암호학의 시작

김 솔

CONTENTS

001/ 용어 설명

암호학 - 정보를 보호하기 위한 언어학적 및 수학적 방법론을 다루는 학문으로 수학을 중심으로 컴퓨터, 통신 등 여러 학문 분야에서 공동으로 연구, 개발되고 있다.

평문 – 보호해야 할 메시지

암호문 – 평문을 암호학적 방법으로 변환한 것

암호화 – 변환하는 과정

복호화 - 암호문을 다시 평문으로 변환하는 과정

001/ 용어 설명

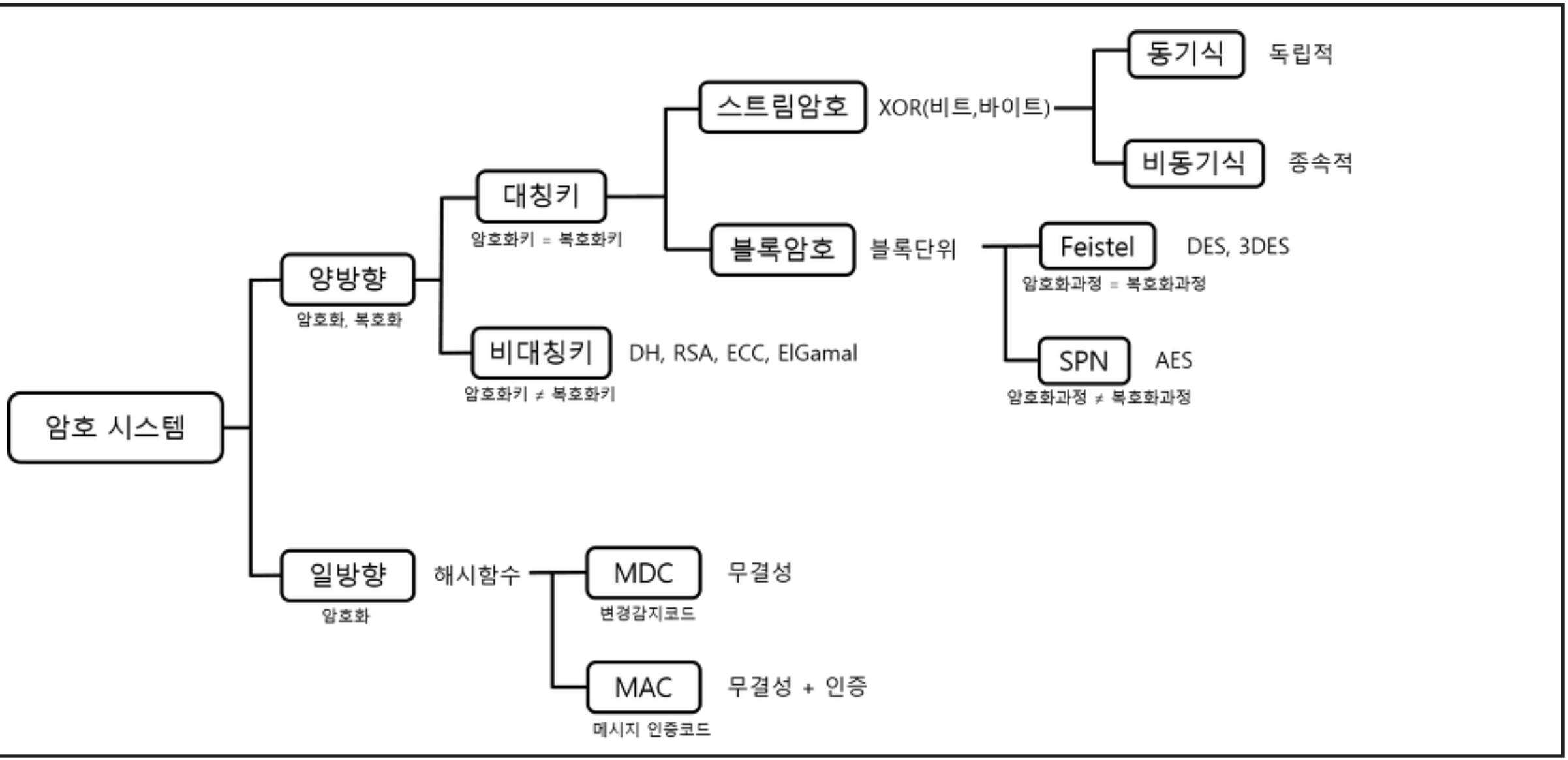
기밀성

무결성

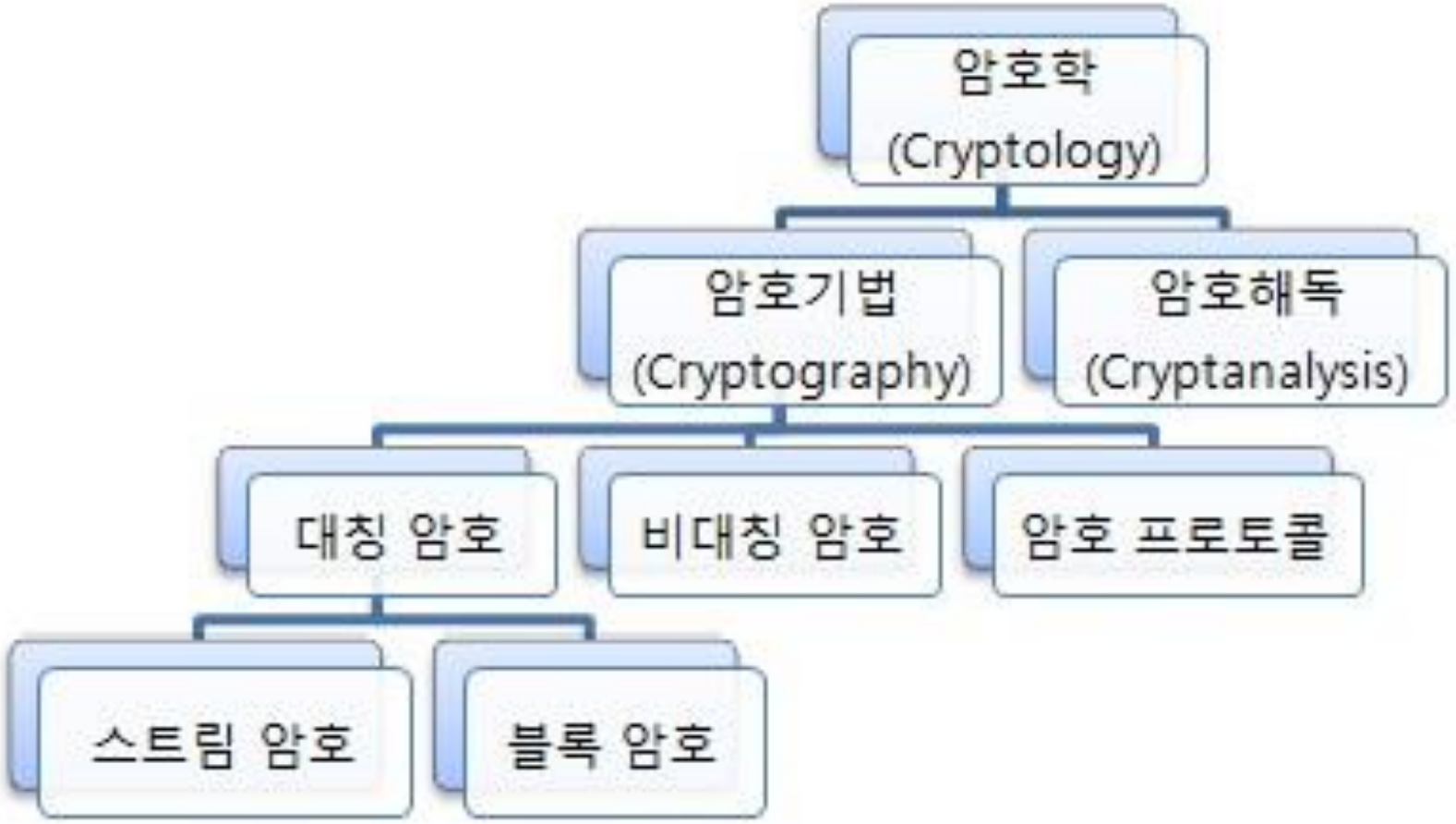
