TUGAS 1

PRAKTIKUM KRIPTOGRAFI

Laura Azra Aprilyanti 140810200036

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PADJADJARAN

2022

Affine Cipher

Enkripsikan dan kembalikan menjadi plain teks kalimat “aku cakep bangets” menggunakan Affine Cipher dengan nilai a=17 b=5

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**

Enkripsi ⇒ (ax+b)mod 26

a	k	u		c	a	k	e	p		b	a	n	g	e	t	s
0	10	20		2	0	10	4	15		1	0	13	6	4	19	18

E(0) = (17(0) + 5) mod 26 = 5 mod 26 = 5 → f

E(10) = (17(10) + 5) mod 26= 175 mod 26 = 19 → t

E(20) = (17(20) + 5) mod 26= 5 mod 26 = 7 → h

E(2) = (17(2) + 5) mod 26 = 39 mod 26 = 13 → n

E(0) = (17(0) + 5) mod 26 = 5 mod 26 = 5 → f

E(10) = (17(10) + 5) mod 26= 175 mod 26 = 19 → t

E(4) = (17(4) + 5) mod 26 = 73 mod 26 = 21 → v

E(15) = (17(15) + 5) mod 26= 260 mod 26 = 0 → a

E(1) = (17(1) + 5) mod 26 = 22 mod 26 = 22 → w

E(0) = (17(0) + 5) mod 26 = 5 mod 26 = 5 → f

E(13) = (17(13) + 5) mod 26= 226 mod 26 = 18 → s

E(6) = (17(6) + 5) mod 26 = 107 mod 26 = 3 → d

E(4) = (17(4) + 5) mod 26 = 73 mod 26 = 21 → v

E(19) = (17(19) + 5) mod 26= 328 mod 26 = 16 → q

E(18) = (17(18) + 5) mod 26= 311 mod 26 = 25 → z

Aku cakep bangets ⇒ ftc nftva wfsdvqz

Deskripsi ⇒ a^-1 (y - b) mod 26

f	t	c		n	f	t	v	a		w	f	s	d	v	q	z
5	19	2		13	5	19	21	0		22	5	18	3	21	16	25

Cari a^-1 ⇒ a^-1 ⇒ a * x mod 26 = 1 mod 26

GCD (17, 26)	
26	= 17 * **1** + 9
17	= 9 * **1** + 8
9	= 8 * **1** + 1
1	= 1 * **1** + 0

t0 = 0, t1 = 1			
t2	= (t0 - (q1 * t1)) mod 26	= (0 - (1 * 1)) mod 26	= 25
t3	= (t1 - (q2 * t2)) mod 26	= (1 - (1 * 25)) mod 26	= 2
t4	= (t2 - (q2 * t2)) mod 26	= (25 - (1 * 2)) mod 26	= 23
	a^-1	=23	

D(5) = 23(5 - 5) mod 26 = 0 mod 26 = 0 → a

D(19) = 23(19 - 5) mod 26 = 322 mod 26 = 10 → k

D(2) = 23(7 - 5) mod 26 = -69 mod 26 = 20 → u

D(13) = 23(13 - 5) mod 26 = 8 mod 26 = 2 → c

D(5) = 23(5 - 5) mod 26 = 0 mod 26 = 0 → a

D(19) = 23(19 - 5) mod 26 = 322 mod 26 = 10 → k

D(21) = 23(21 - 5) mod 26 = 368 mod 26 = 4 → e

D(0) = 23(0 - 5) mod 26 = -115 mod 26 = 15 → p

D(22) = 23(22 - 5) mod 26 = 391 mod 26 = 1 → b

D(5) = 23(5 - 5) mod 26 = 0 mod 26 = 0 → a

D(18) = 23(18 - 5) mod 26 = 299 mod 26 = 13 → n

D(3) = 23(3 - 5) mod 26 = -46 mod 26 = 6 → g

D(21) = 23(21 - 5) mod 26 = 368 mod 26 = 4 → e

D(16) = 23(16 - 5) mod 26 = 253 mod 26 = 19 → t

D(25) = 23(25 - 5) mod 26 = 460 mod 26 = 18 → s

ftc nftva wfsdvqz ⇒ aku cakep bangets