cryptography

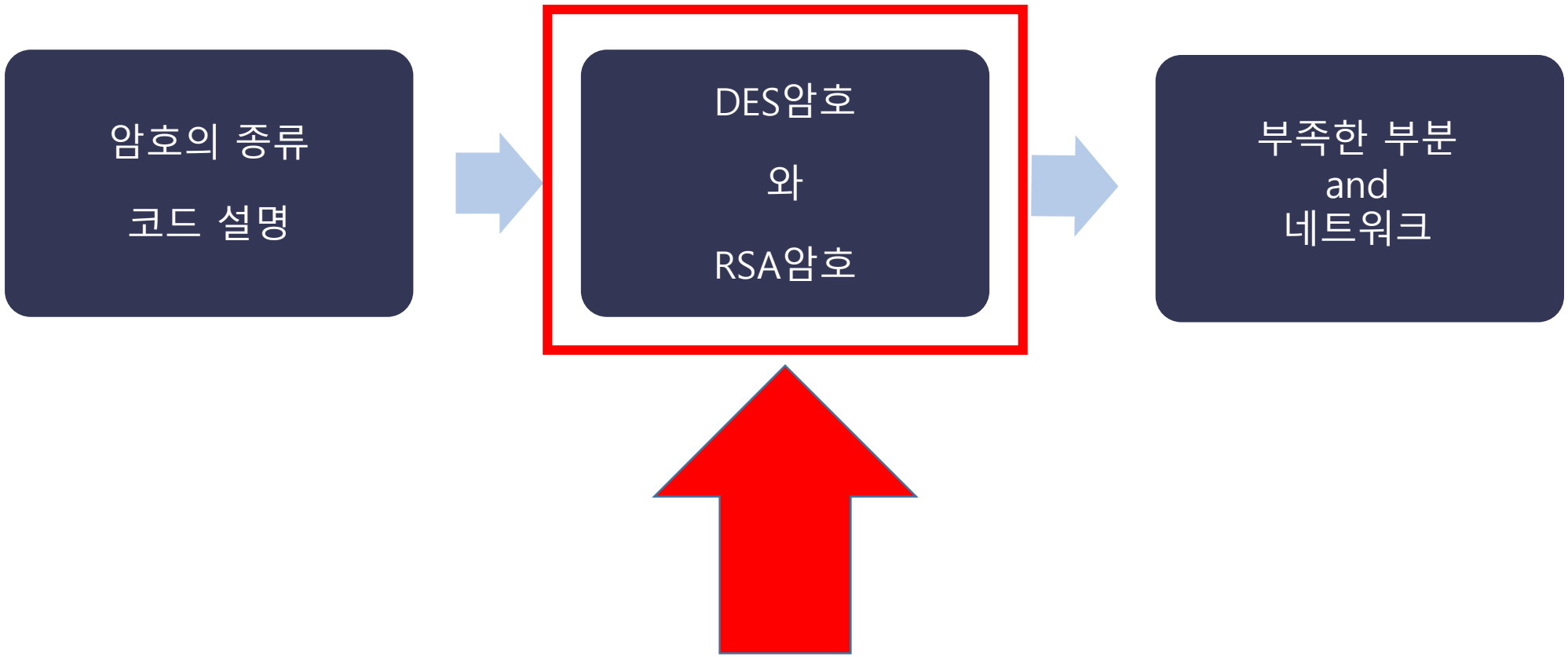
DES & RSA - 문승재

Go!

