SCSX1026-----Cryptography and network Security
UNIT – III

Introduction to number theory – Public key cryptography and RSA – Key management – Diffie-hellman key exchange.

Introduction to number theory

The following properties of numbers are assumed: numbers covered in basic mathematics

1) Commutative laws: $p + q = q + r$ and $pq = qp$
2) Associative laws: $p + (q + r) = (p + q) + r = p + q + r$
3) Laws of Indices:
   a) $a^m \times a^n = a^{m+n}$
   b) $a^m \div a^n = a^{m-n}$
   c) $(a^m)^n = a^{mn}$ where m and $n \neq 0$.
   d) $\frac{1}{a^m} = a^{-m}$
   e) $a^0 = 1$, $a \neq 0$
   f) $a^{-n} = \frac{1}{a^n}$
   g) $a^{\frac{1}{n}} = \sqrt[n]{a}$,$n \neq 0$.
   h) a $a^{m/n} = \sqrt[n]{a^m}$,$n \neq 0$.
   i) $a^m \times b^m = (ab)^m$
   j) $\frac{a^m}{b^m} = \left(\frac{a}{b}\right)^m$
4) Absolute or Modulus value of $|p| = p$ if p is positive and $|p| = {}^{-}p$ if p is negative. The modulus function gives the numerical value of an input. It converts negative numbers to positive and is written as $y = |x|$ and read as "y equals mod x"

   Example:
   Stat the value of $|7 - x|$ for $x = 15$.
   Solution: When $x = 15$, $|7 - 15| = |{}^{-}8| = 8$

5) Solutions of quadratic equations: you should be able to solve linear and quadratic simultaneous equations using an algebraic method.

Exercise: Indices

Solve for x:

1. $4^{x+2} = 8^{2x}$
2. $2^{2x+1} - 5(2^{x}) + 2 = 0$
3. $\log_x 6 = ½$

Evaluate:

4. $\left(\frac{4}{49}\right)^{\frac{-3}{2}}$
5. $\log_{10} 0.001$

Answers

1. $x=1$
2. $x=1$, $x = {}^{-}1$
3. $x=36$
4. $\left(\frac{7}{2}\right)^{3}$
5. $x= {}^{-}3$

Notation

1) If p is divisible by q, we write p $|$ q. If p is not divisible by q, we write p $\not|$ q
2) $\forall$ means “for all”
3) $\ni$ means “such that”
4) Iff means “ if and only if”
5) $\in$ means “is a member of”
6) Z means “set of integers”
7) $\Rightarrow$ means “ implies “
8) $\exists$ means “there exists”
9) ≡ means “ equivalent”
10) $\notin$ means “ is not a member of“

Let p,q and r be integer*s*. Then:

a) $p|q$, a>0,q>0 $\Rightarrow p \le q$
b) $p|q \Rightarrow p|qr$, $\forall$ intege*r*s r
c) $p|q$, $p|r \Rightarrow p|(\ qx + ry)$ fo*r* x,y $\in$ Z
d) $p|q$, $q|p \Rightarrow p = \pm\ q$
e) $p|q$, $q|r \Rightarrow p|r$

MATHEMATICAL PROOFS: BY INDUCTION AND CONTRADICTION

The Number Theory module uses mathematical induction and indirect proof or proof by contradiction extensively.

Example 1: Proof by Induction

Prove by mathematical induction that

$$1 + 2 + \ldots\ldots\ldots\ldots\ldots + m = \frac{m(m+1)}{2}$$

Proof:

Step 1: Technique of Induction

Mathematical induction proves by checking if a proposition hold's for m=1, and m= k+1 whenever it holds for m=k, then the proposition holds for all positive integers m= 1,2, 3,……..

Step 2: Substitute m=1 in the equation:

$$1 = \frac{1(1+1)}{2} = 1$$

Step 3: Assume that the formula holds for m= k

$$1 + 2 + \ldots\ldots\ldots\ldots\ldots + k = \frac{k(k+1)}{2}$$

Step 4: Proof that the formula holds for *m* = *k*+1.

$$1 + 2 + \ldots\ldots\ldots\ldots\ldots + k + (k + 1) = \frac{(k+1)\{(k+1)+1\}}{2}$$

We write:

$$1 + 2 + \ldots\ldots\ldots\ldots\ldots + k = \frac{k(k+1)}{2}$$

$$\Rightarrow \quad \frac{k(k+1)}{2} + (k + 1) = \frac{(k+1)\{(k+1)+1\}}{2} \Rightarrow \frac{k(k+1)+2k+2}{2} = \frac{(k+1)\{(k+2)}{2}$$

$$\Rightarrow \quad \frac{(k+1)\{(k+2)}{2} = \frac{(k+1)\{(k+2)}{2}$$ { by factorization} [PROVED]

This is proof by inductionExample: Proof by Induction

Example 2:

Prove by induction that for every positive integer n, then:

$1^2 + 2^2 + 3^2 + 4^2 + \ldots\ldots\ldots\ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Step 1: Technique of Induction

Mathematical induction proves by checking if a proposition hold's for $n = 1$, and $n = k + 1$ whenever it holds for $n = k$, then the proposition holds for all positive integers n= 1,2, 3,……..

Step 2: Substitute $n = 1$ in the equation:

$1 = \frac{1\{1+1\}\{(2\times 1)+1\}}{6} = 1$

Step 3: Assume that the formula holds for k

$1^2 + 2^2 + 3^2 + 4^2 + \ldots\ldots\ldots\ldots + k^2 = \frac{k(k+1)(2k+1)}{6}$

Step 4: Proof that the formula holds for n= k+1.

$1^2 + 2^2 + 3^2 + 4^2 + \ldots\ldots\ldots\ldots + (k+1)^2 = \frac{(k+1)(k+1+1)\{2(k+1)+1\}}{6}$

We write

$1^2 + 2^2 + 3^2 + 4^2 + \ldots\ldots\ldots\ldots + (k+1)^2 = (1^2 + 2^2 + 3^2 + 4^2 + \ldots\ldots\ldots\ldots + k^2) + (k+1)^2$

$\Rightarrow \frac{k(k+1)(2k+1)}{6} + (k+1)^2$

$\Rightarrow \frac{(k+1)(2k^2+k+6k+6)}{6} \Rightarrow \frac{(k+1)(k+2)(2k+3)}{6}$ {by factorization} [PROVED]

Exercise: Proof by Induction

1. Prove that $1 + 2 + 2^2 + \ldots\ldots + 2^n = 2^{n+1} - 1$ for $n \geq 1$.
2. Prove that $1 + 3 + 5 + 7 + \ldots\ldots + (2n-1) = n^2$
3. Prove that $a + ar + ar^2 + \ldots + ar^n = \frac{a(1-r^{n+1})}{1-r}$, for $n > 0$

4. Prove that $1^4 + 2^4 + 3^4 + 4^4 + \ldots\ldots + n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$

5. Prove that for $n < 2^n$ for all positive integers n.

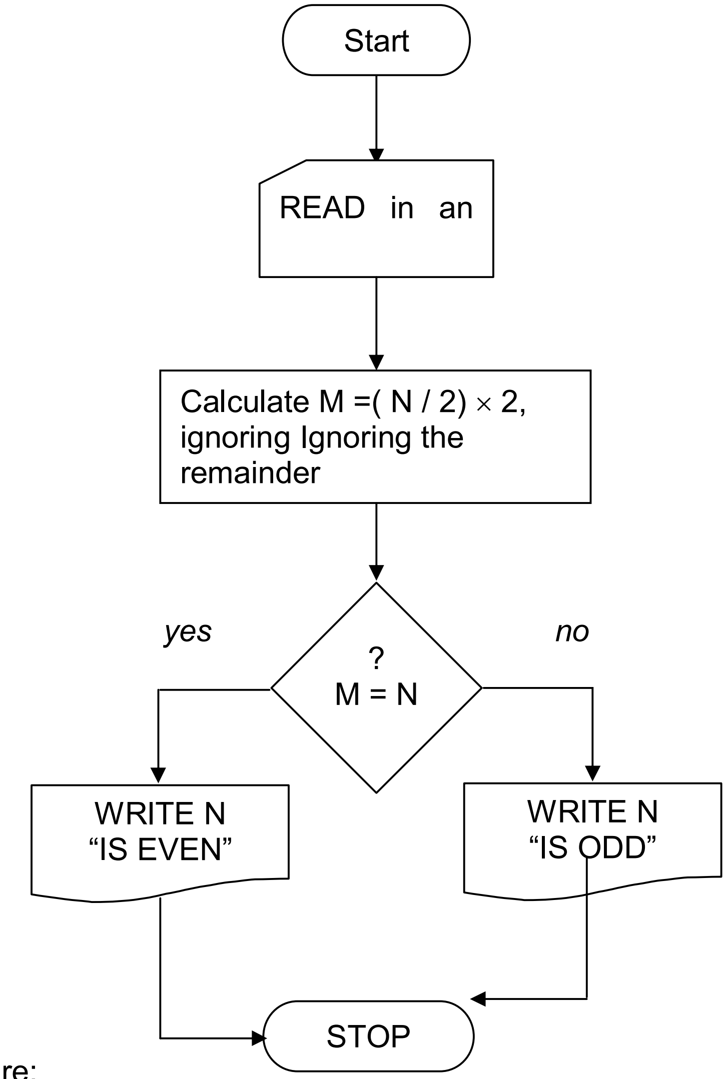
6. Prove that $(ab)^n = a^n b^n$

7. Prove that $1 + 4 + 7 + 10 + \ldots\ldots + (3n - 2) = \frac{n}{2}(3^n - 1)$

Odd and Even Numbers

Even and Odd Numbers Activity
Case 1 What do you understand by even and odd numbers? Give one simple way of distinguishing even from odd numbers? How many months of the year have number of days that are odd? How many even years are there from 1960 to 2010 ? Answer Numbers divisible by 2 are called Even and numbers not divisible by 2 are called Odd.

Flow Chart for Testing Even and Odd numbers.



Procedure:

1. Input an integer N
2. Calculate M as indicated
3. Make the decision if N is even or odd.

The activity is a flow chart representation of sorting even and odd integers. Tabulate your results:

Number, N									
Even									
Odd									

PROPERTIES OF INTEGERS

DIVISOR

A divisor of an integer n, also called a factor of n, is an integer which evenly divides n without leaving a remainder.

Example:

7 is a divisor of 35 because 35|7 = 5. We also say 35 is divisible by 7 or 35 is a multiple of 7 or seven divides 35 and we usually write 7|35.

In general, we say m|n (read: m divides n) for non-zero integers. If there exists an integer k such that n=km. Thus divisors can be negative as well as positive e.g. divisors of 6 are 1,2,3,6,-1,-2,- 3,-6 but one would usually mention the positive ones 1,2,3 & 6. 1 and –1 divide (are divisors of) every integer, every integer is a divisor of itself and every integer is a divisor of 0.

A divisor of n that is not 1,-1, n or –n is known as non-trivial divisor, numbers with non-trivial divisors are known as composite numbers while prime numbers have non-trivial divisors.

If a|b=c, then a is the dividend, b the divisor and c the quotient.

The Remainder for natural Numbers.

If a and d are natural numbers, with d non-zero, it can be proved that there exist unique integers q and r, such that a = qd + r and $0 \leq r < d$. The number q is called the quotient, while r is called the remainder.

Example:

1) When diving 17 by 10, 1 is the quotient and 7 is the remainder because 17 = $1 \times 10 + 7$
2) $22 / 4 = 5 \times 4 + 2$ 5 is the quotient & 2 the remainder.
3) When dividing 42 by 7, 6 is the quotient and 0 is the remainder, because $42 = 7 \times 6 + 0$

The Case of General Integers.

If a and d are integers, with d non-zero, then a remainder is an integer r such that a=qd+r for some integer q, and 0<= |r| <= |d|

When defined this way, there are two possible remainders.

Example:

The division – 37 by 5 can be expressed as either – 37 = 8 × (-5) +3 or – 37 = 7 × (-5)+(-2). So the remainder is then 3 or –2

Note: When dividing by d, if the positive remainder is r_1, and the negative one is r_2 , then $r_1 = r_2 + d$

Modulo Operation.

The modulo operation finds the remainder of division of one number by another. Given two numbers a and n, a modulo n { abbreviated a mod n } is the remainder, on division of a by n. eg 10 mod 3 evaluates to 1 and 12 mod 3 evaluates to 0 i.e 1 and 3 are the remainders after division.

Divisibility

Definition:
An integer p is divisible by an integer q iff ∃ an integer r ∍ p = q × r

The Division Theorem

If m and n are integers, with n ≠ 0, then there exists unique integers q and r, 0 ≤ r< I n I, ∍ m = qn + r.
The integers

a) m is called the dividend
b) q is called the quotient
c) n is called the divisor
d) r is called the remainder

Case 1

Dividing an 11 hectares piece of land among 5 people. What does each get? Each person gets a whole number and a fraction.

In this case, identify the dividend (a), quotient (q), divisor (b) and remainder(r).

Examples:

<table>
<tr><td colspan="5">If m and n are integers, with n ≠ 0, then there exists unique integers q and r,</td></tr>
<tr><td>0 ≤ r< I n I, ∍ m = qn + r.</td><td>n</td><td>q</td><td>r</td><td>m= qn + r</td></tr>
<tr><td>The integers</td><td>2</td><td>7</td><td>1</td><td>m=7(2) + 1</td></tr>
<tr><td>m is called the dividend</td><td>5</td><td>6</td><td>3</td><td>m =5(6) + 3</td></tr>
</table>

q is called the quotient	- 10	2	1	m = -10(2) + 1
n is called the divisor	-9	5	8	m = -9 (5) +8

Definition:
A natural number which divides into another an exact number of times is called a factor.

