UNIT-2

Topic :- 1 - Mathematics of symmetric key cryptography and Algebraic structures.

-> Symmetric algorithms are used by symmetric ciphers for encrypting the data.

-> A symmetric algorithm uses the same key for both encryption and decryption of given data.

-> Ex:- A symmetric encryption algorithm uses k to encrypt the data means, then same k should be used for decryption.

-> This symmetric ciphers are opposite to Asymmetric ciphers. As, Asymmetric cipher encryption process uses different key for encryption and decryption process.

-> The key used for encryption is public key and the key used for decryption is private in nature.

-> Ex for Asymmetric encryption is RSA.

characteristics of symmetric encryption :-

-> This algorithm has high speed

-> But lack in security and also in key management

-> Yet, this is used in many domains today.

Popular symmetric key: AES (Advanced Encryption Standard)

-> It is used on single machine for encryption and decryption.

-> This eliminates Need for sharing secret keys as this was used in first modern computing.

Algebraic structures

→ Cryptography requires set of integers and some sepcific operations that are defined for those sets

→ The combination of set and operation which are applied to the element of set is called algebraic structure

GROUPS

A Group G, denoted by $\{G, *\}$ set of element with a binary operation denoted by '*'.

Modular arithmetic

mod operation

→ $7 \bmod 4 = 3$

→ $-11 \bmod 7 = 3$ $-x \bmod y = y - (x \bmod y)$

$-7 \bmod 3$

$= 7 - (4 \bmod 7)$

$y - (x \bmod y)$

$3 - (7 \bmod 3) -$ $= 7 - (4)$

$3 - 1 = 2$ $= 3$

→ $-11 \bmod 17 = 6$ $-11 + 17 \Rightarrow 6$

Congruent modulo :-

Two integers are said to be congruent, where a and b are congruent modulo (n) if

$$(a \bmod n) = (b \bmod n)$$

This can be written as

$$a \equiv (b \bmod n) \text{ or } b \equiv (a \bmod n)$$

Ex:- $73 \equiv (4 \bmod 23)$ as $a = 73$ $b = 4$ $n = 23$.

$(73 \bmod 23) = (4 \bmod 23)$

$4 = 4$

23×2
46×2

23×3
69

Congruent properties:

→ $a \equiv b \pmod{n}$ iff $n | (a-b)$

→ $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$

→ If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$

then $a \equiv c \pmod{n}$.

Modular arithmetic operations / properties:-

→ $(a+b) \bmod n = [(a \pmod{n}) + b \pmod{n})] \bmod n$.

→ $(a-b) \bmod n = [a \pmod{n} - b \pmod{n}] \bmod n$

→ $(a*b) \bmod n = [a \pmod{n} \times b \pmod{n}] \bmod n$.

Take example:

$a=11 \quad b=15 \quad n=8$

Ex: $(6+8) \bmod 2 \quad a=6 \quad b=8 \quad n=2$

according to property 1

$(14) \bmod 2 = [6 \pmod{2}) + 8 \pmod{2}] \bmod n$

$0 = (0+0) \bmod 2$

$0 = 0 \bmod 2$

$0 = 0$

hence proved.

$(6-8) \bmod 2 = [6 \pmod{2}) - 8 \pmod{2})] \bmod 2$

$-2 \bmod 2 = [(6 \bmod 2) - (8 \bmod 2)] \bmod 2$

$0 = (0-0) \bmod 2$

$0 = 0$ by Property 2 of congruent modulo.

Hence Proved.

Ex:- $a = 11$ $b = 15$ $n = 8$

$(a \times b) \bmod n = (11 \times 15) \bmod n$

$= 165 \bmod 8 = 5$ LHS

RHS:-

$[(a \bmod n) \times (b \bmod n)] \bmod n$

$\Rightarrow (11 \bmod 8) \times (15 \bmod 8)] \bmod 8$

$= (3 \times 7) \bmod 8$

$= 21 \bmod 8$

$= 5$

LHS = RHS.

hence proved for property ③

Note:- Exponentiation is performed by the repeated multipuication.

$11^7 \bmod 13$

$\Rightarrow$ This can be written as $11^2 = 121$ hence $121 \bmod 13 = 4$

Next take $= 11^4$ which is $(11^2)^2 = 4^2 \bmod 13$

$= 3.$

hence $11^7 = 11 \times 4 \times 3$

$\Downarrow$

$11^1 \times 11^2 \times 11^4$

$11^7 = (11 \times 4 \times 3) \bmod n$

$11^7 \bmod n = 132 \bmod 13$

$\boxed{11^7 \bmod n = 2}$