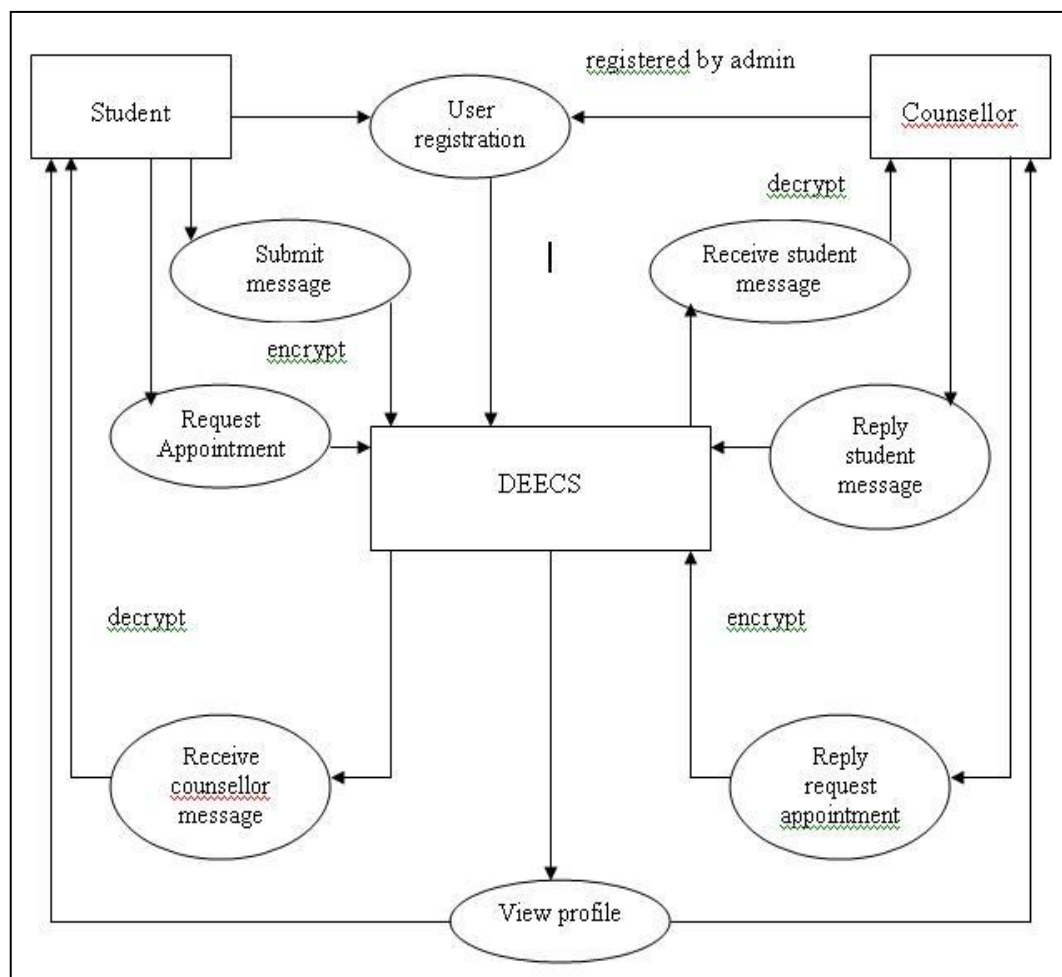


Figure 3.20 : Flow of overall system in general

The figures below show interface of typing message

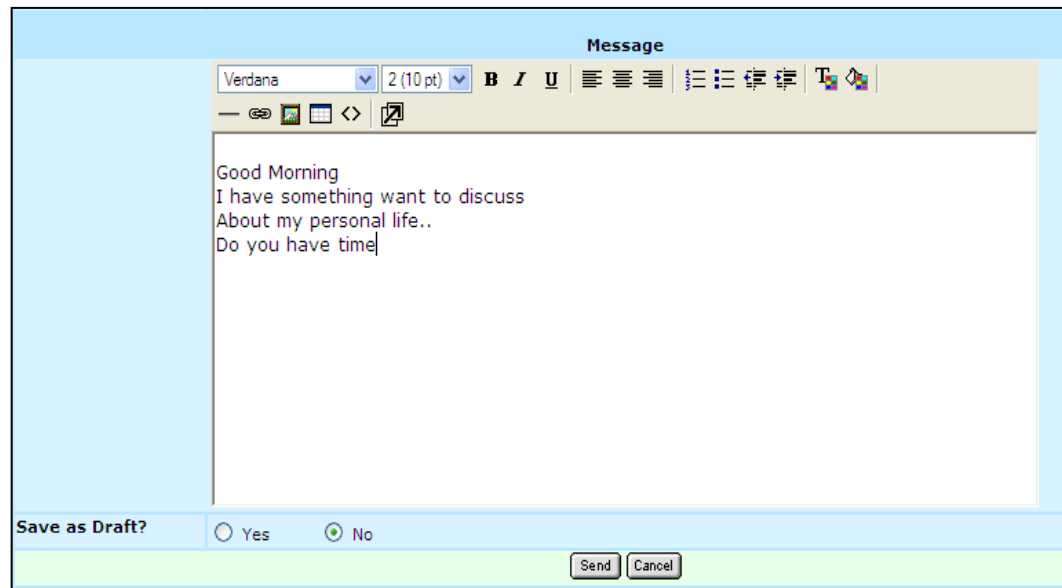


Figure 3.21 : Typing message

Below are process occur in the system after user press button 'send'.

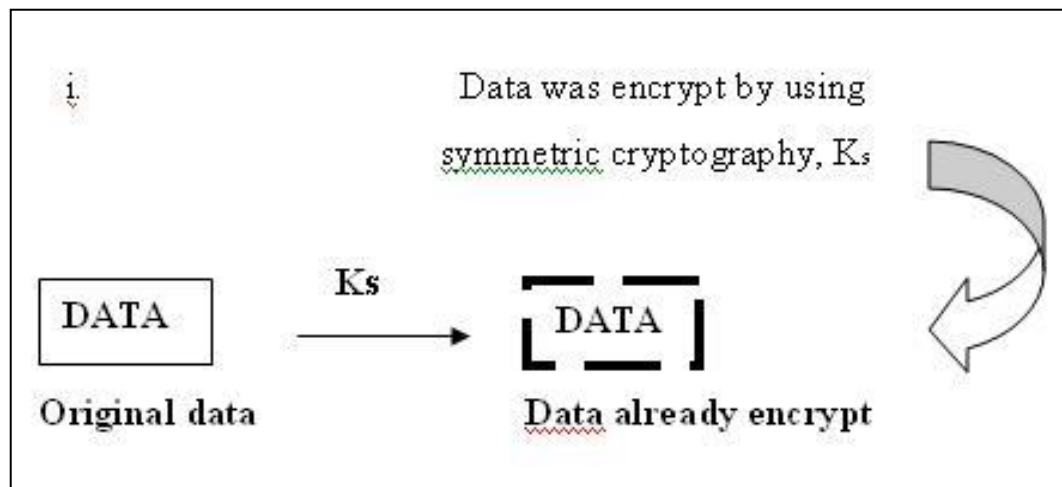


Figure 3.22 : Data encryption process in hybrid system [3]

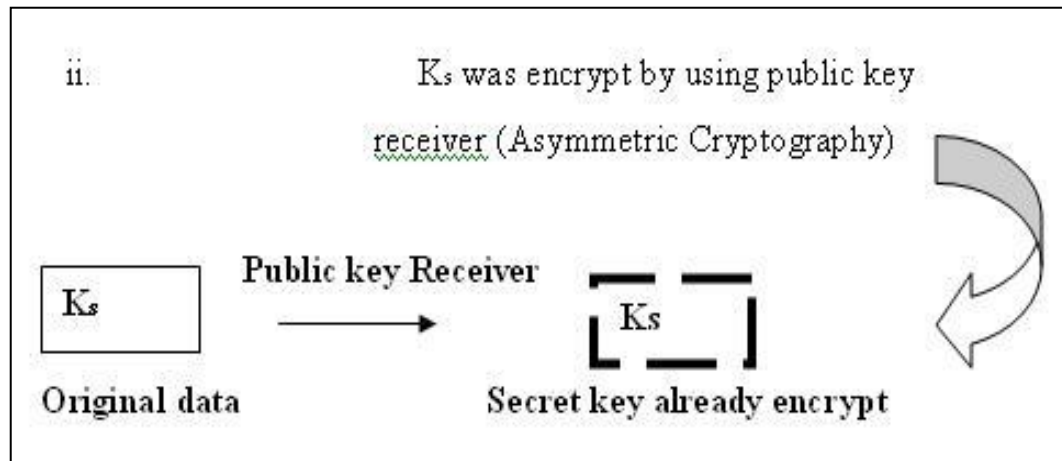


Figure 3.23 : Secret key encryption process in hybrid system [3]

3.2.3.1 Business Modeling Workflow

The goal is to understand the business of the organization, usually confined to the scope of the business that is relevant to the system being developed. On this process all the possible users of this system are identified. The users identified for this *DEECS* are student and counsellor. The relation between these users is drawn in the context diagram below. A context diagram is constructed to show a graphical model of the information of this system. It is used to show the interaction between a system and other actors.

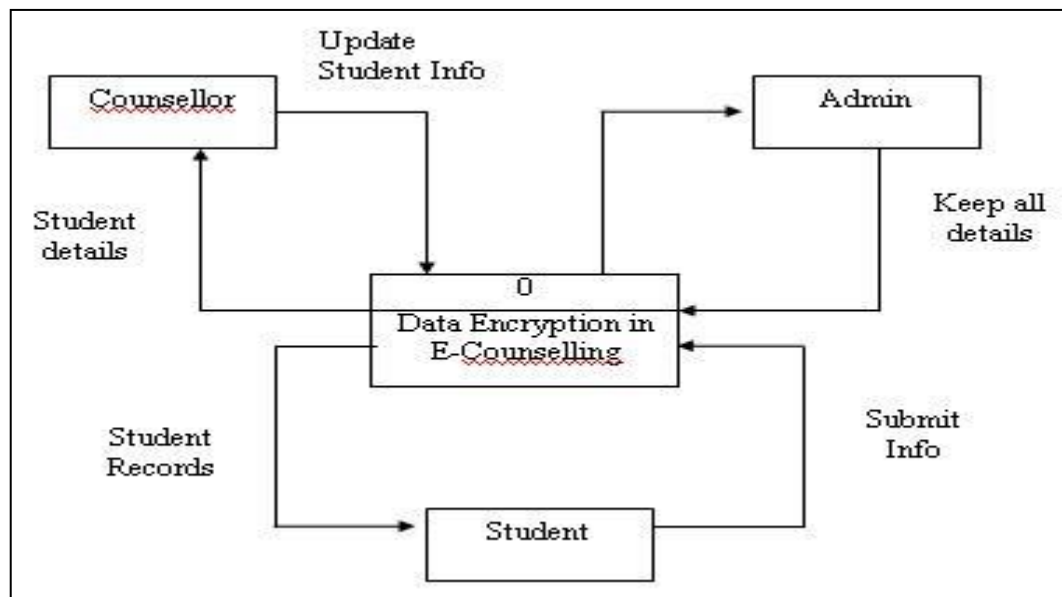


Figure 3.24 : Context diagram for DEECS

3.2.3.2 Data Flow Diagram

Figure 3.25 below is the Data Flow Diagram of this system. That diagram illustrated how information moves through various processes and how people outside the system provide and receive information.

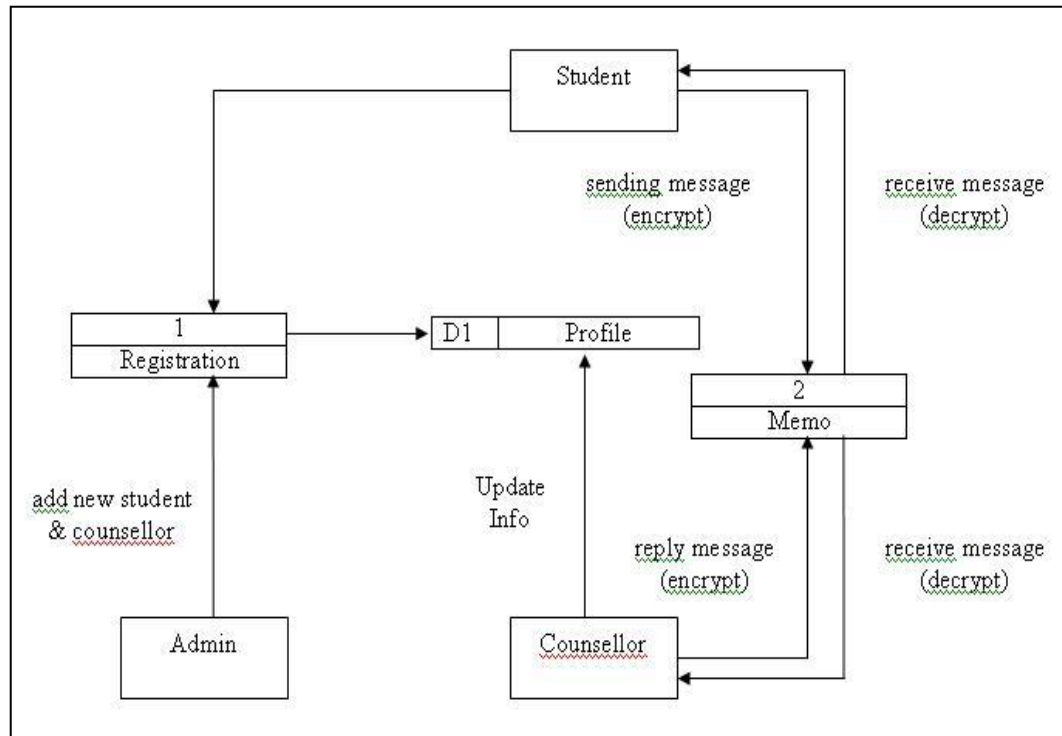


Figure 3.25 : DFD for DEECS

3.2.3.3 Database Design

The following table below had shown the database design for this system. There are eight table that are used in this system which are *studinfo*, *staffinfo*, *compose*, and *request* table. Entity Relationship Diagram (ERD) below, show the relationship between all tables.

