

# 101-2 Preliminary Syllabus, Da-Yeh Univ

Information			
Title	密碼學	Serial No. / ID	1419 / 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	(一)567 / H713	Language	Chinese

Introduction
<p>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.</p>

Outline
<ol style="list-style-type: none"><li>1. Introduction</li><li>2. Number theory</li><li>3. symmetric cipher</li><li>4. asymmetric cipher</li><li>5. Hash function</li><li>6. Signature</li><li>7. SET and PGP</li></ol>

Prerequisite
algorithm and Fundamental Mathematics.