# Number Theory for Information Security

D C Jinwala, PhD
dcj@svnit.ac.in
http://www.svnit.ac.in/dcj/

Department of Computer Engineering,
S V National Institute of Technology, Surat

1

## Contents

# One-to-one & onto functions

- def: one-to-one:
  - A function is 1-1, if each element in the codomain Y is the image of **at most** one element in the domain X.
- def: onto:
  - A function is onto, if each element in the codomain Y is the image of **at least** one element in the domain X. A function f: X →Y is onto, if Im(f) = Y.





# Tutorial#1

- Consider a function F whose domain-range are f: {a,b,c,d,e,f…z} → {0,1,2,3,4,5……25} with the definition as follows:

  f($i^{th}$ letter of alphabet) = i-1

  Analyze whether this function is one-to-one and onto or not ?
- Consider a function g whose domain-range are g: {binary bit strings of length 4} → {binary bit strings of length 3} with the definition as follows:

  $g(b_1b_2b_3b_4) = b_1b_2b_4$

  Analyze whether this function is one-to-one and onto or not ?

# Bijection of a function

- def: If a function f: X → Y is 1-1 and Im(f) = Y, then f is called a bijection.
- Obserⁿ1: If f: X → Y is 1-1 then f: X → Im(f) is a bijection
  - i.e. if f: X → Y is 1-1 and X and Y are finite sets of the same size. Why the latter ?





# Inverse of a function

- def: If f is a bijection from X to Y,
  - then there exists a bijection g from Y to X also i.e.
  - for each y ∈ Y, g(y) = x, where x ∈ X and f(x) = y.
  - Then, the function g so obtained from f is called the inverse function of f i.e $g = f^{-1}$

## Bijection & inverse of a function (contd)

- Let X = {a,b,c,d,e} and Y = {1,2,3,4,5} and let
  f be defined such that
  f(a) = 5, f(b) = 3, f(c)=4, f(d)=1, f(e)=2, then
  - f is one-to-one
  - Since Im(f) = {1,2,3,4,5} =Y, f is onto and it is bijection
  - The inverse function of f can be formed by defining a g such that……
  - If f is a bijection, so is $f^{-1}$
- Bijections are the heart of the crytography…..Why ?





## Bijection & inverse of a function (contd)

- In cryptography,
  - bijections are used to as a tool for encryption and the
    - inverse are used for decryption
  - Why bijections are required for encryption ?

# Tutorial#3: Bijection Functions

- Are the DES or the AES – the symmetric key cryptography algorithms bijections ?
- Is the RSA function a bijection ?

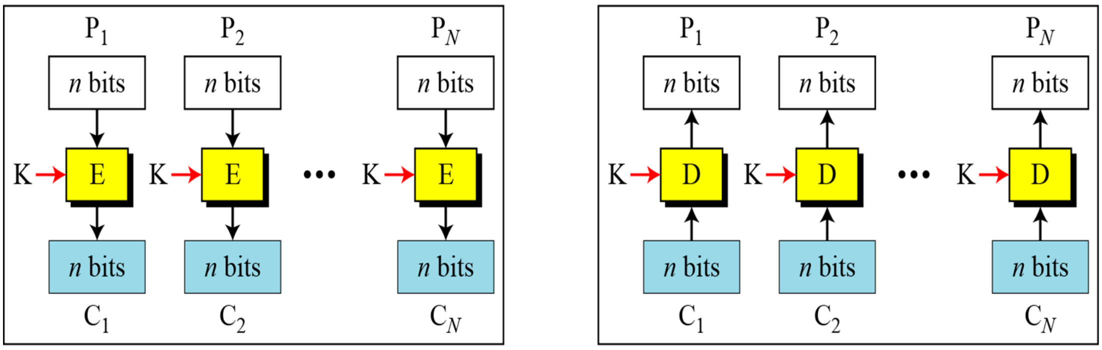


# Ciphers and the property of Determinism

- AES, DES, RC5……are these ciphers deterministic or probabilistic ?
- Determinism and Semantic Security
- How to introduce probabilistic nature in cipher implementation ?