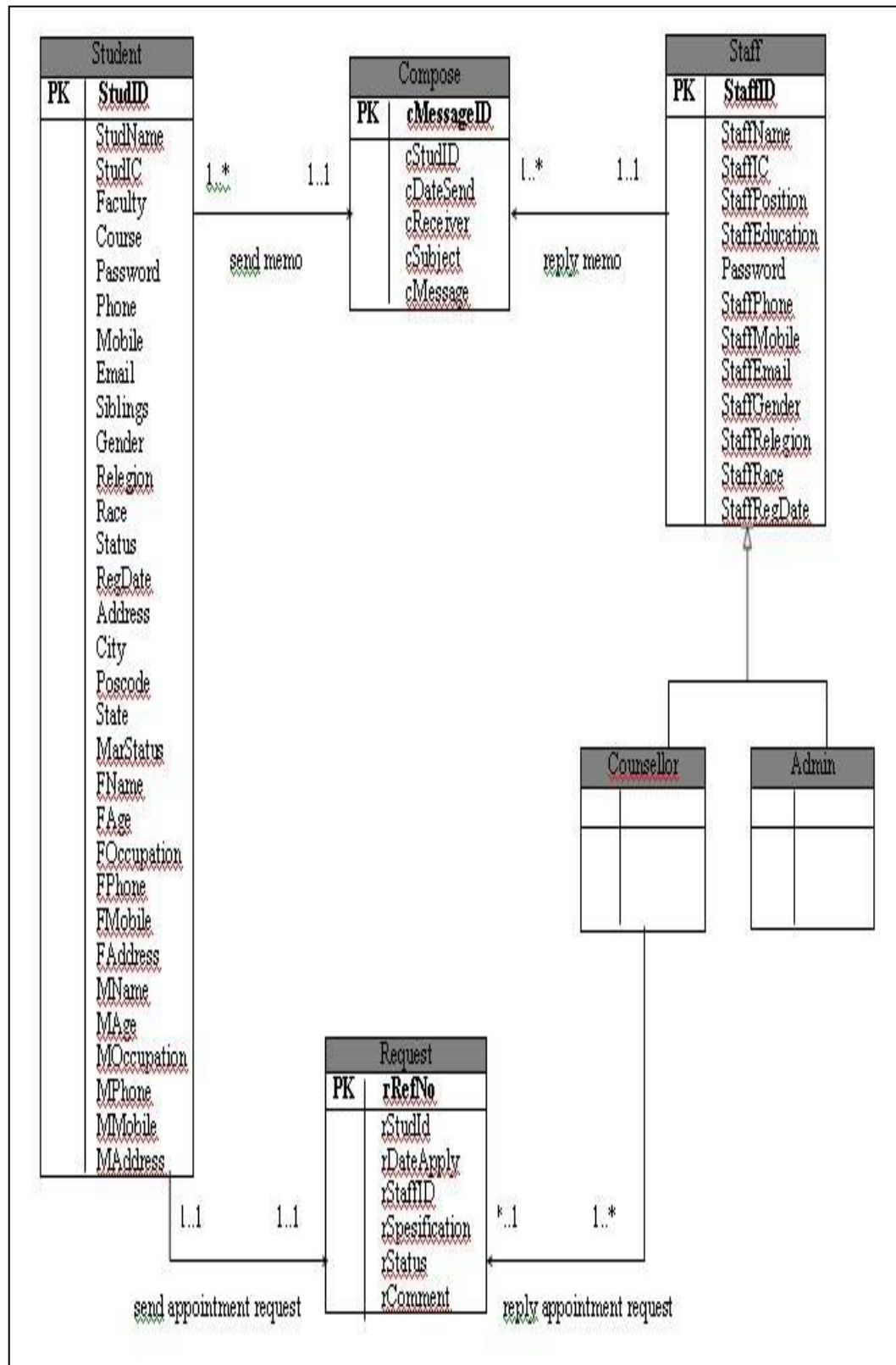


Figure 3.26 : ERD for DEECS

Table 3.2 – 3.5 are details up the attributes needed for each table.

Table 3.2: Table *studinfo*

Field Name	Data Type	Constraint
StudName	varchar(70)	
StudID	varchar(7)	PK
StudIC	varchar(12)	
Faculty	varchar(50)	
Course	varchar(50)	
Password	varchar(8)	
Phone	varchar(10)	
Mobile	varchar(10)	
Email	varchar(20)	
Siblings	varchar(2)	
Gender	varchar(6)	
Relegion	varchar(20)	
Race	varchar(20)	
Status	varchar(8)	
RegDate	varchar(10)	
Address	text	
City	varchar(20)	
Postcode	varchar(6)	
State	varchar(20)	
MarStatus	varchar(8)	
FName	varchar(50)	
FAge	varchar(3)	
FOccupation	varchar(50)	
FPhone	varchar(10)	
FMobile	varchar(10)	
FAddress	text	
MName	varchar(50)	
MAge	varchar(3)	
MOccupation	varchar(50)	
MPhone	varchar(10)	
MMobile	varchar(10)	
MAddress	text	

Table 3.3 : Table of *staffinfo*

Field Name	Data Type	Constraint
StaffName	varchar(70)	
StaffID	varchar(7)	PK
StaffIC	varchar(12)	
Position	varchar(50)	
Education	varchar(50)	
Password	varchar(8)	
StaffPhone	varchar(10)	
StaffMobile	varchar(10)	
StaffEmail	varchar(20)	
StaffGender	varchar(6)	
StaffRelegion	varchar(20)	
StaffRace	varchar(20)	
StaffRegDate	varchar(10)	

Table 3.4 : Table of *compose*

Field Name	Data Type	Constraint
cMessageID	int(7)	PK
cStudID	varchar(7)	
cDateSend	varchar(10)	
cReceiver	varchar(70)	
cSubject	text	
cMessage	text	

Table 3.5 : Table of *request*

Field Name	Data Type	Constraint
rRefNo	varchar(10)	PK
rStudID	varchar(7)	
rDateApply	Varchar(10)	
rStaffID	varchar(7)	
rSpecification	text	
rStatus	int(7)	
rComment	text	

3.2.3.4 Interface Design

The following Figure 3.27 is a prototype interface for this project.

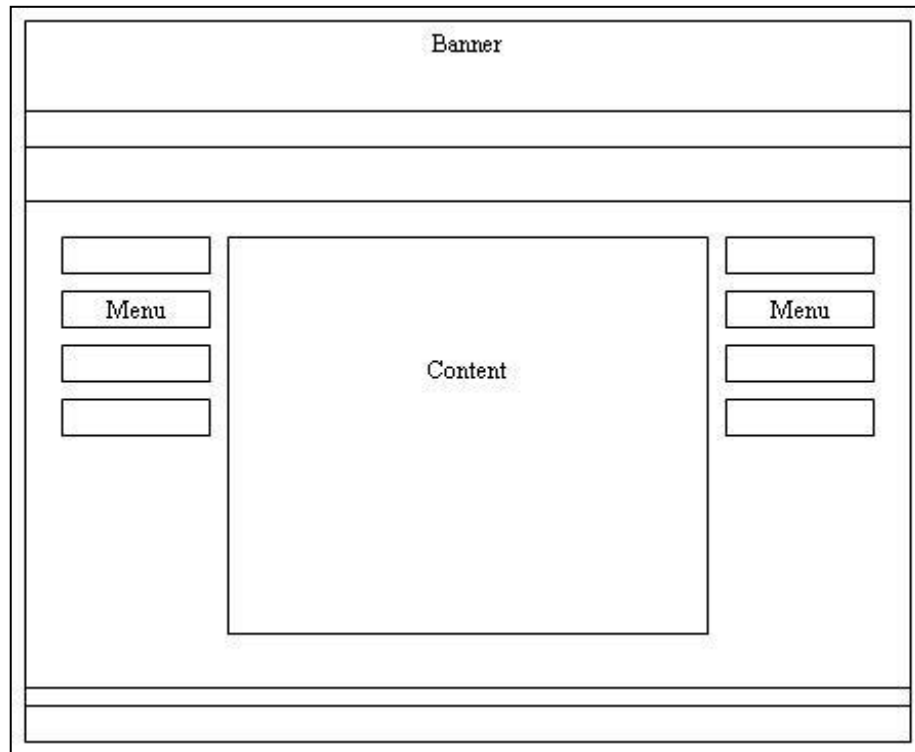


Figure 3.27 : Prototype interface of DEECS

3.2.3.5 System Design

This system will have three (3) types of features which are :

- i. Student Registration Module
 - This module are responsible for all the registration process that happen in this E-Counselling System (ECS)
- ii. Sending Data Module
 - This module is able student and counsellor to communicate with each other during counselling session
- iii. Manage Student Details
 - System must continuously update the database for any new information or changes on student details.

3.2.4 Implementation

Implementation is the next phase in SDLC. In this phase, the information system consist of coded, tested, installed, and supported in the organization. During implementation, analysts turn system specifications into a working system. The activities are divided into two parts. The first part involves the coding, testing and installation and the second part involves documentation, training and support. The purpose of this activities is to convert the physical system specifications into working and reliable software and hardware, documented the work, and provide help for users and care of the system [2].

Once the coding had begun, the testing can begin and proceed in parallel. System will be test incrementally starting by test the module by unit, by integrate the module and then test the overall system. In this phase every module in DEECS was tested. The system was tested to make sure that it can run well and achieve the objective. The program test cases are based on the specification. The following items below are module in DEECS that has been tested.

- i. Testing on student registration function
 - Enter a wrong password
 - Try to enter input of phone number in 'char' not 'int'
- ii. Testing on sending memo in student module
 - Try to submit message in encrypted form
 - Check at database whether message was saved in encrypted form or not
 - Insert wrong counsellor ID
- iii. Testing on read message in counsellor module
 - Try to decrypted message in cipher text to original text
 - Try to reply student message and encrypt it

- iv. Testing on student appointment request
 - Try to not select the counsellor in charge and send request
- v. Testing on view appointment status in student module
 - Try to view whether the status of appointment is update or not after counsellor reply the appointment request

The installation is a process where the current system is replace by the new system [2]. This process also involved converting the existing data, software, and documentation to the new system. Documentation will be prepared for the system. About the user training process, it will not be a problem because there have user manual about the system and help make users understand and know to use the new system as provided at Appendix H.

3.2 Hardware

Below are hardware that used in this system :

Table 3.6 : Hardware specification

Item Type	Minimum Requirement	Quantity
Laptop	Intel(R) Pentium(R) M processor 1.80GHz Standard 101/102-Key or Microsoft Natural PS/2 Keyboard 55.7 GB (hard disk) 504MB (RAM)	2
Printer	CANON PIXMA IP 1600	1
Pen Drive	Kingston 2 GB	1
External Hard Disk	HITACHI HD-SIDI-45	1

3.4 Software

Below are software that used in this system :

Table 3.7 : Software specification

Item Type	Detail Description	Version	Purpose
Word Processor	Office 2003	Office Professional	To make a report, presentation, documentation
Schedule	Microsoft (MS) Project 2003	Office Professional	To make a project schedule
Antivirus	AVIRA AntiVir Personal	8.1.0.331	To protect laptop from viruses
Interface Design	Macromedia Dreamweaver 8	2004	To make an interface design & coding for developing system
Database	MySQL Database	4.14.0.0	Storage of all information

Why I choose this software because it is easy for me to make a design of my system and automatically get coding. I only just add some coding to make the system run effectively and can link directly for each system interface. Macromedia Dreamweaver also have PHP language that will be use in my system.

3.4.1 PHP

PHP, originally derived from *Personal Home Page* Tools, now *PHP stand for Hypertext Preprocessor*. Nowadays, PHP is a widely-used general-purpose scripting language that originally design for producing dynamic web pages that can be embedded into HTML. PHP can be used to connect to a database such as MySQL [4]. User can be able to retrieve data, add or update content in the web page. There are several of advantages when using PHP :

- i. developers can quickly create high performance Web sites
- ii. dynamically generated Web sites
- iii. flexibility and ease of use
- iv. data types and structures of PHP are easy to use and understand.

3.4.2 MySQL Server

MySQL is an open source relational database management system (RDBMS). The program runs as a server providing multi-user access to a number of databases. Information in a MySQL database is stored in the form of related tables. MySQL databases are queried using a subset of the standard Structured Query Language (SQL) commands and use for web application development. MySQL database has become the world's most popular open source database because of it is consistent fast performance, high reliability and easy to use [4].

CHAPTER 4

IMPLEMENTATION

4.1 Introduction

In this chapter, it will devote to describe the implementation of the project. The implementation stage of software development is the process of converting a system specification into an executable system.

4.2 MYSQL Statement

This system is using MYSQL as database platform in this software project development. All the data collected will be stored in the MYSQL database. This database consists of 8 tables which are *studinfo*, *staffinfo*, *compose* and *request table*. The SQL query for creating database and tables are shown in figure below.

```
create database 'ecounselling';
```

Figure 4.10 : MYSQL query to create database

```

CREATE TABLE `studinfo` (
  `StudName` varchar(70) NOT NULL,
  `StudID` varchar(7) NOT NULL,
  `StudIC` int(12) NOT NULL,
  `Faculty` varchar(50) NOT NULL,
  `Course` varchar(50) NOT NULL,
  `Password` varchar(8) NOT NULL,
  `Phone` int(10) NOT NULL,
  `Mobile` int(10) NOT NULL,
  `Email` varchar(20) NOT NULL,
  `Siblings` varchar(2) NOT NULL,
  `Gender` varchar(6) NOT NULL,
  `Relegion` varchar(20) NOT NULL,
  `Race` varchar(20) NOT NULL,
  `Status` varchar(7) NOT NULL,
  `RegDate` varchar(10) NOT NULL,
  `Address` text NOT NULL,
  `City` varchar(20) NOT NULL,
  `Postcode` int(6) NOT NULL,
  `State` varchar(20) NOT NULL,
  `MarStatus` varchar(7) NOT NULL,
  `FName` varchar(70) NOT NULL,
  `FAge` int(3) NOT NULL,
  `FOccupation` varchar(50) NOT NULL,
  `FPhone` int(10) NOT NULL,
  `FMobile` int(10) NOT NULL,
  `FAddress` text NOT NULL,
  `MName` varchar(70) NOT NULL,
  `MAge` int(3) NOT NULL,
  `MOccupation` varchar(50) NOT NULL,
  `MPhone` int(10) NOT NULL,
  `MMobile` int(10) NOT NULL,
  `MAddress` text NOT NULL,
  PRIMARY KEY (`StudID`)
)

```

Figure 4.11 : MYSQL query to create 'studnfo' table

```
CREATE TABLE `staffinfo` (
  `StaffName` varchar(70) NOT NULL,
  `StaffID` varchar(7) NOT NULL,
  `StaffIC` int(12) NOT NULL,
  `StaffPosition` varchar(50) NOT NULL,
  `StaffEducation` varchar(50) NOT NULL,
  `Password` varchar(8) NOT NULL,
  `StaffPhone` int(10) NOT NULL,
  `StaffMobile` int(10) NOT NULL,
  `StaffEmail` varchar(20) NOT NULL,
  `StaffGender` varchar(6) NOT NULL,
  `StaffRelegion` varchar(20) NOT NULL,
  `StaffRace` varchar(20) NOT NULL,
  `StaffRegDate` varchar(10) NOT NULL,
  PRIMARY KEY (`StaffID`)
)
```

Figure 4.12 : MYSQL query to create 'staffinfo' table

```
CREATE TABLE `compose` (
  `cMessageID` int(7) NOT NULL auto_increment,
  `cStudID` varchar(7) NOT NULL,
  `cDateSend` varchar(10) NOT NULL,
  `cReceiver` varchar(70) NOT NULL,
  `cSubject` text NOT NULL,
  `cMessage` text NOT NULL,
  PRIMARY KEY (`cMessageID`)
)
```

Figure 4.13 : MYSQL query to create 'compose' table

```
CREATE TABLE `request` (
  `rRefNo` int(10) NOT NULL auto_increment,
  `rStudID` varchar(7) NOT NULL,
  `rDateApply` varchar(10) NOT NULL,
  `rStaffID` varchar(7) NOT NULL,
  `rSpecification` text NOT NULL,
  `rStatus` int(7) NOT NULL,
  `rComment` text NOT NULL,
  PRIMARY KEY (`rRefNo`)
)
```

Figure 4.14 : MYSQL query to create 'request' table

For this system, Figure 4.11 - 4.14 shows how tables are created using Integrated Development Environment (IDE) that is phpMyAdmin, where provide visual environment to create a table. There are two ways to creating a table which are through code or visual. The project implementation use visual ways to creating all tables.

