조이강_HW2

1. We choose primes p=19. q=29, and n=37. Encrypt 234 using the public key (z, n) (Do not use calculator) (1 point)

1.

$p=19$, $q=29$, $n=37$ 이고, 234를 암호화합니다.

공개키 (z, n) 에서 $z = p \times q = 19 \times 29 = 551$ 이므로, $(z, n) = (551, 37)$ 입니다.

$\phi = (19-1)(29-1) = 504$ 이며,

개인키 s에 대하여 $ns \bmod \phi = 1$ = $37s \bmod 504 = 1$ 이므로,

$gcd(37, 504)$을 유클리드 알고리즘을 이용해 풀어보면,

$$504 = 37 \times 13 + 23$$
$$37 = 23 \times 1 + 14$$
$$23 = 14 \times 1 + 9$$
$$14 = 9 \times 1 + 5$$
$$9 = 5 \times 1 + 4$$
$$5 = 4 \times 1 + 1$$
$$4 = 1 \times 4 + 0$$

$\therefore$ $gcd(37, 504) = 1$ 입니다.

이를 역추적하여 모듈러 연산의 역원을 구합니다.

$$1 = 5 - (1 \times 4)$$
$$1 = 5 - (9-5) = 2 \times 5 - 9$$
$$1 = 2(14-9) - 9 = 2 \times 14 - 3 \times 9$$
$$1 = 2 \times 14 - 3(23-14) = 5 \times 14 - 3 \times 23$$
$$1 = 5 \times (37-23) - 3 \times 23 = 5 \times 37 - 8 \times 23$$
$$1 = 5 \times 37 - 8(504 - 13 \times 37) = 109 \times 37 - 8 \times 504$$

따라서 $37 \bmod 504$의 역원은 109 이며, 개인키 $s = 109$ 입니다.

암호화할 정수가 234이고, 메시지를 C라고 하면.

$C = 234^{37} \bmod 551$ 입니다.

$234 \bmod 551 = 234$

$234^2 \bmod 551 = (234 \times 234) \bmod 551 = 207$

$234^4 \bmod 551 = (207 \times 207) \bmod 551 = 422$.

$234^8 \bmod 551 = (422 \times 422) \bmod 551 = 111$

$234^{16} \bmod 551 = (111 \times 111) \bmod 551 = 199$

$234^{32} \bmod 551 = (199 \times 199) \bmod 551 = 480$.

$234^5 \bmod 551 = (422 \times 234) \bmod 551 = 119$.

$\therefore 234^{37} \bmod 551 = (480 \times 119) \bmod 551 = 367$.

$\therefore C = 367$ 입니다.

2. Susan purchased computers from A, B, and C, respectively 550ea, 100ea, and 350ea. Defective rate of computers from A, B, and C are 1%, 3%, and 3%, respectively.

2-1) What is the probability that the computer was bought from A when it is defective? (0.2 points)

2-2) What is the probability that the computer was bought from B when it is defective? (0.2 points)

2-3) What is the probability that the computer was bought from C when it is defective? (0.2 points)

2.

A에서 550개를 구매, 불량률은 1% 입니다.

B에서 100개를 구매, 불량률은 3% 입니다.

C에서 350개를 구매, 불량률은 3% 입니다.

각 A, B, C 업체에서 구매한 컴퓨터일 확률은.

$P(A) = \frac{550}{1000}$ $\quad P(B) = \frac{100}{1000}$ $\quad P(C) = \frac{350}{1000}$.

각 업체에서 구매한 컴퓨터가 불량일 확률은.

$P(D|A) = 0.01$ $\quad P(D|B) = 0.03$ $\quad P(D|C) = 0.03$.

구매한 컴퓨터에 결함이 있을 확률은.

$$P(D) = P(D|A)P(A) + P(D|B)P(B) + P(D|C)P(C)$$

$$= 0.01 \times 0.55 + 0.03 \times 0.01 + 0.03 \times 0.35$$

$$= 0.019.$$

1) 결함이 있을 때, 그 컴퓨터가 A에서 왔을 확률.

$$P(A|D) = \frac{P(A\cap D)}{P(D)} = \frac{P(D|A)\times P(A)}{P(D)} = \frac{0.01\times 0.55}{0.019}.$$

$$\therefore P(A|D) \simeq 0.289.$$

2) 결함이 있을 때, 그 컴퓨터가 B에서 왔을 확률.

$$P(B|D) = \frac{P(B\cap D)}{P(D)} = \frac{P(D|B)\times P(B)}{P(D)} = \frac{0.03\times 0.1}{0.019}$$

$$\therefore P(B|D) \simeq 0.158.$$

3) 결함이 있을 때, 그 컴퓨터가 C에서 왔을 확률.

$$P(C|D) = \frac{P(C\cap D)}{P(D)} = \frac{P(D|C)\times P(C)}{P(D)} = \frac{0.03\times 0.35}{0.019}$$

$$\therefore P(C|D) \simeq 0.553.$$

3. Find particular solution of the linear nonhomogeneous recurrence relations of $a_n = 7a_{n-1} - 10a_{n-2} + 16n$ where $a_0 = 1, a_1 = 1$ (1점)

3) 주어진 점화식

$$a_n = 7a_{n-1} - 10a_{n-2} + 16n \quad (a_0 = 1,\ a_1 = 1) \text{ 에서.}$$

동차 점화식의 일반해를 먼저 구합니다.

$$a_n = 7a_{n-1} - 10a_{n-2}.$$

이 동차 점화식을 풀면,

$r^2 - 7r + 10 = 0$ 이므로.