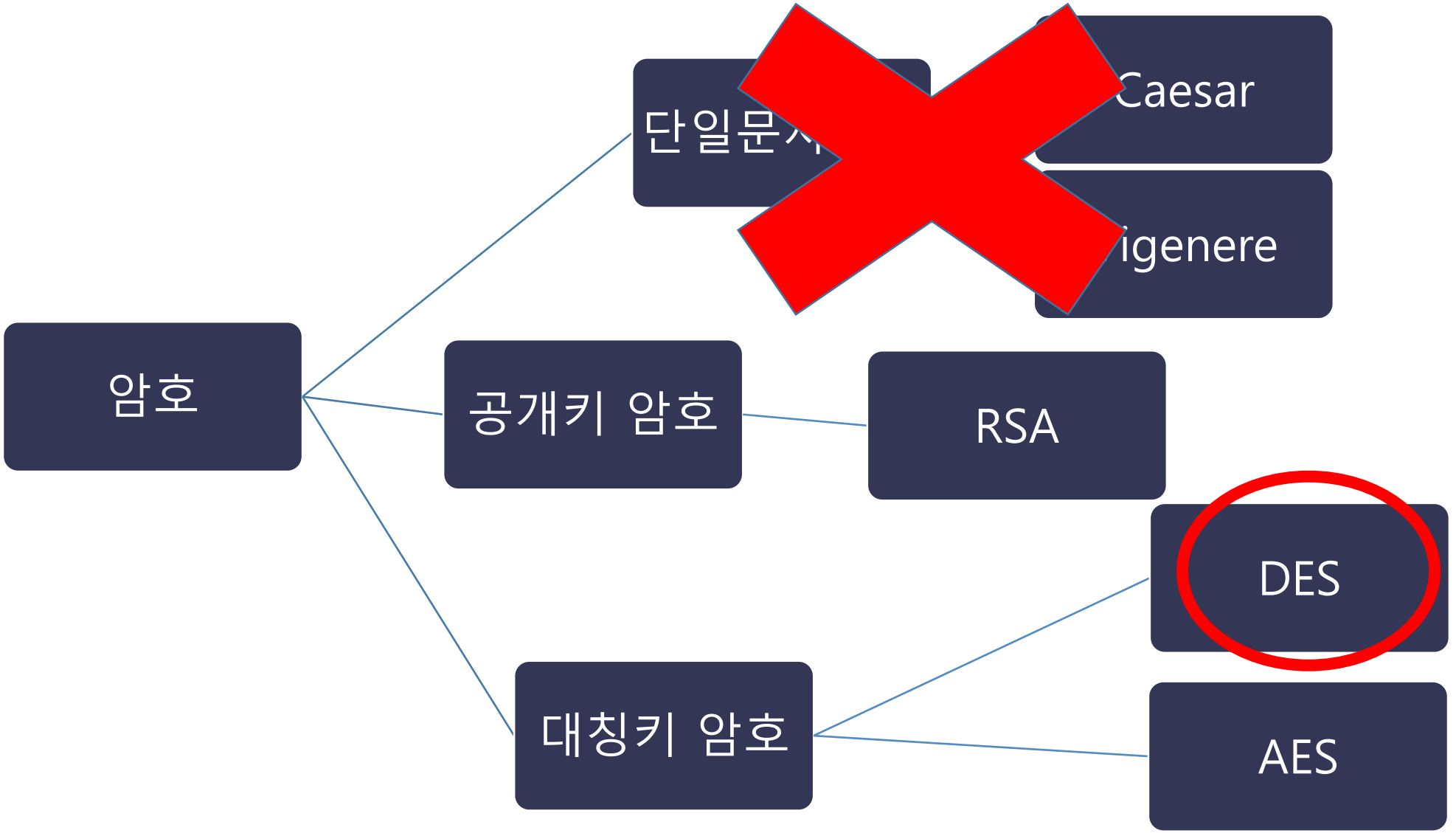
목 차

- DES암호
- RSA암호

앞으로의 발표 계획



암호의 종류



대칭키 암호

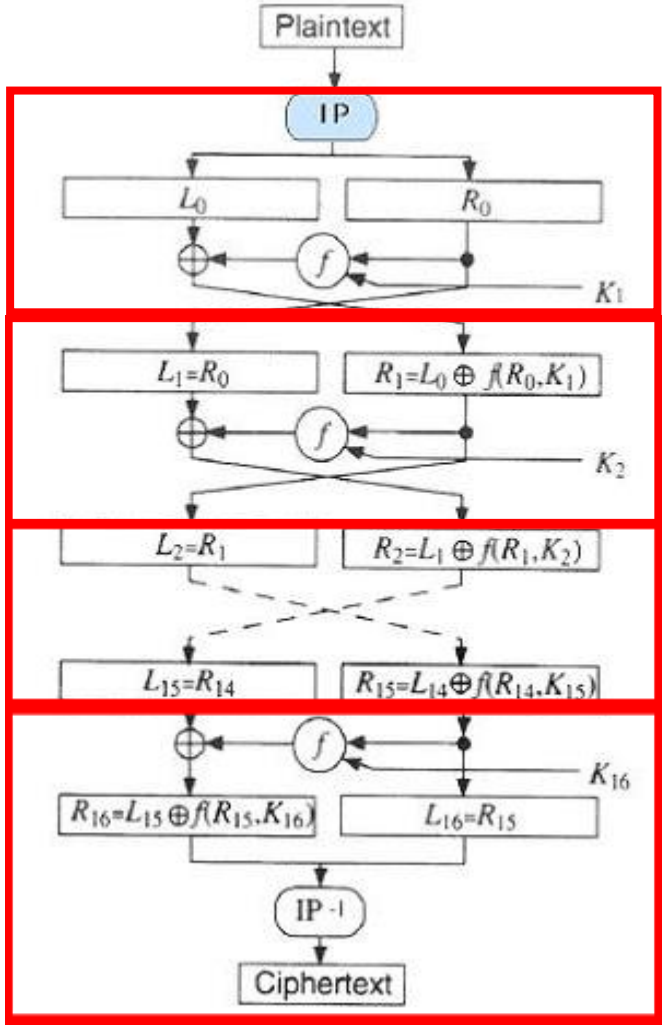
대칭키암호

알고리즘	블록 암호화	스트림 암호화
암호화 과정	평문 전체를 블록단위로 배열하고 순차적으로 암호화	평문을 각 문자를 순서대로 즉시 암호화 스트림으로 만듦
장점	• 평문에 혼돈성을 주어 해독이 어렵다. • 완성 암호문에 내용 추가,변경이 어렵다	• 암호화 속도가 상대적으로 빠름 • 에러 파급효과가 적음
단점	• 암호화 속도가 상대적으로 느림 • 에러의 파급효과가 큼	• 평문의 특성이 암호문에 반영 • 내용의 첨가가 가능
예시	• DES암호 • AES암호	• RC4 • Vigenere암호 • CAESAR암호

빈도 분석법이 이 특성을 이용함

DES란

- 데이터 암호화 표준(Data Encryption Standard)의 준말
- IBM에서 고안되어 NIST가 미국 표준 암호 알고리즘으로 채택된 **대칭 암호화 알고리즘**이다.
- 1998년도에 해독된 암호화 기술이기 때문에, 현재의 일반 컴퓨팅 파워로도 쉽게 뚫린다.



16번 반복
(16-round)