4.3 PHP Code

One of the features in PHP is the ease of connection and manipulation of the database. PHP provide several functions for connecting to a wide range of database like MySQL [4]. The database manipulation is a major part to complete the system module in DEECS. DEECS have “add”, “edit”, “view” and “delete” function implemented in the database. The SQL command will be used in order to manipulate the data. The following figures below, will describe about the basic operation in this system such as *add*, *delete*, *update* and *view* data. I will show only student module operation as an example since the entire modules (counsellor modules) also use the same method. Others, only coding for main function (compose memo, request appointment and AES algorithm) was shown and discuss in this topic. The following PHP codes below are shown the some process in DEECS that had been converting into executable code.

```
35
36 //set the database connection
37 $dbHost = "localhost";
38 $dbUser = "root";
39 $dbPass = "";
40 $dbDatabase = "ecounselling";
41
```

Figure 4.15 : Variables declaration

Database connection is used to connect the database with the user interface. The connection must get the permission from the database server to access the database. It must include hostname, database name, user and password.

```

41
42 //connect to the database
43 $db = mysql_connect("$dbHost", "$dbUser", "dbPass") or die("Error conneting to database");
44 mysql_select_db("$dbDatabase", $db) or die ("Couldn't select the database");
45

```

Figure 4.16 : Database connection query

This function is used to add new data into the database. The query for basic adding function sample taken from the student registration module was shown in figure below.

```

46 mysql_query("INSERT INTO StudInfo
  (StudName,StudID,StudIC,Faculty,Course>Password,Phone,Mobile,Email,Siblings
  ,Gender,Relegion,Race,Status,RegDate,Address,City,Postcode,State,MarStatus,
  FName,FAge,FOccupation,FPhde,FMobile,FAddress,MName,MAge,MOccupation,MPhone
  ,MMobile,MAddress) VALUES ('".$Name."','".$ID."','".$IC."','".$Faculty.
  "','".$Course."','".$Password."','".$Phone."','".$Mobile."','".$Email."','".$
  ".$Siblings."','".$Gender."','".$Relegion."','".$Race."','".$Status."','".$
  $RegDate."','".$Address."','".$City."','".$Postcode."','".$State."','".$
  $MarStatus."','".$FName."','".$FAge."','".$FOccupation."','".$FPhone."','".$
  $FMobile."','".$FAddress."','".$MName."','".$MAge."','".$MOccupation."','".$
  $MPhone."','".$MMobile."','".$MAddress."')");
47
48 echo'<meta http-equiv="refresh" content="3" url=StudRegPreview.php>';
49 mysql_close($db);
50
51 ?>

```

Figure 4.17 : Registration new student

This function is used to delete existing data from the database. The query for basic deleting function sample taken from the student module was shown in Figure 4.18.

```

6
7  if ($_REQUEST['act']=="delete")
8  {
9    $id=$_REQUEST['id'];
10   $deletesql= "DELETE FROM compose WHERE cMessageID='$id'";
11   if($dresult = mysql_query($deletesql))
12   {
13     echo "<script language = 'Javascript'>
14     alert('Message Deleted Succesfully');
15     </SCRIPT>";
16   }

```

Figure 4.18 : Delete message

This function is used to edit existing data from the database. The query for basic editing function sample taken from student module was shown in Figure 4.19.

```

54
55  $query = "update StudInfo set StudIC = '". $IC. "',
Faculty = '". $Faculty. "', Course = '". $Course. "',
Password = '". $Password. "', Password = '". $Password.
"', Phone = '". $Phone. "', Mobile = '". $Mobile. "', Email
= '". $Email. "', Siblings = '". $Siblings. "', Gender = '".
$Gender. "', Relegion = '". $Relegion. "', Race = '".
$Race. "', Status = '". $Status. "', RegDate = '".
$RegDate. "', Address = '". $Address. "', City = '". $City
"', Postcode = '". $Postcode. "', State = '". $State. "',
MarStatus = '". $MarStatus. "', FName = '". $FName. "',
FAge = '". $FAge. "', FOccupation = '". $FOccupation. "',
FPhone = '". $FPhone. "', FMobile = '". $FMobile. "',
FAddress = '". $FAddress. "', MName = '". $MName. "', MAge
= '". $MAge. "', MOccupation = '". $MOccupation. "', MPhone
= '". $MPhone. "', MMobile = '". $MMobile. "', MAddress = '".
$MAddress. "' where StudID = '". $username1. "'";
56  $rs=mysql_query($query);
57

```

Figure 4.19 : Edit existing student query

This function is used to view existing data from the database. The query for basic view function was taken from student module was shown in Figure 4.20.

```

104 <?php
105
106 $query2 = "Select * from studinfo where StudID='$studid'";
107 $result2 = mysql_query($query2);
108 $row2 = mysql_fetch_array($result2);
109 ?>

```

Figure 4.20 : View existing data

Figure 4.21 show the query of compose operation. 'aes-lib.php' was called from this page which is contain AES algorithm that required in the operation to encrypt the message.

```

1 <?php
2 ob_start();
3 session_start();
4 require 'aes-lib.php';
5 include("EcConnect.php");
6 include("EcSession.php");
7
8 $timer = microtime(true);
9 $username1=$_SESSION['id'];
10 $lvl=$_SESSION['lvl'];
11
12 $pw = isset($_POST['pw']) ? stripslashes($_POST['pw']) : "LOck it up saf3";
13 $pt = isset($_POST['pt']) ? stripslashes($_POST['pt']) : "pssst ... don't tell anyone!";
14 $cipher = isset($_POST['cipher']) ? $_POST['cipher']: '';
15 $plain = isset($_POST['plain']) ? stripslashes($_POST['plain']): '';
16 $encr = isset($_POST['encr']) ? AESEncryptCtr($pt, $pw, 256) : $cipher;
17 $decr = isset($_POST['decr']) ? AESDecryptCtr($_POST['cipher'], $pw, 256) : $plain;
18
19 if (!$_REQUEST['msgid']==""){
20     $msgid=$_REQUEST['msgid'];
21     $repquery = "SELECT * FROM compose WHERE cMessageID='$msgid'";
22     $represult = mysql_query($repquery) or die(mysql_error());
23     if($reply = mysql_fetch_array($represult)){
24
25         $repdate=$reply['cDateSend'];
26         $repto=$reply['cStudID'];
27         $pw=$reply['cSubject'];
28     }
29 }
30
31 $query = "Select * from studinfo where StudID='$username1'";
32 $result = mysql_query($query);
33 if($row = mysql_fetch_array($result)){
34     ?>
35

```

Figure 4.21 : Compose query

```

<?php
/* ----- */
/* AES implementation in PHP (c) Chris Veness 2005-2009. Right of free use
is granted for all */
/* commercial or non-commercial use under LGPL licence. No warranty of
any form is offered. */
/* ----- */

/**
 * AES Cipher function: encrypt 'input' with Rijndael algorithm
 * @param input message as byte-array (16 bytes)
 * @param w key schedule as 2D byte-array (Nr+1 x Nb bytes) -
 * generated from the cipher key by KeyExpansion()
 * @return ciphertext as byte-array (16 bytes)
 */

function Cipher($input, $w) { // main Cipher function [§5.1]
    $Nb = 4; // block size (in words): no of columns in state (fixed at 4 for AES)
    $Nr = count($w)/$Nb - 1; // no of rounds: 10/12/14 for 128/192/256-bit keys
    $state = array(); // initialise 4xNb byte-array 'state' with input [§3.4]
    for ($i=0; $i<4*$Nb; $i++) $state[$i%4][floor($i/4)] = $input[$i];
    $state = AddRoundKey($state, $w, 0, $Nb);

    for ($round=1; $round<$Nr; $round++) { // apply Nr rounds
        $state = SubBytes($state, $Nb);
        $state = ShiftRows($state, $Nb);
        $state = MixColumns($state, $Nb);
        $state = AddRoundKey($state, $w, $round, $Nb);
    }

    $state = SubBytes($state, $Nb);
    $state = ShiftRows($state, $Nb);
    $state = AddRoundKey($state, $w, $Nr, $Nb);

    $soutput = array(4*$Nb); // convert state to 1-d array before returning [§3.4]
    for ($i=0; $i<4*$Nb; $i++) $soutput[$i] = $state[$i%4][floor($i/4)];
    return $soutput;
}

function AddRoundKey($state, $w, $rnd, $Nb) { // xor Round Key into state
    S [§5.1.4]
    for ($r=0; $r<4; $r++) {
        for ($c=0; $c<$Nb; $c++) $state[$r][$c] ^= $w[$rnd*4+$c][$r];
    }
    return $state;
}

```

```

function SubBytes($s, $Nb) { // apply SBox to state S [§5.1.1]
global $Sbox; // PHP needs explicit declaration to access global
variables!
for ($r=0; $r<4; $r++) {
    for ($c=0; $c<$Nb; $c++) $s[$r][$c] = $Sbox[$s[$r][$c]];
}
return $s;
}

function ShiftRows($s, $Nb) { // shift row r of state S left by r bytes [§5.1.2]
$t = array(4);
for ($r=1; $r<4; $r++) {
for ($c=0; $c<4; $c++) $t[$c] = $s[$r][($c+$r)%$Nb]; // shift into temp copy
for ($c=0; $c<4; $c++) $s[$r][$c] = $t[$c]; // and copy back
} // note that this will work for Nb=4,5,6, but not 7,8 (always 4 for AES):
return $s; // see
fp.gladman.plus.com/cryptography_technology/rijndael/aes.spec.311.pdf
}

function MixColumns($s,$Nb) { // combine bytes of each col of state S
[§5.1.3]
for ($c=0; $c<4; $c++) {
    $a = array(4); // 'a' is a copy of the current column from 's'
    $b = array(4); // 'b' is  $a \cdot \{02\}$  in  $GF(2^8)$ 
    for ($i=0; $i<4; $i++) {
        $a[$i] = $s[$i][$c];
        $b[$i] = $s[$i][$c]&0x80 ? $s[$i][$c]<<1 ^ 0x011b : $s[$i][$c]<<1;
    }
    //  $a[n] \wedge b[n]$  is  $a \cdot \{03\}$  in  $GF(2^8)$ 
    $s[0][$c] = $b[0] ^ $a[1] ^ $b[1] ^ $a[2] ^ $a[3]; //  $2 \cdot a_0 + 3 \cdot a_1 + a_2 + a_3$ 
    $s[1][$c] = $a[0] ^ $b[1] ^ $a[2] ^ $b[2] ^ $a[3]; //  $a_0 \cdot 2 + 3 \cdot a_1 + a_2 + a_3$ 
    $s[2][$c] = $a[0] ^ $a[1] ^ $b[2] ^ $a[3] ^ $b[3]; //  $a_0 + a_1 + 2 \cdot a_2 + 3 \cdot a_3$ 
    $s[3][$c] = $a[0] ^ $b[0] ^ $a[1] ^ $a[2] ^ $b[3]; //  $3 \cdot a_0 + a_1 + a_2 + 2 \cdot a_3$ 
}
return $s;
}

/**
 * Key expansion for Rijndael Cipher(): performs key expansion on cipher key
 * to generate a key schedule
 *
 * @param key cipher key byte-array (16 bytes)
 * @return key schedule as 2D byte-array (Nr+1 x Nb bytes)
 */

```

```

function KeyExpansion($key) { //generate Key Schedule from Cipher Key
[5.2]
global $Rcon; // PHP needs explicit declaration to access global variables!
$Nb = 4; // block size (in words): no of columns in state (fixed at 4 for AES)
$Nk = count($key)/4; // key length (in words): 4/6/8 for 128/192/256-bit keys
$Nr = $Nk + 6; // no of rounds: 10/12/14 for 128/192/256-bit keys

$w = array();
$temp = array();

or ($i=0; $i<$Nk; $i++) {
    $r = array($key[4*$i], $key[4*$i+1], $key[4*$i+2], $key[4*$i+3]);
    $w[$i] = $r;
}

for ($i=$Nk; $i<($Nb*($Nr+1)); $i++) {
    $w[$i] = array();
    for ($t=0; $t<4; $t++) $temp[$t] = $w[$i-1][$t];
    if ($i % $Nk == 0) {
        $temp = SubWord(RotWord($temp));
        for ($t=0; $t<4; $t++) $temp[$t] ^= $Rcon[$i/$Nk][$t];
    } else if ($Nk > 6 && $i%$Nk == 4) {
        $temp = SubWord($temp);
    }
    for ($t=0; $t<4; $t++) $w[$i][$t] = $w[$i-$Nk][$t] ^ $temp[$t];
}
return $w;
}

function SubWord($w) { // apply SBox to 4-byte word w
global $Sbox; // PHP needs explicit declaration to access global variables!
for ($i=0; $i<4; $i++) $w[$i] = $Sbox[$w[$i]];
return $w;
}

function RotWord($w) { // rotate 4-byte word w left by one byte
$tmp = $w[0];
for ($i=0; $i<3; $i++) $w[$i] = $w[$i+1];
$w[3] = $tmp;
return $w;
}

