## Tutorial-4

PAGENO.

						100000					
91	a) li	ven a	=84	and	b=320	fin	d gco	d (a, b)	and	vale	ie of
	5 an					, 0,		200 =	Libo	01013	D
$\rightarrow$	Q	A	В	R	51	52	6	ti	to	t	
	0	84	320	84	1	0	101	0	1	0	
	3	320	84"	68	0	1	-3	1	0	1	
	1	84	68	16	1	-34	4	0	1	-1	
	4	68	16	4	-3	45	-19	1	-1	5	
	4	16	4	0	4	-19"	80	-1	5	-21	
	-	4	0	-		804	-	5	-21	043	
		gid			+5			¥t.			
	gcd	84,3	20) = 4	. 5=	=-190,	t=5	.10	Mens	211-	breit	11.8
	0		races			111	Decre	(88) =	ctbo	and Sign	ton
	6) Give	m. a=	161 ar	nd b=	28 , fr	ind 9	cd (a.	b) and	d valu	u of	s and t
	8	a	ь	R	51	52	5	ti	t <sub>2</sub>	t	
	5	161	28	21	1	000	(10)	0	1	-5	1.11/9/19
	1	28	21		05	11	-1	01.4	-5"	6	
	3	21	74		1-	-1	4	-5	6	-23	
	-	174	0-	-	-1-	4	r	6	-23	C-13.	
		gcd			*		10000	¥	100		
	gcd(	161,2	8)=7	, 5=	-1,4	=6.	Lta	Hock	Contr	4 257	A
	U	1						MM		32400	
	c) ljiv	en a=	it an	d b=0	, fine	d go	1(0,6)	and	value	1 5	and t
	Q	a	b	RI	Sin	52	5	to	· + 2	t.	
1007	-00	1-17	DOT	the	1	O	Holy	0	1	5-4c :	
	784333	gcd		nois	3	ore	1 - 7	¥			
	gcd	(17,0)	= 17, 5	5=1,	£=0.	apesit	Con	1873		9	
	in mi	more S	17"	10/4	Phone		صامار	, Cale	L(X)	T	
	d) eyi	yen o	1=0 8	b=40	1.0	()	(a,b)	& Vo	alues	0 S	& t.
	0	a	b	R	5.	52	5	t	+2	t	gcd (0,45)
	10	10	45	0	1	0	113 3	0	1	0	75
		45t	TAV		04	16		15	05	(pus)	0011

2. Find the result of 610 mod 11 > 610 mod 11 = (62)5 mod 11  $= (36)^5 \mod 11$ = 35 mod 11. = (27)(9) mod 11 = (27 mod 11 x 9 mod 11) mod 11  $= 9(5x9) \mod 11$ = 45 mod 11 610 mod 11 = 1. 3. Find the result of 312 mod 112 > 312 mod 11 = (33)4 mod 11 = (27)4 mod 11 = (54) mod 11. = (25)(25) mod 11 = (25 mod 11 x 25 mod 11) mod 11 = 9mod 11 312 mod 11 = 9. 4. We know that 61 is a prime, let us see if it passes the Miller-Rabin test. > Miller-Rabin test - by 5-1) Find m and k such that n-1=mx2k 5-2) If K & 1, Calculate T such that T= am modn Ff T= ±1, no. is prime Else composite - 10 11 10 11 10 If kys, calculate T'such that T'= T2 madn, T=ammodmy and a de o mo If T'=1, no is composite prime Else Composite 603) choose a such that 1 kg < n-1.

```
n-1 = mx2k
     60 = 15 \times 2^2
    let a=2, T=am mod n.
         n=61, m=15 hand(3)(22)(23)(2)
         => T = 215 mod 61
        T=(26x26x23) mod 61
              = (64)(64)(8) mod 61
              =((642mod61)(8mod61))mod61
            = (9x8) mod 61 9 x 101 barre 11) 5
             = 72 mod 61 lollhouse (0) 4 (1) =
         => T=11.
       T'= T2 mnd 61
          = 112 mod 61 Dea morkwaspa and water worth
          = (122-1)mod 61
       T'=-1. => n=61 is a prime number
5. a) Show that inverse of 5 mod 101 is 599
   5-mod 101
    ap-1 = 1 mod p. 101 bom (18x18)=
    at mod p. = ap-2 mod p las borrelles (us-)
              = 5101-2 mod 2101000 x (a) bame(1-) =
     5-1 mod 101 = 599 mod 101 101 borne (MIXOO) =
  b) Use repeated squaring to simplify 599 mod los
> 51 mod 191=5
  52 mod 101=25
  54 mod 101 = 625 mod 101 = 19
  58 mod 101 = (54)2 mod 101 = 192 mod 101 = 58
  56 mod 101 = (58)2 mod 101 = 582 mod 101 = (116) (29) mod 101 = 31
  532 mod 101 = (31)2 mod 101 = 52
  564 mod 101 = 522 mod 101 = 492 mod 101 = (343) (7) mod 101 = 78.
```

	V STORY CONTROLL OF
	99 in binary = 1100011
	-99 164 c32 c2 c mpd 101
	= (78)(52)(25)(5) mod 101
	(00 - \( ( ) 000 bd \( ( ) \)
	= (2ahamad lal x 260 mod lal
	- 11.1x 6/2) x 5) mod 101
	= (111)(215) mod (01
	= (14 mod 101 x 215 mod 101) mod 101
	= (14x13) mod 101 ( ) barre
	599 mod 101 = 81.
	La bacce T a'T
	c) Hence solve the equation 5x=31 mod 101
>	5x=31 mod tol (2 barre(2-221) =
	5-1 x 5 x = 5-1 x 31 mod 101
	x = (5-1 mod 101 x 31 mod 101) mod 101
	= (599 mod 101 x 31 mod 101) mod (101)
	(From Fermat's little theorem)
	= (81 x 31) mod 101
	= (-20)(31) mod 101 g bom 5 9 = g bom
	oc = ((-1) mod 101 x 620 mod 101) mod 101
	= (100×14) mod 101 las borne Pez = 101 borne 1-2
	= 1400 mod 101
	1 90 = 87. Hillands at promote belonging sell (s
	S=181 poor 2
	52 mod 161=25
	RISIOI borro 302 stat barro #2
	58 med at a Calemodia 19 modia 101 5 98
-	101 baper (85) (341) = 101 barref88 = 101 barre \$(83) = 101 barre