# ECB Block Cipher Mode

E: Encryption　　D: Decryption
$P_i$: Plaintext block $i$　　$C_i$: Ciphertext block $i$
K: Secret key

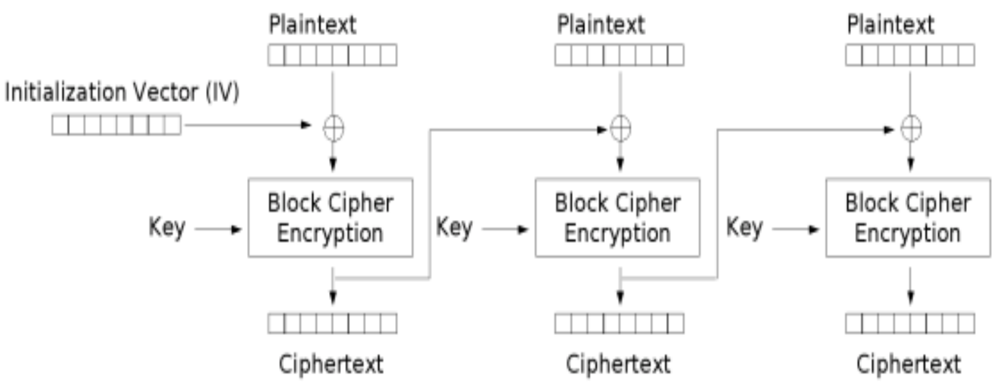



Encryption　　Decryption



11

# CBC Encryption & Use of an IV [wiki]

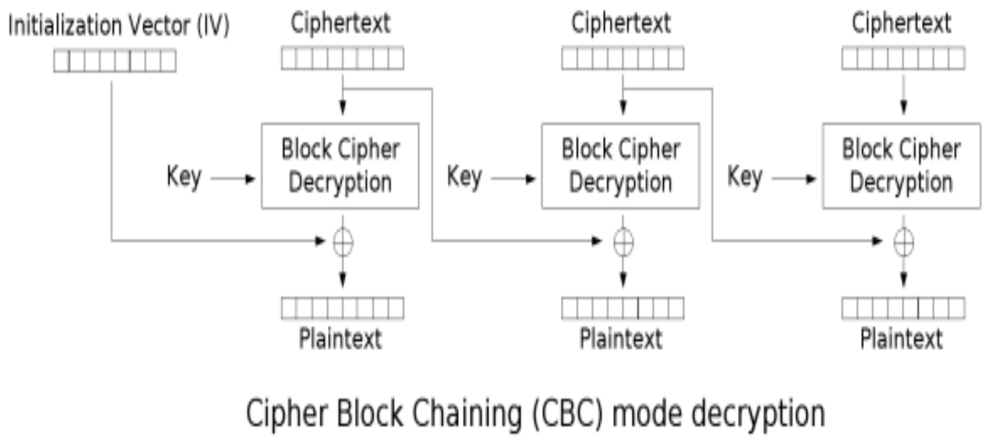



Cipher Block Chaining (CBC) mode encryption



12

## CBC decryption & Use of an IV [wiki]








## One way functions

- def: A function f: X →Y is called a one way function
  - if f(x) is *easy* to compute for all x ∈ X, but
  - for "essentially all" elements of y ∈ Im(f), it is computationally infeasible to find any x ∈ X, such that f(x)=y.

# One way function (contd)

- Illustration: Let X = {1,2,3,…..16} and let $f(x) = r_x$ for all $x \in X$, where $r_x$ is the remainder when $3^x$ is divided by 17. What is then f(x) ?
- Is it feasible to compute f(x) from x ?

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |

- Is it feasible to compute x from f(x) ?





# The Trapdoor oneway functions

- Illustration: Let
  - primes p = 48611 and q = 53993, number n = pq = 2624653723 and let X = {1,2,3,4,….n-1}.
  - let a function $f_x = r_x$ be defined for each $x \in X$, where $r_x$ is the remainder when $x^3$ is divided by n.
  - e.g. f(248991) = 1981394214 as
    - $2489991^3 = 5881949859 * n + 1981394214$
  - IS it easy to compute the value of f(x) given x ?
- Finding the reverse …i.e. is it easy to compute x given f(x) ?
  - Computation of modular cuberoot with modulus n
  - if the factors of n are unknown and large then it is a difficult problem.
- Such functions are the trapdoor oneway functions……

# The Trapdoor oneway functions (contd)

- def: a function f: X→Y is a trapdoor one way function, it is one-way function
  - with the additional property that given some extra trapdoor information it becomes feasible to find for any given y∈Im(f), an x∈X, such that f(x)=y.
- In the example above, knowing p and q (each five digits long), it is easy to invert the function.
- What should be the length of digits in p and q to make it infeasible?
  - at least 100 digits
  - well-known integer factorization problem.
- The existence of such functions is difficult to rigoroulsy prove, mathematically.