Examples:

- Factors of 24 are 1, 2, 3, 4, 6, 8, 12 and 24.
- Factors of 15 are 1, 3, 6,and 15.

Exercise: Factors

What are the factors of:

1. 20
2. 28
3. 36
4. 120
5. 169
6. 180

Common Multiples

An integer that is divisible by two integers p and q is called a multiple of p and q. The common multiples of 2 and 3 are 0, 6, 12, 18, 24,…. And the common multiples of 4,and 5 are 0, 20, 40,60,…….

Exercise: Common Multiples

List the first 8 multiples each of:
1). 3 2). 7 3). 11 4). 23 5). 61 6). 138

Least Common Multiple (LCM)

Market Story

Madam Safi goes for shopping in the nearest shopping center to her home where things are measured in tins. She visits three shops, which use different sizes of tins. Shop A uses 2 litre tins, shop B uses 4 litre tins and shop C uses 5 litre tins. She needs to carry a container that enables her buy a whole number of tins irrespective of which shop she visits. What is the minimum volume of the container she needs to carry?

Definition:
The least common multiple of p and q is defined as the smallest positive integer that is divisible by both p and q. It may be denoted as [p, q].

Examples:

- [4, 9] = 36
- [$^{-}$3, 4] = 12
- [7, 8] = 56

Calculation of LCM using prime factors

Example: Find the LCM of 16, 24 and 840.

STEP 1*:* Express each of the numbers as prime factors

16 = 2^4
24 = $2^3 \times 3$
840= $2^3 \times 3 \times 5 \times 7$

STEP 2: Pick out the highest power of each of the prime factors that appears. The factors need not be common. For example, the highest powers of 2,3 ,5 and 7 are 4,1, 1, and the LCD becomes $2^4 \times 3 \times 5 \times 7 = 1680$.

Exercise: Finding the LCM
Find the LCM'S of

1. 18, 20,and 24
2. 30, 45,and 50
3. 252, 990 and 3150
4. 450, 2100 and 990

Common Divisors

Definition:
An integer p is a common divisor of q and r if p|q and p|r.

Greatest Common Divisor

Given three numbers 20,24, and 28, what is the greatest number that can divide each of this numbers? How do you calculate this number ?

Definition:
Any two integers p and q have at least one positive divisor in common, called greatest common divisor (gcd). If at least one of the integers p and q is different from zero, then there exists a largest positive integer d which divides both p and q. This integer d is called the greatest common divisor (gcd) of p and q and may be denoted as gcd (p,q) or (p,q).

Examples:

- ♦ gcd(6,12) = 3
- ♦ gcd(0,18) = (0,$^{-}$18)=18
- ♦ gcd(9, 27) = 9
- ♦ gcd(14, 28) = 7

Calculation of gcd using prime factors

Example:

Find the gcd of 60, 100, and 840.

STEP 1:
Express each of the numbers as prime factors

$60 = 2^2 \times 3 \times 5$
$100= 2^2 \times 5^2$
$840= 2^3 \times 3 \times 5 \times 7$

STEP 2:
Pick out the highest common power of each common factor. The product of these highest powers gives the gcd.
For example, the common prime factors are 2 and 5. The highest powers of 2 and 5 which are common are $2^2 \times 5^1$=20 their gcd.

Exercise: Prove the following corollaries:

1. For every m > 0, m(b,c)= (mb,mc)

2. If d|a, d|b, d> 0,then $\left(\frac{a}{d},\frac{b}{d}\right)$ = $\frac{1}{d}(a,b)$

Proof the following propositions

1. If (a,m)= (b,m)= 1 then (ab,m)=1
2. If c|ab and (b,c) =1 then c|a

EUCLIDEAN ALGORITHM

Eulidean algorithm (Euclid’s algorithm) is an algorithm to determine the greatest common divisor (GCD or gcd) of two integers by repeatedly dividing the two numbers and the remainder in turns.

Description of the algorithm

Given two natural numbers m and n, check if n = 0. If yes, m is the gcd. If not, repeat the process using n and the remainder after integer division of m and n {written as m modulo n}

Theorem: Euclidean algorithm

Either m is a multiple of n, or there is a positive integer k, and integers $q_1, q_2, \ldots\ldots, q_k$, $r_1, r_2, \ldots\ldots. r_{k-1}$ (and r = 0) such that

$m = q_1 n + r_1$ $\quad (0 \le r_1 < I\ n\ I\ )$

$n = q_2 r_1 + r_2$ $\quad (0 \le r_1 < r_2)$

……

$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$ $\quad (0 \le r_{k-1} < r_{k-2})$

$r_{k-2} = q_k r_{k-1}$ $\quad (0 \le r_k)$

Example: Compute the gcd of 1071 and 1029.

Euclid (400 B.C) developed a systematic procedure for finding the greatest common divisor of two integers. It is called the Euclidean algorithm.

a	b	Expression	Explanation
1071	1029		Step 1: Put the large number on the left and the smaller one on the right.
1071	1029	1071=1029×1+42	Step 2: The remainder of 1071 ÷1029 is 42, which is put on the right, and the divisor 1029 is put on the left.
1029	42	1029=42×24+21	Step 3: Repeat step, dividing 1029 by 42, and get 21 as remainder.
42	21	42=21×2+0	Step 4: Repeat step 2again, since 42 is divisible by 21, we get 0 as remainder, and algorithm terminates.
21	0		The number 21 is the gcd as required

Example: Compute the gcd of 1071 and 1029.

Examples: Illustration of Euclid's algorithm in computing gcd (Division algorithm)	
Example 1	Example 2
Find the gcd of 5775 and 1008	Find the gcd of 2261 and 1275
Solution.	Solution.
m=5775 and n = 1008.	m=2261 and n= 1275
5775 = 5 x 1008 + 735	2261 = 1 x1275 + 986
1008 = 1 x 735 + 273	1275= 1 x986 + 289
735 = 2 x 273 + 189	986=3 x 289 +119
189 = 2 x 84 + 21	289=2 x119+51
84 = 4 x 21	119=2 x 51+17
Thus the gcd = 21, ie the largest integer that divides 5775 and 1008.	Thus the gcd = 17.

Exercise: Finding gcd's Using Euclidean Algorithm

Find the greatest common divisor in each case using Euclidean algorithm:

1. (276, 336, 396, 468, 972)
2. (1387, 1292,722,836)
3. (924, 798, 1358,1827)
4. (60,84)
5. (190,72)

Solutions:
1). 12 2). 19 3). 7 4). 12 5). 2

Prime Numbers and Their Distribution

Introduction

The set of natural numbers is Z = {1,2,3,4,…}and
the set of integers N = {……-2,-1,0,1,2…..}

Definition: Prime and Composite

An integer p > 1 is prime iff it has no divisors d with 1< d< p. In other words, the only positive divisors of p are 1 and p. We call p composite if p is not prime.

The number 1 is neither prime nor composite. The first few primes of N are 2,3,5,7,11,13,17,23,29,31,37,42,43,47,…… and the first few composite are 4,6,8,9,10,12,14,16,18,20,21,22,24,26,27,….

Definition:
Two integers p and q are relatively prime if gcd (p,q) = 1.

Theorem

If p is composite, then p has a prime factor

Example:
Composite number 12 can be factored into primes i.e 12 =2 x 2 x 3, and
90 = 2 x 3 x 3 x 5

Fundamental Theorem of Arithmetic

Every integer greater than 1 is either prime or can be expressed as a product of primes.

Corollary:
The following are equivalent:

1. a and b have no common divisors i.e (n|a and n|b) ⇒ n = ± 1.
2. (a,b)=1 i.e the subgroup generated by a and b is all of Z.
3. $\exists$ m,n$\in$ Z with ma +nb = 1.

Definition:
If any one of these three conditions is satisfied, we say that a and b are Relatively Prime.

Theorem:
If a and b are relatively prime with a not zero, then a|bc = a|c

Proof: Suppose a and b are relatively prime, c $\in$ Z and a|bc, then there exist m,n with ma+nb =1, and thus mac + nbc = c. Now a|mac and a|nbc. Thus a|(mac + nbc) and so a|c.

Theorem

Suppose p is a prime

1. If a is an integer which is not a multiple of p, then (p,a) = 1. In other words, if a is any integer (p,a)=p or (p,a)=1.
2. If p|ab then p|a or p|b.
3. If p|a_1,a_2,…. a_n then p divides a_i . Thus if each a_i is a prime, then p is equal to some a_i.

The Unique Factorisation Theorem

Suppose a is an integer which is not 0,1 or -1. Then a may be factored into the product of primes and except for order, this factorisation is unique. That is, ∃ a unique collection of distinct primes $p_1, p_2, \ldots\ldots, p_k$ and positive integers $s_1, s_2, \ldots, s_k$ such that a=± $p_1^{S_1}, p_2^{S_2}, \ldots. p_k^{S_k}$.

Solving Linear Diophantine Equations

Definition

A Diophantine Equation is a polynomial equation (e.g mx = k, mx + ny = k ,etc) with integer coefficients (m and n) for which only integer solutions are allowed.

First Degree Linear Diophantine equation

This is an equation in one variable for example, mx = k, where m and k are integers and m ≠ 0, is a linear first degree Diophantine equation.
The linear Diophantine equation has an integer solution, x = k/m.

Diophantine Equations in Two Variables

These are of the nature $mx + ny = k$. (m,n and k integers and m ≠ 0,n ≠ 0)
This equation is solvable if k is the gcd (m,n), where m ≠ 0,n ≠ 0

Theorems

1. Given the integers m ≠ 0 and n ≠ 0, there exist integers x and y such that the Diophantine equation mx + ny = gcd (m,n)
2. The Diophantine equation mx+ny = k, is solvable in integers iff gcd (m,n) divides k.

Activity: Solving Diophantine Equations

Example 1:

Solve the Diophantine equation
2772x + 390y = (2772,390)

Solution:

STEP 1: Applying the Euclidean algorithm to find gcd of 2772 and 390

$\Rightarrow$ 2772 = 7 × 390 + 42……………………………………(i)
$\Rightarrow$ 390 = 9 × 42 + 12………………………………………(ii)
$\Rightarrow$ 42 = 3 × 12 + 6…………………………………………(iii)

The gcd = 6

STEP 2: Substitute the gcd in the equation ie 2772x + 390y = 6
Substitute backwards in (iii), then (ii) and finally in (i) to obtain solutions for the Diophantine
$\Rightarrow 6 = 42 - 3 \times 12$
$\Rightarrow \quad = 42 - 3 \times (390 - 9 \times 42) = 42 - 3(390)$
$\Rightarrow \quad = 42 + 27(42) - 3(390)$
$\Rightarrow \quad = 28(42) - 3(390)$
$\Rightarrow \quad = 28(2772 - 7 \times 390) - 3(390)$
$\Rightarrow \quad = 28(2772) - 196(390) - 3(390)$
$\Rightarrow \quad = 28(2772) - 199(390)$
i.e. (mx + ny)

$\Rightarrow x = 28,\ y = {}^{-}199$

Example 2:

Solve the Diophantine equation
$7472x + 2624y = (7472, 2624)$

STEP 1: Applying the Euclidean algorithm to find gcd of 7472 and 2624

$\Rightarrow$ 7472 = 3 × 2624 + 80…………………………………(i)
$\Rightarrow$ 2624 = 30 × 80 + 64……………………………………(ii)
$\Rightarrow$ 80 = 1 × 64 + 16………………………………………. (iii)

The gcd = 16

STEP 2: Substitute the gcd in the equation ie 7472x + 2624y = 16
Substitute backwards in (iii), then (ii) and finally in (i) to obtain solutions for the Diophantine

$\Rightarrow$ 16 = 80 – 1 × 64

$\Rightarrow$ = 80 – 1 (2624 – 30 × 80)

$\Rightarrow$ = 80 – 1(2624) + 30 × 80

$\Rightarrow$ = (1)80 + 30(80) – 1(2624)

$\Rightarrow$ = 31(80) – 1(2624)

$\Rightarrow$ = 31(7472 – 3 × 2624) – 1(2624)

$\Rightarrow$ = 31(7472) – 93(2624) – 1(2624)

$\Rightarrow$ = 31(7472) – 94(2624)

$\Rightarrow$ i.e. (mx + ny)

$\Rightarrow$ x= 31, y = $^-$94.

