알고리즘 시간복잡도와 암호의 안정성

2019. 05. 12. 권혁동

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

시간복잡도 개념

- 실행 시간의 관점에서 알고리즘의 효율을 측정
- 시간복잡도가 낮을 수록 좋은 알고리즘

O(1)	상수(constant)	$O(N^2)$	다차(polynomial)
O(log N)	로그(logarithmic)	$O(2^N)$	지수(exponential)
O(N)	선형(linear)	O(N!)	계승(factorial)
O(N log N)	선형로그(log linear)		

시간복잡도 개념

시간	1	2	4	8	16	32	64
O(1)	1	1	1	1	1	1	1
O(log N)	0	1	2	3	4	5	6
O(N)	1	2	4	8	16	32	64
O(N log N)	0	2	8	24	64	160	384
$O(N^2)$	1	4	16	64	256	1024	4096
$O(2^N)$	2	4	16	256	66536	42949672976	$1.84*10^{19}$
O(N!)	1	2	24	40320	$2.09*10^{13}$	$2.63*10^{35}$	$1.27*10^{89}$

시간복잡도 개념

- 알고리즘의 반복 횟수를 계산
- 모든 반복 횟수를 더한 다음 최고차항만 잔류

```
int i, j                        // 1
for(i = 0 to n – 1)             // n
        for(j = I + 1 to n)     // (n – 1) * n
```

$N^2 + 1 \rightarrow O(N^2)$

시간복잡도 개념

- 일반적인 알고리즘은 시간복잡도가 낮을수록 좋다
  - 동작속도가 빠름을 의미
- 암호 알고리즘은 시간복잡도가 높아야 한다
  - 시간복잡도가 높을 수록 키를 계산하기 어렵기 때문
- 암호 알고리즘의 시간복잡도는 대체로 키 길이에 비례

암호 알고리즘 별 시간복잡도

- DES
- 1975년 IBM에서 개발
- 56비트 키를 사용하므로 $O(2^{56})$
- 1993년 Matshi의 계산 $O(2^{47})$
- 2001년 Junod의 계산 $O(2^{39})$ ~ $O(2^{43})$

P. Junod, “On the Complexity of Matsui’s Attack”

암호 알고리즘 별 시간복잡도

- Triple-DES
- DES를 3회 반복하는 형식
- 1, 3회의 DES 키가 동일한 2키 방식을 주로 사용
- 1981년 Merkle과 Hellman이 제시
  - $2^{56} * 2^{56} = 2^{112}$ -> $O(2^{112})$
- 단, 첫번째 키를 찾는 시간에 따라 최소 $O(2^{56})$까지 감소

Ralph C. Merkle, Martin E. Hellman, “On the security of multiple encryption”

암호 알고리즘 별 시간복잡도

- AES
- 2001년 Rijndael 알고리즘
- 128, 192, 256비트 키 길이 지원
- Bicilique 공격에 대해서 각각 $O(2^{126.1})$, $O(2^{189.7})$, $O(2^{254.4})$
- Related-key 공격에 대해서 $O(2^{126})$

A. Bogdanov, D. Khovratovich, C. Rechberger, “Biclique Cryptanalysis of the Full AES”
A. Biryukov, D. Khovratovich, “Related-Key Cryptanalysis of the Full AES-192 and AES-256”

암호 알고리즘 별 시간복잡도

- SEED
- 1999년 한국정보보호센터에서 개발
- 128, 256비트 키 길이 지원
- SEED-128의 차분 공격에 대해서 $O(2^{122})$

J. Sung, “Differential cryptanalysis of eight-round SEED”

암호 알고리즘 별 시간복잡도

- ARIA
- 2004년 한국인터넷진흥원에서 개발
- 128, 192, 256비트 키 길이 지원
- MITM 공격의 5, 6, 7, 8라운드에 대해서

$O(2^{265.4})$, $O(2^{121.5})$, $O(2^{185.3})$, $O(2^{251.6})$

X. Tang, B. Sun, R. Li, C. Li, “A Meet-in-the-Middle Attack on ARIA.”

암호 알고리즘 별 시간복잡도

- LEA
- 2013년 한국인터넷진흥원에서 개발
- 128, 192, 256비트 키 길이 지원
- 각 키에 대해 오류 주입 공격에 대해서 $O(2^{35})$, $O(2^{99})$, $O(2^{163})$

M. Park, J. Kim, “Differential Fault Analysis of the Block Cipher LEA”

시간복잡도 위협요소

- 쇼어 알고리즘
- 피터 쇼어가 제안한 양자 알고리즘
- 크기 N인 정수를 소인수 분해 시 $O(\log^3 N)$
- 공개키 암호에 위협적
- 단, 아직 실존하는 알고리즘이 아님

시간복잡도 위협요소

- 그로버 알고리즘
- N개의 데이터를 가진 DB에서 검색 시간이 $O(\sqrt{N})$
- 대칭키 암호, 해시 함수에 위협적
  - 대칭키: 키 길이를 2배로 증가
  - 해시: 역상 공격 – N/2 | 충돌쌍 공격 - N/3을 지닐 수 있도록 출력 길이 증가
- 단, 아직 실존하는 알고리즘이 아님

시간복잡도 위협요소

- P-NP 문제
- 시간복잡도 NP인 문제가 시간복잡도 P에 속할 수 있는가
- 결정 문제의 분류
- 아직 암호 알고리즘은 NP에 속하기에 안전
- 단, P-NP 문제가 참으로 밝혀진다면 붕괴 가능성 존재