# Modular Arithmetic

- Any integer a can be expressed as a = qn + r; $0 \leq r < n$; $q = \lfloor a/n \rfloor$
  - e.g. in modulo 7 arithematic, 11 = 1 x 7 + 4 i.e. r = 4 and
  - -11 = ?
    - -11 = -2 x 7 + 3 to yield r = 3.
- def: modulo operator "a mod n" is defined as the remainder b
  - when a is divided by n, b is called the residue of a mod n
  - usually choose the smallest positive remainder as residue 0 <= b <= n-1
  - the process is known as modulo reduction

# Congruent modulo n

- Finite fields have become increasingly important in cryptography.
- Two integers a and b are said to be **congruent modulo n** if (a mod n) = (b mod n)
  - i.e. when divided by *n,* a & b have the same remainder
  - i.e. when n divides b-a
  - e.g. (100 mod 11) = (34 mod 11)
  - denoted as 100 ≡ 34 mod 11
    - Is -12 ≡ -5 mod 7 true ?
    - Is 2 ≡ 9 mod 7 true ?
    - Is 73 ≡ 4 mod 23 true ?
    - Is 21 ≡ -9 mod 10 true?



# Tutorial #4&#5:

- State whether true or false:
  - Is 13 ≡ 523 mod 17 ?
  - Is -15 ≡ 6 mod 7 true ?
  - Is -14 ≡ 1 mod 3 true ?
  - Is 73 ≡ 4 mod 23 true ?
  - Is 21 ≡ -9 mod 10 true?
  - Is 82 ≡ 1 mod 9 true ?
  - Is -82 ≡ 1 mod 9 true ?
  - Is 63 ≡ 8 mod 11 true ?
  - Is -63 ≡ 3 mod 11 true ?
  - Is 121 ≡ 1 mod 15 true
  - Is -119 ≡ 1 mod 15 true ?

# Congruence

- Congruence modulo n is an equivalence relation on the integers.
- What is an equivalence relation ?
- Congruence modulo n is an equivalence relation on the integers…..given the three properties are true. Which ones ?
  - any integer is congruent to itself modulo n (reflexivity). How ?
  - $a \equiv b \bmod n$ implies that $b \equiv a \bmod n$ (symmetry). How?
  - $a \equiv b \bmod n$ and $b \equiv c \bmod n$ implies that $a \equiv c \bmod n$ (transitivity). How ?



# $Z_n$ - The integers modulo n

- def: The set of integers modulo n i.e. $Z_n$ is the set of (equivalence classes of) integers {0,1,2,…..n-1}.
- All the operations in $Z_n$ viz.
  - multiplication, addition and subtraction are performed modulo n.
  - e.g. $Z_{25}$ = {0,1,2,3, ……24}. Then,
    - 6+14 = ? in $Z_{25}$ 14+14 = ? in $Z_{25}$
    - 15+35 = ? in $Z_{25}$ 20+32 = ? in $Z_{25}$
  - e.g. $Z_{49}$ = {0,1,2,3,…48}. Then
    - 21+23 = ? in $Z_{49}$
    - 35 + 35 = ? in $Z_{49}$

# The additive inverse

- The additive inverse of a number a in modular arithmetic is the integer y such that x + y = 0 mod n.
- e.g. addition arithmetic modulo 8 is as shown in the table.
- What are the AIs of 1, 2, 3, 5 in modulo 8 ?

| + | 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 |





# The multiplicative inverse

- The multiplicative inverse of a number a is a number b such that a * b = 1 mod n.
  - if exists, it is unique
- e.g. the table shows the multiplication modulo 7
- unlike additive inverse, the multiplicative inverse of a number may not exist e.g.
  - what are the MIs of 2,3,4 ?
  - what are the MIs of 4 in modulo 8 ?

| × | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

# Abstract Algebra

- Finite fields
  - are of increasing importance in cryptography
    - AES, Elliptic Curve, IDEA, Public Key
  - concern with operations on "numbers" where
    - what *constitutes* a "number" and the *type* of operations varies considerably
  - start with concepts of groups, rings, fields from abstract algebra



# Group

- A Group is a set of elements or "numbers" with some operation * such that
  - closure: whose result is also in the set
  - associative law: (a.b).c = a.(b.c)
  - has identity e: e.a = a.e = a
  - has inverses $a^{-1}$: $a.a^{-1} = e$
- Semigroup, Monoid, Group ……….in that order
- A group
  - if is commutative a.b = b.a then it forms an **abelian group**
- Finite group, order of a finite group
- Infinite group

## Group…

- def: A group $(G, *)$ consists of a set G with a binary operation * on G satisfying the following three axioms:
  - the group operation is associative i.e. $a*(b*c) = (a*b)*c$ for all $a,b,c \in G$.
  - there is an element $1 \in G$, called the identity element, such that $a * 1 = 1 * a = a$ for all $a \in G$
  - for each $a \in G$ there exists an element $a^{-1} \in G$, called the inverse of a such that $a * a^{-1} = a^{-1} * a = 1$
- for a group G, if $a * b = b * a$ for all $a, b \in G$, then the group G is abelian or commutative.



