97-2 Preliminary Syllabus, Da-Yeh Univ

Information			
Title	密碼學	Serial No. / ID	1320 / IFR5007
Dept.	資訊工程學系碩士班	School System / Class	研究所碩士班1年1班
Lecturer	張世旭	Full or Part-time	專任
Required / Credit	Optinal / 3	Graduate Class	NO
Time / Place	(四)678 / H717-1	Language	Chinese

Introduction

This course gives an introduction to the basic theory and practice of cryptographic techniques used in computer security. The students will realize the following important topics:
Number theory, Symmetric Cryptosystem (DES, Triple DES, AES), Public-key Cryptosystem (DH,RSA,DSS), Hash function, digital signature, and SET.

Outline

1. Introduction
2. Number theory
3. symmetric cipher
4. asymmetric cipher
5. Hash function
6. Signature
7. SET and PGP

Prerequisite

algorithm and Fundamental Mathmatics.