1. 입력을 L과 R로 나눈다

2. R을 그대로 R로 보낸다

3. R을 라운드 함수 F로 보낸다

4. 라운드 함수 F는 R과 서브 키 K1을 입력으로 사용하여 랜덤하게 보이는 비트열을 계산한다

5. 얻어진 비트열과 L을 XOR 한다

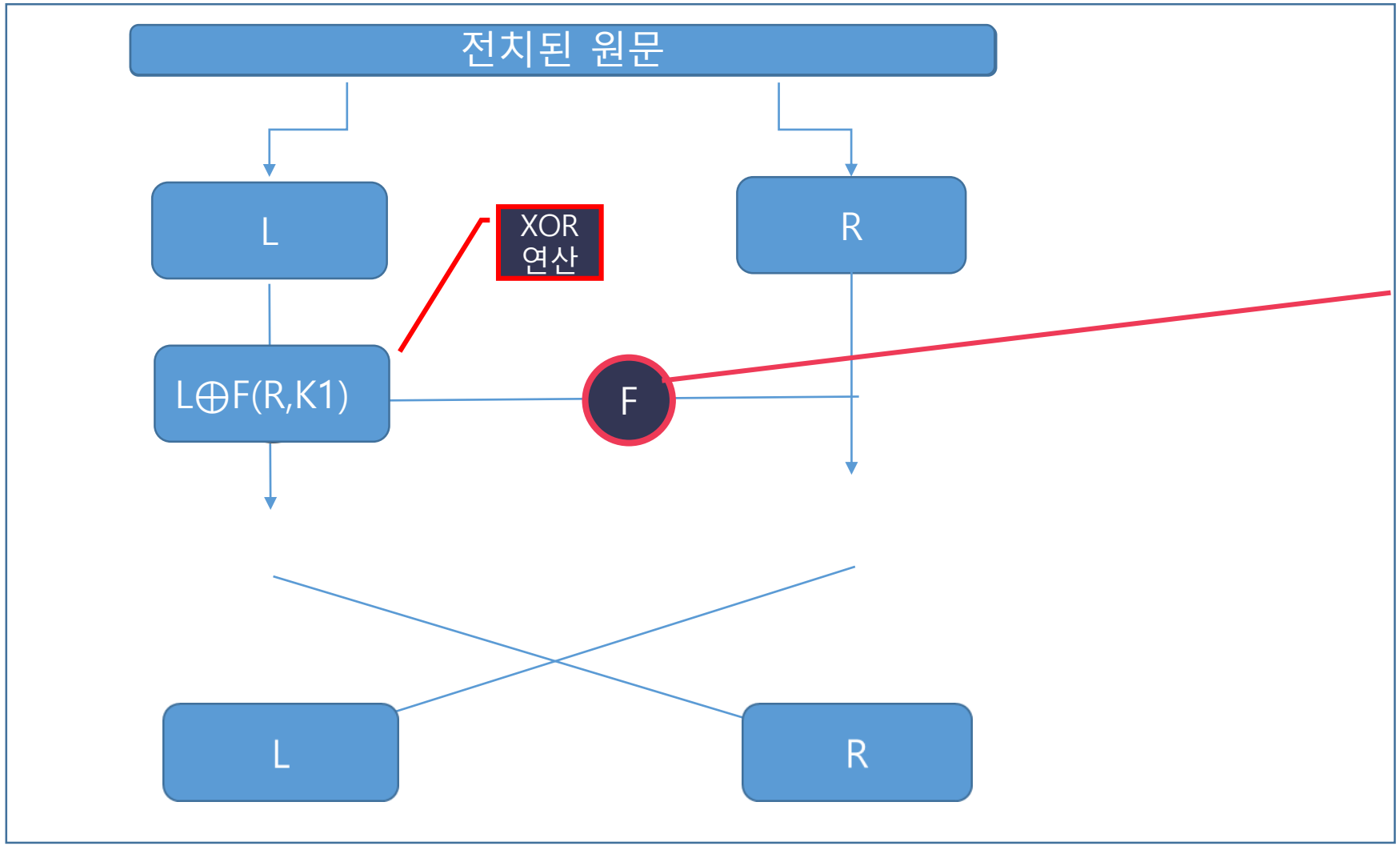
6. 그 결과를 다음 라운드의 L로 사용한다

IP(Initial Perm

58 50 42 34
60 52 44 36
62 65 46 48
64 56 48 40
57 49 41 33
59 51 43 35
61 53 45 37
53 55 47 39