## Group – illustrations

- The set of integers $Z_n$ with the operation of addition modulo n forms a group of order n. Identity element = ? Inverse of a = ?
  - Is it an abelian group, too?
- The set of real numbers under multiplication is an abelian group.
- Is the set of integers $Z_n$ with the operation of multiplication modulo n, a group of order n ?
- Is the set of integers $Z_n$ with the operation of multiplication modulo n, a monoid ?

# The multiplicative inverse

- e.g. the table shows the multiplication modulo 7
- unlike additive inverse, the multiplicative inverse of a number may not exist e.g.
  - what are the MIs of 2,3,4 ?
- what are the MIs of 4 in modulo 8 ?

| × | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |



# Group – illustration

- Ex: Let set $G_{XOR}$= {EVEN, ODD} and a binary operation ⊕ be defined as

| ⊕ | EVEN | ODD |
|---|---|---|
| EVEN | EVEN | ODD |
| ODD | ODD | EVEN |

  - Is it a closed under operation ⊕ ?
  - Does it exhibit associativity ?
  - What is the identity element?
    - EVEN
  - Does every element have an inverse?
    - What are the inverses of ODD and EVEN elements?

# Ring

- A set of "numbers"
  - with two operations (addition and multiplication) denoted as (R, +, X) and
    - which forms an abelian group with addition operation (identity 0)
    - multiplication operation
      - has closure
      - is associative i.e. a x (b x c) = (a x b) x c for all a,b,c ∈ R
      - distributive over addition i.e. a x (b+c) = a x b + a x c
- i.e. a ring is a set in which we can do addition, subtraction and multiplication without leaving the set.
- e.g. the set of integers Z with + supported is a ring
- e.g. is the set of integers Z with x supported a ring ?





# Invertible element and Field

- An element a of a ring R is called a unit or an invertible element
  - if there is an element b ∈ R such that a x b = 1.
- A **FIELD** is a set in which we can do addition, subtraction, multiplication, and division without leaving the set.
  - Division is defined with the following rule: $a/b = a\,(b^{-1})$. We denote a Field as {F,+,.}

# Field…

- def: A field is a commutative ring in which all the non-zero elements have multiplicative inverses.
  - e.g. the set of integers under the + & x operations is not a field. Why ?
- Are the sets (of) rational numbers, real numbers, complex numbers a field ?
- $Z_n$ is a field iff n is a prime number.
- These have hierarchy with more axioms/laws
  - group -> ring -> field



# Galois Fields

- Infinite fields are of not much interest. But, finite fields play a key role in cryptography.
- The number of elements in a finite field
  - i.e. the order of a finite filed must be a power of a prime $p^n$, $n \geq 1$
  - the finite field of the order of $p^n$ are known as Galois fields
- denoted $GF(p^n)$
- in particular often use the fields
  - $GF(p)$
  - $GF(2^n)$

# Galois Fields GF(p)

- GF(p) is the set of integers $Z_p = \{0,1, \dots , p\text{-}1\}$ with arithmetic operations modulo prime p
- these form a finite field - since each element has multiplicative inverse
- hence arithmetic is "well-behaved" and
  - can do addition, subtraction, multiplication, and division without leaving the field GF(p)





# Addition modulo 7

| + | 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 |

# GF(7) Multiplication Example

| × | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

How to find inverses when the numbers involved are very large ???



# Finding Inverses – Extended Euclidean algorithm

```
EXTENDED_EUCLID(m, b)
1. (A1, A2, A3)=(1, 0, m);
   (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = gcd(m, b); no inverse
3. if B3 = 1
   return B3 = gcd(m, b); B2 = b^-1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 – Q B1, A2 – Q B2, A3 – Q
   B3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2
```

# Inverse of 17 in GF(29)

i.e. calling Extended_Euclid(29, 17)

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| — | 1 | 0 | 29 | 0 | 1 | 17 |
| 1 | 0 | 1 | 17 | 1 | –1 | 12 |
| 1 | 1 | –1 | 12 | –1 | 2 | 5 |
| 2 | –1 | 2 | 5 | 3 | –5 | 2 |
| 2 | 3 | –5 | 2 | -7 | 12 | 1 |



# Inverse of 17 in GF(29)

i.e. calling Extended_Euclid(29, 17)

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| — | 1 | 0 | 29 | 0 | 1 | 17 |
| 1 | 0 | 1 | 17 | 1 | –1 | 12 |
| 1 | 1 | –1 | 12 | –1 | 2 | 5 |
| 2 | –1 | 2 | 5 | 3 | –5 | 2 |
| 2 | 3 | –5 | 2 | -7 | 12 | 1 |