```

```
// Sbox is pre-computed multiplicative inverse in GF(2^8) used in SubBytes
and KeyExpansion [§5.1.1]
$Sbox = array
(0x63,0x7c,0x77,0x7b,0xf2,0x6b,0x6f,0xc5,0x30,0x01,0x67,0x2b,0xfe,0xd7,
0xab,0x76,
0xca,0x82,0xc9,0x7d,0xfa,0x59,0x47,0xf0,0xad,0xd4,0xa2,0xaf,0x9c,0xa4,0
x72,0xc0,
0xb7,0xfd,0x93,0x26,0x36,0x3f,0xf7,0xcc,0x34,0xa5,0xe5,0xf1,0x71,0xd8,0
x31,0x15,
0x04,0xc7,0x23,0xc3,0x18,0x96,0x05,0x9a,0x07,0x12,0x80,0xe2,0xeb,0x27,
0xb2,0x75,
0x09,0x83,0x2c,0x1a,0x1b,0x6e,0x5a,0xa0,0x52,0x3b,0xd6,0xb3,0x29,0xe3,
0x2f,0x84,
0x53,0xd1,0x00,0xed,0x20,0xfc,0xb1,0x5b,0x6a,0xcb,0xbe,0x39,0x4a,0x4c,0
x58,0xcf,
0xd0,0xef,0xaa,0xfb,0x43,0x4d,0x33,0x85,0x45,0xf9,0x02,0x7f,0x50,0x3c,0
x9f,0xa8,
0x51,0xa3,0x40,0x8f,0x92,0x9d,0x38,0xf5,0xbc,0xb6,0xda,0x21,0x10,0xff,0
xf3,0xd2,
0xcd,0x0c,0x13,0xec,0x5f,0x97,0x44,0x17,0xc4,0xa7,0x7e,0x3d,0x64,0x5d,0
x19,0x73,
0x60,0x81,0x4f,0xdc,0x22,0x2a,0x90,0x88,0x46,0xee,0xb8,0x14,0xde,0x5e,
0x0b,0xdb,
0xe0,0x32,0x3a,0x0a,0x49,0x06,0x24,0x5c,0xc2,0xd3,0xac,0x62,0x91,0x95,
0xe4,0x79,
0xe7,0xc8,0x37,0x6d,0x8d,0xd5,0x4e,0xa9,0x6c,0x56,0xf4,0xea,0x65,0x7a,0
xae,0x08,
0xba,0x78,0x25,0x2e,0x1c,0xa6,0xb4,0xc6,0xe8,0xdd,0x74,0x1f,0x4b,0xbd,
0x8b,0x8a,
0x70,0x3e,0xb5,0x66,0x48,0x03,0xf6,0x0e,0x61,0x35,0x57,0xb9,0x86,0xc1,
0x1d,0x9e,
0xe1,0xf8,0x98,0x11,0x69,0xd9,0x8e,0x94,0x9b,0x1e,0x87,0xe9,0xce,0x55,
0x28,0xdf,
0x8c,0xa1,0x89,0x0d,0xbf,0xe6,0x42,0x68,0x41,0x99,0x2d,0x0f,0xb0,0x54,
0xbb,0x16);
```

```

// Rcon is Round Constant used for the Key Expansion [1st col is 2^(r-1) in
GF(2^8)] [§5.2]
$Rcon = array( array(0x00, 0x00, 0x00, 0x00),
    array(0x01, 0x00, 0x00, 0x00),
    array(0x02, 0x00, 0x00, 0x00),
    array(0x04, 0x00, 0x00, 0x00),
    array(0x08, 0x00, 0x00, 0x00),
    array(0x10, 0x00, 0x00, 0x00),
    array(0x20, 0x00, 0x00, 0x00),
    array(0x40, 0x00, 0x00, 0x00),
    array(0x80, 0x00, 0x00, 0x00),
    array(0x1b, 0x00, 0x00, 0x00),
    array(0x36, 0x00, 0x00, 0x00) );

/* ----- */

/**
 * Encrypt a text using AES encryption in Counter mode of operation
 * - see http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
 *
 * Unicode multi-byte character safe
 *
 * @param plaintext source text to be encrypted
 * @param password the password to use to generate a key
 * @param nBits number of bits to be used in the key (128, 192, or 256)
 * @return encrypted text
 */
function AESEncryptCtr($plaintext, $password, $nBits) {
    $blockSize = 16; // block size fixed at 16 bytes / 128 bits (Nb=4) for AES
    if (!($nBits==128 || $nBits==192 || $nBits==256)) return ""; // standard
    allows 128/192/256 bit keys
    // note PHP (5) gives us plaintext and password in UTF8 encoding!
    // use AES itself to encrypt password to get cipher key (using plain password
    as source for
    // key expansion) - gives us well encrypted key
    $nBytes = $nBits/8; // no bytes in key
    $pwBytes = array();
    for ($i=0; $i<$nBytes; $i++) $pwBytes[$i] = ord(substr($password,$i,1)) &
    0xff;
    $key = Cipher($pwBytes, KeyExpansion($pwBytes));
    $key = array_merge($key, array_slice($key, 0, $nBytes-16)); // expand key
    to 16/24/32 bytes long

```

```

// initialise counter block (NIST SP800-38A §B.2): millisecond time-stamp
for nonce in
// 1st 8 bytes, block counter in 2nd 8 bytes
$counterBlock = array();
$nonce = floor(microtime(true)*1000); // timestamp: milliseconds since 1-
Jan-1970
$nonceSec = floor($nonce/1000);
$nonceMs = $nonce%1000;
// encode nonce with seconds in 1st 4 bytes, and (repeated) ms part filling 2nd
4 bytes
for ($i=0; $i<4; $i++) $counterBlock[$i] = urs($nonceSec, $i*8) & 0xff;
for ($i=0; $i<4; $i++) $counterBlock[$i+4] = $nonceMs & 0xff;
// and convert it to a string to go on the front of the ciphertext
$ctrTxt = "";
for ($i=0; $i<8; $i++) $ctrTxt .= chr($counterBlock[$i]);

// generate key schedule - an expansion of the key into distinct Key Rounds
for each round
$keySchedule = KeyExpansion($key);

    $blockCount = ceil(strlen($plaintext)/$blockSize);
    $ciphertext = array(); // ciphertext as array of strings

    for ($b=0; $b<$blockCount; $b++) {
// set counter (block #) in last 8 bytes of counter block (leaving nonce in 1st 8
bytes)
// done in two stages for 32-bit ops: using two words allows us to go past 2^32
blocks (68GB)
for ($c=0; $c<4; $c++) $counterBlock[15-$c] = urs($b, $c*8) & 0xff;
for ($c=0; $c<4; $c++) $counterBlock[15-$c-4] = urs($b/0x100000000,$c*8);

$cipherCntr = Cipher($counterBlock, $keySchedule); // -- encrypt counter
block –

// block size is reduced on final block
$blockLength = $b<$blockCount-1 ? $blockSize : (strlen($plaintext)
1)%$blockSize+1;
$cipherByte = array();

```



```

for ($i=0; $i<$blockLength; $i++) { // -- xor plaintext with ciphered counter
byte-by-byte --
$cipherByte[$i] = $cipherCntr[$i] ^ ord(substr($plaintext, $b*$blockSize+$i,
1));
$cipherByte[$i] = chr($cipherByte[$i]);
}
$ciphertxt[$b] = implode("", $cipherByte); // escape troublesome characters in
ciphertext
}

// implode is more efficient than repeated string concatenation
$ciphertext = $ctrTxt . implode("", $ciphertxt);
$ciphertext = base64_encode($ciphertext);
return $ciphertext;
}

/**
 * Decrypt a text encrypted by AES in counter mode of operation
 *
 * @param ciphertext source text to be decrypted
 * @param password the password to use to generate a key
 * @param nBits number of bits to be used in the key (128, 192, or 256)
 * @return decrypted text
 */
function AESDecryptCtr($ciphertext, $password, $nBits) {
    $blockSize = 16; // block size fixed at 16 bytes / 128 bits (Nb=4) for AES
    if (!$nBits==128 || $nBits==192 || $nBits==256) return ""; // standard
    allows 128/192/256 bit keys
    $ciphertext = base64_decode($ciphertext);

    // use AES to encrypt password (mirroring encrypt routine)
    $nBytes = $nBits/8; // no bytes in key
    $pwBytes = array();
    for ($i=0; $i<$nBytes; $i++) $pwBytes[$i] = ord(substr($password,$i,1)) &
    0xff;
    $key = Cipher($pwBytes, KeyExpansion($pwBytes));
    $key = array_merge($key, array_slice($key, 0, $nBytes-16)); // expand key to
    16/24/32 bytes long

    // recover nonce from 1st element of ciphertext
    $counterBlock = array();
    $ctrTxt = substr($ciphertext, 0, 8);
    for ($i=0; $i<8; $i++) $counterBlock[$i] = ord(substr($ctrTxt,$i,1));

```

```

// generate key schedule
$keySchedule = KeyExpansion($key);

// separate ciphertext into blocks (skipping past initial 8 bytes)
$nBlocks = ceil((strlen($ciphertext)-8) / $blockSize);
$cct = array();
for ($b=0; $b<$nBlocks; $b++) $cct[$b] = substr($ciphertext,
8+$b*$blockSize, 16);
$ciphertext = $cct; // ciphertext is now array of block-length strings

// plaintext will get generated block-by-block into array of block-length
strings
$plaintext = array();

for ($b=0; $b<$nBlocks; $b++) {
// set counter (block #) in last 8 bytes of counter block (leaving nonce in 1st 8
bytes)
for ($c=0; $c<4; $c++) $counterBlock[15-$c] = urs($b, $c*8) & 0xff;
for ($c=0; $c<4; $c++) $counterBlock[15-$c-4] = urs(($b+1)/0x100000000-1,
$c*8) & 0xff;

$cipherCntr = Cipher($counterBlock, $keySchedule); // encrypt counter
block

$plaintextByte = array();
for ($i=0; $i<strlen($ciphertext[$b]); $i++) {
// -- xor plaintext with ciphered counter byte-by-byte --
$plaintextByte[$i] = $cipherCntr[$i] ^ ord(substr($ciphertext[$b],$i,1));
$plaintextByte[$i] = chr($plaintextByte[$i]);
}
$plaintext[$b] = implode("", $plaintextByte);
}

// join array of blocks into single plaintext string
$plaintext = implode("", $plaintext);

return $plaintext;
}

```

```

/*
 * Unsigned right shift function, since PHP has neither >>> operator nor
 unsigned ints
 *
 * @param a number to be shifted (32-bit integer)
 * @param b number of bits to shift a to the right (0..31)
 * @return a right-shifted and zero-filled by b bits
 */
function urs($a, $b) {
    $a &= 0xffffffff; $b &= 0x1f; // (bounds check)
    if ($a & 0x80000000 && $b > 0) { // if left-most bit set
        $a = ($a >> 1) & 0x7fffffff; // right-shift one bit & clear left-most bit
        $a = $a >> ($b-1); // remaining right-shifts
    } else { // otherwise
        $a = ($a >> $b); // use normal right-shift
    }
    return $a;
}

/* ----- */
?>

```

Figure 4.22 : aes-lib.php

Figure 4.22 is library that contain AES cipher function which is use in process of compose memo and read message. This library contain process of generate key, encrypt and decrypt. This library use Rijndael algorithm to encrypt input (message).

Figure 4.23 and 4.24 show the process of encryption and decryption. Encryption process occur during sending data and will be save directly to database in cipher text. Data can change to original message (plaintext) and be read after receiver click 'Decrypt' button.

```

154 <?php
155 if ($_POST['encr']=="Submit") //jika klik button Submit
156 {
157     $date = $_POST['cDateSend'];
158     $receiver = $_POST['Receiver'];
159     $subject = $_POST['pw'];
160     $StudID = $_POST['cStudID']; //hardcoded id. sepatutnya value diambil dr
                                session, mase mule2 login lagi.
161
162     $query2 = "INSERT INTO compose (cStudID, cDateSend, cReceiver, cSubject, cMessage)
VALUES('$username1', '$date', '$receiver', '$subject', '$encr;')";
163     //simpan encrypted messages kt db
164     $result2 = mysql_query($query2) or die(mysql_error());
165     echo $username1;
166     echo "<br>Date:". $date. "<br>";
167     echo "Receiver:". $receiver. "<br>";
168     echo "Subject:". $subject. "<br>";
169     echo "Messages:". $pt. "<br><br>";
170     echo "Your message has been encrypted & successfully submitted.<br>
171     <a href='StudInbox.php' target=_self>Inbox</a>";
172     //echo $encr;
173 }
174 else {
175     ?>

```

Figure 4.23 : Encryption process

```

1 <?php
2
3 session_start();
4 //include ("EcConnect.php");
5 include("EcConn.php");
6 include("EcSession.php");
7
8 $conn = phpmkr_db_connect(HOST, USER, PASS,DB);
9 $username1 = $_SESSION['id'];
10 $lvl=$_SESSION['lvl'];
11 $ids = $_REQUEST['ids']; //dptkan id dari <a href>
12
13 require 'aes-lib.php'; // from www.movable-type.co.uk/scripts/aes-php.html
14 $timer = microtime(true);
15
16 // initialise password & plaintesxt if not set in post array (shouldn't need
stripslashes if magic_quotes is off)
17 $pw = isset($_POST['pw']) ? stripslashes($_POST['pw']) : "L0ck it up saf3";
18 $pt = isset($_POST['pt']) ? stripslashes($_POST['pt']) : "psst ... don't tell anyone!";
19 $cipher = isset($_POST['cipher']) ? $_POST['cipher'] : '';
20 $plain = isset($_POST['plain']) ? stripslashes($_POST['plain']): '';
21 $encr = isset($_POST['encr']) ? AESEncryptCtr($pt, $pw, 256) : $cipher;
22 $decr = isset($_POST['decr']) ? AESDecryptCtr($_POST['cipher'], $pw, 256) : $plain;
23
24 $query = "Select * from studinfo where StudID='$username1'";
25 $result = mysql_query($query);
26 if($row = mysql_fetch_array($result)){
27     ?>

