CONTOH SOAL LATIHAN ALGORITMA RSA

1. Diketahui :

   Misal Ali akan mengirim pesan HOME (48 4F 4D 45) dengan p = 11, q = 13, dan kunci umum e = 19

   Lakukan enkripsi menggunakan algoritma RSA

   Jawab

   p = 11

   q = 13

   n = p*q = 143

   Φ(n) = (p-1)*(q-1) = (11-1)(13-1) = 120

   Kunci umum e = 19

   maka kunci khusus nya adalah:

   d = (1+k*120) /19 ; k=1,2,3, ... (cari d dengan hasil yg bulat dengan mencoba nilai-nilai k

   = 19

k=1	→ d	=	121/19	=	6.37	tidak bulat
k=2	d	=	241/19	=	12.37	tidak bulat
k=3	d	=	361/19	=	19	bulat

   Jadi kunci umum = (19,120)

   kunci khusus = (19,120)

Enkripsi

Plainteks	H	O	M	E
Hexa	48	4F	4D	45

Ubah ke kode desimal

										Desimal				
H	48	0	1	0	0	1	0	0	0	2^6+2^3	=	72	=	64+8
O	4F	0	1	0	0	1	1	1	1	$2^6+2^3+2^2+2^1+2^0$	=	79	=	64+8+4+2+1
M	4D	0	1	0	0	1	1	0	1	$2^6+2^3+2^2+2^0$	=	77	=	64+8+4+1
E	45	0	1	0	0	0	1	0	1	$2^6+2^2+2^0$	=	69	=	64+4+1

__Enkripsi__

$C = P^e \bmod n$ →

	Des		Cipher		Des
H	72	→	72^{19} mod 120	=	48
O	79	→	79^{19} mod 120	=	79
M	77	→	77^{19} mod 120	=	53
E	69	→	69^{19} mod 120	=	69

__Mengubah nilai desimal ke Hexa__

48

	48	
2	24	0
2	12	0
2	6	0
2	3	0
2	1	1
2	0	1

48 = 110000 atau 00110000

= 30

79

	79	
2	39	1
2	19	1
2	9	1
2	4	1
2	2	0
2	1	0
2	0	1

79=1001111 atau 01001111

= 4 f

53

	53	
2	26	1
2	13	0
2	6	1
2	3	0
2	1	1
2	0	1

53=110101 atau 00110101

69

	69	
2	34	1
2	17	0
2	8	1
2	4	0
2	2	0
2	1	0
2	0	1

69=1000101 atau 01000101

Cara menghitung bilangan pangkat

1. Ubah 19 ke sistem bilangan 2

	19				2^4	2^3	2^2	2^1	2^0
2	9	1	19 =		1	0	0	1	1
2	4	1		=	16	0	0	2	1
2	2	0		=	16+2+1				
2	1	0							
2	0	1							

2. Hitung bil pangkat

72^1 mod 120	=	72 mod 120				
72^2 mod 120	=	72^2 mod 120	=	5184 mod 120	=	24 mod 1
72^4 mod 120	=	24^2 mod 120	=	576 mod 120	=	96 mod 1
72^8 mod 120	=	96^2 mod 120	=	9216 mod 120	=	96 mod 1
72^{16} mod 120	=	96^2 mod 120	=	9216 mod 120	=	96 mod 1
79^1 mod 120	=	79 mod 120				
79^2 mod 120	=	79^2 mod 120	=	6241 mod 120	=	1 mod 12
79^4 mod 120	=	1^2 mod 120	=	1 mod 120	=	1 mod 12
79^8 mod 120	=	1^2 mod 120	=	1 mod 120	=	1 mod 12
79^{16} mod 120	=	1^2 mod 120	=	1 mod 120	=	1 mod 12
77^1 mod 120	=	77 mod 120				
77^2 mod 120	=	77^2 mod 120	=	5929 mod 120	=	49 mod 1
77^4 mod 120	=	49^2 mod 120	=	2401 mod 120	=	1 mod 12
77^8 mod 120	=	1^2 mod 120	=	1 mod 120	=	1 mod 12
77^{16} mod 120	=	1^2 mod 120	=	1 mod 120	=	1 mod 12
69^1 mod 120	=	69 mod 120				
69^2 mod 120	=	69^2 mod 120	=	4761 mod 120	=	81 mod 1
69^4 mod 120	=	81^2 mod 120	=	6561 mod 120	=	81 mod 1
69^8 mod 120	=	81^2 mod 120	=	6561 mod 120	=	81 mod 1
69^{16} mod 120	=	81^2 mod 120	=	6561 mod 120	=	81 mod 1

Jadi cipherteks nya

Des	Biner	Hexa	Chr

Plainteks **H O M E** **Cipherteks** **0 O 5 E**

48	0	0	1	1	0	0	0	0	30	0
79	0	1	0	0	1	1	1	1	4f	O
53	0	0	1	1	0	1	0	1	35	5
69	0	1	0	0	0	1	0	1	45	E