$(r-2)(r-5) = 0 \quad \therefore r = 2, 5$ 입니다.

따라서 동차 점화식의 일반해는

$x_n = j \cdot 2^n + k \cdot 5^n$ 입니다.

이제 특수해를 구합니다.

$f(n) = 16n$ 이므로. 특수해는 $An + B$의 형태를 가집니다.

이를 점화식에 대입하면.

$$An + B = 7(A(n-1) + B) - 10(A(n-2) + B) + 16n$$

$$An + B = 7An - 7A + 7B - 10An + 20A - 10B + 16n.$$

$$= -3An + 13A - 3B + 16n.$$

$\therefore A = -3A + 16$

$B = 13A - 3B$ 가 성립합니다.

$\therefore A = 4$ 이며, $B = 52 - 3B$ 이므로 $B = 13$입니다.

따라서 비동차 점화식의 특수해는

$a_n = 4n + 13$ 입니다.

이 둘을 합친 비동차 점화식의 전체 일반해는

$a_n = j \cdot 2^n + k \cdot 5^n + 4n + 13$ 이 됩니다.

$a_0 = 1 = j + k + 13$.

$a_1 = 1 = 2j + 5k + 17$. 이므로

$2j + 5k + 16$

$= 2j + 2k + 24$.

$\therefore k = \frac{8}{3}$.

$j = -\frac{44}{3}$ 입니다.

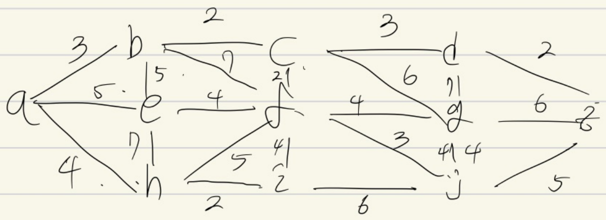
$\therefore a_n = -\frac{44}{3} \cdot 2^n + \frac{8}{3} 5^n + 4n + 13$ 입니다.

5. Exercises

5-1) #2 in 8.4 Exercises (0.4 points)

5.1).

$a \rightarrow g$ 까지의 최단 경로를 다익스트라 알고리즘으로 찾습니다.



1. a로 부터 갈 수 있는 모든 경로를 찾습니다.

$b=3$
$e=5$. 이때, a는 방문 노드가 됩니다. $(a=0)$
$h=4$

2. 최단 거리로 갈 수 있는 b가 다음 노드가 됩니다.

$a \rightarrow b \rightarrow e > a \rightarrow e$ 이므로 $e=5$
$h=4$ 입니다. b는 방문 노드가 됩니다. $(b=3)$
$c=5$
$f=10$

3. 다음 노드를 최단 거리의 h로 정합니다.

$i=6$ 입니다. h는 방문 노드입니다 $(h=4)$.
$f=9$

4. 다음 노드는 최단거리 인 e 입니다.

e에서는 f 밖에 방문할수 없으며.

a→e→f = 9 이므로.

f = 9 가 되게 됩니다. , e는 방문완료 됩니다 (e=5).

5. 다음 노드는 c입니다.

d=8
g=11 이 되며, c는 방문완료 됩니다. (c=5)
f=7

6. 다음 노드는 i입니다.

j=12 가 되며, i는 방문완료 됩니다 (i=6)

7. 다음 노드는 f입니다.

f→g에서 g=11이라 이미 g=11이므로 갱신되지 않습니다.

j=10 이 되며 f는 방문 완료됩니다. (f=7).

8. 다음 노드는 d입니다

i=10. 이 되며, d는 방문 완료됩니다 (d=8).

9. 다음 노드는 j가 됩니다.

j에서는 갱신 가능한 최단 거리가 없습니다.

j는 방문 완료가 됩니다. (j = 10).

10. 다음 노드는 e가 됩니다.

e에서도 갱신 가능한 최단 거리가 없습니다.

e는 방문 완료 됩니다 (e=10)

11. 마지막으로 g를 방문합니다.

다른 모든 노드가 방문 완료이므로 알고리즘이 종료됩니다.

g는 방문 완료되며, g = 11 입니다.

따라서 a, g 사이의 최단 경로는.

$a \to b \to c \to g$ 이며

최단 거리는 11입니다.

5-2) #4 in 8.7 Exercises (0.4 points)

5-2). 주어진 그래프가 평면이 아님을 보입니다.

주어진 그래프를 K_5 그래프와 비교해 보겠습니다.

주어진 그래프의 다섯개의 정점 a, b, c, d, e의 모든 간선을
나열해 보면,

a - b
a - c.
a - d
a - e.
b - c
b - d
b - e
c - d
c - e
d - e.

모든 정점이 다른 모든 정점에 대해 간선을 가집니다.

따라서 주어진 그래프는 K_5와 동형인 완전 그래프를 포함하고 있으며,

따라서 평면 그래프가 아닙니다.