첫번째 비트는
와 바꾸는 형식

DES



F함수에서 내부키의 56bit중 48비트로 R과 계산

P-box를 통해 48비트로 늘려서 계산 후 S-box치환과 축소 전치를 통해 다시 압축

여기서 잠깐

–외부 키(64bit)에서 실제 쓰이는 키(내부키)의 비트 길이는 56비트

–7비트마다 오류 검출을 위해 정보 비트(1bit) 추가

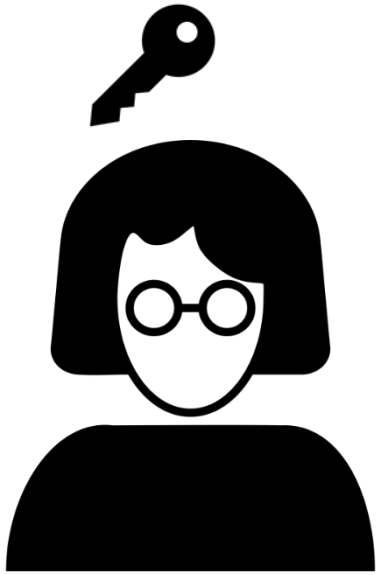
– 56비트 중 48비트씩 뽑아 키로 씀

암호의 종류

공개키

Created by Nikita Kozin
from Noun Project

Created by Angelina
from Noun Project



Created by Angelina
from Noun Project

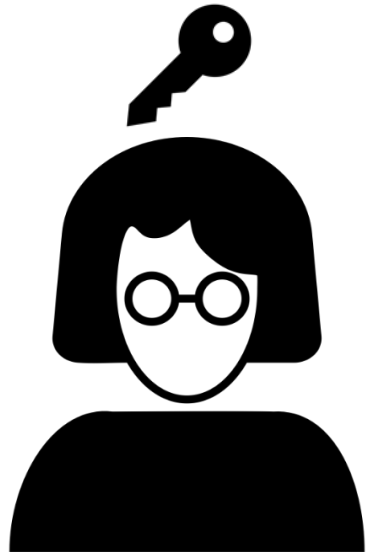
전자서명

Created by Nikita Kozin
from Noun Project

Created by Angelina
from Noun Project

Created by Monsente Design
from Noun Project

Created by Monsente Design
from Noun Project



Created by Angelina
from Noun Project

공개키로 복호화가 된다는 것은 개인 키에 의하여 암호화 되었다는 것을 의미→ 데이터 제공자의 신원이 확인

Ex)공인 인증서

RSA

1. p와 q라는 두개의 서로 다른 소수를 구한다
2. N=pq (두 소수를 곱한다.)
3. φ(N)=(p-1)(q-1) → 오일러 파이 함수라 불리며 n이 소수 일 때 1부터 n-1까지의 n과 서로소관계에 있는 정수의 개수를 말한다.
4. φ(N)보단 작고 φ(N) 와 서로소인 정수 e를 구한다
5. (e*d)mod φ(N) = 1이 되는 d를 구한다
6. 암호화 할 때의 공식은 c=m^e mod N
7. 복호화 할 때의 공식은 m=c^d mod N

<실제로 적용해보기>

```
#### NEW PROBLEM ####
q : 60413
p : 76753
##### PRODUCE THE FOLLOWING ####
n
IS THIS POSSIBLE and FEASIBLE? (Y/N):y
#### TIME TO SHOW ME WHAT YOU GOT! ###
n:4636878989
Outstanding move!!!


#### NEW PROBLEM ####
p : 54269
n : 5051846941
##### PRODUCE THE FOLLOWING ####
q
IS THIS POSSIBLE and FEASIBLE? (Y/N):y
#### TIME TO SHOW ME WHAT YOU GOT! ###
q: 93089
Outstanding move!!!


#### NEW PROBLEM ####
e : 3
n : 127381628029105465038219208869053933163863627595674808394284565252242264451730316353066837261825224949108085189204090194140348144093300942458257496809132045668323377047001659931988917957869691242321388697846262025013661359752238272878123262505771486253608876989306255043343258045873299056179365811163927846843346642043097714308144496061472213498883204034516378824477022170647023962529229798876649374620968488084311113817060003988811240441131097475853260399860805700881183638459757914724473760608875629993965426508689909635907066726616775494458794869584391504861984628287376941348907224347776435007178732791
##### PRODUCE THE FOLLOWING ####
q
p
IS THIS POSSIBLE and FEASIBLE? (Y/N):n
Outstanding move!!!
```

발표 후 남은 과제

다음 시간엔 DES암호의 전치 과정과 F함수의 계산과정들을 자세히 알아 가지고 오겠습니다..... + 네트워크

감사합니다!