UJIAN TENGAH SEMESTER TEORI
SISTEM KEAMANAN DATA

DISUSUN OLEH

Christo Gustawan Nugraha

V3422071

D3 TEKNIK INFORMATIKA

FAKULTAS SEKOLAH VOKASI

UNIVERSITAS SEBELAS MARET

2023

1. Apabila suatu algoritma Caesar Cipher memiliki persamaan seperti berikut:
   c = E(p) = (p + k) mod (26) -> *encode function*
   p = D(c) = (c – k) mod (26) -> *plaintext function*
   apabila kunic dengan konstanta k = 11, maka buatlah *encode text* dari kalimat *plaintext* =
   "tolong saya pinjam duit seratus ribu"

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

   a. c = E(p) = (p + k) mod (26) -> *encode function*

      t = (19 + 11) mod (26) = 4 → E
      o = (14 + 11) mod (26) = 25 → Z
      l = (11 + 11) mod (26) = 22 → W
      o = Z
      n = Y
      g = R

      s = D
      a = L
      y = J
      a = L

      p = A
      i = T
      n = Y
      j = U
      a = L
      m = X

      d = O
      u = F
      i = T
      t = E

      s = D
      e = P

r = C
a = L
t = E
u = F
s = D

r = C
i = T
b = M
u = F

Hasil enkripsi: “EZWZYRDLJLATYULXOFTEDPCLEFDCTMF”

b. p = D(c) = (c – k) mod (26) -> *plaintext function*
Chipertext: “EZWZYRDLJLATYULXOFTEDPCLEFDCTMF”

E = (30 - 11) mod 26 = 19 → T
Z = (25 - 11) mod 26 = 14 → O
W = (22 - 11) mod 26 = 11 → L
Z = O
Y = N
R = G

D = S
L = A
J = Y
L = A

A = P
T = I
Y = N
U = J
L = A
X = M

O = D
F = U
T = I
E = T

D = S
P = E

C = R
L = A
E = T
F = U
D = S

C = R
T = I
M = B
F = U

Dekripsi : “Tolong saya pinjam duit seratus ribu”

2. Suatu algoritma Vigenere Cipher memiliki persamaan yang sama dengan Caesar Cipher,
yaitu:
c = E(p) = (p + k) mod (26) → encode function
p = D(c) = (c – k) mod (26) → plaintext function
apabila kunci Vigenere Ciphernya adalah *becanda* maka buatlah *encode text* dari kalimat
plain text = “Selamat anda semua dapat nilai A”

   a. Ciphertext: c = E(p) = (p + k) mod (26) → encode function
      Plaintext : “S e l a m a t a n d a s e m u a d a p a t n i l a i A”
      Kunci (ulang) : “b e c a n d a b e c a n d a b e c a n d a b e c a n d”
      Enkripsi : “t i n a z d t b r f a f h m v e f a c d t o m n a v D”

   b. Plaintext: p = D(c) = (c – k) mod (26) → plaintext function
      Ciphertext : “t i n a z d t b r f a f h m v e f a c d t o m n a v D”
      Kunci (ulang) : “b e c a n d a b e c a n d a b e c a n d a b e c a n d”
      Deskripsi : “S e l a m a t a n d a s e m u a d a p a t n i l a i A”

3. Jelaskan hasil pergeseran baris ke-3 dari algoritma AES diketahui memiliki input sebagai
berikut:

state

31	e0	32	88
31	37	43	5a
98	07	f6	30
a2	34	a8	8d

cipher key

2b	28	ab	09
7e	Ae	f7	cf
15	d2	15	4f
16	a6	88	3c

Penjelasan :
Pergeseran baris ke-3 pada algoritma AES adalah proses pergeseran baris ke-3 dari state ke baris ke-1, baris ke-1 ke baris ke-2, dan baris ke-2 ke baris ke-3.