# Inverse of 37 in GF(49)

i.e. calling Extended_Euclid(49, 37)

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| — | 1 | 0 | 49 | 0 | 1 | 37 |
| 1 | 0 | 1 | 37 | 1 | -1 | 12 |
| 3 | 0 | 1 | 12 | -3 | 4 | 1 |

- Hence $37^{-1} \equiv 4 \bmod 49$ OR $4 = 37^{-1} \bmod 49$





# Inverse of 550 in GF(1759)

i.e. calling Extended_Euclid(1759, 550)

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| — | 1 | 0 | 1759 | 0 | 1 | 550 |
| 3 | 0 | 1 | 550 | 1 | –3 | 109 |
| 5 | 1 | –3 | 109 | –5 | 16 | 5 |
| 21 | –5 | 16 | 5 | 106 | –339 | 4 |
| 1 | 106 | –339 | 4 | –111 | 355 | 1 |

# Inverse of 49 in GF(37)

i.e. calling Extended_Euclid(37, 49)

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| — | 1 | 0 | 37 | 0 | 1 | 49 |
| 0 | 0 | 1 | 49 | 1 | 0 | 37 |
| 1 | 1 | 0 | 37 | -1 | 1 | 12 |
| 3 | -1 | 1 | 12 | 4 | -3 | 1 |

- Hence $49^{-1} \equiv (-3) \bmod 37$
- But, -3 (mod 37) ≡ 34 (mod 37). Hence,
- $34 = 37^{-1} \bmod 49$





# Tutorial #11

- Find the inverse of the following elements in the GF as indicated::
  1. Inverse of 8 GF(19)
  2. Inverse of 17 in GF(29)
  3. Inverse of 13 in GF(29)
  4. Inverse of 49 in GF(37)
  5. Inverse of 351 in GF(771)
  6. Inverse of 17 in GF(331)

# The Euler Totient function

- def: For n ≥ 1, let ø(n) denote the number of integers in the interval [1,n] which are relatively prime to n.
- The function ø is called the Euler Totient function.
- Note that, when we are doing arithmetic modulo n
  - the complete set of residues is : 0……n-1, whereas,
  - the reduced set of residues is those numbers (residues) which are relatively prime to n
    - eg for n=10,
      - the complete set of residues is {0,1,2,3,4,5,6,7,8,9}
      - the reduced set of residues is {1,3,7,9}



# The Euler Totient function - Properties

- So, the number of elements in reduced set of residues is called the Euler Totient Function ø(n)
- Properties:
  1. If p is prime then ø(p) = p -1.
  2. The function ø is multiplicative i.e. if gcd(m,n)=1, then ø(mn) = ø(m). ø(n).
  3. If $n = p_1^{e1} p_2^{e2} p_3^{e3} \ldots\ldots p_k^{ek}$ is the prime factorization of n, then,

$$ø(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\ldots\ldots\ldots\left(1-\frac{1}{p_k}\right)$$

# Euler Totient Illustration

- ø(1), ø(2), ø(3), ø(4), ø(6),ø(7), ø(14), ø(23) ø(15)
  - ø(1)= 0 - given by p = p-1
  - ø(2)=|{1}| - given by p = p-1
  - ø(3)=|{1,2}| - given by p = p-1
  - ø(4)=|{1,3}| - 4 is not a prime
  - ø(6)=|{1,5}| - 6 is not a prime
    - ø(6) = ø(3)*ø(2) = 2*1 = 2
  - ø(7)=|{ 1, 2, 3, 4, 5, 6}| - given by p = p-1
  - ø(14) = |{1,3,5,9,11,13}| - 14 is not a prime
    - ø(14) = ø(7)*ø(2) = 6*1 = 6
  - ø(23) = |{1,2,3,………22}| - 23 is prime
  - ø(15) = ?
    - 4 * 2 = 8





# Euler's Totient Function

- If $n = p_1^{e1} p_2^{e2} p_3^{e3} \ldots\ldots p_k^{ek}$ is the prime factorization of n, then,

$$ø(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\ldots\ldots\ldots..\left(1-\frac{1}{p_k}\right)$$

- e.g. $616 = 2^3 * 7 * 11$
- Therefore,
  - ø(616) = 616 * (1 – 1/2) * (1 – 1/7) * (1 – 1/11)
    = 616 * 1/2 * 6/7 * 10/11
    = 240.

