SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

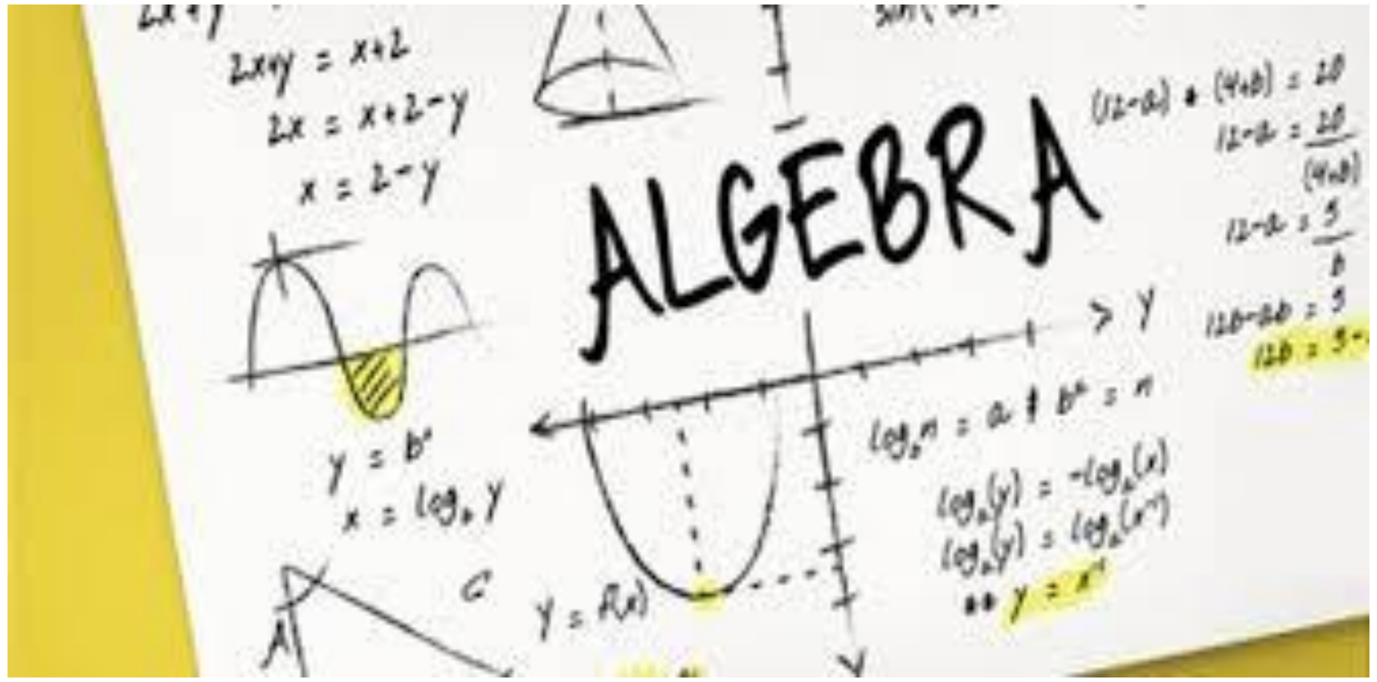
Course Code and Name : 19CS503 – CRYPTOGRAPHY AND NETWORK SECURITY

Unit 2: Symmetric Cryptography

Topic : MATHEMATICS OF SYMMETRIC KEY CRYPTOGRAPHY: Algebraic structures-Groups, Rings, Fields