Pada state pertama, baris ke-3 adalah sebagai berikut:

31 e0 32 88
31 37 43 5a
98 07 f6 30
a2 34 a8 8d

Langkah pertama memindahkan baris ke-3 ke baris ke-1. Baris ke-3, yaitu a2 34 a8 8d, dipindahkan ke baris ke-1. Baris ke-2 dan ke-3 bergeser ke bawah satu baris.

Hasilnya menjadi sebagai berikut:

31 e0 32 88
98 07 f6 30
a2 34 a8 8d
31 37 43 5a

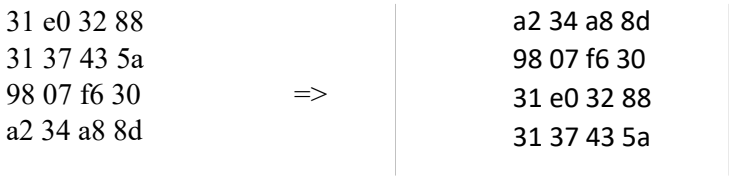
Langkah kedua memindahkan baris ke-1 ke baris ke-2. Baris ke-1, yaitu a2 34 a8 8d, dipindahkan ke baris ke-2. Baris ke-3 bergeser ke bawah satu baris. Hasilnya menjadi sebagai berikut:

98 07 f6 30
31 e0 32 88
a2 34 a8 8d
31 37 43 5a

Langkah ketiga memindahkan baris ke-2 ke baris ke-3. Baris ke-2, yaitu 98 07 f6 30, dipindahkan ke baris ke-3. Baris ke-1 bergeser ke bawah satu baris. Hasilnya menjadi sebagai berikut:

a2 34 a8 8d
98 07 f6 30
31 e0 32 88
31 37 43 5a

Diagram pergeseran baris ke-3 dapat digambarkan sebagai berikut:



Hasil transformasi dari pergeseran baris ke-3 adalah sebagai berikut:

a2 34 a8 8d
98 07 f6 30
31 e0 32 88
31 37 43 5a

Pergeseran baris ke-3 pada algoritma AES bertujuan untuk meningkatkan kompleksitas algoritma dan mempersulit peretas untuk memecahkan enkripsi.

4. Jelaskan proses perhitungan langkah per langkah untuk *encrypt* dan *decrypt* dari algoritma
RSA berikut:
misal diberikan *public key* = (e,n) = (3, 15) dan *private key* = (d,n) = (7, 15) dengan p = 3, q = 5 dan e = 3, d = 7
plain text = cuan

Penjelasan
Algoritma RSA adalah metode kriptografi yang memanfaatkan kunci publik dan kunci privat untuk mengamankan proses enkripsi dan dekripsi. Dalam penggunaannya, langkah-langkah untuk melakukan enkripsi dan dekripsi pesan menggunakan algoritma RSA dapat dijelaskan dengan contoh kunci publik (3, 15) dan kunci privat (7, 15), serta nilai p = 3, q = 5, e = 3, dan d = 7.

Enkripsi
a. Ubah pesan "cuan" menjadi bilangan sesuai dengan tabel ASCII: C = 67, U = 117, A = 97, N = 110.
b. Hitung nilai enkripsi untuk setiap karakter menggunakan rumus: $C = M^e \ mod \ n$
Untuk C: $673 \ mod \ 15 = 7$
- Untuk U: $1173 \ mod \ 15 = 12$
- Untuk A: $973 \ mod \ 15 = 7$
- Untuk N: $1103 \ mod \ 15 = 10$

c. Pesan terenkripsi adalah 7 12 7 10.
Dekripsi
a. Hitung nilai dekripsi untuk setiap karakter terenkripsi menggunakan rumus: $M = C^d \ mod \ n$
- Untuk 7: $7^7 \ mod \ 15 = 67$
- Untuk 12: $12^7 \ mod \ 15 = 117$
- Untuk 7: $7^7 \ mod \ 15 = 97$
- Untuk 10: $10^7 \ mod \ 15 = 110$

b. Ubah bilangan kembali menjadi karakter: 67 = C, 117 = U, 97 = A, 110 = N.
c. Pesan terdekripsi adalah "cuan".