2. 암호 기초

2.1 개요

2.2 암호 용어

2.3 고전 암호

2.4 고전 암호의 역사

2.5 현대 암호의 역사

2.6 암호학의 분류

2.7 암호 분석의 분류

2.8 요약

2.1 개요

- 이 장에서 다룰 내용
  - 암호의 기초
  - 정보보안이 '무엇'인가뿐만 아니라 '왜' 그렇게 해야 하는가를 이해하는 데 필요한 세부 내용을 다룸

2.2 암호 용어

■ 암호화(Encryption)

- 평문(Plaintext)를 암호문(Chipertext)로 변환
- 데이터를 암호화하는 데 사용하는 것을 암호 또는 암호체계라 함
- 평문은 원본 데이터, 암호문은 암호화된 데이터를 의미

■ 복호화

- 암호문을 원본 데이터인 평문으로 복원하는 것
- 암호체계를 구성하는 데에는 키를 사용
  - 키(Key) : 암호화 복호화를 위한 비밀 값

그림 2-1 블랙박스 암호체계

2.2 암호 용어

- 대칭키 암호(Symmetric Key Cryptography)
  - 암호화와 복호화에 같은 키 사용

- 공개키 암호(Public Key Cryptography)
  - 암호화 복호화에 서로 다른 키 사용
  - 암호화에 사용되는 공개되어 있는 키
  - 공개키 암호에서 암호화 키는 공개되어 있지만 복호화 키는 비밀키로 유지해야 함(개인키)
    - 공개키 : 누구나 사용 가능
    - 개인키 : 소유자만 보관
- 암호체계의 목표
  - 키를 사용하지 않고는 암호문을 복호화할 수 있는 방법이 없도록 하는 것
  - 보안성 = 키 관리

2.2 암호 용어

- 케르크호프스 원칙(현대 보안의 토대)
  - "암호체계 자체는 비밀이 아니다. 공격자는 암호체계를 쉽게 파악할 수 있기 때문이다"
  - 보안 설계 자체가 공개되어 있으니 더 많은 사람이 분석할수록 보안 결함을 더 확실하게 발견할 수 있다는 의미
  - 암호뿐만 아니라 다른 보안 분야에도 확대 적용 가능

2.3 고전 암호

■ 고전 암호의 종류

- 수천 년 동안 사용된 전통적 암호 방식
- 현대 암호학의 기초 개념을 이해하는데 중요한 역할
- 대표 유형 네 가지 :
  - 단순 치환 암호 : 평문의 각 문자를 다른 문자로 치환
  - 이중 전위 암호 : 평문을 특정 규칙에 따라 재배열 하고, 이를 두 번 수행
  - 일회성 암호 : 무작위로 생성된 키(평문 길이와 동일)을 한 번만 사용
  - 코드북 암호 : 단어 구문 전체를 코드 번호로 대체하는 방식

2.3 고전 암호 – 단순 치환 암호

■ 가장 오래된 암호체계

- 가장 기본적인 방법은 현재 문자를 *n*번째 앞에 있는 문자와 서로 치환해서 암호화하는 것
- 예) *n*=3을 키로 사용하면 치환되는 문자

```
평문:  a b c d e f g h i j k l m n o p q r s t u v w x y z
암호문: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

- 키는 문자의 이동 자릿수를 나타내는 '3' / 키 '3'을 사용해 다음 평문을 암호화

