쇼어 알고리즘
(Shor's Algorithm)

김상원

https://youtu.be/wfJDGFvzKFc

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

쇼어 알고리즘 개요

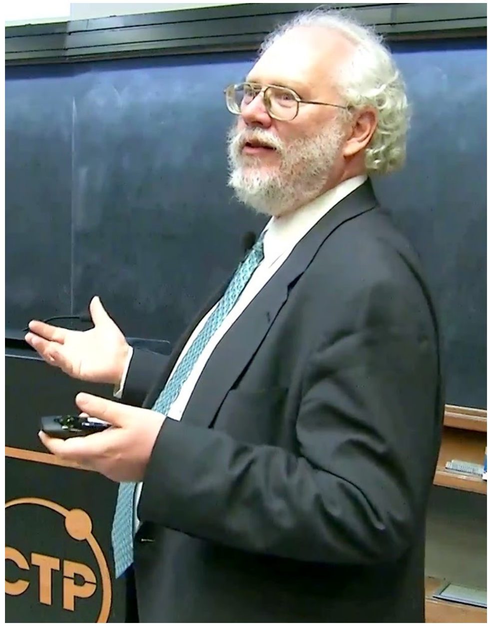
RSA 암호에 대한 이해

쇼어 알고리즘 구현

Q & A

쇼어 알고리즘 개요

- 1994년 벨연구소의 피터 쇼어(Peter Shor)가 제안한 알고리즘
- 양자계의 중첩이라는 성질을 이용해서 푸리에 변환을 모든 데이터에 대해 병렬적으로 동시에 처리함으로서 주기를 빠르게 찾음
- 양자컴퓨터를 이용해 **RSA 암호체계 무력화** 가능
- 현재 다항 시간안에 소인수분해를 하는 알고리즘 중 가장 빠른 알고리즘



RSA암호에 대한 이해

- 1977년 론 리베스트, 애디 샤미르, 레오나르도 애들먼의 이름을 따서 만들어진 암호
- 최초로 개발된 공개키 암호 체계
- 두 소수를 곱해서 큰 수를 만드는 연산은 쉽지만, 반대로 큰 수를 두 개의 소수로 소인수분해 하기는 어렵다는 비대칭성을 이용해서 만들어짐
- 실제로 여러 금융기관에서 공인인증서를 발급하여 거래할 때 RSA암호가 많이 사용됨
- 양자컴퓨터를 이용해 **RSA 암호체계 무력화**시 사회혼란 야기

쇼어 알고리즘 구현

Input: 두 개의 소수 p, q의 곱으로 만들어진 합성수 $N=p\times q$
Output: N의 소인수 p, q

1. 1보다 크고 N보다 작은 정수 a를 임의적으로(randomly) 선택한다.
2. 만일, $gcd(N,a) \neq 1$, 운이 좋게 소인수 p를 발견한 것이다. 따라서 $p=gcd(N,a)$, $q=N/gcd(N,a)$
3. 함수 $f(x)=a^x \pmod N$의 주기 r을 찾는다. 여기서 찾은 주기 r이 짝수가 아니라면, 1번 단계부터 다시 시작한다.
4. 주기 r로부터 두 개의 최대공약수 $gcd_1=gcd(N, a^{r/2}) + 1)$, $gcd_2=gcd(N, a^{r/2} - 1)$를 찾는다.
5. 여기서 찾은 두 개의 수 gcd_1, gcd_2 중 하나라도 1이거나 N이라면 1번 단계부터 다시 시작한다. 아니면, 마침내 소인수들을 찾았으므로 gcd_1, gcd_2를 리턴하고 종료한다.

쇼어 알고리즘 구현

$$N = 15 = 3 \times 5$$

1. 1보다 크고 N보다 작은 정수 a를 임의적으로(randomly) 선택

a = { 3, 5, 6, 9, 10, 12}

a = {2, 4, 7, 8, 11, 13, 14}

gcd(N,a) = {3, 5, 3, 3, 5, 3}

gcd(N,a) = {1, 1, 1, 1, 1, 1, 1}

쇼어 알고리즘 구현

$$N = 15 = 3 \times 5$$

N = 15 = 3 × 5

a = {2, 4, 7, 8, 11, 13, 14}

gcd(N,a) = {1, 1, 1, 1, 1, 1, 1}

- 함수 $f(x) = a^x (\text{mod } N)$의 주기(period) r을 찾는다.
- 여기서 찾은 주기 r이 짝수가 아니면, 1번 단계부터 다시 시작한다.

a = 2: f(0), f (1), f(2), f(3), f(4), f(5), …

1(mod 15), 2 (mod 15), 4 (mod 15), 8(mod 15), 16(mod 15), 32(mod 15), …

$\boxed{1, 2, 4, 8,}$ 1, 2, 4, 8, 1, …

주기 r = 4

쇼어 알고리즘 구현

$$N = 15 = 3 \times 5$$

a=7

1(mod 15), 7 (mod 15), 49(mod 15), 343(mod 15), 2401 (mod 15), …

$\boxed{1, 7, 4, 13}$ 1, 7, 4, 13, 1, 7, …

주기 r = 4

a=4

1(mod 15), 4(mod 15), 16(mod 15), 64 (mod 15), 256(mod 15), …

$\boxed{1, 4}$ 1, 4, 1, 4, 1, 4, 1, 4, …

주기 r = 2

쇼어 알고리즘 구현

$$N = 15 = 3 \times 5$$

- 주기 r로부터 두 개의 최대공약수 gcd1, gcd2 를 찾는다.

$gcd_1 = gcd(N, a^{r/2} + 1)$, $gcd_2 = gcd(N, a^{r/2} - 1)$

a =7, r = 4:

$gcd_1 = gcd\ (15,50) = 5$

$gcd^2 = gcd\ (15,48) = 3$

Q & A