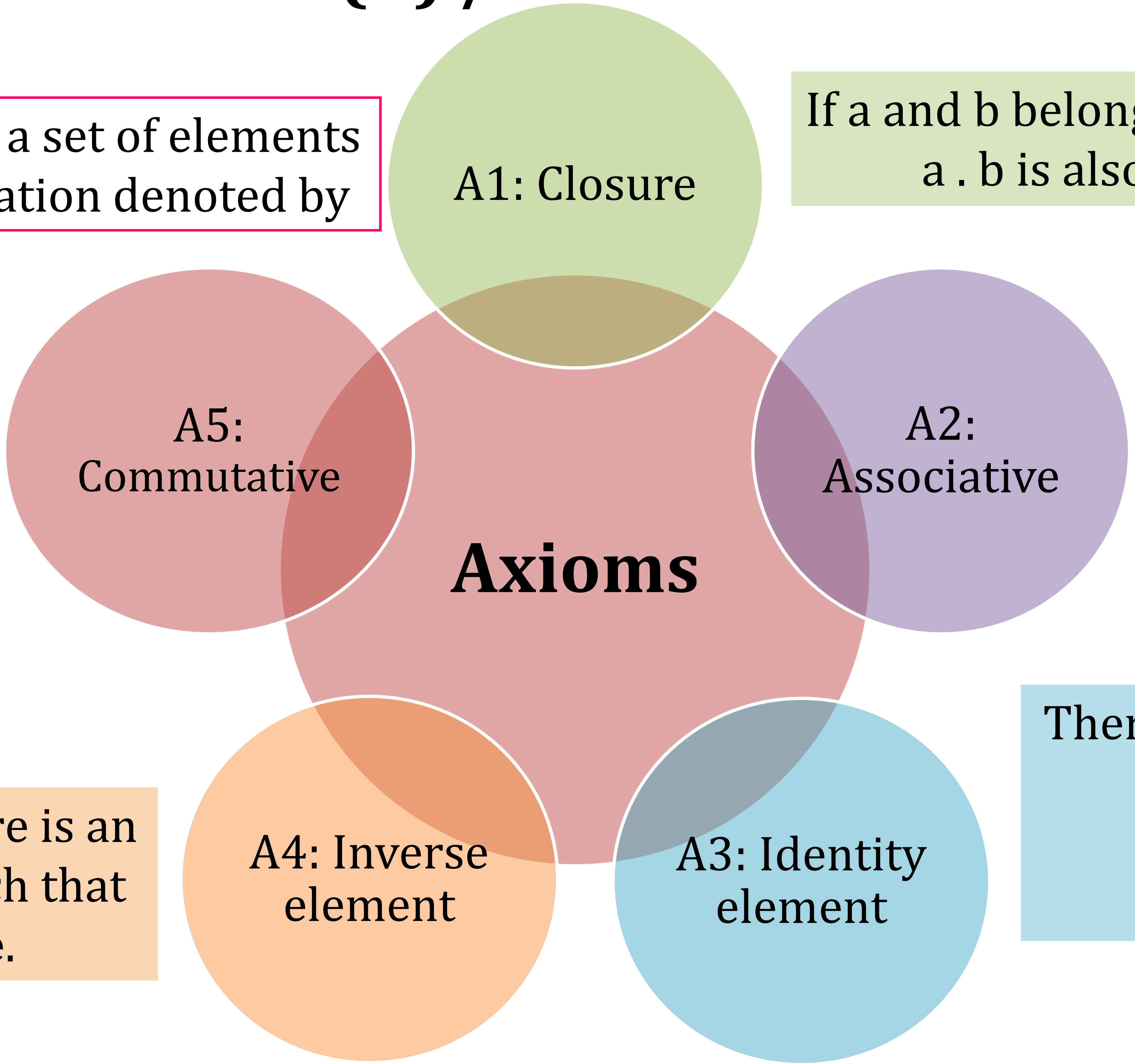
COMMON ALGEBRAIC STRUCTURES

- Algebraic Structures
  - Group
  - Ring
  - Field



GROUP (G) / ABELIAN GROUP

denoted by {G, .}, is a set of elements with a binary operation denoted by



If a and b belong to G, then a . b is also in G.

a . (b . c) = (a . b) . c for all a, b, c in G.

There is an element e in G such that a . e = e . a = a for all a in G.

