Tutorial 4

Q1 Find gcd (a,b) & values of s & t.

a) $a = 84$
$b = 320$

b) $a = 161$ $\quad b = 28$

c) $a = 17$ $\quad b = 0$

d) $a = 0$ $\quad b = 45$

Q2) Find $6^{10} \bmod 11$.

Q3) Find $3^{12} \bmod 11$.

Q4) We know that 61 is a prime. Let's see if it passes the Miller-Rabin test.

Q5) a) Show that the inverse of 5 modulo 101 is 5^{99}.

b) Use repeated squaring to simplify $5^{99} \pmod{101}$.

c) Hence, solve the equation $5x \equiv 31 \pmod{101}$

1) a) $a = 84$ $\qquad b = 320$ $\qquad (s \times a + t \times b = \gcd(a,b))$

q	$r_1 = a$	$r_2 = b$	r	$s_1 = 1$	$s_2 = 0$	s	$t_1 = 0$	$t_2 = 1$	t
0	84	320	84	1	0	1	0	1	0
3	320	84	68	0	1	-3	1	0	1
1	84	68	16	1	-3	4	0	1	-1
4	68	16	4	-3	4	-19	1	-1	5
4	16	4	0	4	-19	80	-1	5	-21
	4	0		-19	80		5	-21	

$\gcd(a,b) = 4$

$s = -19$ $\qquad t = 5$

b) $a = 161$ $b = 28$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

$gcd(a, b) = 7$
$s = -1$
$t = 6$

d) $a = 0$ $b = 45$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	0	45	0	1	0	1	0	1	0
	45	0		0	1		1	0	

$gcd(a, b) = 45$
$s = 0$
$t = 1$

8) $6^{10} \bmod 11$
$= (36)^5 \bmod 11$
$= 3^5 \bmod 11$
$= 243 \bmod 11$
$= 1$

3) $3^{12} \bmod 11$

$= (81)^3 \bmod 11$

$= 4^3 \bmod 11$

$= 64 \bmod 11$

$= 9$

1) c) $a = 17$ $b = 0$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	17	0		1	0		0	1	

$\gcd(a, b) = 17$

$s = 1$

$t = 0$

4) Miller-Rabin test for 61

$n = 61$

$61 - 1 = 60$

$= 2^2 \times 15$

$n - 1 = a^k \times m$

$k = 2$

$m = 15$

$b_0 = a^m \bmod n$

$= 2^{15} \bmod 61$

$= 2 \bmod 61 \times (2^7)^2 \bmod 61$

$= 2 \times (128 \bmod 61)^2 \bmod 61$

$= 2 \times 6^2 \bmod 61$

$= 72 \bmod 61$

$= 11 \neq 1$

$b_1 = b_0^2 \bmod n$

$= 121 \bmod 61$

$= 60$

$= -1 \bmod 61$

$\therefore$ 61 is a prime

~~5) (a)~~ $\cancel{(5 \bmod 101)^{-1}}$

$\cancel{5^{99} \bmod 101}$

$\cancel{\equiv (125)^{33} \bmod 101}$

$\cancel{\equiv (14)^{33} \bmod 101}$

$\cancel{\equiv (2744)^{11} \bmod 101}$

$\cancel{\equiv 5^{3} \times 5^{96} \bmod 101}$

$\cancel{= 24 \times}$

5) (a) $5^{-1} \bmod 101$

$$a^{-1} \bmod p = a^{p-2} \bmod p$$
$$= 5^{101-2} \bmod 101$$
$$= 5^{99} \bmod 101$$

$\therefore$ 5^{99} is inverse ~~—~~ of $5^{1} \bmod 101$

(b) $5^{99} \bmod 101$

$\Rightarrow$ $5^{2} \equiv 25$

$5^{4} \equiv 19$

$5^{8} \equiv 19^{2} \equiv 58$

$5^{16} \equiv 58^{2} \equiv 31$

$5^{32} \equiv 31^{2} \equiv 52$

$5^{64} \equiv 52^{2} \equiv 78$

$$5^{99} \equiv 5^{64+32+2+1}$$
$$\equiv 78 \times 52 \times 25 \times 5$$
$$\equiv 81 \bmod 101$$

Page :
Date : / /

(c) $5x \equiv 31 \pmod{101}$

$x \equiv 5^{-1} \cdot 31$
$\equiv 81 \cdot 31$
$\equiv 87 \bmod 101$

Tutorial 5

Q1 Use a hill cipher to encipher the message "we live in an insecure world". Use the following key

$$K = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$$

messages = [we, li, ve, in, an, in, se, cu, re, wo, rl, dz] = [22, 4; 11, 8; 21, 4; 8, 13; 0, 13; 8, 13; 18, 4; 2, 20; 17, 4; 22, 14; 17, 11; 4, 25]

message	vector
we	22, 4
li	11, 8
ve	21, 4
in	8, 13
an	0, 13
in	8, 13
se	18, 4
cu	2, 20
re	17, 4
wo	22, 14
rl	17, 11
dz	4, 25

cipher = K x message, vector

= [74, 138
49, 111
71, 133
50, 131
26, 91
50, 131
62, 118
46, 150
59, 113
94, 208
63, 162
62, 195]

mod 26

Page :
Date : / /

$$\equiv \begin{bmatrix} 22, & 8 \\ 23, & 7 \\ 19, & 3 \\ 24, & 1 \\ 0, & 13 \\ 24, & 1 \\ 10, & 14 \\ 20, & 20 \\ 7, & 9 \\ 16, & 0 \\ 11, & 6 \\ 10, & 13 \end{bmatrix} = \begin{bmatrix} w & i \\ x & h \\ t & d \\ y & b \\ a & n \\ y & b \\ k & o \\ u & u \\ h & j \\ q & a \\ l & g \\ k & n \end{bmatrix}$$

$\Rightarrow$ cipher = wixhtdybanybkouuhjqalgkn

Q2 The plaintext "letusmeetnow" and the corresponding ciphertext "HBCDFNOPIKLB" are given. You know that the algorithm is a Hill cipher, but you don't know the size of the key. Find the key matrix.

$P = [11, 4, 19, 20, 18, 12, 18, 22, 14, 22, 23]$
$C = [7, 1, 2, 3, 5, 13, 15, 10, 8, 11, 1]$

Key matrix, $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$\therefore \quad C = K \times P \bmod 26$