15강

Security Goals (보안 목적)

- Confidentiality (기밀성)
- Integrity (무결성)
- Non repudiation (부인방지)
- Authentication (인증)

Confirming the identity of a person

Authentication Factors

Ownership factors 가지고 있으면 인증

ex) wrist band, ID card ···

Knoledge factors

특정정보를 알면 인증 ex) PIN

↳ Smudge Attack 주의

Inherence factors

사용자 고유를 인증 (생체정보)

Human Authentication

CAPTCHA (보안문자)

- 한글자의 끝 알수없음
- 컴퓨터와 인간을 구별하기 위함 = Turing Test

4강

나눗셈 특성

- b|g , b|h → b(mg|mh)

* a와 n이 서로소일때

$a \times b \equiv (a \times c) \bmod n$ 일 $b \equiv c \pmod n$

a의 곱셈에 대한 역원 찾을 때

Extended Euclidean Algorithm

$d = ax + by$, $d = (a, b)$ gcd

ex) a = 1759, b = 550

r	q	x	y
1759		1	0
550		0	1
109	3	1	-3
5	5	-5	16
4	21	106	-339
1	1	-111	355
0		-3 - (16 · 21)	

1759 ÷ 550 = 3 ... 109

550 ÷ 109 = 5 ... 5

109 ÷ 5 = 21 ... 4

5 ÷ 4 = 1 ... 1

GROUP : 군 하나의 연산자.

Closure (닫힘). Associative 결합

Identity 항등. Inverse element 역원

Field : 2개 연산자.

곱 덧셈 같게

GF(p^n)

계수: Z_p , m(x)의 차수 : n

Feistel Cipher Structure

암호화와 역함수 ⇒ 암호화 과정 역함수 X

DES (data encryption Standard)

64 bit block size, 58 key, 16 round

안전도: Brute force attack → 2^{56}

AES (Advanced encryption standard)

GF(2^8) $m(x) = x^8 + x^4 + x^3 + x + 1$

128 bit 블록사이즈 고정

AES-128 , AES-256 ...

각 과정에서 역함수 필요

ECB (electronic code book)

deterministic 하여서 안전하지 X

CBC (Ciper block Chaning)

IV ⊕ plain