```

Figure 4.24 : Decryption process

Figure 4.25 show the query of request appointment process in student module.

```

104 <?php
105
106 $query2 = "Select * from staffinfo where StaffID='$staffid'";
107 $result2 = mysql_query($query2);
108 $row2 = mysql_fetch_array($result2);
109
110 ?>

```

Figure 4.25 : Request appointment process

Figure 4.26 show the query and process of reply student request appointment by counsellor in counsellor module. When counsellor reply the request, status of student request will be automatically update

```

1 <?php
2
3 include("EcConn.php");
4 include("EcSession.php");
5
6 $conn = phpmkr_db_connect(HOST, USER, PASS, DB);
7
8 session_start();
9 $username1=$_SESSION['id'];
10 $lvl=$_SESSION['lvl'];
11 $do=$_REQUEST['do'];
12
13 if($do=='update'){
14 $refcomment=$_REQUEST['Comment'];
15 $refstatus=$_REQUEST['Status'];
16 $refno=$_REQUEST['RefNo'];
17 $refsql="UPDATE request SET
18 rComment='$refcomment', rStatus='$refstatus' where
19 rRefNo='$refno'";
20 if(mysql_query($refsql)){
21
22 echo "<script language = 'Javascript'>
23 alert('Appointment Request Updated');
24 location.href = 'ReplyStudRequest.php';
25 </SCRIPT>";
26 }
27 }
28 $sql = "SELECT * from staffinfo where StaffID =
29 '$username1'";
30 $result = mysql_query($sql);
31
32 if($row = mysql_fetch_array($result)){
33
34 ?>

```

Figure 4.26 : Reply student appointment request

Figure 4.27 and 4.28 show the login and logout coding of the system. User will be back to login page after logout.

```
<?PHP
if($_POST['level'] == 1){
$query = "SELECT * FROM staffinfo WHERE StaffID='$username1'";
}
else{
$query = "SELECT * FROM studinfo WHERE StudID='$username1'";
}

$result = mysql_query($query);
if ($row = mysql_fetch_array($result)){
    if ($row["Password"] == $password1){
        $datetime = date("d-m-Y G:i ");
        $_SESSION['password'] = $password1;
        $_SESSION['id'] = $username1;
        $_SESSION['lv'] = $_POST['level'];
        if($_POST['level'] == 1)
        {
            echo "<font color='#000000' size='2' face='Verdana, Arial, Helvetica, sans-serif' align='center'>Login Successful<br><br><a href='home.php'>To home</a></font>";
        }
        else
        {
            echo "<font color='#000000' size='2' face='Verdana, Arial, Helvetica, sans-serif' align='center'>Student Login<br><br><a href='home.php'>Login Page</a></font>";
        }
    }
    else
    {
        echo "<font color='#000000' size='2' face='Verdana, Arial, Helvetica, sans-serif' align='center'>Invalid Username or Password<br><br><a href='EcLogin.php'>Login Page</a></font>";
    }
}
else{
    echo "<font color='#000000' size='2' face='Verdana, Arial, Helvetica, sans-serif' align='center'>Invalid Username or Password<br><br><a href='EcLogin.php'>Login Page</a></font>";
}
?>
```

Figure 4.27 : Login

```
1  <?PHP
2  session_start();
3  session_unset();
4  session_destroy();
5  echo "<script language = 'Javascript'>
6  alert('Log out Succesful');
7          location.href = '../EcLogin.php';
8  </SCRIPT>";
9  ?>
10
11
```

Figure 4.28 : Logout

CHAPTER 5

RESULT AND DISCUSSION

5.1 Introduction

This chapter describes in detail the result of *DEECS* development. The objective of the system basically to change the manual system to computerize system.

There are two types of user that can access this system. The first type of user is staff which is counsellor and admin. Admin like as an Administrator. Where they can register for new counsellor and delete counsellor profile that has been exist. Admin also can view list profile counsellor. Counsellor are able to reply memo which is send by student, update their profile and reply/approve appointment request by student.

The second type of user is student. The main function of student module is students are able to submit their message or share their problem with counsellor by compose a message. The process of sending data is using cryptographic technique which is the data will be encrypt. They also can request/booked an appointment with counsellor and view counsellor profile. For this sub topic I will only discuss the main function for student and staff module. Other function or application will be discuss in detail at user manual.

5.2 Student Module

The following figures are described for student main module in this system. There are three main functions in this module, which are sending memo to counsellor, sending appointment request and view appointment status.

5.2.1 Homepage



Figure 5.10 : Homepage for student module

The figure above shown homepage for student module. From this page, student can access all their application.

5.2.2 Sending Memo

The screenshot shows the 'E-COUNSELLING' interface of the University Malaysia Pahang Counselling Unit. The user is logged in as 'Fatem binti Kamarudin'. The main menu includes 'Home', 'MY PROFILE', and 'Student Detail'. The 'Memo' section is active, showing 'Inbox' and 'Compose' buttons. The 'Compose' form includes fields for 'Date' (2009-11-12), 'To' (0337), 'Subject' (Selamat Pagi), and a 'Message' text area containing the text: 'Puan saya ingin meluahkan masalah. Saya harap puan dapat membantu saya. Boleh ke?'. A 'Submit' button is at the bottom.

Figure 5.11 : Interface of sending memo

Figure 5.11 shows the interface of sending memo. In order to send memo, student must enter required data (**) first and enter which counsellor student want to send memo by type their id. Message will be encrypt and save into database after enter button 'Submit'. This data cannot be read or understand by anyone as shown in figure below.

	43	cc06990	2009-11-12	0337	Selamat Pagi	umn+Sj8/Pz9fk00MNoMEml9oqC9C9FP1HbVIEv67p
--	----	---------	------------	------	--------------	---

Message in encrypted form save in database

Figure 5.12 : Database of 'compose' table

5.2.3 Sending Appointment Request

The screenshot shows the web interface of the University of Malaysia Pahang Counselling Unit. The header includes the university logo and name, along with navigation links for 'Sitemap' and 'Contact Us'. The user is logged in as 'User : Fatem binti Kamarudin' with a '<Log Out>' link. The main navigation menu on the left includes 'E-COUNSELLING' (with a 'Home' link), 'MY PROFILE' (with a 'Student Detail' link), and 'APPLICATION' (with links for 'Counsellor Detail', 'Memo', 'Appointment', and 'View Request'). The main content area shows the breadcrumb 'Student Management > Request Appointment'. Below this is a form with the following fields:

Student Name :	Fatem binti Kamarudin
Faculty :	FSKKP
Date Apply :	2009-11-12
Counsellor Incharge :	Paridah binti Mohd Ali
Specification :	saya nak jumpa puan jam 3 petang di

At the bottom of the form are 'Reset' and 'Submit' buttons.

Figure 5.13 : Interface of sending appointment request

Figure 5.13 shows the interface of sending appointment request. In order to send appointment request, student must select counsellor in charge first and specification (eg : place or time to meet).

5.2.4 View Appointment Status

The screenshot displays the web interface of the University Malaysia Pahang Counselling Unit. The header features the university's logo and name, along with navigation links for Sitemap and Contact Us. The main content area shows the user's name, 'User : Fatem binti Kamarudin', and a '<Log Out>' link. The left sidebar contains navigation menus for E-COUNSELLING (Home), MY PROFILE (Student Detail), and APPLICATION (View Counsellor Detail, Memo, Appointment, View Request). The main content area displays the 'Appointment Application > Status' section, which includes a 'Status Information' table.

Counsellor ID	Date Applied	Status	Comment
Paridah binti Mohd. Ali	2009-11-12	Accepted	
Paridah binti Mohd. Ali	2009-11-13	Accepted	

At the bottom of the page, there is a copyright notice: © All rights reserved, 2009 University Malaysia Pahang, Lebuhraya Tun Razak, 26300 Kuantan, Pahang Darul Makmur. Phone : 09-5492020 Fax : 09-5492222.

Figure 5.14 : Interface of view appointment status

Figure 5.14 shows the interface of view appointment status. The figures above show all the appointment request status that belongs to “Fatem binti Kamarudin”. From here student are able to view their appointment status whether approve or reject by counsellor.

5.3 Staff Module

The following figures are described for student main module in this system. There are three main functions in this module, which are sending memo to counsellor, sending appointment request and view appointment status .

5.3.1 Homepage



Figure 5.15 : Homepage for staff module

The figure above are shown homepage for staff module. From this page, staff can access all their application.

5.3.2 View Inbox

From	Inbox Subject	Date	Action
cb06011	salam		
cb06011	salam		
cb06090	salam	2/11/2009	
cb06011	hello		
cc06990	salam?	03/10/2009	
cb06011	Re: Re: salam	14/5/2009	
cb06011	Re: Re: salam		
cb06011	Salam puan	11/09/2009	
cc06990	salam8	11/09/2009	
cb06011	assalamualaikum	11/09/2009	
cb06011	salam puan	11/09/2009	
cc06990	assalamualaikum	11/09/2009	
cc06990	Selamat Pagi	2009-11-12	

Figure 5.16 : Interface of counsellor inbox

Figure 5.16 shows the interface of counsellor inbox. Counsellor can view all list of message which is send by same or different student. By click at subject of message (eg : ‘Selamat Pagi’), counsellor can read the message. Counsellor also can delete (action) message from this page.

View Inbox

[Reply](#)

Date : 2009-11-12
 From : 0337
 To : cc06990
 Subject : Selamat Pagi

Message :

Puan saya ingin meluahkan masalah. Saya harap puan dapat membantu saya. Boleh ke?

Message which is called from database is in encrypted form and only at receiver page this data can be read by click button 'Decrypt it'

Figure 5.17 : Interface of view message

5.3.3 Reply Memo

The screenshot shows the 'E-COUNSELLING' system interface. At the top, the user is identified as 'User : Paridah binti Mohd Ali' with a '<Log Out>' link. The navigation menu on the left includes 'Home', 'MY PROFILE', and 'Counsellor Detail'. The main content area is titled 'Memo' and contains 'Inbox' and 'Compose' buttons. On the right, the 'APPLICATION' menu lists 'Memo', 'Appointment', and 'View Pending Request'. The form for replying a memo includes fields for 'Date' (set to 2009-11-12), 'To' (cc06990), and 'Subject' (Re: Selamat Pagi). A 'Message' text area contains the text: 'Salam.. ye. Apa masalah yang ingin dikongsi. InsyAllah, kalau saya boleh bantu, saya akan membantu'. A 'Submit' button is located below the message field.

Figure 5.18 : Interface of reply memo

Figure 5.18 shows the interface of reply memo. Counsellor can reply the memo that send by student after read the message. 'To' and 'Subject' would be automatically called. Therefore, counsellor only just enter date and message during reply session.

5.3.4 Reply Student Appointment Request

The screenshot shows the web interface of the University Malaysia Pahang Counselling Unit. At the top, there is a banner with the university's logo and name. Below the banner, the user is logged in as 'Paridah binti Mohd Ali'. The navigation menu includes 'Counsellor' and 'Application'. The current page is 'Counsellor Application > Reply Request Appoinment'. Under 'Application Information', there is a table with columns: Student ID, Student Name, Date Applied, Specification, Student Details, Action, and Comment. A single row of data is shown for student 'cc06990' with the name 'Fatem binti Kamarudin' and the date '2009-11-13'. The 'Specification' column contains the text 'Saya nak jumpa puan di pejabat puan jam 3 petang'. The 'Student Details' column has a 'View' link. The 'Action' column has an 'Approve' button. The 'Comment' column has a text input field and an 'OK' button. Below the table is a 'View Appointment' button. At the bottom, there is a copyright notice for 2005 University College of Engineering & Technology Malaysia.

Student ID	Student Name	Date Applied	Specification	Student Details	Action	Comment
cc06990	Fatem binti Kamarudin	2009-11-13	Saya nak jumpa puan di pejabat puan jam 3 petang	View	Approve	<input type="text"/>

View Appointment

© All rights reserved. 2005 University College of Engineering & Technology Malaysia.
 Locked Bag 12, 25000, Kuantan Pahang Darul Makmur
 Phone : 09-5492020 Fax : 09-5492222 .

Figure 5.19 : Interface of reply student appointment request

Figure 5.19 shows the interface of reply student appointment request. Counsellor can approve or reject appointment request that made by student and leave the comment (eg : whether counsellor want to change the place or time that request by student). After reply the student appointment request, counsellor can view their appointment schedule.

5.3.5 View Appointment Schedule



The screenshot displays the 'E-COUNSELLING' interface of the University Malaysia Pahang Counselling Unit. The user is logged in as 'Paridah binti Mohd Ali'. The interface includes a navigation menu on the left with options like 'Home', 'MY PROFILE', and 'Counsellor Detail'. The main content area shows the 'Appointment Application > Status' section. Below this, there is a 'Status Information' table listing appointment details for two students.

Counsellor ID	Student Name	Date Applied	Specifications	Comment
cc06990	Fatem binti Kamarudin	2009-11-12	saya nak jumpa puan jam 3 petang di pejabat puan	
cc06990	Fatem binti Kamarudin	2009-11-13	boleh saya jumpa puan jam 4 petang	

At the bottom of the page, there is a copyright notice: © All rights reserved. 2009 University Malaysia Pahang, Lebuhraya Tun Razak, 26300 Kuantan, Pahang Darul Makmur. Phone : 09-5492020 Fax : 09-5492222.

Figure 5.20 : Interface of view appointment schedule

Figure 5.20 shows the interface of view appointment schedule. Counsellor can view all information list of their appointment schedule with student. Therefore, counsellor can manage their work schedule.

5.4 Constraint

During the development of the DEECS, there are several constraints that need to overcome in order to develop the system successfully. This project constraint can be divided into two parts which is development constraint and system constraint.

5.4.1 Development Constraint

The development constraint discuss about the problems that arises during the development of the DEECS. There are several problems had been faced such as:

- Lack of AES algorithm in PHP language on internet.

The lack of AES algorithm in PHP language on internet give problem for me to find it since PHP language was used to build this overall system. This code was required to make the main function of the system (data encryption) run.

- Hardware and software problems.

During the development laptop sometimes attacked by virus, lagging and windows corrupt. This constraints make lap top sometimes hang and make the development slow in progress because the problems need to be settled down first.