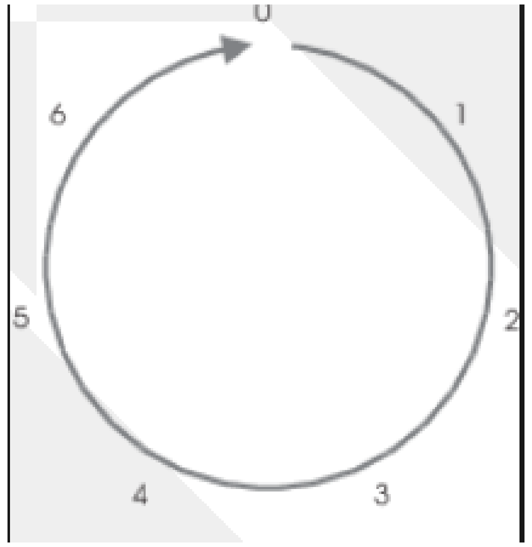
For each a in G, there is an element a′ in G such that a .a′ = a′ . a = e.

Abelian Group

a . b = b . a for all a, b in G.

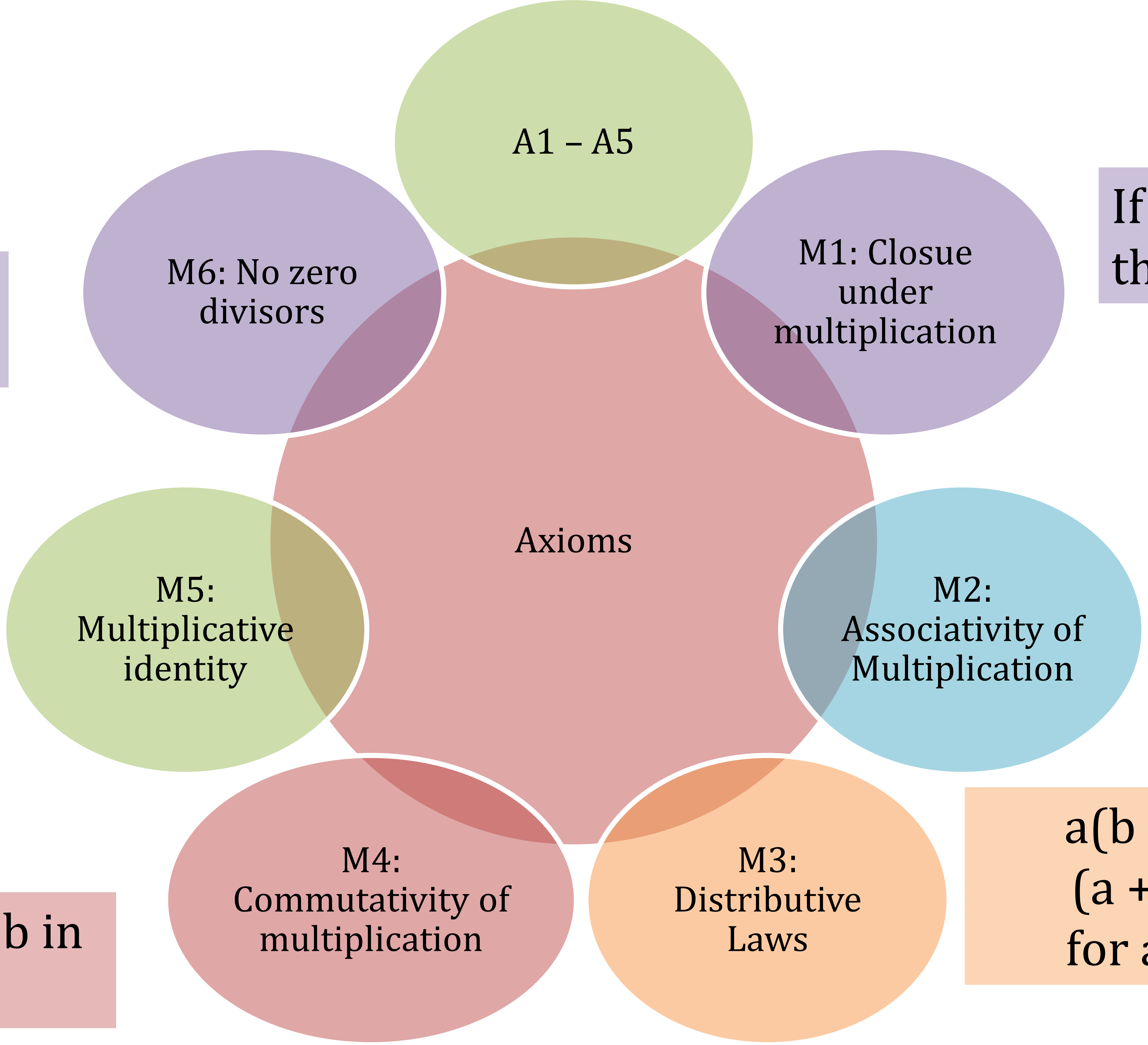
CYCLIC GROUP

- A group is cyclic if every element is a power of some fixed element
- ie $b = a^k$ for some a and every b in group
- a is said to be a generator of the group



