풀이

STEP III 1987, 문제 5

순수수학 • 모듈러 산술을 이용한 암호

STEP III 1987, 5번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

step.maths.org/questions/87-s3-q5

핵심 아이디어

이 암호는 서로 독립인 두 개의 이동 암호(shift cipher)로 이루어져 있다. 하나는 짝수 번째 자리에 쓰이고(키 n_0), 다른 하나는 홀수 번째 자리에 쓰이며(키 n_1), 각각에 j만큼의 추가 이동이 더해진다. 먼저 이미 알고 있는 이동 j를 벗겨 낸다. 그러면 메시지의 각 절반이 알 수 없는 하나의 상수만큼 이동된 것만 남는데, 50을 법(modulo)으로 하는 이동은 전단사(bijection)이므로 같은 수는 같은 수로, 다른 수는 다른 수로 보낸다. 세 번 나타나는 43이 바로 n_0을 드러내는 지문이다. 그다음에는 50을 법으로 한 합을 이용해 n_1을 결정한다.

풀이

n_0과 n_1은 50을 법으로 한 값만 중요하므로 $0 \le n_0, n_1 \le 49$로 놓는다. 모든 a_k는 0과 49 사이에 있으므로, 50을 법으로 한 나머지를 알면 각 a_k가 정해진다.

알고 있는 이동 제거하기

짝수 번째 자리에 대해서는 $j = 1, \ldots, 6$에 대해 $c_j = b_{2j} - j$로 놓는다. 홀수 번째 자리에 대해서는 $j = 0, \ldots, 5$에 대해 $d_j = b_{2j+1} - j$로 놓는다. 그러면

$$a_{2j} \equiv c_j - n_0, \qquad a_{2j+1} \equiv d_j - n_1 \pmod{50}.$$

암호화된 메시지로부터 다음을 얻는다.

j	1	2	3	4	5	6
b_{2j}	27	36	35	40	37	48
c_j	26	34	32	36	32	42

j	0	1	2	3	4	5
b_{2j+1}	35	2	15	8	40	24
d_j	35	1	13	5	36	19

n_0 구하기

50을 법으로 고정된 n을 빼는 것은 일대일(one-to-one)이다. 따라서 홀짝이 같은 두 자리의 a가 같을 필요충분조건은 그 자리의 c(또는 d)가 같은 것이다.

생각해 보기 세 개의 43은 어디에 들어갈 수 있을까?

여섯 개의 d_j는 모두 다르므로 홀수 번째 자리에는 서로 다른 여섯 개의 수가 들어 있고, 그 중 43은 많아야 하나이다. 따라서 적어도 두 개의 43은 짝수 번째 자리에 있다. c_j 가운데 반복되는 것은 32뿐이며, 이는 정확히 두 번($j = 3, 5$) 나타난다. 그러므로 짝수 번째 자리에는 같은 수가 정확히 두 개 있고, 메시지에서 두 번 이상 나타나는 수는 43뿐이므로 이 둘은 두 개의 43이어야 한다. 따라서

$$32 - n_0 \equiv 43 \pmod{50} \quad \Longrightarrow \quad n_0 \equiv -11 \equiv 39 \pmod{50}.$$

이제 $a_{2j} \equiv c_j - 39 \equiv c_j + 11$이므로

$$(a_2, a_4, a_6, a_8, a_{10}, a_{12}) = (37,\ 45,\ 43,\ 47,\ 43,\ 3),$$

을 얻는다. 여기서 $42 + 11 = 53 \equiv 3$이다. 여섯 수가 모두 메시지에 있으며, 당연히 그래야 한다.

n_1 구하기

메시지에서 이 여섯 수를 제거하면 홀수 번째 자리의 수들

$$S = \{1,\ 7,\ 23,\ 24,\ 39,\ 43\},$$

이 남으므로, $\{d_j - n_1\}$은 50을 법으로 S와 같아야 한다.

생각해 보기 쉰 개의 값을 모두 시도하지 않고 n_1을 어떻게 구할 수 있을까?