- Server down

Some of the resources and references came from the internet. It consists of research papers, journals and others. These references are needed for gaining information related to the project.

5.4.2 System Constraint

System constraint makes the system look a bit difficult and hard to understand. There are several system constraints that occur during the system testing which are:

i. Photo not provided.

The system does not show the photo of the user. User needs to login E-Community to find photo or know the face with whom they are sending message.

ii. File attachment.

User cannot attach any file in this system.

iii. Security issues.

There are certain places where the system did not apply the security features (eg : during login) where it has high possibility of data hacking and manipulating by other irresponsible parties.

- Take time to reply message.

This system uses memo as a medium to communicate between student and counsellor. So, when a message has been sent, the user does not know except they login. Within that, the user needs to login many times to check whether their message has already been replied or not.

5.5 Suggestions and Project Enhancements

For further research, there are several recommendations to enhance and improve the system. The recommendations are:

- i. The system security can be improved by implementing also public and private key, cryptographic hash function in order to achieve authentication, integrity and high security system.
 - ii. Generate report for all counselling session should be made in order to manage and review record/data more proper and systematically.
 - iii. The system should testing in real network (server) in order to ensure the algorithm can function properly in online system and not just called from database.
 - iv. Instead of using memo, the system also can add another communication medium such as real time chatting because counsellor and student can communicate directly and get the answer faster better than sending memo.
- For further development, add some function for counsellor module such as can update and publish work schedule of every day for every month. So student can view and manage their schedule to make an appointment based on counsellor reliable.
 - Forum is a best platform to share opinions and advices. By implement forum in this system, all user can get more advice, information and opinion. From all information student get, they can compare it and take the best answer and for counsellor they maybe can get new way to improve their skills in order to handle counselling session.

CHAPTER 6

CONCLUSION

In conclusion, the main concern of this project, *Data Encryption in E-Counselling System (DEECS)* are to implement security by encrypting memo and improving the process of counseling. This system can save time because student can request an appointment with counsellor by online and just as a platform for student to build confidence and trusty before they see counsellor face to face.

Besides that, by using encryption techniques in this system, user need not to worryabout the data (message) that they share with the counsellor. The original message in plaintext will be encrypted and change to cipher text which is no one will know and read that message except the receiver (counsellor). This security mechanism could ensure that such data was handled in secure manner. Even this system make the counseling session could be handle in easier way than manual system, but it is still not the effective way of counseling session. Student still need to see counsellor for further effective session based on student willing.

This system was developed according to the Software Development Life Cycle (SDLC) methodology. The software/tool used to design this system is Macromedia Dreamweaver 8, PHP as programming language and MySQL (wamp server) as database platform. During development of the system, there were also several constraints that occurred and that need to overcome so that the project progress will run smoothly. The constraints were divided into two; development constraints and system constraints. Several recommendations for future work on this project have been proposed in Chapter 5.

Finally, all the objectives stated in this thesis was archived. This system is very efficient to implement because using this DEECS, counsellor are able to reduce the quantity of monitoring document and student able to save time of make an appointment at JHEPA by manually .

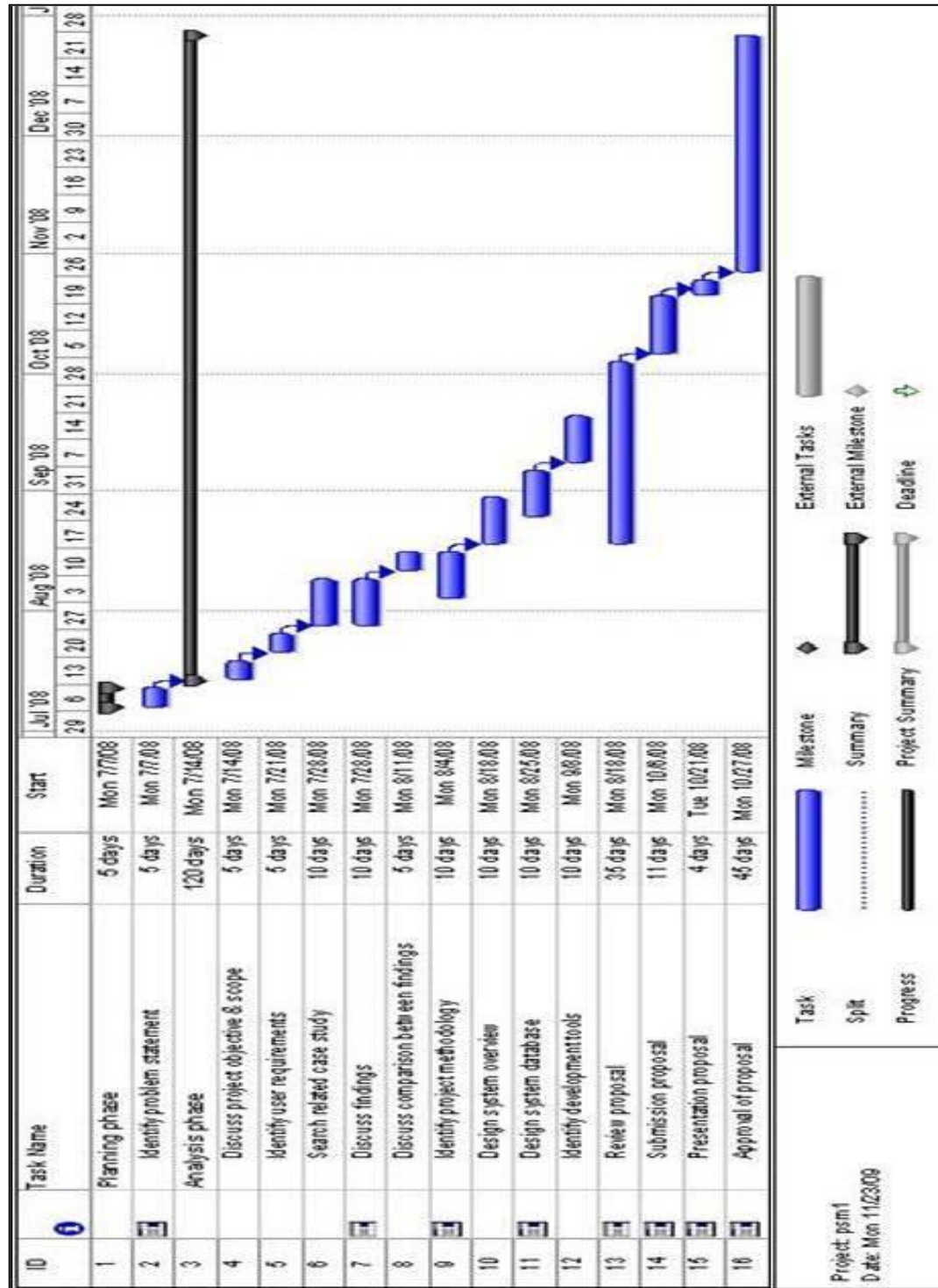
REFERENCES

1. Deitel, Deitel, Goldberg. *Internet & World Wide Web How To Program*. 3rd Edition. Pearson Education.
2. Ian Sommerville. 2007. *Software Engineering*. 8th Edition. Pearson Education.
3. Mohd Aizani Maarof, Mazleena Salleh, Subariah Ibrahim, Rabiah Ahmad. 2003. *Asas Kriptografi*. Mohd Zubil Bahak. 1st Edition. Universiti Teknologi Malaysia Skudai, Johor Darul Takzim.
4. Rosli Ab Ghani. *Asas Pengaturcaraan Pangkalan Data Web PHP-MYSQL*. Venton Publishing (M) Sdn Bhd.
5. About e-counselling.
<http://www.relationshiphelponline.com.au/modules.php?op=modload&name=News&file=article&sid=5>
Accessed : 20 Julai 2008

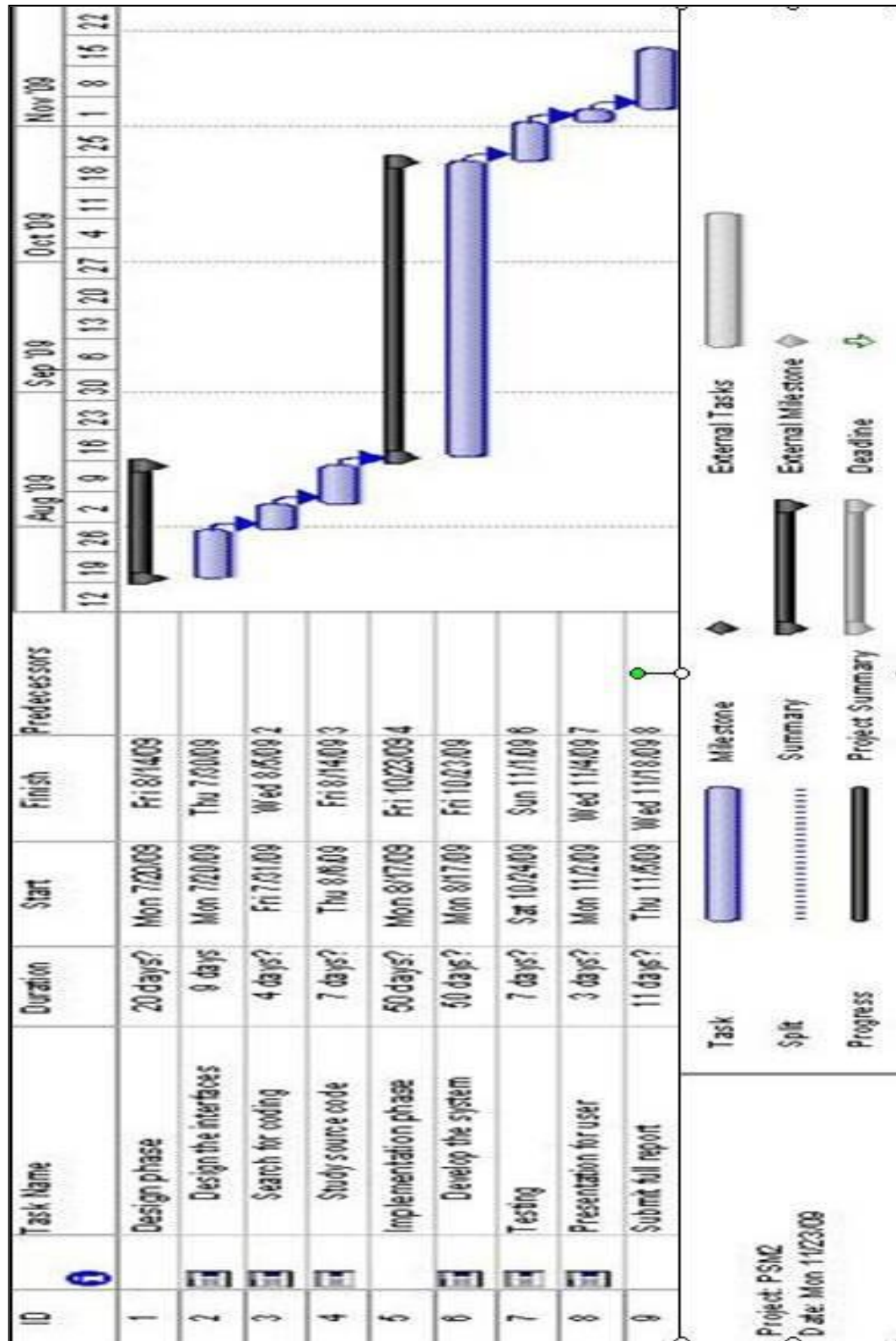
6. AES implementation in PHP (c) Chris Veness 2005-2009.
<http://www.movabletype.co.uk/scripts/aes-php.html>
Accessed : 11 October 2009
7. Evaluation of Kooth.com : E-counselling and Early Intervention service.
www.isb.gov.uk/hmt.isb.application.2/BIDDERS/Final%20Evaluations/5%20361%20eval-Kooth%20ODPM.doc
Accessed : 20 Julai 2008
8. PHP : Mcrypt – Manual. Copyright © 2001-2009 The PHP Group.
<http://php.net/manual/en/book.mcrypt.php>
Accessed : 11 October 2008
9. Two Way Encryption With PHP Mcrypt. Copyright 2008 PHPRO.ORG.
<http://www.phpro.org/classes/Two-Way-Encryption-With-PHP-Mcrypt.html>
Accessed : 20 Julai 2009

APPENDIX A

Gantt Chart



Gantt Chart



APPENDIX B

Interview Question

Followings are list of question to counsellor during interview session.

1. How long have you work as counsellor at UMP?
2. Can you briefly explain flow work of counseling session, start from make an appointment until finish the counselling session?
3. What information will you take during this session?
4. Do you have the any appendices which is related to this unit like flowchart, form or others?
5. What problem have you face and identify since you work in this unit?
6. What comment that you got from student about current counseling system?
7. In general, how many student come here and make an appointment?
8. How about your opinion if this system is convert to online system? Do you agree?
9. What do you expect from online system? For example application that should implement, improvement of manual system which is you think can apply in online system?
10. What is your hope for this proposed system?

APPENDIX C

Answer of interview session

1. -
2. - student dftg is form - to kt kamber steps ,
counselor approve , set appointment
- name , id , no phone , name opt dlu form . Sifat n
bunga bps beli n is .
- student x dftg pokok up pengumpulan , bps x detail
- x rana yg dftg , kebetulan yg ade pprn je
for islati x rana dftg
- bps tom kekhataa opton je . x is x pe
- instrument ade dipeleto smp set kauselng .
Berapa abar bar student cite dlu ms/k , dprc dlu
- ktr ktr online ok , to kps skdr platforme /g . Kauselng
yg efektif urah prjngaan . Online kauselng x bps ktr
bng kegalman d kepercayaan smp jua ada ktr kauselng
jua kauselng
- rujuk ltr phg online kauselng d bps ktr kauselng .
kps smp bps ktr x smp is
- jua er .
- smp bps ktr dftg smp ada ada smp bps ktr , d
ada kauselng d smp ktr , rana x ktr kauselng
chattng - I

APPENDIX D**Questionnaire**

Please fill and answer all question honestly and completely.

1. Do you ever go or make an appointment at counseling unit?

☐ Yes ☐ No

2. Is it manual counselling system give problem to you?

☐ Yes ☐ No ☐ Don't know

3. For your opinion, which action will you take if have problem?

☐ Meet counsellor
☐ Enjoy with friend
☐ Others. Such as : _____

4. Which suitable condition you prefer to do counseling session?

☐ Face to face
☐ Online
☐ Both

5. Which application below that you hope provide in online counseling system?

☐ Booked appointment
☐ Counsellor Schedule
☐ Forum
☐ Others. _____

APPENDIX E

Sample answer of questionnaire

Questionnaire

Please fill and answer all question honestly and completely.