Example 3:

Solve the Diophantine equation
803*x* + 154*y* = (803,154)

STEP 1: Applying the Euclidean algorithm to find gcd of 803 and 154

$\Rightarrow$ 803 = 5 × 154 + 33……..……………………… (i)

$\Rightarrow$ 154 = 4 × 33 + 22…………………………………… (ii)

$\Rightarrow$ 33 = 1 × 22 + 11..………………………………… (iii)

The gcd = 11

STEP 2: Substitute the gcd in the equation ie 803x + 154y = 11
Substitute backwards in (iii), then (ii) and finally in (i) to obtain solutions for the Diophantine

$\Rightarrow$ 11 = 33 – 1 × 22

$\Rightarrow$ = 33 – 1(154 – 4 × 33)

$\Rightarrow$ = 33 –154 + 4(33)

$\Rightarrow$ = 5(33) – 154

$\Rightarrow$ = 5(803 – 5(154)) – 154

$\Rightarrow$ = 5(803) – 25(154) – 154

$\Rightarrow$ = 5(803) – 26(154)

$\Leftrightarrow$ 5(803) – 26(154) ≡ 803x + 154y

$\Rightarrow$ x = 5 and y = $^-$26

CONGRUENCES and INTEGERS (MOD N)

If two numbers b and c have the property that their difference b-c is integrally divisible by a number m { i.e (b-c)|m is an integer}, then b and c are said to be "congruent modulo m". The number m is called the modulus, and the statement "b is congruent to c (modulo m)" is written mathematically as

$$b \equiv c \pmod{m}$$

If b-c is not integrally divisible by m, we say "b is not congruent to c(modulo m)" which is written

$$b \not\equiv c(\mathrm{modm})$$

The quantity b is sometimes called the "base", and the quantity c is called the "residue or remainder".

(Wikipedia)

Definition: If $m \neq 0$, is a positive integer and a, $b \in Z$; then we say a is congruent to b modulo m if m|a-b.

Notation: In $a \equiv b \pmod{m}$, the positive integer m is called a modulus

Examples:

45 ≡ 3 mod 6 ie. m|a-b $\frac{6}{45-3} = \frac{1}{7}$

72 ≡ 0 mod 12 i.e m|a-b $\frac{12}{72-0} = \frac{1}{6}$

-27 ≡ 0 mod 4

The idea of congruence and the notation a ≡ b(mod m) are due to Carl Friedrich Gauss (1777-1855).

PROPERTIES OF CONGRUENCES MODULO M

Let a ≡ a'(mod m) and b=b'(mod m), then important properties of congruences include the following;

1) Equivalence: a ≡ b(mod 0) $\Rightarrow$ a ≡ b.
2) Determination: either a ≡ b(mod m) or a $\not\equiv$b(modm)
3) Reflexivity: a ≡ a(mod m)
4) Symmetry: a ≡ b(mod m) $\Rightarrow$ b ≡ a(mod m)
5) Transivity: a ≡ b (mod m) and b ≡ c(mod m) $\Rightarrow$ a ≡ c (mod m)
6) a+b ≡ a'+b'(mod m)
7) a-b ≡ a'-b'(mod m)

8) ab ≡ a'b'(mod m)
9) a ≡ b(mod m) $\Rightarrow$ ka ≡ kb(mod m)
10)a ≡ b(mod m) $\Rightarrow$ $a^n \equiv b^n$ (mod m)
11)a ≡ b (mod m_1) and a ≡ b(mod m_2) $\Rightarrow$ a ≡ b (mod[m_1,m_2]), where [m_1,m_2] is the least common multiple (LCM)
12)ak ≡ bk(mod m) $\Rightarrow$ a ≡ b (mod $\frac{m}{(k,m)}$), where (k,m) is the greatest common divisor (GCD).
13)If a ≡ b (mod m), then p(a) ≡ p(b)(mod m), for p(x) a polynomia.

Theorem

If a,b,c and d $\in$ Z, then:

1) a ≡ b (mod m) iff b ≡ a (mod m) iff b – a ≡ 0 (mod m)
2) If a ≡ b (mod m) and b ≡ c, then a ≡ c (mod m)
3) If a ≡ b (mod m) and d|m, d $\neq$ 0, then a ≡ b(mod d)
4) If a ≡ b(mod m) and c $\neq$ 0, then ac ≡ bc (mod mc)
5) If a ≡ b (mod m) and c ≡ d (mod m), then a+c≡ b+d (mod m)
6) If a ≡ b (mod m) and c ≡ d (mod m), ac ≡ bd(mod m)

Theorem (Cancellation Law)

Let m be any fixed modulus and suppose ab ≡ ac (mod m).
Then b ≡ c (mod m/d), where d = (a, m).
In particular, if a and m are relatively prime, then ab ≡ ac(mod m) implies
b ≡ c(mod m).

Propositions

1. Cancellation

If gcd(c, n)=1 and ac ≡ bc (mod n), then a ≡ b (mod n)

2. Units

If gcd(a,n)=1, then the equation ax ≡ b(mod n) has a solution, and the solution is unique modulo n.

3. Solvability

The equation ax ≡ b(mod n)has a solution iff gcd(a,n) divides b.

Algorithm (Inverse Modulo n)

Suppose a and n are integers and gcd(a,n)=1. The algorithm finds an x such that $ax \equiv 1 \pmod{n}$

Procedure: Compute extended GCD using Extended Euclidean Algorithm to compute integers x,y such that $ax + ny = 1$

Example: Find an integer $37x \equiv 1 (\text{mod } 101)$

Solution

$37x \equiv 1 \pmod{101}$

Step 1: Forming the equation

$37x + 101y = 1$

Step 2: Finding gcd = 1

Using the Extended Euclidean Algorithm,
$101 = 2 \times 37 + 27$ ………………… (i)
$37 = 1 \times 27 + 10$…………………. (ii)
$27 = 2 \times 10 + 7$ …………………… (iii)
$10 = 1 \times 7 + 3$ …………………….. (iv)
$7 = 2 \times 3 + 1$…………………….. (v)
Thus gcd(101,37) = 1

Step 3: Working through the following steps (i) ,(ii),(iii),(iv) and finally (v), backwards;

i. $27 = 101 - 2(37)$

ii. $10 = 37 - 1(27)$
$= 37 - 1[101 - 2(37)]$ i.e Substituting the value of 27 in (i) above.
$= 37 - 1(101) + 2(37)$
$= {}^{-}101 + 3(37)$

iii. $7 = 27 - 2(10)$
$= 101 - 2(37) - 2[{}^{-}101 + 3(37)]$
i.e. Substituting the final values of 27 and 10 in (i) & (ii) above
$= 101 - 2(37) + 2(101) - 6(37)$
$= 3(101) - 8(37)$

iv. $3 = 10 - 1(7)$
$= {}^{-}101 + 3(37) - 1[3(101) - 8(37)]$
i.e. Substituting the values of 10 and 7 in (ii) and (iii) above
$= {}^{-}101 - 3(101) + 3(37) + 8(37)$
$= {}^{-}4(101) + 11(37)$

v. $1 = 7 - 2 \times 3$

$= 3(101) - 8(37) – 2[^{-}4(101) + 11(37)]$
$= 3(101) +8(101) – 8(37) -22(37)$
$= 11(101) -30(37)$
Hence $37x + 101y \equiv {}^{-}30(37) + 11(101)$

$\Rightarrow x = {}^{-}30$ is a solution to $37x \equiv 1(\text{mod } 101)$.

EULER’S ∅ - FUNCTION

Definition: Arithmetic Function (f)
An arithmetic function is a function whose domain is the set of positive integers e.g if a function f(p)= p for p = 1,2,3,4,…..assigns only positive values of the root, then we say that the function is an arithmetic function.

Definition: Multiplicative

A function G is multiplicative if G(pq) = G(p) G(q) whenever p and q are relatively prime positive integers, and completely multiplicative if G(pq)=G(p)G(q) for all positive integers p and q.

Definition: Euler’s ∅ - Function (Euler’s totient function)
The symbol ∅ - (phi) is used to represent the Euler function.
∀ p>1, let ∅ (p) designate the number of positive integers less than p and relatively prime to p.

Example: ∅ (15)= 8 ie there are 8 positive integers, 1,2,4,7, 8,11, 13, 14 less than and relatively prime to 15. If given ∅ (1) = 1, then ∅ is an arithmetic function. This function is called the Euler’s ∅ function or Euler’s Totient function (Leonhard Euler 1701 – 1783, Swiss mathematician)

Properties of ∅

1. For any prime p, ∅ (p) = p -1 =p(1-$\frac{1}{p}$)

∅ is multiplicative ie ∅ (pq) =∅ (p).(∅ (q).

Theorem

∅ (m) of the m distinct residue classes mod m are relatively prime to m, which is the number of integers $0 \leq r < m$.

Fermat’s Little Theorem

If p is a prime and a is any integer, then

1. $a^{p} \equiv a(\text{mod } p)$.
2. If a and p are relatively prime, then $a^{p-1} \equiv 1(\text{mod } p)$.

Theorem

The system of congruences
$x \equiv$ a(mod m)
$x \equiv$ b(mod n)
Is solvable if and only if (m, n) divides b – a. In the case where a solution x_o exists, a number x is also a solution and if only $x \equiv x_o$ (mod[m,n]), where [m, n] is the least common multiple of m and n.

PRIMITIVE ROOTS

A primitive root of a prime p is an integer g such that g (mod p) has modulo order p-1.
Generally, if gcd(g,n)=1 { g and n are relatively prime) and g is of modulo order ϕ(n) modulo n where ϕ(n) is the totient function, then g is a primitive root of n.
If n has a primitive root, then it has exactly ϕ[ϕ(n)] of them, which means that if p is prime number, then there are exactly ϕ(p-1) incongruent primitive roots of p.for n=1,2,3,…., the first few values of ϕ[ϕ(n)] are 1,1,1,1,2,1,2,2,2,2,4,2,4,2,4,4,8.

N has a primitive root if it is of the form 2,4,p^a or $2p^a$, where p is an odd prime and a $\geq$1. the first few n for which primitive roots exist are 2,3,4,5,6,7,8,9,10,11,13,14,17,18,19,22,…….., so the number of primitive roots of order n for n=1,2,….are 0,1,1,1,2,1,2,0,2,2,4,0,4,……. The smallest primitive root for the first few primes p are 1,2,2,3,2,2,3,2,5,2,3,2,6,3,5,2,2,2……..

Table of the primitive roots for the first few n for which a primitive root exists.

n	g(n)
2	1
3	2
4	2
5	2,3
6	5
7	3,5
9	2,5
10	3,7
11	2,6,7,8
13	2,6,7,11

The largest primitive roots for n=1,2,…… are 0,1,2,3,5,5,0,5,7,8,0,11,………

Let m be a positive integer. Let a be any positive integer relatively prime to m and let k be the smallest positive integer such that $a^k \equiv 1 \pmod{m}$.The number k is called the exponent to which a belongs modulo m.

Example:
7 belongs to the exponent 2 modulo 4 since $7^2 \equiv 1 \pmod{4}$

but$7^1 \not\equiv 1 (\mathrm{mod}\ 4)$

Theorems:

1) If k is the exponent to which a belongs modulo m, then k divides $\phi(m)$.
2) For any prime p there are exactly $\phi(p - 1)$incongruent primitive roots modulo p.
3) If p is any prime and g is any primitive root modulo p, then the powers g, $g^2, \ldots, g^{p-1}$ form a reduced system of residues modulo p.
4) Let m be any integer greater than 1. Primitive roots exist modulo m if and only if $m=2$, $m=4$, $m=p^n$, $m=2p^n$ where p is an odd prime

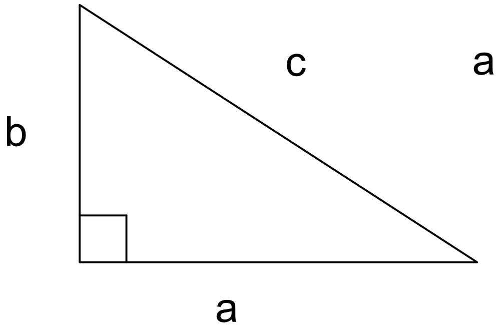
Pythagorean Triples

History of Pythagorean Triples

The study of Pythagorean triples began long before the time of Pythagoras. Babylonians and ancient Egyptians used the triples

Pythagorean Triples

Figure 1: Pythagorean Triangle



$$a^2 + b^2 = c^2$$

Examples of Pythagorean Triples

- $3^2 + 4^2 = 5^2$
- $5^2 + 12^2 = 13^2$
- $8^2 + 15^2 = 17^2$
- $28^2 + 45^2 = 53^2$

Table 1:

S/No	a" Odd"	b " Even"	c "Odd"	Equation
1	3	4	5	$3^2 + 4^2 = 5^2$
2	5	12	13	$5^2 + 12^2 = 13^2$
3	7	24	25	$7^2 + 24^2 = 25^2$
4	9	40	41	$9^2 + 40^2 = 41^2$
5	11	60	61	$11^2 + 60^2 = 61^2$
6	15	8	17	$15^2 + 8^2 = 17^2$
7	21	20	29	$21^2 + 20^2 = 29^2$
8	33	56	65	$33^2 + 56^2 = 65^2$
9	45	28	53	$45^2 + 28^2 = 53^2$

PRIMITIVE PYTHAGOREAN TRIPLES

Definition:

A Primitive Pythagorean triple is a triple of numbers (a,b,c) so that a, b and c have no common factors and satisfy $a^2 + b^2 = c^2$

Observations on the Pythagorean Triples (Table 1)

- One of a and b is odd and the other even and it seems c is always odd.
- Taking a to be odd and b to be even, then for $a^2 + b^2 = c^2$

We can find a as $a^2 = c^2 - b^2 = (c - b)(c + b)$.

Examples

3,4,5 $\Rightarrow 3^2 = (5^2 - 4^2) = (5 - 4)(5 + 4) = 1 \times 9 = 1^2 \times 3^2$

5,12,13 $\Rightarrow 5^2 = (13^2 - 12^2) = (13 - 12)(13 + 12) = 1 \times 25 = 1^2 \times 5^2$

7,24,25 $\Rightarrow 7^2 = (25^2 - 24^2) = (25 - 24)(25 + 24) = 1 \times 49 = 1^2 \times 7^2$

15,8,17 $\Rightarrow 15^2 = (17^2 - 8^2) = (17 - 8)(17 + 8) = 9 \times 25 = 3^2 \times 5^2$

- From observations, it seems

1. (c – b) and (c + b) are always Prime odd squares
2. (c – b) and (c + b) have no common factors.