가용성

부인봉쇄

002/ 암호 시스템


암호 시스템
양방향
암호화, 복호화
대칭키
암호화키 = 복호화키
스트림암호
XOR(비트,바이트)
동기식
독립적
비동기식
종속적
블록암호
블록단위
Feistel
DES, 3DES
암호화과정 = 복호화과정
SPN
AES
암호화과정 ≠ 복호화과정
비대칭키
DH, RSA, ECC, ElGamal
암호화키 ≠ 복호화키
일방향
암호화
해시함수
MDC
무결성
변경감지코드
MAC
무결성 + 인증
메시지 인증코드

002/ 암호 시스템


암호학
(Cryptology)
암호기법
(Cryptography)
암호해독
(Cryptanalysis)
대칭 암호
비대칭 암호
암호 프로토콜
스트림 암호
블록 암호

003/ 대칭키

장점 – 공개키 암호방식에 비해 상대적으로 빠르다

단점 – 인증, 부인방지 기능 사용 불가. 다수의 사람이 사용하기 어려움

$$_nC_2 = n(n-1)/2$$

002/ 암호 시스템

암호화 키

복호화 키

평문 -> 암호문 -> 평문

003/ 대칭키

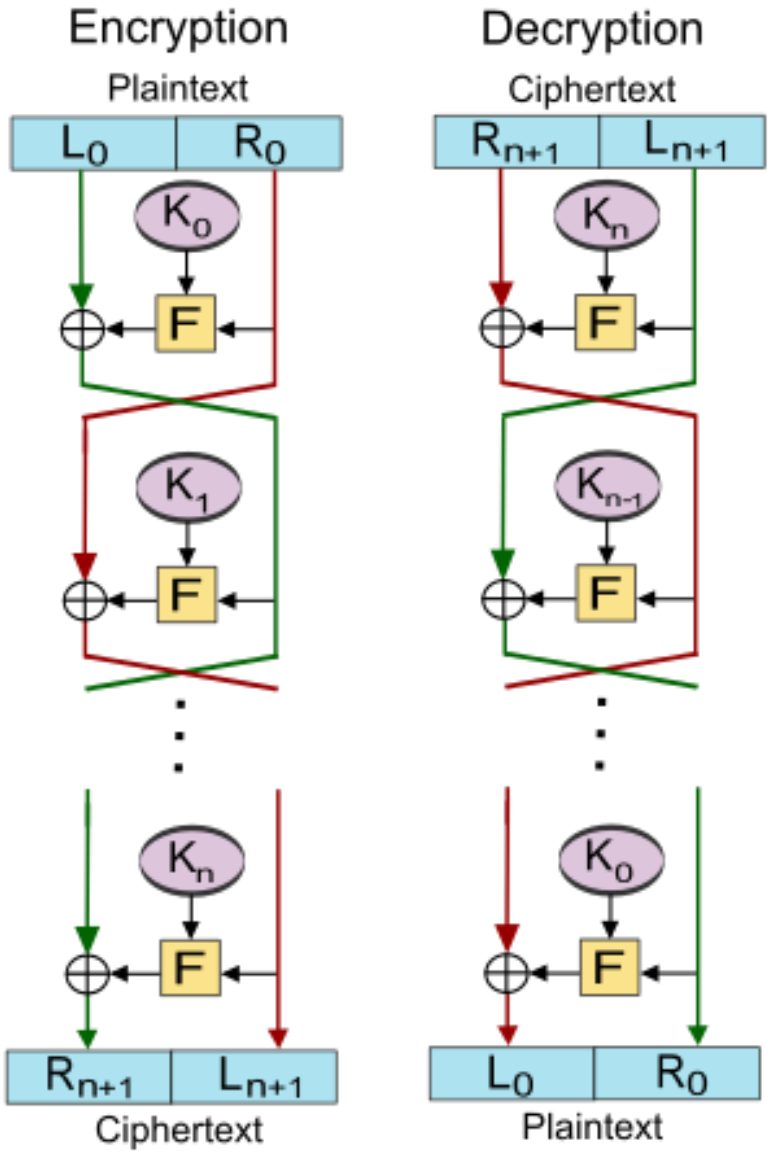
블록 암호 알고리즘 – 세로 방향 자리 옮김 알고리즘, 모르스부호 응용 알고리즘

