MODULE **DESCRIPTOR**

MODULE TITLE	CRYPTOLOGY		
MODULE CODE	MA2812 (L5)	**CREDIT VALUE**	20 CREDITS (10 ECTS)
CAMPUS	UCLAN CYPRUS		
SCHOOL	SCHOOL OF SCIENCE		

MODULE **AIMS**

To enable students to understand the mathematics for the implementation of the public key crypto systems RSA and El Gamal as well as attacks on such systems.

MODULE **CONTENT**

Congruences: Properties, solution of linear congruences, inverses,

Symmetric cipher: How to encrypt, decrypt and break a symmetric cipher such as Hill or Vigenere

The Euler-Phi function: Euler's Theorem, Primitive roots, search algorithm

Public Key Cryptography: Diffie-Hellman key exchange, RSA Cipher, ElGamal Cipher

Primality Tests: FLT and (Fermat) Pseudoprimes, Strong Pseudoprimes, Miller-Rabin Test.

Factorization methods: Such as Pollard's p-1 and UEF and using them to break RSA.

Discrete Log evaluation: Such as Baby-step Giant-step and using them to break ElGamal

INTENDED **LEARNING OUTCOMES**

On successful completion of this module a student will be able to:	
1.	Solve problems about divisibility and congruences.
2.	Prove properties about the underlying mathematics used in RSA and ElGamal
3.	Encrypt and Decrypt using rsa and elgamal
4.	Use Factorization methods like pollards p-1 and uef to attack rsa
5.	Evaluate discrete logs using baby step giant step to attack elgamal

TEACHING **METHODS**

The direct contact will consist of lectures. During these lectures theory will be introduced and developed. Examples will be demonstrated throughout the module during these lectures. The lectures will also contain assisted problem solving. Regular non-assessed work sheets will be provided.

ASSESSMENT **METHODS**

The module is assessed through 2 assignments and a written examination.