Pythagorean Triples and the Unit Circle

Given $a^2 + b^2 = c^2$, dividing through by $c^2 \Rightarrow (\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$

It follows the rational numbers $\left(\frac{a}{c}\right)$ and ($\left(\frac{b}{c}\right)$) is a solution to the equation of a circle
$x^2 + y^2 = 1$, which describes a circle of radius 1 with center (0, 0) on the Cartesian plane.

List of Pythagorean Triples

(a, b, c)	(a, b, c)	(a, b, c)	(a, b, c)
3,4,5	64,1023,1025	84,13,85	96,2303,2305
5,12,13,	68,285,293	84,187,205	100,621,629
7,24,25	63,1155,1157	84,437,445	100,2499,2501
9,40,41	72,65,97	84,1763,1765	
15,8,17	72,1295,1297	88,105,137	
21,20,29	76,357,365	88,1935,1937	
35,12,37	76,1443,1445	92,525,533	
45,28,53	80,39,89	92,2115,2117	
63,16,65	80,1599,1601	96,247,265	

THE FIELD OF INTEGERS (MOD P), SQUARES AND QUADRATIC RESIDUES

Definition
If xn = a(mod m), has a solution, where a and m are relatively prime, then a is called an nth power residue modulo m.If the congruence has no solution, then a is called an nth power non-residue modulo m.

QUADRATIC RECIPROCITY, THE QUADRATIC RECIPROCITY LAW AND THE LEGENDRE SYMBOL

Definition:
The linear equation $a \equiv b \pmod{n}$ has a solution if and only if gcd(a.n)divides b.
Quadratic reciprocity searches for a criterion for whether or not equation
$ax^2 + bx + c \equiv 0 \pmod{n}$.

Definition
Fix a prime p. An integer a not divisible by p is quadratic residue modulo p if a is a square modulo p; otherwise, a is a quadratic nonresidue.

Definition: Legendre Symbol
Let p be an odd prime and let a be an integer coprime to p. Set

$$\left(\frac{a}{p}\right) = \begin{cases} +1 \text{ if a is a quadratic residue} \\ {}^{-}1 \text{ otherwise} \end{cases}$$

We call this symbol $\left(\frac{a}{p}\right)$ the Legendre symbol. This notation is well entrenched in the literature even though it is also the notation for “ a divided by p”.

Note: $\left(\frac{a}{p}\right)$ only depends on a(modp), it makes sense to define $\left(\frac{a}{p}\right)$ for a є Z / $_p$Z to

be $\left(\frac{\tilde{a}}{p}\right)$ for any lift $\tilde{a}$ of a to Z.

Legendre Symbol of 2

Definition:
Let p be odd prime.

$$\begin{cases} +1 \text{ if } p \equiv \pm 1 \text{ (mod 8)} \\ {}^{-}1 \text{ if } p \equiv \pm 3 \text{ (mod 8)} \end{cases}$$

EULER’S CRITERION, GAUSS LEMMA AND THE QUADRATIC RECIPROCITY LAW

EULER’S CRITERION

Let p be an odd prime and a an integer not divisible by p. Euler used the existence of primitive roots to show that $\left(\frac{a}{p}\right)$ is congruent to a$^{(p-1)/2}$ modulo p.

Eulers criterion: We have $\left(\frac{a}{p}\right) \equiv 1$ if and only if a$^{(p-1)/2}$ = 1 (mod p)

Let p be an odd prime and let a be an integer not equal to 0 (mod p). From the numbers

a, 2a, 3a,………, $\frac{p-1}{2}a$ and reduce them modulo p to lie in the interval $\left(\frac{-p}{2}, \frac{p}{2}\right)$.

Let υ be the number of negative numbers in the resulting set. Then $\left(\frac{a}{p}\right)$ =($^{-}$1)$^{\upsilon}$.

EVALUATING THE QUADRATIC CHARACTER BY THE RECIPROCITY LAW

Theorems:

1. Let p be an odd prime and let a be relatively prime to p. Then 2 is a quadratic residue for all primes of the form 8n ± 1; 2 is a quadratic non-residue for all primes of the form 8n ± 3.
2. If p is prime and (a,p) = 1, then the congruence ax^2 + bx + c ≡ 0 (mod p) has at most two incongruent solutions modulo p.

Step 1: Technique of Induction

Mathematical induction proves by checking if a proposition hold's for n=1, and n= k+1 whenever it holds for n=k, then the proposition holds for all positive integers n= 1,2, 3,……..

Step 2: Substitute n=1, in the equation:

$1^3 = \frac{1^2(1+1)^2}{4} \Leftrightarrow$ 1=1 i.e It holds for n =1.

Step 3: Assume that the formula holds for n= k

$1^3 + 2^3 + 3^3 + 4^3 + ...+ k^3 = \frac{k^2(k+1)^2}{4}$

Step 4: Proof that the formula holds for n= k+1.

$1^3 + 2^3 + 3^3 + 4^3 + ...+ k^3 + (k+1)^3 = \frac{(k+1)^2(k+1+1)^2}{4}$

We write

$1^3 + 2^3 + 3^3 + 4^3 + \ldots\ldots + k^3 = \dfrac{k^2(k+1)^2}{4}$

$\Rightarrow \dfrac{k^2(k+1)^2}{4} + (k+1)^3 = \dfrac{(k+1)^2(k+1+1)^2}{4}$

$\Rightarrow \dfrac{k^2(k+1)^2 + 4(k+1)^3}{4} = \dfrac{(k+1)^2(k+2)^2}{4}$ Cancelling the 4 on both sides

$\Rightarrow k^2(k+1)^2 + 4(k+1)^3 = (k+1)^2(k+2)^2$

$\Rightarrow (k+1)^2[(k^2 + 4(k+1)] = (k+1)^2(k+2)^2$ Dividing by $(k+1)^2$

$\Rightarrow k^2 + 4k + 4 = k^2 + 4k + 4$ (Proved)

This is proof by induction

(ii). Prove that $a+ar+ar^2+\ldots+ar^n = \dfrac{a(1-r^{n+1})}{1-r}$, n>0

Proof:

Step 1: Technique of Induction

Mathematical induction proves by checking if a proposition hold's for n=1, and n= k+1 whenever it holds for n=k, then the proposition holds for all positive integers n= 1,2, 3,……..

Step 2: Substitute n=1, in the equation:

$a+ar = \dfrac{a(1-r^{1+1})}{1-r} = \dfrac{a(1-r^2)}{1-r} = \dfrac{a(1-r)(1+r)}{1-r} = a + ar$ i.e It holds for n =1.

Step 3: Assume that the formula holds for n= k

$a+ar+ar^2+\ldots+ar^k = \dfrac{a(1-r^{k+1})}{1-r}$

Step 4: Proof that the formula holds for n= k+1.

a+ar+ar^2+…, + ar^k +ar^{k+1}= $\frac{a(1-r^{k+1+1})}{1-r}$

We write

a+ar+ar^2+…+ar^k= $\frac{a(1-r^{k+1})}{1-r}$

$\Rightarrow$ $\frac{a(1-r^{k+1})}{1-r}$ + ar^{k+1} = $\frac{a(1-r^{k+2})}{1-r}$

$\Rightarrow$ $\frac{a(1-r^{k+1})}{1-r}$ + $\frac{ar^{k+1}(1-r)}{1-r}$ = $\frac{a(1-r^{k+2})}{1-r}$

$\Rightarrow$ $\frac{a(1-r^{k+1})+ar^{k+1}(1-r)}{1-r}$ = $\frac{a(1-r^{k+2})}{1-r}$

$\Rightarrow$ $\frac{a-ar^{k+2})}{1-r}$ = $\frac{a(1-r^{k+2})}{1-r}$ Opening brackets and simplifying

$\Rightarrow$ $\frac{a(1-r^{k+2})}{1-r}$ = $\frac{a(1-r^{k+2})}{1-r}$ (Proved)

This is proof by induction

3. a) By definition, n|ac –bc = (a-b)c and since gcd(n,1), it follows that n|a-b, so a ≡ b(mod n).

   b).Use Euclid's algorithm to solve 17x ≡ 1(mod 61)

   Solution:
   Step 1: Find x and y such that 17x + 61y = 1

   Using Euclid's algorithm
   61= 3 x 17 + 10
   17 = 1 x 10 + 7
   10 = 1 x 7 + 3
   7 = 2 x 3 + 1

   Step 2:
   10 = 61 – 3 x 17
   7 = 17 – 1 x 10 = 17 -1[61 -3(17)]
   = 17 – 1(61) +3(17)
   =4(17) – 61
   = -61 + 4(17)

$3 = 10 - 1(7)$
$=61 - 3 \times 17 - 1(7)$
$= 61 - 3 \times 17 - 1[-61 + 4(17)]$
$= 61 + 1(61) -3(17) - 4(17)$
$=2(61) - 7(17)$

$1 =7 - 2x3$
$= -61 + 4(17) - 2[2(61) - 7(17)]$
$= -61 - 4(61) +4(17) + 14(17)$
$= -5(61) + 18(17)$

Hence $17x + 61y \equiv 18(17) - 5(61)$
$\Rightarrow x = 18$ is a solution to $17x \equiv 1(\text{mod } 61)$

4. a)From the table, when q=6, then x=5 and y= 2
$\Rightarrow (5 + 2 \sqrt{6})^2 = 25 + 20\sqrt{6} +24 = 49 +20\sqrt{6}$
$\Rightarrow$ x = 49 and y = 20 are the fundamental solutions of Pell's equation
Larger solutions are:
$(5 + 2\sqrt{6})^3 = (5 + 2\sqrt{6})(49 +20\sqrt{6}) = 485 + 198\sqrt{6}$.
Hence x=485 and y = 198.

b) From the table, when q=14 then x=15 and y = 4.
$\Rightarrow (15 + 4 \sqrt{14})^2 = 225 + 120\sqrt{14} +224 = 449 +120\sqrt{14}$
$\Rightarrow$ x = 449 and y = 120 are the fundamental solutions of Pell's equation
Larger solutions are:
$(15 + 4\sqrt{14})^3 = (15 + 4\sqrt{14})(449 +120\sqrt{14}) = 13\,455 + 3596\sqrt{14}$.
Hence x=13 455 and y = 3596.

5. Solve for x and y in the Diophantine equation

$$2261x+1275y= \gcd(2261,1275).$$

Step1:gcd(2261,1275)
$2261=1 \times 1275 + 986$
$1275 = 1 \times 986 + 289$
$986 = 3 \times 289 + 119$
$289 = 2 \times 119 + 51$
$119 = 2 \times 51 + 17$
Hence gcd (2261,1275) = 17

Substituting the gcd in equation
$2261x + 1275y = 17$

Applying back substitution:
$17 = 119 - (2 \times 51)$
$=119 - 2(289 -2(119))$

$=119 -2(289) +4(119)$
$=5(119) – 2(289)$
$=5(119)-2(1275-1(986))$
$=5(986 -3 \times 289) -2(1275 – 1(986))$
$=5(986) – 15(289) –2(1275) +2(986)$
$=7(986) – 15(1275 – 1(986)) – 2(1275)$
$=7(986) – 15(1275) +15(986) – 2(1275)$
$=22(986) -17(1275)$
$=22(2261 – 1(1275)) -17(1275)$
$=22(2261) – 22(1275) -17(1275)$
$=22(2261) – 39(1275) \Leftrightarrow 2261x + 1275y$

Hence $x = 22$ and $y = -39$.

ELEMENTARY NUMBER THEORY

DIVISIBILITY AND FACTORS

Every positive whole number has a finite set of *factors* – numbers that divide it evenly.

2 has factors 2 and 1
4 has factors 4,2 and 1
6 has factors 6,3,2, and 1
24 has factors 24, 12, 8, 6, 4, 3, 2, and 1.

If a is a factor of b, we write a|b.

This relation is reflexive and transitive:

a|a (a divides itself)
if a|b and b|c, then a|c

DIVISIBILITY TESTS:

A number is divisible by:

2 if it ends in 0,2,4,6,8
3 if repeated summing of digits gives 3,6,9
4 if its ones digit plus twice its tens digit is divisible by 4
5 if it ends in 0 or 5
6 if it’s divisible by 2 and 3
9 if repeated summing of its digits gives 9
10 if it ends in 0
11 if repeated alternating subtracting and adding of its digits gives 0

EXAMPLES:

12,665,328 is divisible by 2: it ends in 8.

12,665,328 is divisible by 3:
1+2+6+6+5+3+2+8 = 33, 3+3 = 6

So 12,665,328 is divisible by 6 (but not by 9)

7645 is divisible by 11: 7-6+4-5 = 0

Testing whether a Single Number is Prime

If n = ab, then at least one of a,b must be less than $\sqrt{n}$. So:

(1) Find all primes up to $\sqrt{n}$. You can use the Sieve of Eratosthenes.

(2) Use divisibility tests for 2,3,5, and 11.
Use trial division for all the others. If you don't find a factor, n is prime.

EXAMPLE: is 443 prime?
$\sqrt{443}$ = 21.04... so we only need to test primes less than 22.

These are 2,3,5,7,11,13,17,19.