# Tutorial #12

- Find the Euler's Totient Function of the following:
  - $\Phi(273)$
  - $\Phi(393)$
  - $\Phi(495)$
  - $\Phi(289)$
  - $\Phi(169)$
  - $\Phi(274)$
  - $\Phi(472)$
  - $\Phi(65)$
  - $\Phi(127)$
  - $\Phi(133)$
  - $\Phi(201)$
  - $\Phi(333)$



# Applications of finding Φ(n) - RSA

- Each user generates a public/private key pair by the following process
  - select two large distinct primes at random - `p, q.`
  - compute their system modulus `n=p.q`
  - compute `ø(n)....How?`
  - select at random the encryption key `e`
    - where `1<e<ø(n), gcd(e,ø(n))=1`
  - solve the following equation to find decryption key `d`
    - `e.d=1 mod ø(n) and 0≤d≤n. How?`
  - publish the public encryption key: PU={e,n}
  - keep secret private decryption key: PR={d,n}
- It is critically important that the factors p & q of the modulus n are kept secret

# Multiplicative Group

- The multiplicative group of $Z_n$ is denoted by $Z^*_n$
- def: defined as $Z^*_n = \{a \in Z_n \mid gcd(a, n) = 1\}$
  - If n is prime, then $Z^*_n = \{a \mid 1 \le a \le n-1\}$
  - If $a \in Z^*_n$ and $b \in Z^*_n$, then $a.b \in Z^*_n$.
- Let n = 21. Then, $Z_{21}{}^* = \{1,2,4,5,8,10,11,13,16,17,19,20\}$





# Multiplicative Group

- The order of a multiplicative group $Z^*_n$ - denoted $|Z^*_n|$ is defined as
  - $|Z^*_n|$ i.e. the number of elements in $Z^*_n$.
- Recollect that if n is prime, then $Z^*_n = \{a \mid 1 \le a \le n-1\}$
- Illustration:
  - Let n = 21. Then, $Z_{21}* = \{1,2,4,5,8,10,11,13,16,17,19,20\}$
  - Now, ø(21) =
    - $ø(7).ø(3)=6.2=12=|Z^*_{21}|$

# Euler's theorem

- Let $n \geq 2$ be an integer. Then if $a \in Z^*_n$,
  $a^{\varnothing(n)} \equiv 1 \pmod n$
- e.g.
  - $a=3; n=10;\ \varnothing(10)=4;$
    hence $3^4 = 81 \equiv 1 \bmod 10$
  - $a=2; n=11;\ \varnothing(11)=10;$
    hence $2^{10} = 1024 = 1 \bmod 11$

What about a=7
i.e. $7^4$ mod 10 ?
And a=5 ?

- If n is a product of distinct primes,
  - and if $r \equiv s \pmod{\varnothing(n)}$, then $a^r \equiv a^s \pmod n$
  - i.e. when working with modulo such as n, exponents can be reduced modulo $\varnothing(n)$



# Order of elements of an MG

- Let $a \in Z^*_n$. Then, the order of a, denoted by ord(a),
  - is the **least** positive integer t such that $a^t \equiv 1 \pmod n$
  - e.g. consider again $Z_{21}^* = \{1,2,4,5,8,10,11,13,16,17,19,20\}$
  - $\varnothing(21)=12=|Z^*_{21}|$.
  - Now the orders of various elements in $Z_{21}^*$ are:

| a | 1 | 2 | 4 | 5 | 8 | 10 | 11 | 13 | 16 | 17 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ord(a) | 1 | 6 | 3 | 6 | 2 | 6 | 6 | 2 | 3 | 6 | 6 | 2 |

  - `Ord(a) = mod(power(a,Ai),21)` in Excel sheet

## Generator, Cyclic group

- Let $\alpha \in Z^*_n$.
  - if the order of $\alpha$ is $\varnothing(n)$, then $\alpha$ is said to be a generator or a primitive element of $Z^*_n$.
  - Are there any generators in the group $Z^*_{21}$ ?

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| a | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Ord(a) | 1 | 6 | - | 3 | 6 | - | - | 2 | - | 6 |
| a | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| Ord(a) | 6 | - | 2 | - | - | 3 | 6 | - | 6 | 2 |



## Generator, Cyclic group

- IF $Z^*_n$ has a generator, then $Z^*_n$ is said to be a cyclic group.
  - In the above example, $Z^*_{21}$ is not a cyclic group, since no generator is equal to $\varnothing(n)$ i.e. 12.

