폰트, 로고, 원, 등록 상표이(가) 표시된 사진

자동 생성된 설명

**컴퓨터 보안**

**레포트**

|  |  |
| --- | --- |
| **학과** | **컴퓨터소프트웨어공학과** |
| **학번** | **20194463** |
| **이름** | **이동규** |

**[문제]**

다음은 Knapsack 알고리즘이다.

주어진 값을 통해 암호화와 복호화를 진행하시오.

a`(쉬운 Knapsack) = [3, 5, 9, 21, 46]

w = 47

m=87

평문 x = 1 0 1 1 0

공개키 : KU = a, 개인키 : KR = {w-1, m, a`}

**[풀이과정]**

**<키 생성>**

1. 역원(w-1) 구하기

gcd(47, 87)를 이용해 역원을 구한다

w \* w-1 ≡ 1(mod m)

47 \* w-1 ≡ 1(mod 87)

|  |
| --- |
| gcd(47, 87)  87=1⋅47+40  47=1⋅40+7  40=5⋅7+5  7=1⋅5+2  5=2⋅2+1 |

역순으로 계산하여 역원을 구한다

|  |
| --- |
| 1=5−(2⋅2)  = 5−2\*(7−5)  = 3⋅5−2\*7  = 3\*(40-5\*7) -2 \* 7  = 3\*40-17\*7  = 3\*40-17(47-1\*40)  = -17\*47+20\*40  = -17 \* 47 +20(87-1\*47)  = 20\*87-37\*47 |

따라서 w-1은 50이다.

2. a 구하기

a = (w \* a`) mod m 이므로

|  |
| --- |
| (47 \* 3) mod 87 = 54  (47 \* 5) mod 87 = 61  (47 \* 9) mod 87 = 75  (47 \* 21) mod 87 = 30  (47 \* 46) mod 87 = 74 |

따라서 a = 54, 61, 75, 30, 74 이다.

**<암호화>**

평문 x = 10110 이고 암호문 S = a\*x이므로

|  |
| --- |
| 54 \* 1 = 54  61 \* 0 = 0  75 \* 1 = 75  30 \* 1 = 30  74 \* 0 = 0  54 + 75 + 30 =159 |

따라서 S = 159이다.

**<복호화>**

S` = S \* w-1 mod m 이므로

|  |
| --- |
| S` = (159 \* 50) mod 87 = 33  33 >= 46 false(x4)  33 >= 21 true(x3)  33-21 >= 9 true(x2)  12-9 >= 5 false(x1)  3 >= 3 true(x0) |

따라서 평문(x) = 1 0 1 1 0 이다