443 is not divisible by 2: 3 is odd.
443 is not divisible by 3: 4+4+3 = 11, 1+1=2.
443 is not divisible by 5: $3 \neq 0$ or 5
443 is not divisible by 11: 4-4+3 = 3
443 is not divisible by 7 (443 = 63x7 + 2)
443 is not divisible by 13 (443= 34x13 + 1)
443 is not divisible by 17 (443= 26x17 + 1)
443 is not divisible by 19 (443= 23x19 + 6)

So 443 is prime.

LAWS FOR DIVISIBILITY

*If a|b and a|c then a|(b+c)

*If a|b and a|c, then a|(b-c)

*if a|b then a|kb for all k.

COUNTING FACTORS

If $n = p_1^{n_1} \; p_2^{n_2} \; ... \; p_k^{n_k}$

where the p_i are *distinct* primes,
then n has exactly $(n_1+1)(n_2+1)...(n_3+1)$
factors.

EXAMPLE: $40 = 2^3 5^1$
and 40 has (3+1)(1+1) factors:

1	2	4	8
5	10	20	40

(the rows correspond to 0 or 1 fives,
the columns to 0,1,2, or 3 twos.)
\\

EXAMPLE: $144 = 2^4 3^2$
and 144 has (4+1)(2+1) factors

1	2	4	8	16
3	6	12	24	48
9	18	36	72	144

EXAMPLE: What is the smallest number with exactly 27 factors?
$27 = 3^3 = (2+1)(2+1)(2+1)$
so the number must have three prime factors, each appearing twice. The smallest three primes are 2,3, and 5, so the answer is
$2^2 \, 3^2 \, 5^2 = 900$. The factors are

1	2	4	5	10	20	25	50	100
3	6	12	15	30	60	75	150	300
9	18	36	45	90	180	225	450	900

GREATEST COMMON FACTOR
(GREATEST COMMON DIVISOR)

The GCF or GCD of two numbers is the largest whole number that divides both of them.

EXAMPLE: Find the GCF of 24 and 40

Factors of 24: 1,2,3,4,6,8,12,24
Factors of 40: 1,2,4,5,8,10,20,40

The largest number in both lists is 8 so this is the GCF.

EXAMPLE: Find the GCF of 36 and 25

Factors of 36: 1,2,3,4,6,9,12,18,36
Factors of 25: 1, 5, 25

The only number common to both lists is 1, so this is the GCF. Numbers with GCF(m,n) =1 are called *coprime.*

A slightly more sophisticated algorithm uses the prime factorizations of m and n. Take each prime factor that appears in both, and choose the lower of the two exponents. This gives the prime factorization of the GCF.

EXAMPLE: find the GCF of 48 and 60.

$24 = 2^4 \times 3^1$ $40 = 2^2 \times 3^1 \times 5^1$

The GCF is thus $2^2 \times 3^1 = 12$.

A really clever algorithm, due to Euclid, uses the fact that any common factor of a and b also divides b-a, b-2a, b-3a, and so on.

Divide the larger of the two numbers by the smaller and take the remainder.

If the remainder is 0 the smaller number is the GCF.

If not, the remainder and the smaller number have the same GCF as the original numbers.

EXAMPLE:

Find GCF (48,40)

$$40\,\overset{1}{\overline{)\,48}}\quad \text{remainder 8}$$

$$8\,\overset{5}{\overline{)\,40}}\quad \text{no remainder}$$

So 8 = GCF(40,8) = GCF(48,40).

EXAMPLE: Find GCF (1200, 720)

1 remainder 480

720 1200

1 remainder 240

480 720

2 no remainder

240 480

So GCF(1200,720) = 240.

Euclid's algorithm typically requires only a few steps even for huge numbers.

EXAMPLE: Find GCF (640, 365)

1 remainder 275

365 640

1 remainder 90

275 365

3 remainder 5

90 275

18 no remainder

5 90

So GCF (640,365) = 5.

The Least Common Multiple (LCM) is the smallest number that they both divide.

EXAMPLE: lcm(25,40) = 200

*We cannot easily compute this by listing all their multiples!

*If we have prime factorizations of m and n, then LCM(m,n) has all the prime factors that appear in either, with the larger of the exponents if p appears twice.

$25 = 5^2$ $40 = 2^3 \text{ x } 5$

$\text{LCM}(25,40) = 2^3 \text{ x } 5^2$

For big numbers, the fastest way to find the LCM is to use the "diamond theorem":

LCM(a,b) GCD(a,b) = ab

$$\begin{tikzcd}
 & LCM(a,b) & \\
a \arrow[ur] & & b \arrow[ul] \\
 & GCD(a,b) \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Therefore $LCM(a,b) = \frac{a \times b}{GCD(a,b)}$.

Example: $LCM(640,365) = \frac{640 \times 365}{5}$

$= 46720$

Public key cryptography and RSA Cipher

The RSA Cipher. It is the most popular cryptosystem among today's secure ciphers. It leads us to Two-Key Cryptography – commonly called Public-Key Cryptography.

1) Alice and Bob publicly pick 2 integers: a) a prime number p b) and an integer s between 1 and p.		1) Alice and Bob publicly pick a) p = 11 and b) s = 3.	
2) Alice picks a random number a that is less than p.	2) Bob picks a random number b that is less than p.	2) Alice picks a=2.	2) Bob picks b=4.
3) Alice computes $A = s^a$ MOD p and sends A to Bob.	3) Bob computes $B = s^b$ MOD p and sends B to Alice.	3) Alice computes $A = 3^2$ MOD 11 = 9	3) Bob computes $B = 3^4 = 81$ = 4 MOD 11
4) Alice computes the key $K = B^a$ MOD p.	4) Bob computes the key $K = A^b$ MOD p.	4) Alice computes $K = 4^2$ MOD 11 = 5	4) Bob computes $K = 9^4 = 6561$ MOD 11 = 5.

We have to answer the following two questions:

1) Why do Alice and Bob always end up with the same key K ?
2) Why can't an eavesdropper compute K ?

Answer to questions 1):
Alice and Bob compute the key K in the final step as follows:

Alice: K = $B^a = s^{ba}$ MOD p.
Bob: K = $A^b = s^{ab}$ MOD p.
Since $s^{ba} = s^{ab}$ MOD p both Alice and Bob compute the same key K.

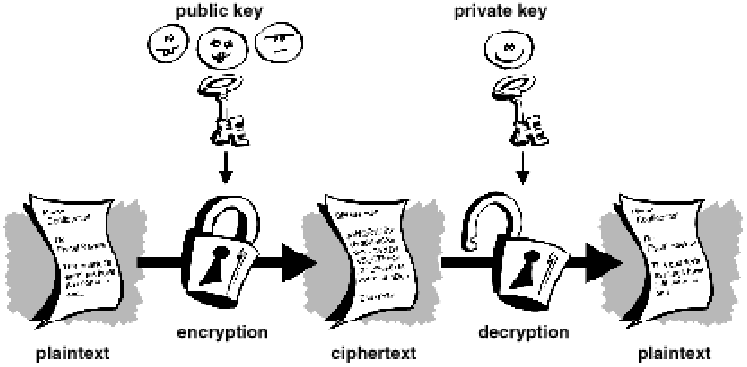
Answer to questions 2):
Say, an eavesdropper did a great job by intercepting the values A and B, p and s. In order to uncover the key K he has to compute either a or b. Mathematics teaches that this is impossible if a, b, p, s, A, B were chosen as of 100-digits numbers or larger.
The reason: although it is quite simple to compute i.e. A = s^a MOD p, however, solving this equation for a is impossible. More formally stated: Although the “discrete exponential function” can be executed, its inverse, the “discrete logarithm function” can not. Hence, the “discrete exponential function” is an example of a “One-Way function”. We will study such functions later on this chapter.

Diffie’s Search for a Public Key Cryptosystem

Each party shall possess a key pair, a public and a private key. I.e. Alice’s public key is used by Bob to encrypt the message for Alice whereas her private key is used to decrypt Bob’s encrypted message.

> Which mathematical function allows anybody to encrypt a secret message for Alice using her publicly known encoding key *e* and prevents everybody but Alice to decrypt such cipher message?

It requires an experienced mathematician to find such one-way functions since most functions are two-way and can thus be reversed. I.e. A Caesar right shift can be reversed by a corresponding left shift. Mathematically, since addition can be reversed by subtraction it is (the simplest) two-way function.



This diagram shows that Public–Key Cryptography uses two different keys for en- and decryption. knowing the public encoding key does not reveal the decoding key.

The RSA Cipher is a Public-Key-Cryptosystem

Given sufficiently large key lengths, RSA realizes the Public-Key Property:

> The knowledge of the encoding key does not reveal the knowledge of the decoding key. Even the usage of the most powerful computers combined will not suffice to crack the secret decoding key based on the knowledge of the publicly known encoding key.

As a consequence:

> Only one key pair per person is needed. Therefore, a total of only n key pairs are needed for n communicating people.

In particular, 100 people communicating just need 100 key pairs. The 100 encoding keys are publicly known.

An Example for RSA Encryption

The 4 steps involved in the RSA Cipher are displayed in the middle column. In the right column I demonstrate how the word “SAFE” is en- and decrypted using the RSA Cipher. We use the same letter values as in the previous chapters to encrypt: S=18, A=0, F=5, E=4. Again, the choice of the letter values is arbitrary. It just matters that sender and recipient use the same letters values. Let’s go ahead and perform the RSA encryption.

Example for RSA Encryption and Decryption:

1. Step: Preparation	a) Choose two primes p and q so that their product n=p*q is greater than the used alphabet length M (i.e. here M=26). c) *Compute $\varphi(n)$.*	*a) Say p=3 and q=11, then n=33* b) $\varphi(33) = (3-1)*(11-1) = 20$

2. Step: Encryption uses the public key (n,e)	a) Choose a public encoding key e that has to be relative prime to $\varphi(n)$.
	b) We now encrypt each plain letter P by computing
	$C=P^e$ MOD n.
		a) Here, possible values for e are 3, 7, 9, 11, 13, 17, 19. Let’s pick e=3.
		b) We encrypt as follows:
		S =18: 18^3 = 24 MOD 33
		A = 0: 0^3 = 0 MOD 33
		F = 5: 5^3 = 26 MOD 33
		E = 4: 4^3 = 31 MOD 33

3. Step: Decryption uses the private key	a) The private decoding key d is chosen as the inverse of e MOD $\varphi(n)$: e * d = 1 MOD $\varphi(n)$	a) d=7 since 3*7 = 1 MOD 20. b) 24^7 = 18 MOD 33, 18=S.

(d,n)	Mathematically, find integers d and k that fulfill: $e * d = 1 + k * \varphi(n)$ via the Extended Euclidean Algorithm. b) We decrypt by computing $P=C^d$ MOD n	$0^7 = 0$ MOD 33, 0=A. $26^7 = 5$ MOD 33, 5=F. $31^7 = 4$ MOD 33, 4=E.

Remark: I computed the above powers MOD 33 using the Windows 98 calculator. Let's verify by hand that i.e. the computation of 31^7 actually yields 4 MOD 33:
Since 31= -2 MOD 33 I can just multiply –2 by itself 7 times to compute $(-2)^7$ and obtain –128. Now, –128 = -95 = -62 = -29 = 4 MOD 33 which produces the calculator answer.

Why does RSA work? – A Proof

Why does the RSA Cipher work? With other words: for what miraculous reason does the final exponentiation C^d MOD n in step 3 yield the correct plain letter P ? Nobody would use the RSA encryption to encrypt highly sensitive data if RSA's encryption scheme is not guaranteed to yield the original plain text. Therefore, it is important to mathematically prove its correctness. The proof demonstrates how Rivest, Shamir and Adleman took advantage of Euler's Theorem

Proof of Correctness of the RSA Cipher
two cases:

I) The vast majority of plain letters values P are relative prime to the modulus n. For this case we take advantage of Euler's Theorem to prove the correct functioning of RSA.

II) We also have to prove the correctness of RSA for the rare instances when P is not relative prime to n. i.e. P and n possess a common divisor that is greater than 1.

I) RSA-proof when P and n are relative prime
We establish that C^d actually yields P by using a chain of identities that involves simple exponent rules and Euler's Theorem. Verify each step in the proof.

C^d	The cipher letter C was encrypted by raising the original plain letter P to the power of e: $C=P^e$. We substitute:
$= (P^e)^d$ MOD n	When raising a power to a power, we multiply the exponents:
$= P^{d*e}$ MOD n	The decoding key d was chosen to be relative prime to the encoding key e which can be stated as: $d*e = 1 + k * \varphi(n)$. Therefore,

$= P^{1 + k * \varphi(n)}$ MOD n	Adding exponents allows to multiply powers:
$= P^{1} * P^{k * \varphi(n)}$ MOD n	Multiplying exponents allows raising a power to a power:
$= P * (P^{\varphi(n)})^{k}$ MOD n	What is the purpose of setting up ($P^{\varphi(n)}$) ? Answer: To make use of Euler's Theorem: $P^{\varphi(n)}$ = 1 MOD n when P and n are relative prime. If P and n don't happen to be relative prime RSA still works properly. I will prove this case in part II) of the proof.
$= P * (1)^{k}$ MOD n	Raising 1 to any power yields 1. Guaranteed.
= P MOD n	The proof is complete. We verified that C^{d} yields P in case P and n are relative prime.