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | 1 | 2 | 4 | 5 | 8 | 10 | 11 | 13 | 16 | 17 | 19 | 20 |
| Ord(a) | 1 | 6 | 3 | 6 | 2 | 6 | 6 | 2 | 3 | 6 | 6 | 2 |

# Generator, Cyclic group (contd)

- Consider now a group $Z_{25}^{*}$
  - $Z_{25}^{*} = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$
  - i.e. $\Phi(25) = |Z_{25}^{*}| = 20$
  - Now the orders of various elements in $Z_{25}^{*}$ are:

| Use the formula Ord(a) = mod(power(a,Ai),25) in Excelsheet | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | 1 | 2 | 3 | 4 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| Ord(a) | 1 | 20 | 20 | 10 | 5 | 5 | 20 | 10 | – | 5 | ? | ? |
| a | 14 | 15 | 16 | 17 | 18 | 19 | 21 | 23 | 24 | | | |
| Ord(a) | ? | ? | ? | ? | ? | ? | | | | | | |

- Thus, $Z_{25}^{*}$ is indeed a cyclic group because 2,3,8,… are the generators of the group.





# Generator, Cyclic group (contd)..

Members of Z*25 are {1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24} and Phi(25)=20

| | $Z^*_{25}$ with α=2 | $Z^*_{25}$ with α=3 | $Z^*_{25}$ with α=4 | $Z^*_{25}$ with α=6 | $Z^*_{25}$ with α=7 | $Z^*_{25}$ with α=8 | $Z^*_{25}$ with α=9 | $Z^*_{25}$ with α=11 | $Z^*_{25}$ with α=12 | $Z^*_{25}$ with α=13 | $Z^*_{25}$ with α=14 | $Z^*_{25}$ with α=16 | $Z^*_{25}$ with α=17 | $Z^*_{25}$ with α=18 | $Z^*_{25}$ with α=19 | $Z^*_{25}$ with α=21 | $Z^*_{25}$ with α=22 | $Z^*_{25}$ with α=23 | $Z^*_{25}$ with α=2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 6 | 7 | 8 | 9 | 11 | 12 | 13 | 14 | 16 | 17 | 18 | 19 | 21 | 22 | 23 | 24 |
| 2 | 4 | 9 | 16 | 11 | 24 | 14 | 6 | 21 | 19 | 19 | 21 | 6 | 14 | 24 | 11 | 16 | 9 | 4 | 1 |
| 3 | 8 | 2 | 14 | 16 | 18 | 12 | 4 | 6 | 3 | 22 | 19 | 21 | 13 | 7 | 9 | 11 | 23 | 17 | 24 |
| 4 | 16 | 6 | 6 | 21 | 1 | 21 | 11 | 16 | 11 | 11 | 16 | 11 | 21 | 1 | 21 | 6 | 6 | 16 | 1 |
| 5 | 7 | 18 | 24 | 1 | 7 | 18 | 24 | 1 | 7 | 18 | 24 | 1 | 7 | 18 | 24 | 1 | 7 | 18 | 24 |
| 6 | 14 | 4 | 21 | 6 | 24 | 19 | 16 | 11 | 9 | 9 | 11 | 16 | 19 | 24 | 6 | 21 | 4 | 14 | 1 |
| 7 | 3 | 12 | 9 | 11 | 18 | 2 | 19 | 21 | 8 | 17 | 4 | 6 | 23 | 7 | 14 | 16 | 13 | 22 | 24 |
| 8 | 6 | 11 | 11 | 16 | 1 | 16 | 21 | 6 | 21 | 21 | 6 | 21 | 16 | 1 | 16 | 11 | 11 | 6 | 1 |
| 9 | 12 | 8 | 19 | 21 | 7 | 3 | 14 | 16 | 2 | 23 | 9 | 11 | 22 | 18 | 4 | 6 | 17 | 13 | 24 |
| 10 | 24 | 24 | 1 | 1 | 24 | 24 | 1 | 1 | 24 | 24 | 1 | 1 | 24 | 24 | 1 | 1 | 24 | #NUM! | #NUM! |
| 11 | 23 | 22 | 4 | 6 | 18 | 17 | 9 | 11 | 13 | 12 | 14 | 16 | #NUM! | #NUM! | #NUM! | #NUM! | #NUM! | #NUM! | #NUM! |
| 12 | 21 | 16 | 16 | 11 | 1 | 11 | 6 | 21 | 6 | 6 | #NUM! | #NUM! | #NUM! | #NUM! | #NUM! | #NUM! | #NUM! | #NUM! | |
| 13 | 17 | 23 | 14 | 16 | 7 | 13 | 4 | #NUM! | #NUM! | #NUM! | #NUM! | | | | | | | | |
| 14 | 9 | 19 | 6 | 21 | 24 | 4 | 11 | #NUM! | #NUM! | #NUM! | #NUM! | | | | | | | | |
| 15 | 18 | 7 | 24 | 1 | 18 | 7 | #NUM! | #NUM! | #NUM! | #NUM! | | | | | | | | | |
| 16 | 11 | 21 | 21 | 6 | #NUM! | 8 | | #NUM! | | | | | | | | | | | |
| 17 | 22 | 13 | 9 | 11 | #NUM! | 23 | | | | | | | | | | | | | |
| 18 | 19 | 14 | 11 | #NUM! | #NUM! | 9 | | | | | | | | | | | | | |
| 19 | 13 | 17 | 19 | #NUM! | #NUM! | 22 | | | | | | | | | | | | | |
| 20 | 1 | 1 | 1 | #NUM! | #NUM! | 1 | | | | | | | | | | | | | |
| 21 | 2 | 3 | 4 | | | 8 | | | | | | | | | | | | | |
| 22 | 4 | 9 | 16 | | | | | | | | | | | | | | | | |
| 23 | 8 | 2 | #NUM! | | | | | | | | | | | | | | | | |

