PRAKTIKUM KRIPTOGRAFI

KUIS 1

Disusun Oleh:
Prames Ray Lapian *140810210059*

UNIVERSITAS PADJADJARAN
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM STUDI TEKNIK INFORMATIKA
JATINANGOR
2023

SOAL

1.

Jawaban

1. Kriptografi Simetris dan Asimetris
   a. Simetris

      Kriptografi Simetris merupakan kriptografi yang memiliki kunci Dekripsi yang sama dengan kunci Enkripsi.

   b. Asimetris

      Kriptografi Asimetris merupakan kebalikan dari Kriptografi Simetris, yaitu dimana kunci untuk Dekripsi berbeda dengan kunci ketika meng-Enkripsi.

2. Tabel Konversi ROT13

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
⇅	⇅	⇅	⇅	⇅	⇅	⇅	⇅	⇅	⇅	⇅	⇅	⇅
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

3. Shift Cipher:

   P R A M E S
   15 17 0 12 4 18

   K = 59 + 6 = 65

   E(x) = (x+K) mod 26

   [P] = (15+65) mod 26 = 2 → [C]
   [R] = (17+65) mod 26 = 4 → [E]
   [A] = (0+65) mod 26 = 13 → [N]
   [M] = (12+65) mod 26 = 25 → [Z]
   [E] = (4+65) mod 26 = 17 → [R]
   [S] = (18+65) mod 26 = 5 → [F]

   E(x) = C E N Z R F

   D(x) = (x-K) mod 26
   [C] = (2-65) mod 26 = -63 mod 26 = 15 → [P]
   [E] = (4-65) mod 26 = -61 mod 26 = 17 → [R]
   [N] = (13-65) mod 26 = -52 mod 26 = 0 → [A]
   [Z] = (25-65) mod 26 = -40 mod 26 = 12 → [M]
   [R] = (17-65) mod 26 = -48 mod 26 = 4 → [E]
   [F] = (5-65) mod 26 = -60 mod 26 = 18 → [S]

D(x) = P R A M E S

4. Afine:
   K U I S K R I P T O
   10 20 8 18 10 17 8 15 19 14

   E(x) = (ax + b) mod 26
   a = 11
   b = 59

   [K] = (11.10 + 59) = 169 mod 26 = 13 -> [N]
   [U] = (11.20 + 59) = 279 mod 26 = 19 -> [T]
   [I] = (11.8 + 59) = 147 mod 26 = 17 -> [R]
   [S] = (11.18 + 59) = 257 mod 26 = 23 -> [X]
   [K] = (11.10 + 59) = 169 mod 26 = 13 -> [N]
   [R] = (11.17 + 59) = 246 mod 26 = 12 -> [M]
   [I] = (11.8 + 59) = 147 mod 26 = 17 -> [R]
   [P] = (11.15 + 59) = 224 mod 26 = 16 -> [Q]
   [T] = (11.19 + 59) = 268 mod 26 = 8 -> [I]
   [O] = (11.14 + 59) = 213 mod 26 = 5 -> [F]

   E(x) = N T R X N M R Q I F

   GCD(a, m) = GCD(11, 26)
   26 = 11 * **2** + 4
   11 = 4 * **2** + 3
   4 = 3 * **1** + 1
   3 = **1** * 3 + 0

   t0 = 0
   t1 = 1
   t2 = (t0 - (q1 . t1)) mod 26
   = (0 - (2 * 1)) mod 26
   = (0 - 2) mod 26
   = -2 mod 26
   = 24
   t3 = (t1 - (q2 . t2)) mod 26
   = (1 - (2 * 24)) mod 26
   = (1 - 48) mod 26
   = -47 mod 26
   = 5
   t4 = (t2 - (q3 . t3)) mod 26
   = (24 - (1 * 5)) mod 26
   = (24 - 5) mod 26
   = 19 mod 26
   = 19
   a^-1 = 19

   D(y) = k^-1 (y - b) mod 26
   [N] = 19*(13 - 59) mod 26 = 10 -> [K]
   [T] = 19*(19 - 59) mod 26 = 20 -> [U]

[R] = 19*(17 - 59) mod 26 = 8 -> [I]
[X] = 19*(23 - 59) mod 26 = 18 -> [S]
[N] = 19*(13 - 59) mod 26 = 10 -> [K]
[M] = 19*(12 - 59) mod 26 = 17 -> [R]
[R] = 19*(17 - 59) mod 26 = 8 -> [I]
[Q] = 19*(16 - 59) mod 26 = 15 -> [P]
[I] = 19*(8 - 59) mod 26 = 19 -> [T]
[F] = 19*(5 - 59) mod 26 = 14 -> [O]

5. Hill:
   Plain Teks: HASKEL 7 0 18 10 4 11
   Cipher Teks: KLSWVZ 10 11 18 22 21 25

   7 0 = 10 11; 18 10 = 18 21

   K = C * P^-1

   = | 10 | 18 | * | 7 | 18 | ^-1 |
     | 11 | 21 | | 0 | 10 | |

   = | 10 | 18 | * | 0.1428571429 | -0.2571428571 |
     | 11 | 21 | | 0 | 0,1 |

   = | **1.428571429** | **-0.771428571** |
     | **1.571428572** | **-0.7285714281** |