II) RSA-proof when P and n are not relative prime
In that case P and n have a common divisor. Consequently, either p or q must be a divisor of P. This results from the choice of n as the product of the primes p and q. In other words, p and q are the only divisors of n and any divisor that n has in common with P must be either p or q or a multiple of p or q. Without limiting the generality of our proof, we assume that p is a divisor of P. That means that there exists an integer x such that P = x * p.

In the first proof, Euler's Theorem is used .now its simplified version, the so-called "Fermat's Little Theorem" is used. If the modulus is a prime number p, the exponent simplifies to φ(p) = p-1. Why is that? Euler's φ-function φ(n) gives the number of integers less than n that are relative prime to n.

Fermat's Little Theorem

Given a prime p, then

$$a^{p-1} = 1 \text{ MOD } p$$

holds true for any integer a.

to start with Fermat's Little Theorem to prove that P^{de} = P MOD n.

Fermat's Little Theorem with the prime q holds true for any integer P. We manipulate the exponent by raising both sides to the	P^{q-1} = 1 MOD q	If p=5 and q=7 then n=p*q=35. Let's encrypt the message P=10. Then $10^{7-1} = 10^{6}$ = 1 MOD 7

power of (p-1)*k for some integer k.		is guaranteed true because of Fermat’s Little Theorem.
Raising powers to powers allows multiplying exponents.	$(P^{q-1})^{(p-1)*k} = 1^{(p-1)*k}$ MOD q	$(10^{6})^{4*k} = 1^{4*k} = 1$ MOD 7
Why did we do so? Because (p-1)*(q-1)*k = φ(p*q) * k = φ(n) * k = de –1 when choosing d and e to be inverse mod φ(n) . We may therefore write	$P^{(q-1)*(p-1)*k} = 1$ MOD q	$10^{6*4*k} = 1$ MOD 7 We choose d=5 and e=5 so that they are inverse MOD 24 where 24 = φ(35) = (7-1)*(5-1) since 5 * 5 = 25 = 1 MOD 24.
Subtracting 1 on both sides yields	$P^{de-1} = 1$ MOD q	With k=1: $10^{6*4*k} =$ $10^{d*e-1} =$ $10^{5*5-1} = 1$ MOD 7
(Adjusting the modulus) If $P^{de-1} - 1$ is a multiple of q then p* ($P^{de-1} - 1$) must be a multiple of p*q. Consider a simple example with p=2: If 15 is a multiple of 5 then 30 is a multiple of 10.	$P^{de-1} - 1 = 0$ MOD q	10^{5*5-1} –1 = 0 MOD 7
Can you finish the proof without looking at the remaining proof? Try it, it is not difficult.	p*($P^{de-1} - 1$) = 0 MOD p*q	5* (10^{5*5-1} –1) = 0 MOD 7 * 5
(Obtaining $P^{de} = P$) Since P is a multiple of p P*($P^{de-1} - 1$) must also be a multiple of p*q. Continuing our example P=7*p: If 30 is a multiple of 10 then 7*30 = 210 is also a multiple of 10.	p*($P^{de-1} - 1$) = 0 MOD p*q	5* (10^{5*5-1} –1) = 0 MOD 35
Distributing yields	P*($P^{de-1} - 1$) = 0 MOD p*q	10* (10^{5*5-1} –1) = 0 MOD 35
Adding P on both sides and substituting n for p*q	$P^{de} - P = 0$ MOD p*q	10^{5*5} – 10 = 0 MOD 35

concludes our proof.		
We verified that P’ = P when P and n are not relative prime. Combining the proofs I) and II), we understand why the RSA encryption works properly in any case.	P^{de} = P MOD n	10^{5*5} = 10 MOD 35

We considered already an example when P and n are relative prime. Let’s now consider two simple examples for the case that P is a multiple of p.

Example 1: Say we choose p=3 and q =5 as two small distinct primes. Then: n = p*q = 15 (allowing us to only encrypt 15 letters) and $\varphi(15) = 2*4 = 8$. We may therefore choose the keys to be e = 3 and d = 3 since their product yields 9 and 9 = 1 MOD 8 where 8 = $\varphi(15)$. It is coincidence that the encryption key equals the decryption key. Instead, we could have also chosen e = 3 and d = 11 (since 33 = 1 MOD 8) or e = 3 and d = 19 (since 57=1 MOD 8). Or e = 5 and d = __ ? Do not miss to fill in the answer. Then continue!
Let’s now select a plain letter P such that it has a common divisor with n = 15, say we have to encrypt letter P = 6. We have to verify that P^{de} = P MOD n (here $6^9 = 6$ MOD 15).
Since $6^2 = 36 = 6$ MOD 15, we deduce that $6^8 = 6^2 * 6^2 * 6^2 * 6^2 = 6 * 6 * 6 * 6 = 6^2 * 6^2 = 6 * 6 = 6^2 = 6$ MOD 15.
Thus, $6^9 = 6^8 * 6 = 6 * 6 = 6$ which shows that the RSA scheme decrypts the correct plain letter P = 6.

Exercise1: Why would it be incorrect to argue as follows: Euler’s Theorem yields $6^{\varphi(15)} = 6^8 = 1$ MOD 15 and therefore $6^9 = 6^8 * 6 = 1 * 6 = 6$ MOD 15. Even though the final answer is correct, where is a mistake in my argument? We computed correctly in example 1 that $6^8 = 6$ MOD 15.

Example 2: Let’s now verify that RSA decrypts the plain letter P = 12 correctly. For that, we have to verify that $12^9 = 12$ MOD 15. Since $12^2 = 144 = 9$ MOD 15 and $12^4 = (12^2)^2 = 9^2 = 81 = 6$ MOD 15, we know that $12^8 = (12^4)^2 = 6^2 = 36 = 6$ MOD 15. This leads us to the final result: $12^9 = 12^8 *12 = 6 *12 = 72 = 12$. Correct.

Exercise 2: Prove that the plain letter P = 10 will be decrypted correctly by showing that $10^9 = 10$ MOD 15.

Exercise 3: Prove that the plain letter P = 8 will be decrypted correctly by showing that $8^9 = 8$ MOD 15.

Why is RSA secure?

How can the RSA Cipher be upgraded to a secure cipher?
Answer: Choose the two primes p and q to be at least 100-digit numbers.

Why does that make RSA secure? Because no eavesdropper (not even the NSA or the FBI) is able to compute φ(n) from the publicly known modulus n since its factors p and q – required to compute φ(n) as φ(p*q) = (p-1) * (q-1) - can not be derived from n. As experienced computer experts, Rivest, Shamir and Adleman knew that the multiplication of two large numbers is not difficult, however, finding the factors of a given large integer is a difficult computer problem.

I.e. we easily find that

35 = 7 * 5	or
70 = 7 * 5 * 2	or
69 = 3 * 23	or
221 = 13 * 17	and using some trial and error even
11413 = 113 * 101	

A factoring program quickly finds the factors of 20-digits numbers such as

10726291417797115873 = 1223233789 * 8768799157

However, even today's best factoring programs can not find the factors of 196-digit numbers such as

1072629139784206448651876669948737985105534479415491719546499789238
6019530990999171954648916062355690020290206172841335185185805481481
63084320989148925926075485185203509876558141111112930000042837

Exercise2:
Realize that the multiplication of large numbers can easily be performed by a computer. Verify that the product of the following two 98-digit numbers

1223233789777777777888888888933333333344444444445555555556666666666
6777777777888888888900000000327

and

8768799135111111111122222222223333333333444444444455555555556666666
6677777777778888888890000000131

yields the above 196-digit number

Reflection on the Security of the RSA Cipher:
Consequently, if n is chosen sufficiently large nobody is able to find the factors p and q of n and thus nobody can compute $\varphi(n)$ in order to then identify the decoding key d. I will show you mathematically that the ability to find the factors of n is equivalent to the ability to compute $\varphi(n)$. The equivalence is based on the following two facts:

I) Knowing the factors p and q is sufficient to compute $\varphi(n)$ since $\varphi(n) = \varphi(p*q) = (p-1) * (q-1)$. I showed you already that if p=3 and q=5 then $\varphi(15) = \varphi(5)* \varphi(3) = 4 * 2 = 8$.

II) "Knowing $\varphi(n)$ and the publicly known value n is sufficient to find the factors p and q" can be seen as follows:
We know that $n = p*q$ and that $\varphi(n) = (p-1)*(q-1)$. How could Mr. X use the two identities to compute p and q? We know how to solve two equations with two variables if only we can set up two equations that allow us to eliminate either p or q. Here is how:

$$\begin{aligned}\varphi(n) &= (p-1)*(q-1)\\ &= (p*q - p - q + 1)\\ &= (p*q – [p + q] + 1)\\ &= (n – [p + q] + 1)\end{aligned}$$

Solving for p+q yields:

$$p+q = n - \varphi(n) +1 \qquad (2)$$

We managed to express p + q in terms of n and $\varphi(n)$. If additionally we manage to express the difference of the two primes, p – q, in terms of n and $\varphi(n)$ we can use those two equations to compute p and q. So, let's express p – q in terms of n and $\varphi(n)$.

$(p-q)^2 = (p-q) * (p-q) = p^2 – 2*p*q + q^2$.	
$(p+q)^2 = (p+q) * (p+q) = p^2 + 2*p*q + q^2$.	
$(p-q)^2 - (p+q)^2 = - 4*p*q$.	This equation stems from subtracting the two previous equation. We add $(p+q)^2$ on both sides.
$(p-q)^2 = (p+q)^2 - 4*p*q$	Taking the square root yields.
$p-q = [(p+q)^2 - 4*p*q]^{1/2}$	We are done since we can express (p+q) as $(n - \varphi(n) +1)$ replace and p*q as n

$p-q = (n - \varphi(n) +1)^2 - 4*n]^{1/2}$ (3)	Combining the equations (2) and (3) yields
$p+q = n - \varphi(n) +1$ $p -q = [(n - \varphi(n) +1)^2 - 4*n]^{1/2}$	p and q can be derived by solving a 2 by 2 system.

Discrete Logarithm Problem

Discrete logarithms are logarithms defined with regard to multiplicative cyclic groups. If G is a multiplicative cyclic group and g is a generator of G, then from the definition of cyclic groups, we know every element h in G can be written as g^x for some x.

The discrete logarithm to the base g of h in the group G is defined to be x . For example, if the group is Z_5^*, and the generator is 2, then the discrete logarithm of 1 is 4 because $2^4 \equiv 1$ mod 5.

The discrete logarithm problem is defined as: given a group G, a generator g of the group and an element h of G, to find the discrete logarithm to the base g of h in the group G. Discrete logarithm problem is not always hard.

The hardness of finding discrete logarithms depends on the groups. For example, a popular choice of groups for discrete logarithm based crypto-systems is Z_p^* where p is a prime number. However, if p 1 is a product of small primes, then the Pohlig–Hellman algorithm can solve the discrete logarithm problem in this group very efficiently. A safe prime is a prime number which equals 2q+1 where q is a large prime number. This guarantees that p-1 = 2q has a large prime factor so that the Pohlig–Hellman algorithm cannot solve the discrete logarithm problem easily. Even p is a safe prime, there is a sub-exponential algorithm which is called the index calculus. That means p must be very large (usually at least 1024-bit) to make the crypto-systems safe.

Euler's Totient Function and Euler's Theorem

The Euler's totient function, or phi (φ) function is a very important number theoretic function having a deep relationship to prime numbers and the so-called order of integers. The totient φ(n) of a positive integer n greater than 1 is defined to be the number of positive integers less than n that are coprime to n. φ(1) is defined to be 1. The following table shows the function values for the first several natural numbers:

n	φ(n)	numbers coprime to n

n	φ(n)	numbers coprime to n
1	1	1
2	1	1
3	2	1, 2
4	2	1,3
5	4	1,2,3,4
6	2	1,5
7	6	1,2,3,4,5,6
8	4	1,3,5,7
9	6	1,2,4,5,7,8
10	4	1,3,7,9
11	10	1,2,3,4,5,6,7,8,9,10
12	4	1,5,7,11
13	12	1,2,3,4,5,6,7,8,9,10,11,12
14	6	1,3,5,9,11,13
15	8	1,2,4,7,8,11,13,14

Can you find some relationships between n and φ(n)? One thing you may have noticed is that:

when n is a prime number (e.g. 2, 3, 5, 7, 11, 13), φ(n) = n-1.

But how about the composite numbers? You may also have noticed that, for example, 15 = 3*5 and φ(15) = φ(3)*φ(5) = 2*4 = 8. This is also true for 14,12,10 and 6. However, it does not hold for 4, 8, 9. For example, 9 = 3*3 , but φ(9) = 6 ≠ φ(3)*φ(3) = 2*2 =4. In fact, this multiplicative relationship is conditional:

when m and n are coprime, φ(m*n) = φ(m)*φ(n).

The general formula to compute φ(n) is the following:

If the prime factorisation of n is given by $n = p_1^{e_1} * ... * p_n^{e_n}$, then $\varphi(n) = n *(1 - 1/p_1)* ... (1 - 1/p_n)$.

For example:

- $9 = 3^2$, $\varphi(9) = 9* (1-1/3) = 6$
- $4 =2^2$, $\varphi(4) = 4* (1-1/2) = 2$
- $15 = 3*5$, $\varphi(15) = 15* (1-1/3)*(1-1/5) = 15*(2/3)*(4/5) =8$

Euler’s theorem generalises Fermat’s theorem to the case where the modulus is not prime. It says that:

if n is a positive integer and a, n are coprime, then $a^{\varphi(n)} \equiv 1 \bmod n$ where φ(n) is the Euler's totient function.

