# Mathematics of Symmetric Key Cryptography
# Unit-II

J. Bhuvana, ASP / CSE

August 29, 2020

# Session Objectives

- To learn about the modular arithmetic operations

# Session Outcomes

At the end of this session, participants will be able to discuss

- Modular arithmetic operations

# Agenda

1. Modular Arithmetic

# Presentation Outline

# Modular Arithmetic

- define modulo operator "a mod n" to be remainder when $a$ is divided by $n$ where integer $n$ is called the modulus
- $b$ is called a residue of $a \ mod \ n$ since with integers can always write: $a = qn + b$
- usually chose smallest positive remainder as residue ie.$0 <= b <= n - 1$
- process is known as modulo reduction
  eg. $-12 \ mod \ 7 = -5 \ mod \ 7 = 2 \ mod \ 7 = 9 \ mod \ 7$
- a & b are congruent if: **a mod n = b mod n** when divided by n, a & b have same remainder
  eg. $100 \ mod \ 11 \cong 34 \ mod \ 11$ so 100 is congruent to 34 mod 11

# Modular Arithmetic Operations

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

e.g. $[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$ ;
$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$

$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$
$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$

$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$
$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$

# Modulo 8 Addition Example

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |

# Modulo 8 Multiplication

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 6 |
| 3 | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 |
| 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 5 | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |
| 6 | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |
| 7 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

# Modular Arithmetic Properties

| Property | Expression |
|---|---|
| Commutative Laws | $(w + x) \bmod n = (x + w) \bmod n$<br>$(w \times x) \bmod n = (x \times w) \bmod n$ |
| Associative Laws | $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$<br>$[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$ |
| Distributive Law | $[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$ |
| Identities | $(0 + w) \bmod n = w \bmod n$<br>$(1 \times w) \bmod n = w \bmod n$ |
| Additive Inverse $(-w)$ | For each $w \in Z_n$, there exists a $z$ such that $w + z \equiv 0 \bmod n$ |

# Additive and Multiplicative Inverses

- Additive inverse: For any integer a $\in Z_m$, b $\in Z_m$ is the additive inverse of a if
  $(a+b)\ mod\ \ m \cong 0$
- Multiplicative inverse: For any integer a $\in Z_m$, integer b is the multiplicative inverse if
  $ab\ \ \cong 1\ mod\ \ m$

# Summary

- Modular arithmetic with integers