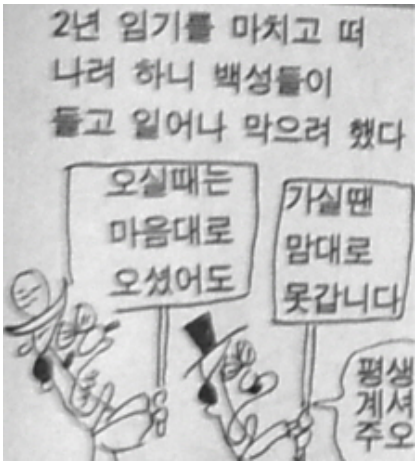
# C++로 구현하기

## RSA암호를 구현해 보자!!(1)

예제 코드

### RSA암호란??




'암호화할 때에는 맘대로 지만 해독할 때에는 아니다'와 "큰 수는 소인 수 분해를 하기 힘들다." 를 기본 모토로 한 공개키 암호 체계 중 하나 이다. 공개키와 개인 키가 한 쌍을 이루며, 공개키로 암호화한 내용은 개인 키로만, 개인 키로 암호화한 내용은 공개키로만 해독할 수 있다.엄청 큰 숫자는 소인 수 분해하기가 힘들다는 것을 이용한다. 1977년 이 체제를 개발한 Rivest, Shamir, Adleman 세 사람의 성을 따서 RSA 라고 이름이 붙은 암호 방식이다.(근데 공학자들 이름 있어 보이게 짓는데 취미 아니었나??)

### RSA암호 키생성 방법

1. 두 소수 p,q를 준비한다
2. N=pq를 계산한다.
3. φ(N)과 서로소인 인 정수 e를 찾는다.(φ(N)는 오일러 피(phi)함수로 뒤에서 이론 설명 할때 설명 예정.)
4. ed를 φ(N)으로 나눈 나머지가 1이 되도록 하는 정수 d를 찾는다.
5. (N,e)가 공개키,(N,d)가 개인키로 저장한다.
6. 이제 p,q, φ(N)은 있어봐야 득 될게 없으니 파기한다.

1번에서 두 소수는 에라토스테네스의 체를 이용한 방법을 생각해볼수 있다. 하지만 이 방법을 쓸 경우 루트p보다 작은 수로 p를 전부 나눠 봐야 한다. 즉 쓸게 못 된다는 소리이다. 그래서 현재는 페르마의 소정리의 대우명제와 다른 소수 판별법을 같이사용해서 소수를 찾는다.

### RSA 암호화 과정

$$1)\ x \equiv a^{e} \pmod{N}$$

보내려는 평서문 a를 1)의 식에 대입해서 암호문을 얻는다.(만약a가 N보다 클 경우 어떠한 복잡한 방법을 통해서 a값을 N보다 작게 만든다.)
((1의 식은 x를 N으로 나눈 값과 a^e을 N으로 나눈 값과 같다는 의미로 "x와a^e는 모듈러 N(modular N)에 대하여 합동이다"라고 읽는다 당연히 여기서의 합동과 기하학에서의 합동은 다르다)

### RSA 복호화 과정

$$2)\ a' \equiv x^{d} \pmod{N}$$

받아온 암호문 x를 2)의 식에 대입해서 암호문을 얻는다.
근데 코딩을 조금이라도 해봤다면 위의 암복호화 방법을 보면서 1) 이나 2)의 식을보면서 e나d가 한 두 자리 수 도 아닌데 컴퓨터가 계산 가능한 범주 내에서 이루어 질 수 있는가 라는 의문이 반드시 들것이다 (아님 말고...) 근데 의외로 엄청 간단한 방법으로 이 문제를 해결할 수 있다. 그 방법은 바로 제곱 한 수를 다시 제곱 하는 것 이다. 예를 들자면2^2047을 계산하자 하면 이 계산을 하기도전에 컴퓨터에 고기를 굽는 게 가능하겠지만 이 식을 조금만 건드려서
2^(2^0+2^1+2^2+2^3+2^4+2^5+2^6+2^7+2^8+2^9+2^10)이를 지수 법칙을 이용해서
2×2^2×(2^2)^2×((2^2)^2)^2....(((((((((2^2)^2)^2)^2)^2)^2)^2)^2)^2)^2)^2로 변환 가능하고 변환 한 식을 모듈러 연산의 특성을 조금 활용하면 금방 계산 가능하다. 모듈러의 특성은 이론설명할때 하기로 하자. 공간 부족...ㅠㅠ