```
fourscoreandsevenyearsago      (2.1)
IRXUVFRUHDQGVHYHQBHDUVDJR
```

2.3 고전 암호 – 단순 치환 암호

■ 시저 암호

- 앞의 예처럼 단순하게 암호화하고 복호화하는 방법
- 시저 암호에서 알파벳 순서상으로 가능한 n번의 이동을 나타내면 $n \in \{0,1,2,\ldots,25\}$가 될 것
- 예) 트루디가 다음과 같은 암호문을 도청했다고 가정

  CSYEVIXIVQMREXIH

  - 평문이 n 이동 방법으로 암호화되어 있다면, 평균 13번의 시도로 암호화 키를 찾아낼 수 있음
  - 이렇게 원초적인 암호 공격법을 전수키 조사(exhaustive key search)라고 함

- 암호화 : $E(x) = (x + n) \; mod \; 26$
- 복호화 : $\mathrm{D}(x) = (x - n) \; mod \; 26$

2.3 고전 암호 – 단순 치환 암호

- 단순 치환 암호를 n 이동 방법으로만 한정할 필요는 없음
- 예) 26개 문자의 순열도 키로 사용 가능

평문:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
암호문:	Z	P	B	Y	J	R	G	K	F	L	X	Q	N	W	V	D	H	M	S	U	T	O	I	A	E	C

- 단순 치환 암호가 모든 순열을 하나의 키로 사용할 수 있다면 가능한 키의 수는 $26! \approx 288$개(전수키 조사가 불가능)

2.3 고전 암호 – 단순 치환 암호에 대한 공격 분석

- 공격 기법 – 무차별 대입 (Brute Force)
  - 가능한 키: 0 ~ 25 (총 26개)
  - 모든 키를 시도하면 반드시 평문을 얻을 수 있음
  - 평균 1번 시도하면 해독 가능
  - 취약점: 연산량이 적어 누구나 쉽게 해독 가능

2.3 고전 암호 – 단순 치환 암호에 대한 공격 분석

- 예) 트루디가 단순 치환 암호문으로 추정되는 문장을 도청