RING (R)

denoted by {R, +, *}, is a set of elements with two binary operations, called addition and multiplication



If a and b belong to R, then ab is also in R.

a(bc) = (ab)c for all a, b, c in R

a(b + c) = ab + ac
(a + b)c = ac + bc
for all a, b, c in R.

Integral Domain

If a, b in R and ab = 0, then either a = 0 or b = 0.

There is an element 1 in R such that a1 = 1a = a for all a in R.

Commutative Ring

ab = ba for all a, b in R

FIELDS (F)

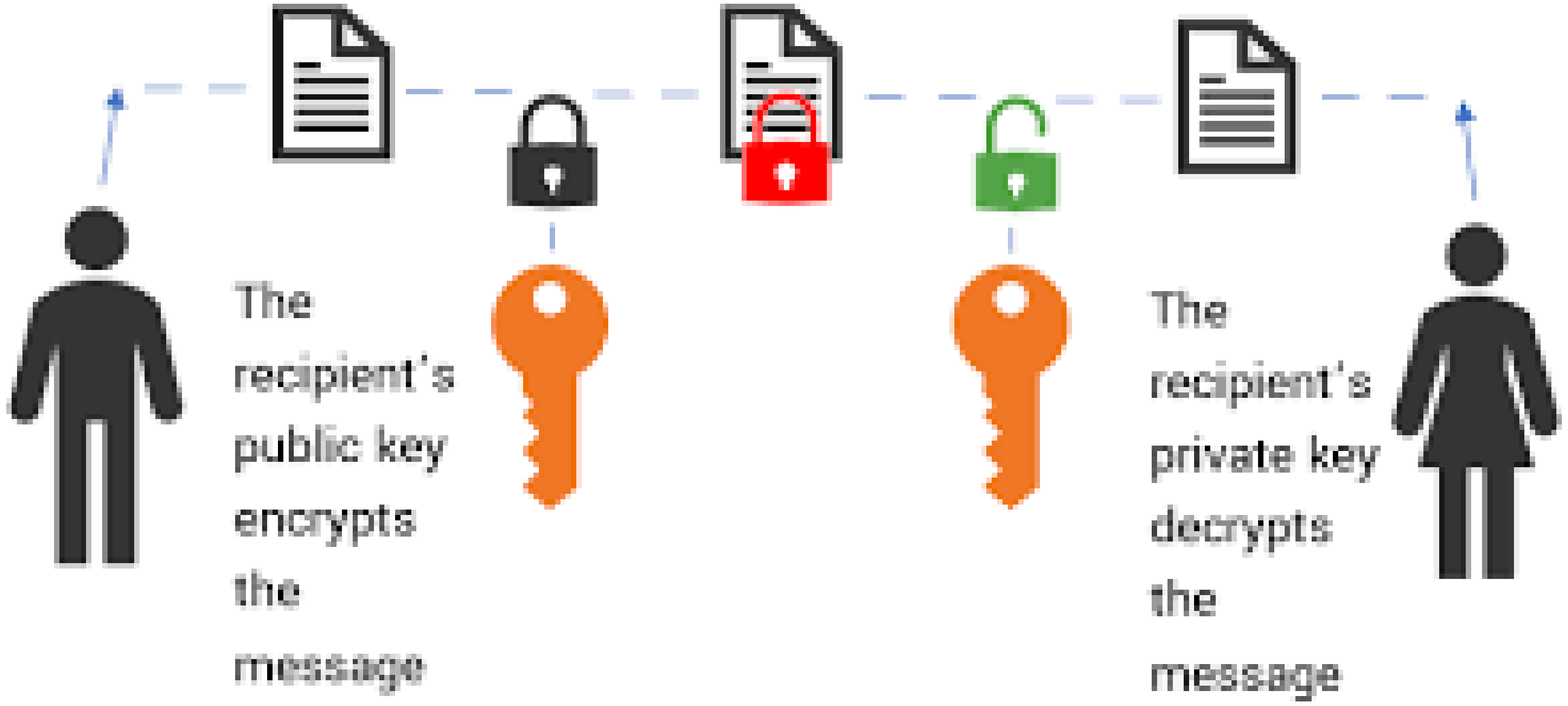
denoted by {F, +, *}, is a set of elements with two binary operations, called addition and multiplication

