P	37
G	3
X	2
Y [1]	9
K	15

KRIPTOGRAFI

10 17 8 15 19 14 6 17 0 5 8

ENKRIPSI

M	10	17	8	15	19	14	6	17	0	5	8
C1 [2]	11	11	11	11	11	11	11	11	11	11	11
C2 [3]	**26**	**22**	**6**	**2**	**5**	**29**	**23**	**22**	**0**	**13**	**6**

DEKRIPSI

C1X	10

GCD

37	=	10	*	**3**	+	7
10	=	7	*	**1**	+	3
7	=	3	*	**2**	+	1
3	=	**1**	*	3	+	0

t(0)	=	0		
t(1)	=	1		
t(2)	=	34		
t(3)	=	4		
t(4)	=	26	=	C1x^-1

M [4]	**10**	**17**	**8**	**15**	**19**	**14**	**6**	**17**	**0**	**5**	**8**
PT	**K**	**R**	**I**	**P**	**T**	**O**	**G**	**R**	**A**	**F**	**I**

[1] $Y = g^x \bmod p$

[2] $C1 = g^k \bmod p$

[3] $C2 = M*(y^k) \bmod p$

[4] $M = C2*(C1x)^{-1} \bmod p$