- Do you ever go or make an appointment at counseling unit?
☐ Yes ☒ No
- Is it manual counselling system give problem to you?
☐ Yes ☐ No ☒ Don't know
- For your opinion, which action will you take if have problem?
☐ Meet counsellor
☒ Enjoy with friend
☐ Others. Such as : _____
- Which suitable condition you prefer to do counseling session?
☐ Face to face
☒ Online
☐ Both
- Which application below that you hope provide in online counseling system?
☒ Booked appointment
☒ Counsellor Schedule
☐ Forum
☐ Others. chatting

Questionnaire

Please fill and answer all question honestly and completely.

1. Do you ever go or make an appointment at counseling unit?

☒ Yes

☐ No

2. Is it manual counselling system give problem to you?

☒ Yes

☐ No

☐ Don't know

3. For your opinion, which action will you take if have problem?

☐ Meet counsellor

☐ Enjoy with friend

☐ Others. Such as : office session

4. Which suitable condition you prefer to do counseling session?

☐ Face to face

☒ Online

☐ Both

5. Which application below that you hope provide in online counseling system?

☒ Booked appointment

☒ Counsellor Schedule

☐ Forum

☐ Others. _____

Questionnaire

Please fill and answer all question honestly and completely.

1. Do you ever go or make an appointment at counseling unit?

☒ Yes

☐ No

2. Is it manual counselling system give problem to you?

☐ Yes

☒ No

☐ Don't know

3. For your opinion, which action will you take if have problem?

☒ Meet counsellor

☐ Enjoy with friend

☐ Others. Such as : _____

4. Which suitable condition you prefer to do counseling session?

☐ Face to face

☐ Online

☒ Both

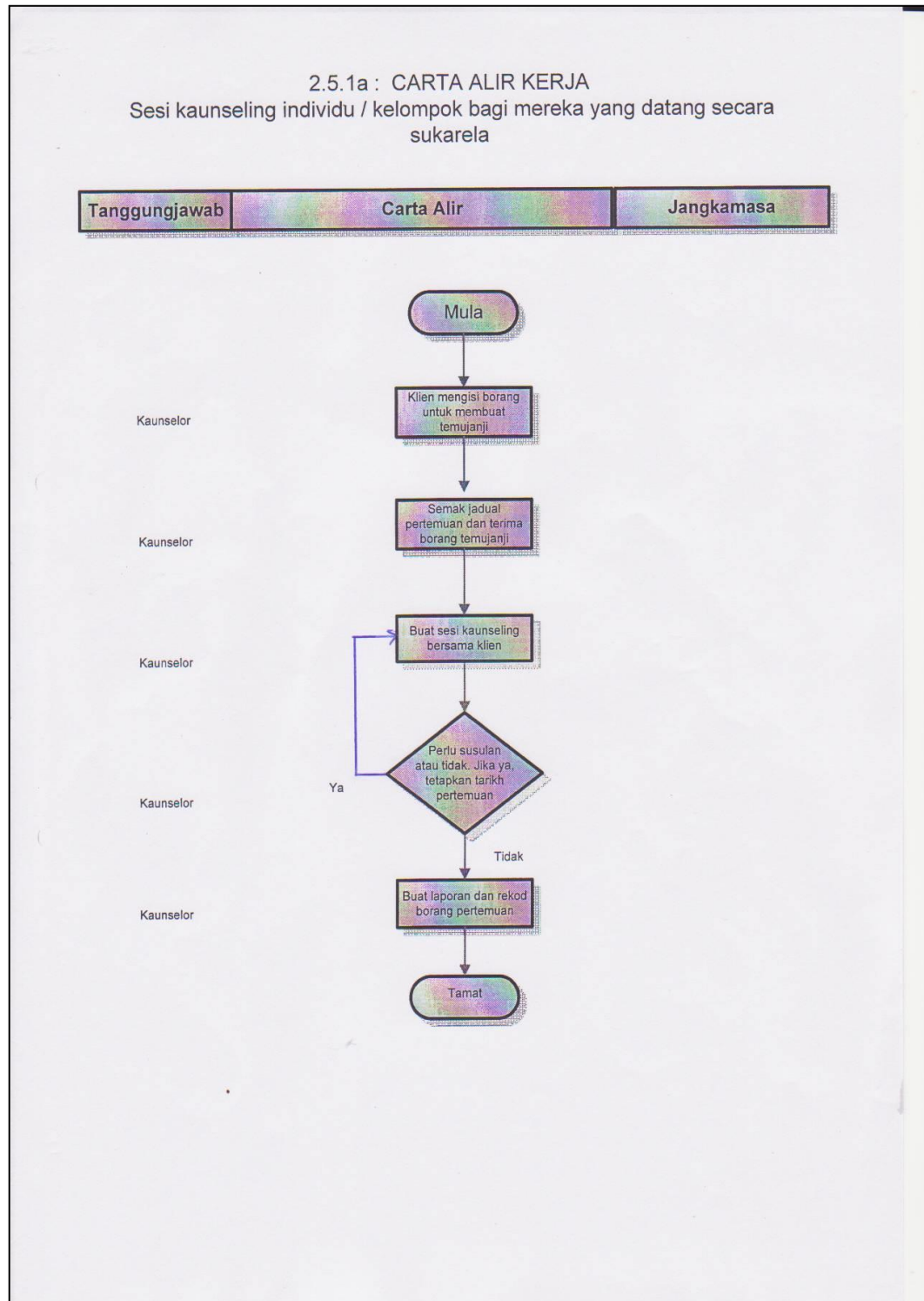
5. Which application below that you hope provide in online counseling system?

☒ Booked appointment

☒ Counsellor Schedule

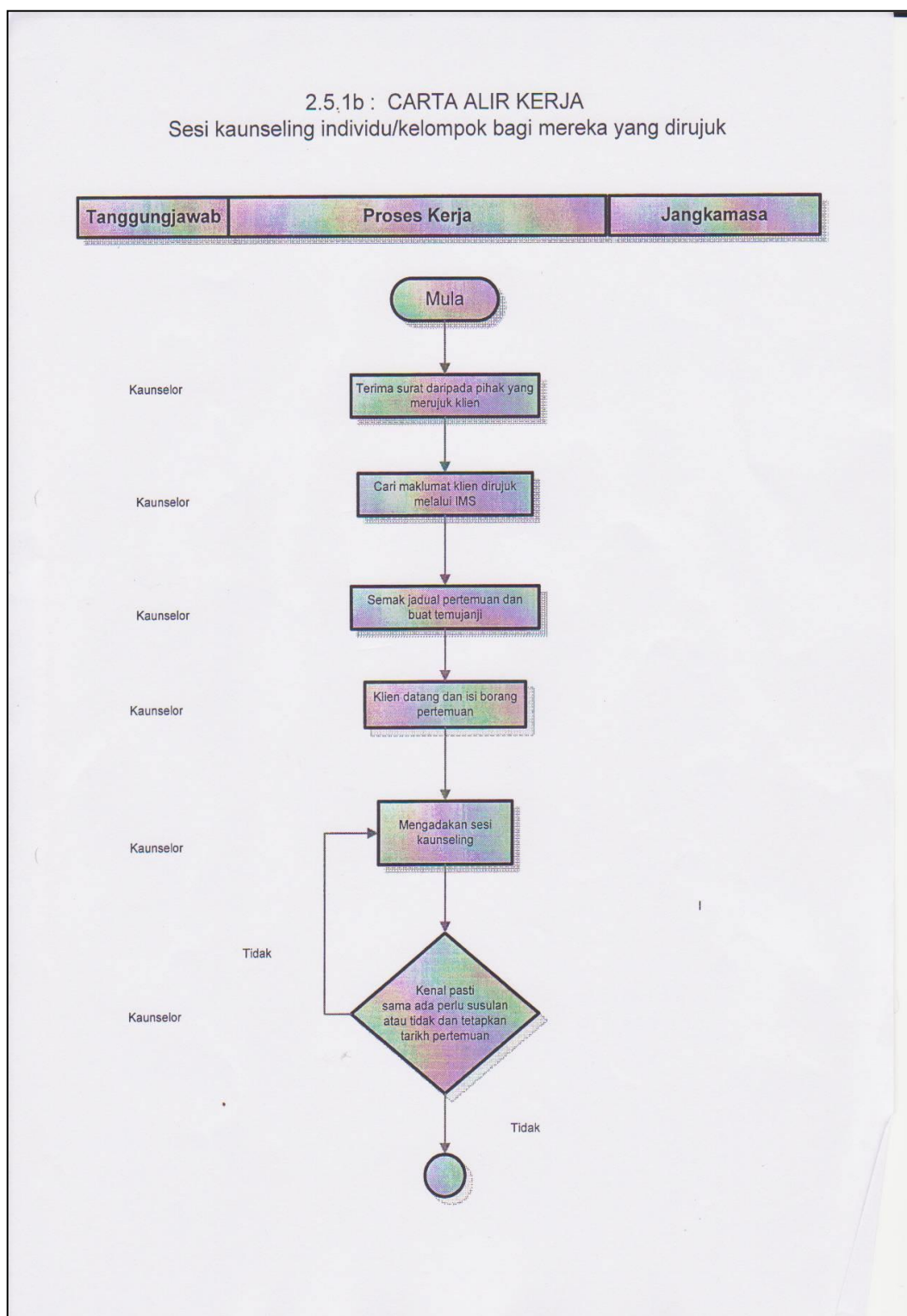
☒ Forum

☐ Others. article

APPENDIX F**Flowchart of counseling session for student who come willingly**

APPENDIX G

Flowchart of counseling session for student who is referred



APPENDIX H

USER MANUAL FOR DATA ENCRYPTION IN E-COUNSELLING SYSTEM (DEECS) - STUDENT MODULE -



Figure S1 : Login page

1. Student need register first before can login and use the application. If already registered, student can login by using ID number as a username and enter the password.

Figure S2 : Registration page

1. This is the interface of student registration. User need enter all required data.

Family Background

Marital Status : **

Father's Name :

Age :

Occupation :

Telephone :

Mobile :

Address :

Mother's Name : **

Age :

Occupation :

Telephone : ** (eg : 09xxxxxxx)

Mobile : ** (eg : 019xxxxxxx)

Address :

Student Detail Successfully Registered...

[Preview](#)

[Save](#)

Click here to submit the registration

Figure S3 : Page of registration after student successfully registered

- After fulfill all required data, submit the form by enter 'Save'. System will automatically inform user that they already success register

UNIVERSITI MALAYSIA PAHANG
Engineering • Technology • Creativity

Counselling Unit

User : Fatem binti Kamarudin

[Home](#)

[MY PROFILE](#)

[Student Data](#)

[View profile](#)

[View counsellor detail](#)

[Sending memo to counsellor](#)

[Request appointment with counsellor](#)

[View request status](#)

[View Counsellor Detail](#)

[Memo](#)

[Appointment](#)

[View Request](#)

Online Counselling ?
Online counselling generally refers to the provision of professional mental health services concerns via internet communication technology.

What is a Counsellor ?
Counsellors assist people to better understand themselves by explaining options, setting goals and helping them to take action. There are no formal qualifications required to be a counsellor, however most professionals will have a degree or diploma in counselling, psychology or social work.

Figure S4 : Student homepage

- Student can access system after success login. Name of user will preview under the header. Above, are all application that student can access and their function.

UNIVERSITI MALAYSIA PAHANG
Engineering • Technology • Creativity
Counselling Unit

User : Fatem binti Kamarudin [<Log Out>](#)

[Home](#) [Student Management](#)

Student Management > Register

Student Detail --> [Edit](#)

Click here to edit profile

*** Required Data

Name :	Fatem binti Kamarudin
ID No :	CC06990
IC No :	2147483647
Faculty :	FSKKP
Course :	BCN
Telephone :	95310123
Mobile :	132321844
Email :	al_islam87@yahoo.com
No Of Siblings :	3 from 3
Gender :	Female
Religion :	Islam
Race :	Malay
Status :	Single

APPLICATION

- [Counsellor Detail](#)
- [Memo](#)
- [Appointment](#)
- [View Request](#)

Figure S5 : View profile

5. Student can view their detail by click at 'Student Detail'. If student want to change their detail information, they can click 'Edit' then system will bring student to edit page.

Family Background

Marital Status :

Father's Name :

Age :

Occupation :

Telephone :

Mobile :

Address :

Mother's Name :

Age :

Occupation :

Telephone : ** (eg : 09xxxxxxx)

Mobile : ** (eg : 019xxxxxxx)

Address :

Click here to update profile

Student Detail Successfully Update...

[Preview](#)

[Update](#)

Click here to update profile

Figure S6 : Update profile

6. Student can change only certain data. After change the profile, click 'Update' then system automatically inform that student detail was succeed update and will automatically save to database.

The screenshot shows the 'E-COUNSELLING' interface of the Universiti Malaysia Pahang Counselling Unit. The user is logged in as 'User : Fatem binti Kamarudin'. The interface includes a navigation menu on the left with 'Home', 'MY PROFILE', and 'Student Detail'. The main content area displays a table of counsellors with columns for StaffID, Staff Name, and Phone Office. A red box highlights the 'Staff Name' column with the text 'Click here to preview counsellor detail' and an arrow pointing to the name 'Paridah binti Mohd Ali'.

StaffID	Staff Name	Phone Office
0337	Paridah binti Mohd Ali	95492538
0339	Yunan bin Abdul Samad	95492569

Figure S7 : View list of counsellors

7. This page will show the list of counsellor and their general detail. Just click on staff name, student can view counsellor profile in detail.

The screenshot shows the 'View Counsellor Details' page. The user is logged in as 'User : Fatem binti Kamarudin'. The interface includes a navigation menu on the left with 'Home', 'MY PROFILE', and 'Student Detail'. The main content area displays the 'Counsellor Detail' for 'Paridah binti Mohd Ali'. The details include Name, ID No, IC No, Position, Education, Phone Office, Mobile, Email, Gender, Religion, Race, and Registration Date.