Let's see some examples:

- $165 = 15*11$, $\varphi(165) = \varphi(15)*\varphi(11) = 80$. $8^{80} \equiv 1 \bmod 165$
- $1716 = 11*12*13$, $\varphi(1716) = \varphi(11)*\varphi(12)*\varphi(13) = 480$. $7^{480} \equiv 1 \bmod 1716$
- $\varphi(13) = 12$, $9^{12} \equiv 1 \bmod 13$

We can see that Fermat's little theorem is a special case of Euler's Theorem: for any prime n, φ(n) = n-1 and any number a 0< a <n is coprime to n. From Euler's Theorem, we can easily get several useful corollaries. First:

if n is a positive integer and a, n are coprime, then $a^{\varphi(n)+1} \equiv a \bmod n$.

This is because $a^{\varphi(n)+1} = a^{\varphi(n)}*a$, $a^{\varphi(n)} \equiv 1 \bmod n$ and $a \equiv a \bmod n$, so $a^{\varphi(n)+1} \equiv a \bmod n$. From here, we can go even further:

if n is a positive integer and a, n are coprime, $b \equiv 1 \bmod \varphi(n)$, then $a^b \equiv a \bmod n$.

If $b \equiv 1 \bmod \varphi(n)$, then it can be written as $b = k*\varphi(n)+1$ for some k. Then $a^b = a^{k*\varphi(n)+1} = (a^{\varphi(n)})^k*a$. Since $a^{\varphi(n)} \equiv 1 \bmod n$, $(a^{\varphi(n)})^k \equiv 1^k \equiv 1 \bmod n$. Then $(a^{\varphi(n)})^k*a \equiv a \bmod n$. This is why RSA works.

Cyclic Groups and Generators

Some groups have an interesting property: all the elements in the group can be obtained by repeatedly applying the group operation to a particular group element. If a group has such a property, it is called a cyclic group and the particular group element is called a generator. A trivial example is the group Z_n, the additive group of integers modulo n. In Z_n, 1 is always a generator:

$1 \equiv 1 \bmod n$

$1+1 \equiv 2 \bmod n$

$1+1+1 \equiv 3 \bmod n$

...

$1+1+1+...+1 \equiv n \equiv 0 \bmod n$

If a group is cyclic, then there may exist multiple generators. For example, we know Z_5 is a cyclic group. The element 1 is a generator for sure. And if we take a look at 2, we can find:

$2 \equiv 2 \bmod 5$

$2+2 \equiv 4 \bmod 5$

$2+2+2 \equiv 6 \equiv 1 \bmod 5$

$2+2+2+2 \equiv 8 \equiv 3 \bmod 5$

$2+2+2+2+2 \equiv 10 \equiv 0 \bmod 5$

So all the group elements {0,1,2,3,4} in Z_5 can also be generated by 2. That is to say, 2 is also a generator for the group Z_5.

Not every element in a group is a generator. For example, the identity element in a group will never be a generator. For example, in Z_n, 0 is the identity element and $0+0+...+0 \equiv 0 \bmod n$ in all cases.

Not every group is cyclic. For example, Z_n^*, the multiplicative group modulo n, is cyclic if and only if n is 1 or 2 or 4 or p^k or $2*p^k$ for an odd prime number p and $k \geq 1$. So Z_5^* must be a cyclic group because 5 is a prime number. Actually all the elements in Z_5^*, {1,2,3,4} can be generated by 2:

$2^1 \equiv 2 \bmod 5$

$2^2 \equiv 4 \bmod 5$

$2^3 \equiv 8 \equiv 3 \bmod 5$

$2^4 \equiv 16 \equiv 1 \bmod 5$

And Z_{12}^* is not a cyclic group. The elements in Z_{12}^* are: {1,5,7,11}. Obviously the identity element 1 cannot be a generator. Let's check the other three elements:

$5^1 \equiv 5 \bmod 12$	$7^1 \equiv 7 \bmod 12$	$11^1 \equiv 11 \bmod 12$
$5^2 \equiv 25 \equiv 1 \bmod 12$	$7^2 \equiv 49 \equiv 1 \bmod 12$	$11^2 \equiv 121 \equiv 1 \bmod 12$

None of the elements can generate the whole group. Therefore, none of them is a generator. So Z_{12}^* is indeed not cyclic.

If Z_n^* is cyclic and g is a generator of Z_n^*, then g is also called a primitive root modulo n.

Data Integrity and Message Authentication

Integrity and protection security services are needed to protect against active attacks, such as falsification of data and transaction. Protection against such attacks is known as message authentication.

Def. Message Authentication – A message, file, document, or other collection of data is said to be authentic when it is genuine and came from its alleged source. Message authentication is a procedure that allows communicating parties to verify that received messages are authentic.

There are two approaches to message authentication:

A. Authentication with Conventional Encryption – If we assume that only the sender and receiver share a key, then only the genuine sender would be able to encrypt a message. Furthermore, if the message includes an error-detection code and a sequence number, the receiver is assumed that no alterations have been made and that sequencing is proper. If the message also includes a timestamp, the receiver is assumed that the message has not been delayed beyond that normally expected for network transit.

B. Message Authentication without Encryption – It is much cheaper and faster to broadcast in plaintext with an associated authentication tag. Another example would be on-line download of a computer program in plaintext, but in a way that assumes its authentication. In this case, if a message authentication tag were attached to the program, it could be checked whenever assurance is required of the integrity of the program. In all of these cases, an authentication tag is generated and appended to each message for transmission. The message itself is not encrypted and can be need at the destination independent of the authentication function.

Message Authentication Code (MAC)

One technique involves the use of a recent key to generate a small block of data, known as a message authentication code (MAC) that is appended to the message. In this technique, the two communicating parties, Alice and Bob, share a common recent key $K_{AB.}$ Alice calculates the MAC as a function of the message and the key:

$$MAC_M=f(K_{AB},M)$$

The message plus this MAC code are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same recent key, to generate a new MAC code. The received MAC code is compared to the calculated code. If they match, then

a) The receiver is assured that the message has not been altered.

b) The receiver is assured that the message is from the alleged sender.

c) if the message includes a sequence number, then the receiver can be assured of the proper sequence. This is shown in Figure

Note 1 – A number of algorithms could be used to generate the MAC code. The NIST, in its publication entitled DES Modes of Operation, recommends the use of Data Encryption Algorithms (DEA). This algorithms is used to generate an encrypted version of the message, and only the last number of lists of ciphertext are used as the MAC code. A 16-bit or 32-bit code is typical.

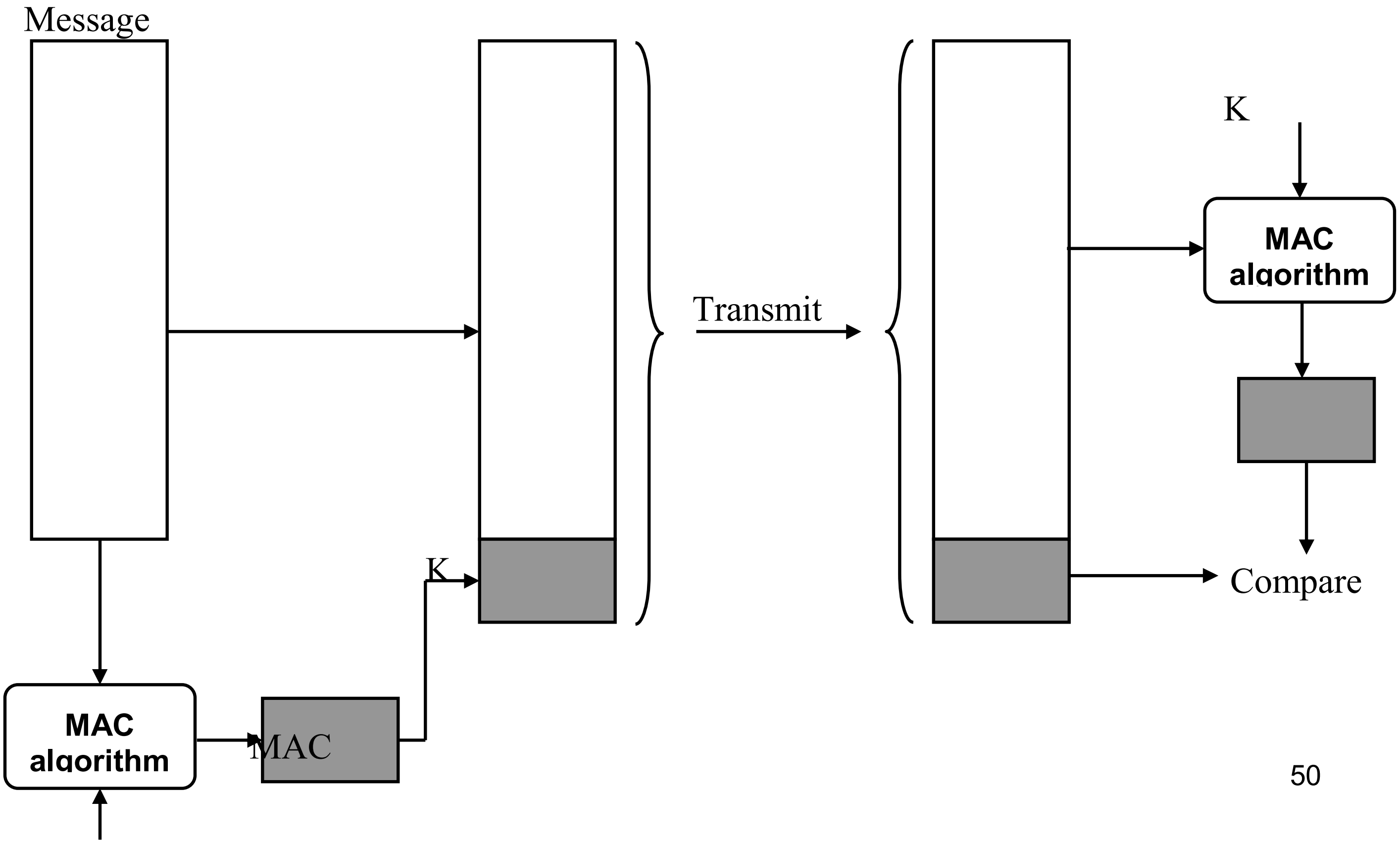
Note 2 – The process just described is similar to encryption. One difference is that the authentication algorithms need not be reversible, as it must for decryption.

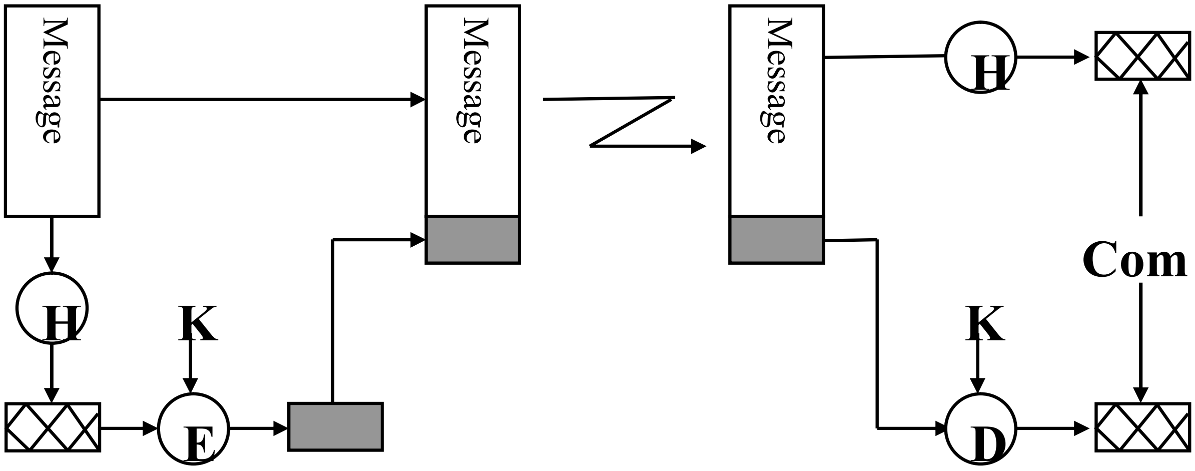
Note 3 – The message authentication code is also known as data authentication code (DAC).