스트림 암호 – 단순 알파벳 암호화 알고리즘, 복합 알파벳 암호화 알고리즘

003/ 대칭키

Feistel 구조 – a b c d e f g h

I J K L m n o p

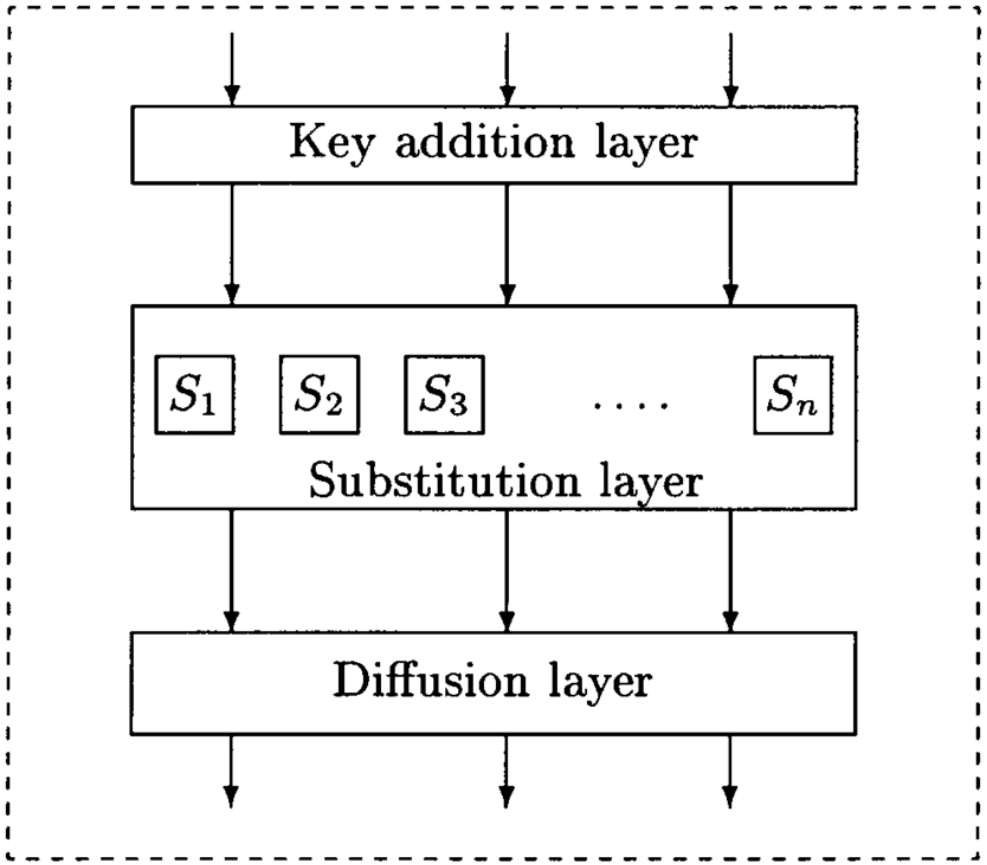


003/ 대칭키

SPN 구조 – 입력을 여러 개의 소블록으로

나누어 각 소블록을 S-Box에서 대치시키고

그 결과를 다시 P-Box를 전치하는 과정을 반복



THANK YOU