RSA algorithm

One by 3 men Rivest shamir Adleman

1) Modulus

select 2 random no.

$p = 11$

$q = 5$

RSA modulus $n = 11 \times 5$

$= 55$

2) Totient

$\phi(n) = (p-1)(q-1)$

$= 40$

e → public key $1 < e < \phi n$.

e must be smaller than $(\phi(n))$ & coprime ($\gcd(e, \phi(n)) = 1$)

3, 7, 9, 11, 13, 17

d → private key $d = e^{-1} \bmod (\phi(n))$

$e * d \bmod \phi(n) = 1$.

Euclidean algorithm

$7 * d \bmod 40 = 1$.

$r1 = q(r2) + r$

$40 = 5(7) + 2$

$7 = 1(5) + 2$

$5 = 2(2) + 1$

$2 = 2(1) + 0$ [stop before zero remainder step]

q	r1	r2	r
	40	7	5
5	7	5	2
1	5	2	1
2	2	1	0
2	1	0	
	1	0	

Q. No.

Back substitution $r = r_1 - q(r_2)$

$1 = 5 - 2(2)$

$1 = 5 - 2(7 - 5)$

$= 5 - 2(7) + 2(5)$

$1 = 3(5) - 2(7)$

$1 = 3(40 - 5(7)) - 2(7)$

$= 3(40) - 15(7) - 2(7)$

$= 3(40) - 17(7)$

$e = 7$

$d = -17$

$d = -ve$ so, $40 - 17 = \underline{23}$

Public key (e, n)

private key (d, n)

Or

find $e^{-1} \bmod (\phi(n))$

$e^{-1} \Rightarrow$

q	r_1	r_2	r	t_1	t_2	t
	40	7	5	0	1	-5
5	7	5	2	1	-5	+6
1	5	2	1	-5	6	-17
2	2	1	0	6	-17	40
2	1	0		-17	40	

$-ve$ so e^{-1} $40 - 17 = 23$

$d = 23 \bmod 40$

$= \underline{23}$

Example 2

p = 7 q = 11

n = p × q = 77

3) $\phi(n) = 6 \times 10 = 60$

$60 = 30 \times 2$
$= 15 \times 2 \times 2$
$= 3 \times 5 \times 2 \times 2$

4) $e \rightarrow$ 1 < e < $\phi(n)$; gcd($\phi(n)$, e) = 1

e = 13

5) $ed \bmod \phi(n) = 1$

$d = e^{-1} \bmod (\phi(n))$ [can't use fermat theorem as 60 is not prime]

$e^{-1} \rightarrow$

q	r_1	r_2	r	t_1	t_2	t
4	60	13	8	0	1	-4
1	13	8	5	1	-4	5
1	8	5	3	-4	5	-9
1	5	3	2	5	-9	14
1	3	2	1	-9	14	-23
2	2	1	0	14	-23	60
	1	0		-23	60	

-ve no; 60 − 23 = 37

d = 37 mod 60 = 37

$c = m^e \bmod n$

$= 5^{13} \bmod n. = 5^{13} \bmod 77 = 26$

$p = c^d \bmod n$

$= 26^{37} \bmod n = (26^3 \times 26^4 \times 26^5 \times 26^5 \times 26^5 \times 26^7 \times 26^3 \times 26^5) \bmod 77$

$= (20 \times 58 \times 20 \times 5 \times 20 \times 5 \times 45 \times 45) \bmod 77$

5

Q. No.

HIDE encryption

$c = m^e \bmod n$

H	I	D	E
|	|	|	|
7	8	3	4

$7^7 \bmod 55 = 28$

$8^7 \bmod 55 = 2$

$3^7 \bmod 55 = 42$

$4^7 \bmod 55 = 4^3 \times 4^4 \pmod{55}$

$= (9 \times 36) \bmod 55$

$= \underline{\underline{49}}$

Decryption $\rightarrow c^d \bmod n = m$

$28 \rightarrow 28^{23} \bmod 55 = (28^3 \times 28^5 \times 28^5 \times 28^{5}) \bmod 55$

$= (7 \times 43 \times 43 \times 43 \times 43) \bmod 55$

$= \underline{\underline{7}} \rightarrow H$

$2 \rightarrow 2^{23} \bmod 55$

$= 8 \rightarrow I$

$42 \rightarrow 42^{23} \bmod 55$

$= 3$

$49 \rightarrow 49^{23} \bmod 55$

$= 4$

Method 2

$60 = (13)4 + 8$

$13 = (8)1 + 5$

$8 = (5)1 + 3$

$5 = (3)1 + 2$

$3 = (2)1 + 1$

$1 = 3 - 2$

$= 3 - [5 - 3]$

$= 3 - 5 + 3$

$= 2(3) - 5$

$= 2(8 - 5) - 5$

$= 2(8) - 2(5) - 5$

$= 2(8) - 3(5)$

$= 2(8) - 3(13 - 8)$

$= 5(8) - 3(13)$

$= 5(60 - 4(13)) - 3(13)$

$= 5(60) - 20(13) - 3(13)$

$= 5(60) - 23(13)$

$= 60 - 23(13)$

Inverse $= 60 - 23$

$= 37$

Method 2

To find $d = \frac{k(\phi(n))+1}{e}$

Replace k by 1, 2 . . . . .
until the remainder is 0
Then the corresponding quotient is Ans

Example $e = 7, \phi(n) = 40$

$d = \frac{1(40)+1}{7} = 5.8$ X

$\frac{2(40)+1}{7} = 11.5$ X

$\frac{3(40)+1}{7} = 17.2$ X

$\frac{4(40)+1}{7} = 23 \rightarrow d$

Example 2 $e = 13$ $\phi(n) = 60$

$d = \frac{k(\phi(n))+1}{e}$

$k = 1 \rightarrow 4.6$ X
$k = 2 \rightarrow 9.3$ X
$k = 3 \rightarrow 13.9$ X
$k = 4 \rightarrow 18.5$ X
$k = 5 \rightarrow 23.1$ X
$k = 6 \rightarrow 27.7$ X
$k = 7 \rightarrow 32.3$ X
$k = 8$ (37) ✓

↓ d.