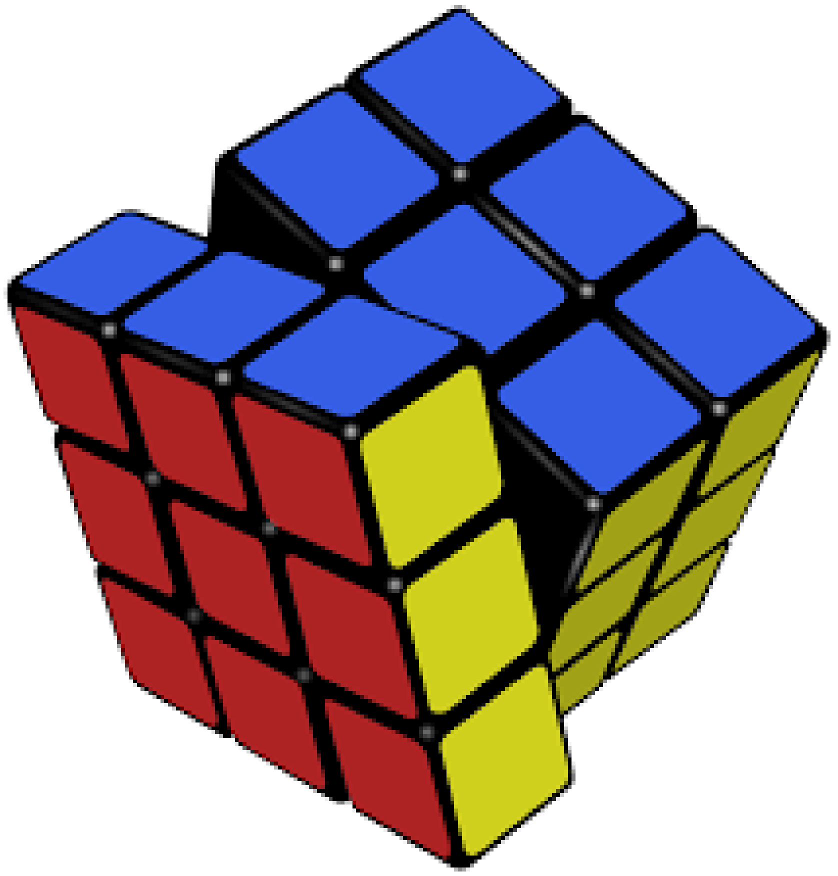
A1 to M6 + **M7: Multiplicative inverse** = **Fields**

For each a in F, except 0, there is an element a^{-1} in F such that

$$aa^{-1} = (a^{-1})a = 1.$$

WHY ALGEBRAIC STRUCTURES IN CRYPTOGRAPHY?