Hexa	**48**	**4F**	**4D**	**45**	
Des	**72**	**79**	**77**	**69**	

Hexa	**30**	**4F**	**35**	**45**	
Des	**48**	**79**	**53**	**69**	

Dekripsi

$P = C^d \bmod n$

Hex	Des			Des
30 →	48 →	$48^{19} \bmod 120$	=	**72**
4f →	79 →	$79^{19} \bmod 120$	=	**79**
35 →	53 →	$53^{19} \bmod 120$	=	**77**
45 →	69 →	$69^{19} \bmod 120$	=	**69**

$48^1 \bmod 120$	=	$48 \bmod 120$					
$48^2 \bmod 120$	=	$48^2 \bmod 120$	=	$2304 \bmod 120$	=	$24 \bmod 120$	
$48^4 \bmod 120$	=	$24^2 \bmod 120$	=	$576 \bmod 120$	=	$96 \bmod 120$	
$48^8 \bmod 120$	=	$96^2 \bmod 120$	=	$9216 \bmod 120$	=	$96 \bmod 120$	
$48^{16} \bmod 120$	=	$96^2 \bmod 120$	=	$9216 \bmod 120$	=	$96 \bmod 120$	
$79^1 \bmod 120$	=	$79 \bmod 120$					
$79^2 \bmod 120$	=	$79^2 \bmod 120$	=	$6241 \bmod 120$	=	$1 \bmod 120$	
$79^4 \bmod 120$	=	$1^2 \bmod 120$	=	$1 \bmod 120$	=	$1 \bmod 120$	
$79^8 \bmod 120$	=	$1^2 \bmod 120$	=	$1 \bmod 120$	=	$1 \bmod 120$	
$79^{16} \bmod 120$	=	$1^2 \bmod 120$	=	$1 \bmod 120$	=	$1 \bmod 120$	
$53^1 \bmod 120$	=	$53 \bmod 120$					
$53^2 \bmod 120$	=	$53^2 \bmod 120$	=	$2809 \bmod 120$	=	$49 \bmod 120$	
$53^4 \bmod 120$	=	$49^2 \bmod 120$	=	$2401 \bmod 120$	=	$1 \bmod 120$	
$53^8 \bmod 120$	=	$1^2 \bmod 120$	=	$1 \bmod 120$	=	$1 \bmod 120$	
$53^{16} \bmod 120$	=	$1^2 \bmod 120$	=	$1 \bmod 120$	=	$1 \bmod 120$	
$69^1 \bmod 120$	=	$69 \bmod 120$					
$69^2 \bmod 120$	=	$69^2 \bmod 120$	=	$4761 \bmod 120$	=	$81 \bmod 120$	
$69^4 \bmod 120$	=	$81^2 \bmod 120$	=	$6561 \bmod 120$	=	$81 \bmod 120$	
$69^8 \bmod 120$	=	$81^2 \bmod 120$	=	$6561 \bmod 120$	=	$81 \bmod 120$	
$69^{16} \bmod 120$	=	$81^2 \bmod 120$	=	$6561 \bmod 120$	=	$81 \bmod 120$	

mod 120

$72^{19} \bmod 120 = 72^{16+2+1}$

$= 72^{16} * 72^{2} * 72^{1} \bmod 120$

$= 96 * 24 * 72 \bmod 120$

$= 165888 \bmod 120$

$= 48$

$79^{19} \bmod 120 = 79^{16+2+1}$

$= 79^{16} * 79^{2} * 79^{1} \bmod 120$

$= 1 * 1 * 79 \bmod 120$

$= 79 \bmod 120$

$= 79$

$77^{19} \bmod 120 = 77^{16+2+1}$

$= 77^{16} * 77^{2} * 77^{1} \bmod 120$

$= 1 * 49 * 77 \bmod 120$

$= 3773 \bmod 120$

$= 53$

$69^{19} \bmod 120 = 69^{16+2+1}$

$= 69^{16} * 69^{2} * 69^{1} \bmod 120$

$= 81 * 81 * 69 \bmod 120$

$= 452709 \bmod 120$

$= 69$

$48^{19} \bmod 120 = 48^{16+2+1}$

$= 48^{16} * 48^{2} * 48^{1} \bmod 120$

$= 96 * 24 * 48 \bmod 120$

$= 10616832 \bmod 120$

$= 72$

$79^{19} \bmod 120 = 79^{16+2+1}$

$= 79^{16} * 79^{2} * 79^{1} \bmod 120$

$= 1 * 1 * 79 \bmod 120$

$= 79 \bmod 120$

$= 79$

$53^{19} \bmod 120 = 53^{16+2+1}$

$= 53^{16} * 53^{2} * 53^{1} \bmod 120$

$= 1 * 49 * 53 \bmod 120$

$= 2597 \bmod 120$

$= 77$

$69^{19} \bmod 120 = 69^{16+2+1}$

$= 69^{16} * 69^{2} * 69^{1} \bmod 120$

$= 81 * 81 * 69 \bmod 120$

$= 452709 \bmod 120$

$= 69$