Counsellor Detail	
Name :	Paridah binti Mohd Ali
ID No :	0337
IC No :	0
Position :	Counsellor
Education :	
Phone Office:	95492538
Mobile :	0
Email :	paridahmdali@ump.edu
Gender :	Female
Religion :	Islam
Race :	Malay
Registration Date :	12/09/1990

Figure S8 : View counsellor details

8. This is the interface of view counsellor detail after click on staff name.



Figure S9 : View list of message in inbox

9. This interface will show list of message in inbox. To preview the message, just click on subject, then system will show the message.

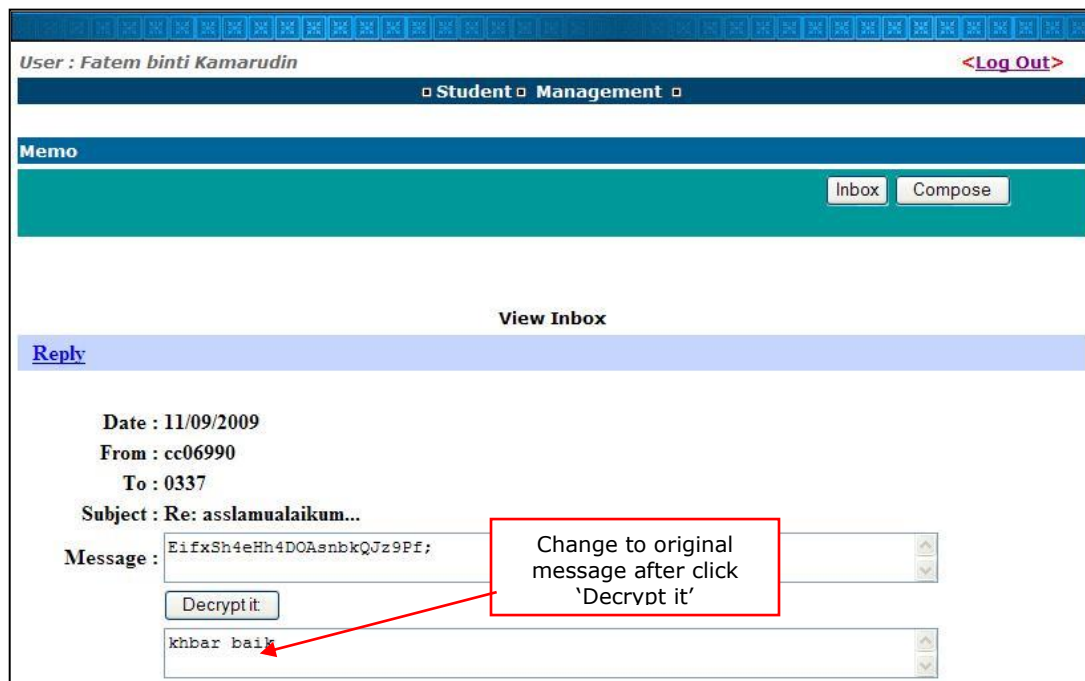


Figure S10 : Read message

10. To read the message, student need to click button 'Decrypt it' to change message which is in cipher text to plaintext (original message).

UNIVERSITI MALAYSIA PAHANG
Engineering * Technology * Creativity
Counselling Unit

User : Fatem binti Kamarudin [<Log Out>](#)

Student Management

Memo

Inbox Compose

enter counsellor ID

Date: 2009-11-12

To: 0337 (0337: P)

Subject: Selamat Pagi

Message:

Puan saya ingin meluahkan saya. Boleh ke?

Submit

Message will be encrypt automatically after click button 'Submit' and will be save to database in form cipher text (encrvnt).

Figure S11 : Compose message

11. To send message to counsellor, student must enter counsellor id in field 'To'. After finish type a message, click 'Submit', then message will automatically encrypt during this time and save to the database in form of cipher text. So no one can read the message.

UNIVERSITI MALAYSIA PAHANG
Engineering * Technology * Creativity
Counselling Unit

User : Fatem binti Kamarudin [<Log Out>](#)

Student Management

Memo

Inbox Compose

cc06990
Date: 2009-11-12
Receiver: 0337
Subject: Selamat Pagi
Messages: Puan saya ingin meluahkan masalah. Saya harap puan dapat membantu saya. Boleh ke?

Your message has been encrypted & successfully submitted.
[Inbox](#)

Figure S12 : Message report

12. After success send message to counsellor, system will show the report of sent message.

UNIVERSITI MALAYSIA PAHANG
Engineering * Technology * Creativity
Counselling Unit

User : Fatem binti Kamarudin [<Log Out>](#)

[Home](#) [Student Management](#)

[MY PROFILE](#) [Student Detail](#)

[APPLICATION](#)
[Counsellor Detail](#)
[Memo](#)
[Appointment](#)
[View Request](#)

Student Management > Request Appointment

Student Name :	Fatem binti Kamarudin
Faculty :	FSKKP
Date Apply :	2009-11-12
Counsellor Incharge :	Paridah binti Mohd Ali
Specification :	saya nak jumpa puan jam 3 petang di

[Reset](#) [Submit](#)

Go to page of appointment request

Figure S13 : Request an appointment with counsellor

13. This is page of appointment request. Student need to select the counsellor they want to see, and leave a specification like place or time want to meet, then click 'Submit'. This request will be sent counsellor whether they want to reject or approve the appointment request.

Your Request Has Been Successfully Sent...

REQUEST APPOINTMENT FORM	
Student ID :	CC06990
Student Name :	Fatem binti Kamarudin
Faculty :	FSKKP
Date Apply :	2009-11-12
Counsellor Incharge :	Paridah binti Mohd. Ali
Specification :	saya nak jumpa puan jam 3 petang di pejabat puan

[Back>>](#)

will take user back to the page of appointment request

Figure S14 : Report after successful sent appointment request

14. This page will be show after appointment request successfully sent.

UNIVERSITI MALAYSIA PAHANG
Engineering * Technology * Creativity
Counselling Unit

User : Fatem binti Kamarudin [Log Out](#)

Student Application

Appointment Application > Status

Status Information

Counsellor ID	Date Applied	Status	Comment
Paridah binti Mohd. Ali	2009-11-12	Accepted	
Paridah binti Mohd. Ali	2009-11-13	Accepted	

© All rights reserved. 2009 University Malaysia Pahang.
Lebuhraya Tun Razak, 26300 Kuantan, Pahang Darul Makmur.
Phone : 09-5492020 Fax : 09-5492222.

Figure S15 : View appointment request status reply by counsellor

15. This page will be show the status of appointment with counsellor which is request by student.

USER MANUAL FOR DATA ENCRYPTION IN E-COUNSELLING SYSTEM (DEECS) - COUNSELLOR MODULE -

2.0



Figure C1 : Login page

1. Counsellor must be register by admin first before can login and use the application. If already registered, counsellor can login by using ID number as a username and enter the password.



Figure C2 : Counsellor homepage

2. Counsellor can access system after success login. Above, are all application that counsellor can access and their function.

UNIVERSITI MALAYSIA PAHANG
Engineering * Technology * Creativity
Counselling Unit

User : Paridah binti Mohd Ali [<Log Out>](#)

Counsellor Management

Counsellor Management > Registrati

Counsellor Detail --> Edit

Required Data

Name : Paridah binti Mohd Ali
ID No : 0337
IC No : 0
Position : Counsellor
Education :
Phone Office : 95492538
Mobile : 0
Email : paridahmdali@ump.edu
Gender : Female
Religion : Islam
Race : Malay
Registration Date : 12/09/1990

APPLICATION

[Memo](#)
[Appointment](#)
[Pending Request](#)

Figure C3 : View profile

3. Counsellor can view their detail by click at 'Counsellor Detail'. If counsellor want to change their detail information, they can click 'Edit' then system will bring counsellor to edit page.

Family Background

Marital Status :

Father's Name :

Age :

Occupation :

Telephone : ** (eg : 09xxxxxxx)

Mobile :

Address : **

Mother's Name :

Age :

Occupation :

Telephone : ** (eg : 09xxxxxxx)

Mobile : ** (eg : 019xxxxxxx)

Address : **

Counsellor Detail Successfully Update...

[Preview](#)

Click here to update profile

Update

Click here to update profile

Figure C4 : Update profile

4. Counsellor can change only certain data. After change the profile, click 'Update' then system automatically inform that counsellor detail was succeed update and will automatically save to database.

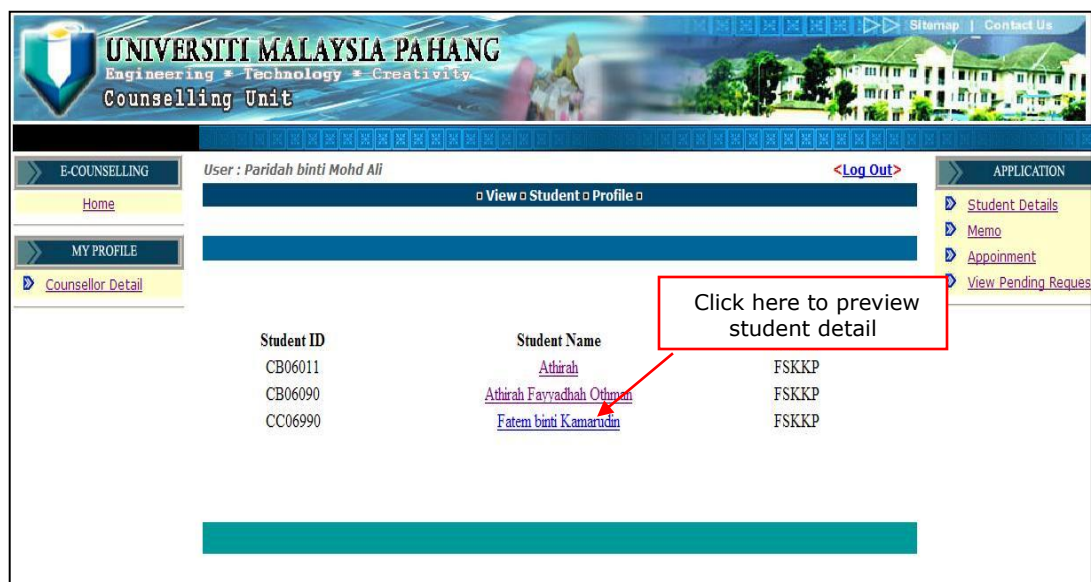


Figure C5 : View list of students

- This page will show the list of student on their general detail. Just click on student name, counsellor can view student profile in detail.



Figure C6 : View student details

- This is the interface of view student detail after click on student name.



Figure C7 : View list of message in inbox

7. This interface will show list of message in inbox. To preview the message, just click on subject, then system will show the message. Beside that, pop up message will show after successful delete message.

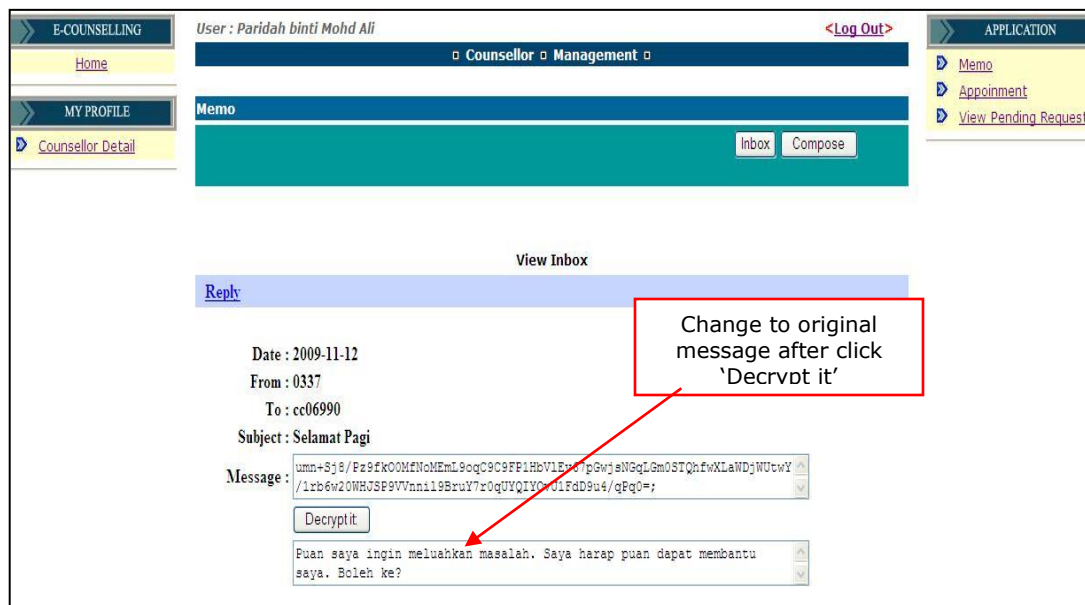


Figure C8 : Read message

8. To read the message, student need to click button 'Decrypt it' to change message which is in cipher text to plaintext (original message).

E-COUNSELLING User : Paridah binti Mohd Ali <Log Out> APPLICATION

Home Counsellor Management Memo Appointment View Pending Request

MY PROFILE Counsellor Detail

Inbox Compose

Receiver ('To') and subject will be automatically called from previous message

Date: 2009-11-12 To: cc06990 Subject: Re: Selamat Pagi

Message: Salam.. ye. Apa masalah yang ingin dikongsi. InsyaAllah, kalau saya boleh bantu, saya akan membantu

Submit

Message will be encrypted automatically after click button 'Submit' and will be save to database in form cipher text (encrypt).

Figure C9 : Reply student message

- After finish type a message, click 'Submit', then message will automatically encrypt during this time and save to the database in form of cipher text. So no one can read the message.

UNIVERSITI MALAYSIA PAHANG
Engineering • Technology • Creativity
Counselling Unit

E-COUNSELLING User : Paridah binti Mohd Ali <Log Out> APPLICATION

Home Counsellor Management Memo Appointment View Pending Request

MY PROFILE Counsellor Detail

Inbox Compose

0337
Date: 2009-11-12
Receiver: cc06990
Subject: Re: Selamat Pagi
Messages: InsyaAllah, boleh je berkongsi masalah dengan saya. Saya sedia membantu

Your message has been encrypted & successfully submitted.

[Inbox](#)

Figure C10 : Message report

- After success reply message to student, system will show the report of sent message.



Figure C11 : Reply appointment request by student

11. This is page of appointment request by student. Counsellor need to decide whether they want to approve or reject the request and leave a comment. Then, click 'OK' to reply/submit the request. The pop up message will appear to inform counsellor that the reply request was successful update/send



Figure C12 : Appointment schedule

12. This page will be show after reply appointment request was successfully sent.

APPENDICES