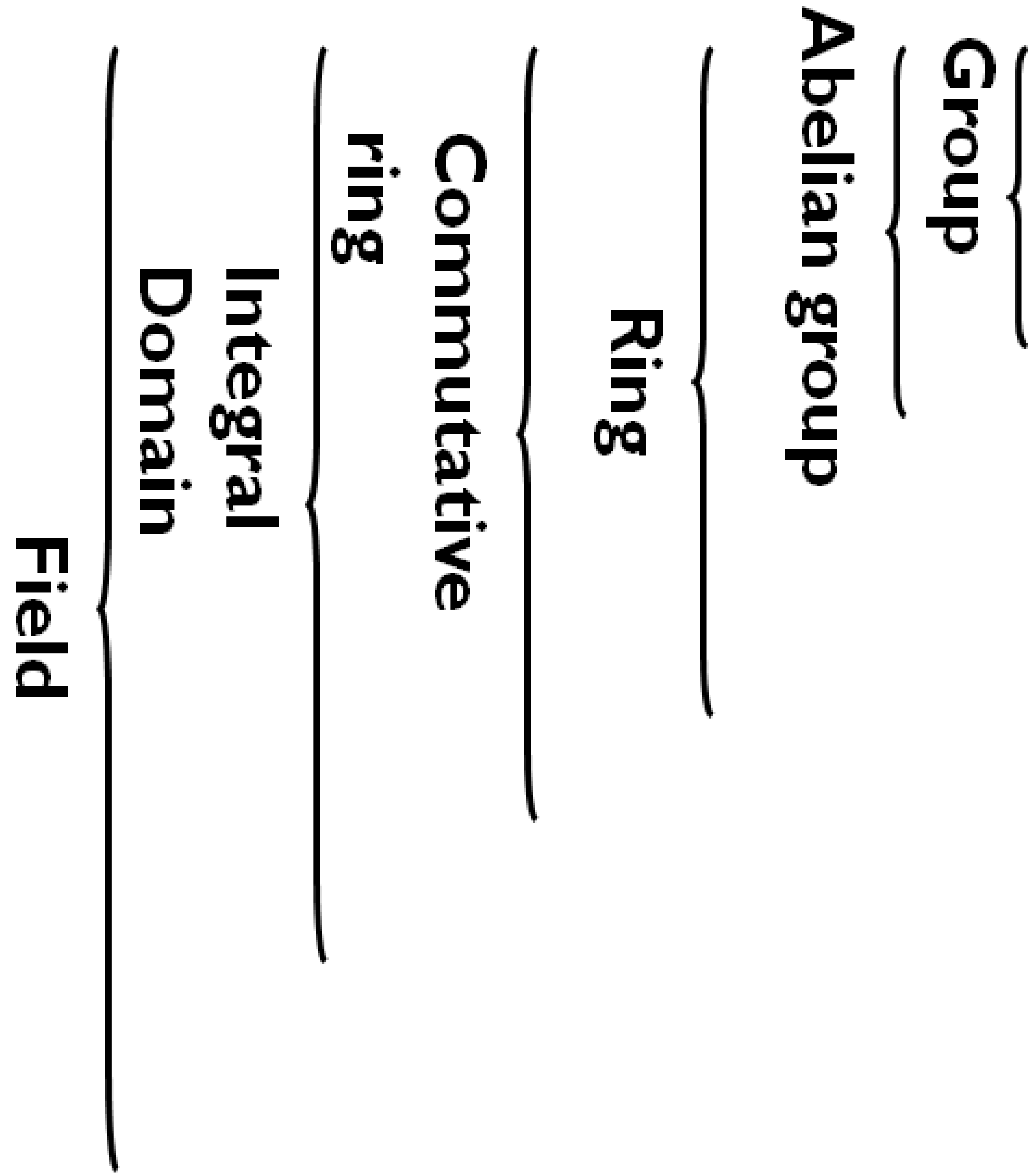




ASSESSMENT - Complete the chart.

(A1) Closure under addition
(A2) Associativity of addition
(A3) Additive identity
(A4) Additive inverse
(A5) Commutativity of addition
(M1) Closure under multiplication
(M2) Associativity of multiplication
(M3) Distributive law
(M4) Commutativity of multiplication
(M5) Multiplicative identity
(M6) No zero divisors
(M7) Multiplicative inverse

ASSESSMENT SOLUTION - Complete the chart.



(A1) Closure under addition
(A2) Associativity of addition
(A3) Additive identity
(A4) Additive inverse
(A5) Commutativity of addition
(M1) Closure under multiplication
(M2) Associativity of multiplication
(M3) Distributive law
(M4) Commutativity of multiplication
(M5) Multiplicative identity
(M6) No zero divisors
(M7) Multiplicative inverse

REFERENCES

William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.

THANK YOU