One-Way Hash Function

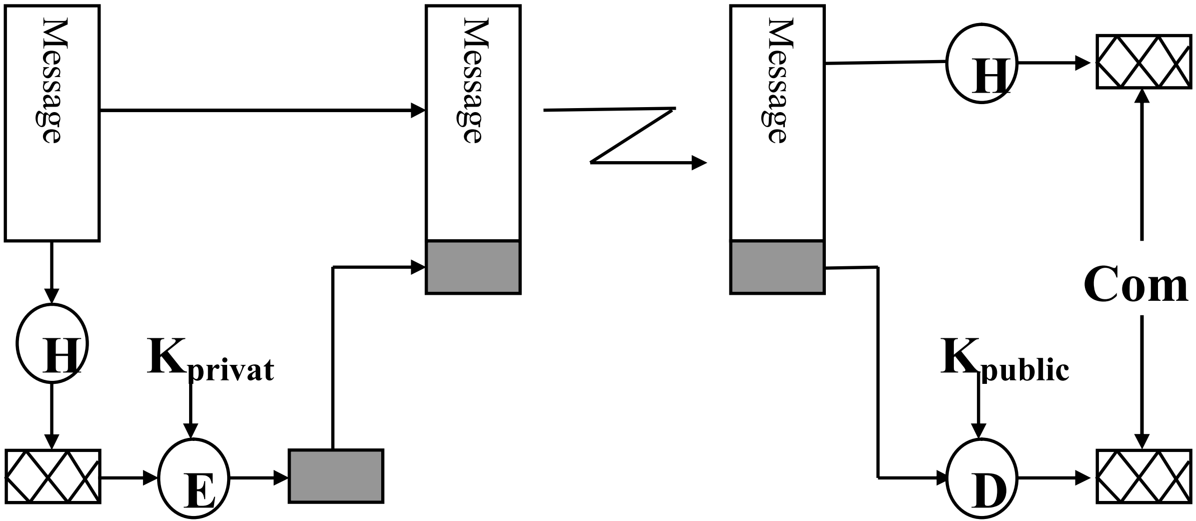
A variation on the MAC code is the one-way hash function. A one-way hash function has many names: compression function, contraction function, message digest, fingerprint, cryptographic checksum, message integrity check (MIC), and modification detection code (MDC). It is central to modern cryptography. As with the message authentication code, a hash function accepts a variable -size message M as input and produces a fixed-size message digest H(M) as output. Unlike the MAC, a hash function does not need a secret key as input. In other words, the one-way hash function is a non-key message digest. To authenticate the message, the message digest is sent with the message in such a way that the message digest is authentic.

Note 4 – A simple hash function would be a function that takes the input message and returns some bytes consisting of the XOR of all the input bytes.

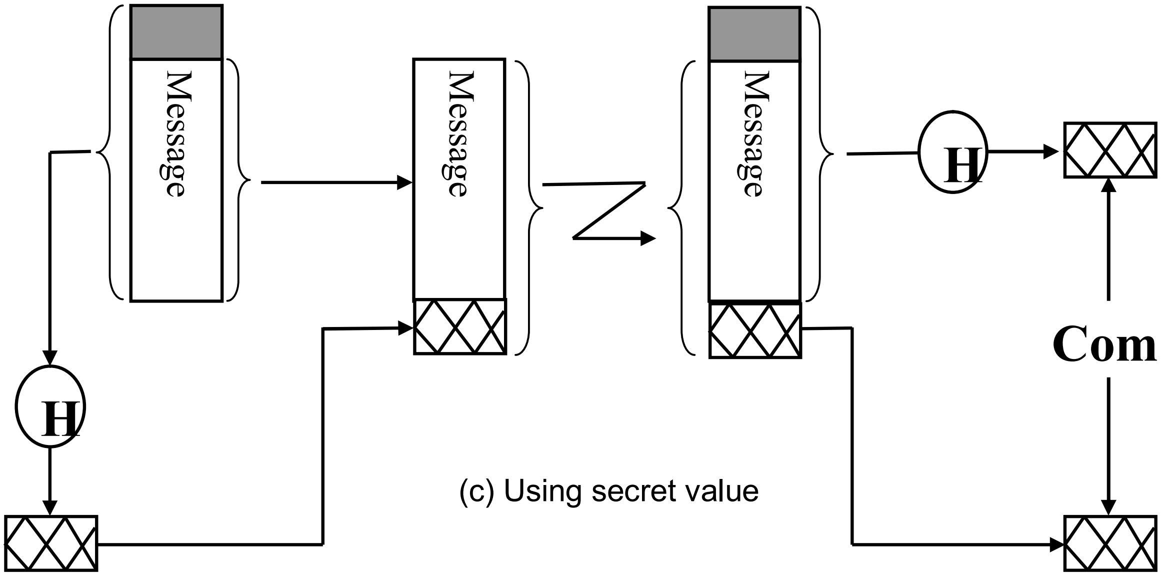




(a) Using conventional encryption



(b) Using conventional encryption



(c) Using secret value

Message Authentications Using a One-Way Function

(a) A message digest can be encrypted using conventional encryption.

(b) The message also can be encrypted using public-key encryption. This has two advantages:

(c) (1) it provides a digital signature (2) it does not require the distribution of keys to communicating parties.assumes that two communicating parties, Alice and Bob, share a common secret value S_{AB} When Alice has a message to send to Bob, she calculates the hash function over the concatenation of the secret value and the message as:

$$MD_M=H(S_{AB}||M)$$

Where || denotes concatenation. Alice then sends $[M||MD_M]$ to Bob. Because Bob possesses S_{AB}, he can recomputed $H(S_{AB}||M)$ and verify MD_M . Because the secret value itself is not sent, it is not possible for an opponent, Oscar, to modify an intercepted message. As long as the secret value S_{AB} remains secret, it is not possible for an opponent to generate a false message.

Note 5 – A variation of the above technique called HMAC, is adopted for IP security protocol. It is called a strong collision resistance property.

Def. – Hash Function – A hash family is a four-tuple (X, Y, K, H), where the following conditions are satisfied:

1) X is a set of possible messages.
2) Y is a finite set of possible message digests or authentication tags.
3) K, the key space, is a finite set of possible keys.
4) For each $k \in K$, there exists a hash function $h_k \in H$, such that for each $h_k: X \rightarrow Y$.

Note 6 – The hash function takes a variable-length input string, called a pre-image, and produces a fixed-length (generally smaller) output string, called a hash value.

Note 7 – To be useful for message authentication, a hash function H must have the following properties:

1) H can be applied to any size of data.

2) H must produce a fixed-length output.

3) H(x) should be relatively easy to compute for any given x, making both hardware and software implementation practical.

4) For any given code h, it should be computationally infeasible to find x such that H(x)=h. this is the “one-way” property.

5) For any given block x, it should be computationally infeasible to find $x \neq y$ with H(y)=H(x). This property is called a weak collision resistance.

6) It should be computationally infeasible to find any pair (x,y) such that H(x)=H(y).

Note 8 – The fourth property listed above is the “one-way” property. That is , it should be virtually impossible to generate a message given a hash value code.

Note 9 – A hash function that satisfies the first five properties in the preceding list is referred to as a weak hash function. If the sixth property is also satisfied, then it is referred to as a strong hash function. The sixth property protects against a sophisticated class of attack known as the birthday attach.

Note 10 – in addition to providing authentication, a message digest also provides data integrity. If performs the same function as a frame check sequence.

Key management

Key management is the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.

Key management concerns keys at the user level, either between users or systems. This is in contrast to key scheduling; key scheduling typically refers to the internal handling of key material within the operation of a cipher.

Successful key management is critical to the security of a cryptosystem. In practice it is arguably the most difficult aspect of cryptography because it involves system policy, user training, organizational and departmental interactions, and coordination between all of these elements.

Cryptographic systems may use different types of keys, with some systems using more than one. These may include symmetric keys or asymmetric keys. In a symmetric key algorithm, the keys involved are identical for both encrypting and decrypting a message. Keys must be chosen carefully, and distributed and stored securely. Asymmetric keys, in contrast, are two distinct keys that are mathematically linked. They are typically used in conjunction to communicate.

• given parties A and B have various key distribution alternatives:

1. A can select key and physically deliver to B

2. third party can select & deliver deliver key to A & B

3. if A & B have communicated previously can use previous key to encrypt a new key
4. if A & B have secure communications with a third party C, C can relay key between A & B

Symmetric schemes require both parties to¬ share a common secret key issue is how to securely distribute this key¬ whilst protecting it from others¬ frequent key changes can be desirable¬ often secure system failure due to a break in¬ the key distribution scheme

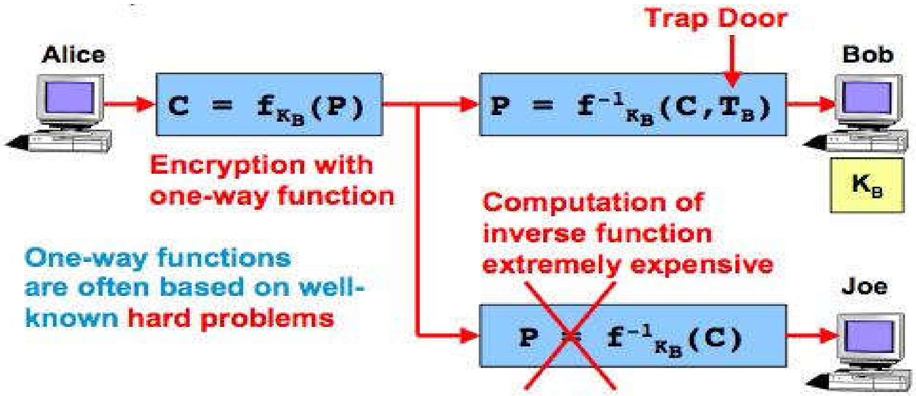
Key Hierarchy typically have a hierarchy of keys¬ session key¬ temporary key used for encryption of data between users for one logical session then discarded master key¬ used to encrypt session keys shared by user & key distribution center

Key Distribution Issues

• hierarchies of KDC's required for large networks, but must trust each other
• session key lifetimes should be limited for greater security
• use of automatic key distribution on behalf of users, but must trust system
• use of decentralized key distribution • controlling key usage

Essential Principles of Public-key Cryptography

Public key cryptographic systems are based on one-way functions which convert plain text into ciphertext using a small amount of computing power. Thus, it is not feasible for someone to decipher the plain text from the ciphertext in a reasonable amount of time.The term "trap door" is used to describe the fact that the intended user of the ciphertext is able to decipher the ciphertext easily since he/she holds the private key. Finally, public key cryptosystems are usually based on the discrete logarithms over a finite field (as in the case of the Diffie-Hellman key exchange).


Trap Door
Alice
Bob
$C = f_{K_B}(P)$
$P = f^{-1}_{K_B}(C, T_B)$
Encryption with one-way function
K_B
Computation of inverse function extremely expensive
One-way functions are often based on well-known hard problems
Joe
$P = f^{-1}_{K_B}(C)$

The Diffe-Hellman Key Exchange

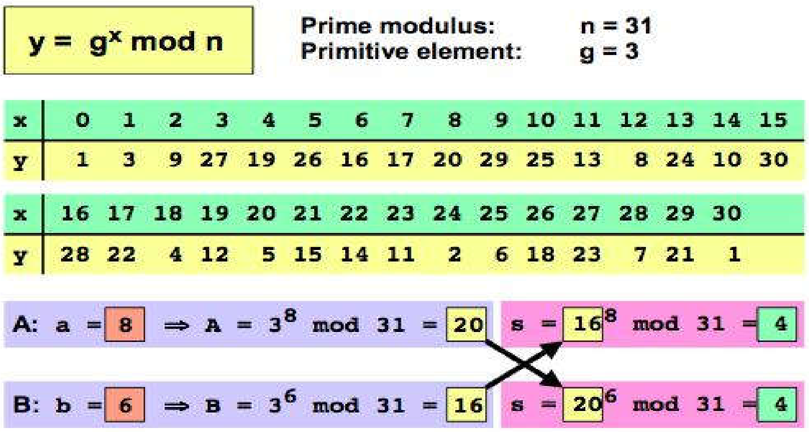
The Diffe-Hellman Key Exchange is one of the more popular and interesting methods of key distribution. It is a pubic-key cryptographic system whose sole purpose is for distributing keys. Diffe-Hellman is an example of a Public-Key Distribution Scheme (PKDS) whereby it is used to exchange a single piece of information, and where the value obtained is normally used as a session key for a private-key scheme.

How Diffe-Hellman Works

The Diffe-Hellman distribution scheme works as follows assuming two people, named Alice and Bob respectively, wish to exchange a key over an in-secure communication channel:

1. Both Alice and Bob agree on the selection of a large prime number *n*, a primitive element *g*, and the one-way function *f(x) = g% mod n* (Note: both *n* and *g* are made public).
2. Alice selects a large random integer *a* and sends Bob the value *A = g& mod n*.

   Bob selects a large random integer *b* and sends Alice the value *B = g' mod n*.
3. Alice computes *s = B& mod n* (= g*+ mod n). Similarly, Bob computes *s = A' mod n* (= g+* mod n).
4. Alice and Bob now both share the same secret key *s*. The computation of *x = f(¹(y)* is extremely hard; therefore, someone attempting to listen to the key-exchange cannot determine *s* even by knowing the values of *A*, *B*, *n*, and *g.*



$y = g^x \bmod n$

Prime modulus: n = 31
Primitive element: g = 3

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
y	1	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30

x	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
y	28	22	4	12	5	15	14	11	2	6	18	23	7	21	1

A: $a = \boxed{8} \Rightarrow A = 3^8 \bmod 31 = \boxed{20}$ $s = \boxed{16}^8 \bmod 31 = \boxed{4}$

B: $b = \boxed{6} \Rightarrow B = 3^6 \bmod 31 = \boxed{16}$ $s = \boxed{20}^6 \bmod 31 = \boxed{4}$

Diffie-Hellman Algorithm Example

The Diffe-Hellman key exchange is vulnerable to attacks whereby an intruder intercepts messages between the sender and receiver, and assumes the identity of the other party (often known as the *man in the middle attack*). Consequently, the Diffe-Hellman algorithm should be used with a form of authentication such as certificates to ensure that symmetric keys are estab-lished between legitimate parties.

Advantages and Disadvantages

- solving the discrete logarithm is very challenging, and that the shared key (i.e. the secret) is never itself transmitted over the channel

- Expensive exponential operations involved in the algorithm , and the algorithm cannot be used to encrypt messages - it can be used for establishing a secret key only.

- Lack of authentication.