Snapshot of $Z^{*}_{25}$ computation from the Excel sheet

# Generator, Cyclic group (contd)

- Consider now a multiplicative group $Z_{13}^{*}$
  - $Z_{13}^{*} = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12\}$
  - i.e. $\Phi(13) = |Z_{13}^{*}| = 12$
  - Compute the orders of various elements in $Z_{13}^{*}$:

| α | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\alpha^i$ mod 13 | 1 | 6 | 12 | 3 | 7 | 4 | 12 | 12 | 4 | 3 | 6 | 12 |

- Thus,
  - $\alpha = 2, 6, 7, 11$ are the generators of the group.
  - Note the case of $5^t$ mod 13 with t=4,12.



# Generators…..

- How many Generators can be there of a group if $Z^{*}_{n}$ is a cyclic group ?
  - if $Z_n^{*}$ is cyclic, then the number of generators is $\Phi(\Phi(n))$.
    - e.g. $Z_{21}^{*}$ is not cyclic – doesn't have a generator because n does not satisfy any of the conditions above in first
- Are $Z^{*}_{11}$, $Z^{*}_{7}$, $Z^{*}_{13}$, $Z^{*}_{17}$, $Z^{*}_{19}$ cyclic ?
- Is $Z_{30}^{*}$ cyclic ? $\Phi(30)$ is $\Phi(6)* \Phi(5) = 2*4=8$.

## How to test for a given number to be a Generator

- Consider a MG $Z^*_{p,}$ where p is a prime.
- Then, it is easy to test whether a given element is its generator or not. How ?
  - As p is a prime, $\Phi(p) = p-1$, and
  - the number of generators in it is $\Phi(p-1)$,
  - now, if $p_1, p_2, p_3 \ldots p_k$ are the distinct prime factors of p-1, then,
    - g is a generator of $Z^*_p$ if and only if

$$g^{(p-1)/pi} \neq 1 \bmod p \text{ for all } p_i \; 1 \leq i \leq k$$





## How to test for a given number to be a

- e.g. consider $Z^*_{13}$. Check whether 7 is a generator or not.
- Now,
  - $\Phi(13) = p-1 = 12$, and
  - the number of generators in it is $\Phi(p-1) = \Phi((12) = 4$.
  - Also, the distinct prime factors of p-1 i.e. 12 are 2,3. Hence, $p_1=2$, $p_2=3$.
  - Then,
    - $g^{(p-1)/p_1} = 7^{12/2} = 7^6 \bmod 13 = 12 \bmod 13 \neq 1 \bmod 13, and$
    - $g^{(p-1)/p_2} = 7^{12/3} = 7^4 \bmod 13 = 9 \bmod 13 \neq 1 \bmod 13$
- Hence, 7 is indeed a generator of $Z^*_{13}$

$$g^{(p-1)/pi} \neq 1 \bmod p \text{ for all } p_i \; 1 \leq i \leq k$$

# How to test for a given number to be a

- e.g. consider $Z^*_{13}$. Now, check whether 8 is a generator or not.
- Now,
  - $\Phi(13)$ = p-1 = 12, and
  - the number of generators in it is $\Phi$(p-1) = $\Phi$((12) = 4.
  - Also, the distinct prime factors of p-1 i.e. 12 are 2, 3. Hence, $p_1=2$, $p_2=3$.
  - Then,
    - $g^{(p-1)/p_1} = 8^{12/2} = 8^6 \bmod 13 = 12 \bmod 13 \neq 1\ mod\ 13, and$
    - $g^{(p-1)/p_2} = 8^{12/3} = 8^4 \bmod 13 = 1 \bmod 13$
- Hence, 8 is NOT a generator of $Z^*_{13}$

$g^{(p-1)/pi} \neq 1\ mod\ p$ for all $p_i$ $1 \leq i \leq k$



# References:


- Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone.
- Introduction to Algorithms by Cormen, Leicerson and Rivest.
- NPTEL Lectures by Debdeep Mukhopadhyay

# Thank You !!!