SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity Including BCT)

COURSE NAME : Fundamentals Of Cryptography

II YEAR / III SEMESTER

Unit I

Topic :Modular Arithematic

Modular Arithemetic

Congruence

In cryptography congruence(≅) instead of equlity(=)

Examples:

15 ≅ 3(mod 12)

23 ≅ 11(mod 12)

33 ≅ 3(mod 10)

10 ≅ -2(mod 12)

So , a ≅ b(mod m)

i.e a = km + b

VALID OR INVALID

$38 \cong 2 \pmod{12}$

$38 \cong 14 \pmod{12}$

$5 \cong 0 \pmod{5}$

$10 \cong 2 \pmod{6}$

$13 \cong 3 \pmod{13}$

$2 \cong -3 \pmod{5}$

One more Analogy

NO of wraps (Quotient)	Remaining Thread (Remainder)	Congruence
1	25	$35 \cong 25 \pmod 1$
2	15	$35 \cong 15 \pmod 2$
3	5	$35 \cong 5 \pmod 3$

Properties Of Modular Arithemetic

1. [(a mod n) + (b mod n)] mod n = (a + b) mod n
2. [(a mod n) - (b mod n)] mod n = (a – b) mod n
3. [(a mod n) * (b mod n)] mod n = (a * b) mod n