양쪽을 모두 더한다. 두 집합이 같으면 그 합도 50을 법으로 같다.

$$\sum d_j - 6n_1 \equiv \sum_{s \in S} s \pmod{50}, \qquad \text{즉,} \qquad 109 - 6n_1 \equiv 137.$$

따라서 $6n_1 \equiv -28 \equiv 22 \pmod{50}$이다. 법도 나누어떨어지게 하는 2로 양변을 나누면 $3n_1 \equiv 11 \pmod{25}$를 얻는다. $3 \times 17 = 51 \equiv 1$이므로 $n_1 \equiv 11 \times 17 = 187 \equiv 12 \pmod{25}$이다. 따라서 $n_1 = 12$ 또는 $n_1 = 37$이다.

합에 대한 조건은 필요조건(necessary condition)이지만 충분조건(sufficient condition)은 아니므로 두 값을 모두 확인한다. $n_1 = 37$이면 $d_0 - 37 = -2 \equiv 48$인데 이는 메시지에 없으므로 $n_1 = 37$은 성립하지 않는다. $n_1 = 12$이면

$$(a_1, a_3, a_5, a_7, a_9, a_{11}) \equiv (23,\ -11,\ 1,\ -7,\ 24,\ 7) \equiv (23,\ 39,\ 1,\ 43,\ 24,\ 7),$$

이고, 이는 정확히 S이다. 따라서 $n_1 = 12$이다.

메시지

두 절반을 번갈아 끼워 넣으면 원래 메시지는

$$23,\ 37,\ 39,\ 45,\ 1,\ 43,\ 43,\ 47,\ 24,\ 43,\ 7,\ 3,$$

이고, $n_0 \equiv 39$, $n_1 \equiv 12 \pmod{50}$이다. 위의 논증은 이 답이 유일함을 보여 준다. n_0은 강제로 정해졌고, n_1의 두 후보 중 하나만 성립하기 때문이다.

검산

답을 다시 암호화해 본다. 예를 들어 $b_{12} \equiv a_{12} + 39 + 6 = 48$이고 $b_7 \equiv a_7 + 12 + 3 = 58 \equiv 8$이며, 둘 다 맞다. 컴퓨터로 2500개의 쌍 (n_0, n_1)을 모두 시도하면, 주어진 수들의 모임으로 복호화되는 쌍은 정확히 하나, $(39, 12)$뿐이며 그 결과가 위의 메시지임을 확인할 수 있다.

흔한 실수

- 첨자를 잘못 다루는 것. 홀수 번째 자리는 b_1에서 $j = 0$으로 시작하지만, 짝수 번째 자리는 b_2에서 $j = 1$로 시작한다.
- 6이 역원을 가지는(invertible) 것처럼 $6n_1 \equiv 22 \pmod{50}$을 6으로 나누는 것. $\gcd(6, 50) = 2$이므로 6은 역원을 갖지 않으며, 이 합동식(congruence)은 50을 법으로 두 개의 해를 가진다.
- 성립하는 n_1의 값 하나를 찾고, 다른 값은 성립하지 않음을 보이지 않는 것. 문제에서 방법을 설명하라고 했으므로 유일성(uniqueness)에 대한 논증이 필요하다.

STEP 너머

이것은 카이사르 암호(Caesar cipher), 즉 이동 암호이며, 여기서 쓴 공격법은 빈도 분석(frequency analysis)의 작은 사례이다. 이동은 반복되는 글자의 패턴을 보존한다. 대학 첫 강좌에서 $6n \equiv 22$로부터 두 개의 해를 얻는 단계는 일차 합동식(linear congruence) $ax \equiv b \pmod{m}$의 이론에 해당하며, 이 합동식은 $\gcd(a, m)$이 b를 나눌 때 그리고 그때에만 해를 가진다. 아핀 암호(affine cipher) $x \mapsto ax + b$와, 나중에 배우는 RSA도 같은 아이디어 위에 세워져 있다. Davenport의 *The Higher Arithmetic*(고등 산술)은 합동식을 아름답게 다룬다.

Beyond STEP 풀이: https://beyondstep.keithmcnulty.org/ko/. 풀이 글은 CC0 1.0이다. 문제 자체의 저작권은 © Cambridge University Press & Assessment에 있으며 여기에 싣지 않는다. 영어 원문을 기계 번역하였으며 아직 검토되지 않았다.