```
PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQWAXBVCXQWAXFQJVW
LEQNTOZQGGQLFXQWAKVWLXQWAEBIPBFXFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVWLX
GDPEQVPQGVPPBFTIXPFHXZHVFAGFOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQP
BQWAQJJTODXQHFOQPWTBDHHIXQVAPBFZQHCFWPFHPBFIPBQWKFABVYYDZBOTHPBQPQJTQ
OTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJIWFFACFCCFHQWAUVWFLQHGFXVAFXQHFUFH
ILTTAVWAFFAWTEVOITDHFHFQAITIXPFHXAFQHEFZQWGFLVWPTOFFA        (2.2)
```

- 암호문이 영어로 쓰여 있으므로 트루디는 일반적인 영어 문자 빈도수([그림 2-2])와 암호문의 영어 문자 빈도수([그림 2-3])를 찾아낼 수 있음
  - 영어에서 가장 많이 등장하는 문자는 E, 빈도가 높은 문자가 E일 가능성 높음

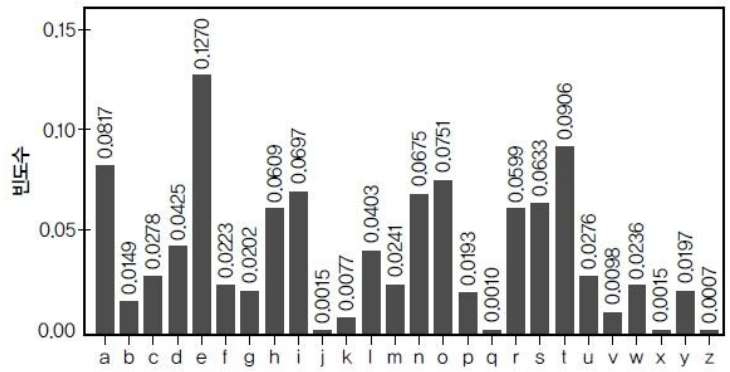


그림 2-2 일반적인 영어 문자 빈도수

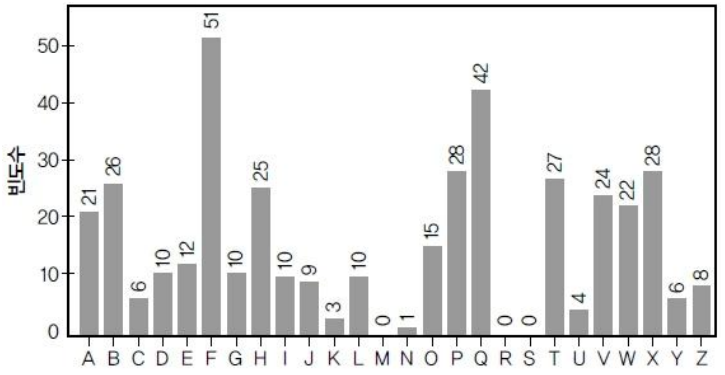


그림 2-3 암호문 (2.2)의 영어 문자 빈도수

2.3 고전 암호 – 단순 치환 암호 실습

■ 실습 1

- (1) 카이사르 암호화
  - 단순 치환 암호의 암호화 복호화 원리 이해

  1. 암호문(KHOOR) 평문으로 변환(Shift 값 적용)
  2. 암호문을 다시 복호화하여 원문 복원

  - ord() -> chr to int, chr() -> int to chr 사용
- (2) 카이사르 암호화 – 부르트포스 공격실습
  - 26가지 shift를 모두 시도하여 평문 찾기

■ 실습2

- (3) 카이사르 암호화 – 빈도 탐색 공격 실습
  - 영문에서 가장 많이 나오는 알파벳 빈도를 이용한 공격 실습
    - E -> T-> A -> O -> I
- (4) 두가지 공격 방법 비교

2.3 고전 암호 – 이중 전위 암호

■ 현대 암호에서 사용되는 중요한 개념을 담고 있음

- 암호화를 하려면 먼저 평문을 주어진 크기의 행렬 형태로 배열하고 행과 열을 기술된 순서에 따라 바꿈
- 예) 평문 attackatdawn을 3×4 행렬로 정리

$$\begin{bmatrix} a & t & t & a \\ c & k & a & t \\ d & a & w & n \end{bmatrix}$$

- 행의 순서를 (1,2,3) → (3,2,1)로 바꾸고 열의 순서를 (1,2,3,4) → (4,2,1,3)으로 바꿈

$$\begin{bmatrix} a & t & t & a \\ c & k & a & t \\ d & a & w & n \end{bmatrix} \longrightarrow \begin{bmatrix} d & a & w & n \\ c & k & a & t \\ a & t & t & a \end{bmatrix} \longrightarrow \begin{bmatrix} n & a & d & w \\ t & k & c & a \\ a & t & a & t \end{bmatrix}$$

- 마지막 행렬이 암호문이 되며 결과는 다음과 같음

  NADWTKCAATAT (2.3)

- 복호화 과정은?

2.3 고전 암호 – 이중 전위 암호

- 단순 치환 암호와 달리 이중 전위 암호는 메시지에 나타나는 문자를 감추지 않음
- 암호문에 대한 평문의 통계적 특성이 암호문 전체에 흩어져 있어서 평문 속에 포함된 통계적 정보에 의존하는 공격은 막을 수 있음

2.3 고전 암호 – 이중 전위 암호 실습

- (1) 이중 전위 암호 암호화
  - 이중 전위 암호의 암호화 복호화 원리 이해
  - attackatdawn

1. 평문과 행 변환 순서 열 변환순서를 입력 받아 암호화
2. 암호문을 다시 복호화하여 원문 복원
   - 행의 순서를 (1,2,3) → (3,2,1)로 바꾸고 열의 순서를 (1,2,3,4) → (4,2,1,3)으로 바꿈

2.3 고전 암호 – 일회성 암호

■ 암호체계 중에서도 가장 안전

- 버넘 암호(vernam cipher)라고 불림
- 안전성이 증명된 암호체계(대부분 실용적이지 못했음)
- 예) 8개의 알파벳 문자로 국한
  - 평문 메시지를 일회성 암호 방법으로 암호화 → heilhitler

표 2-1 설명을 위한 알파벳 일부

문자	e	h	i	k	l	r	s	t
이진수	000	001	010	011	100	101	110	111

  - 비트열로 변환 → P = (001 000 010 100 001 010 111 100 000 101)

2.3 고전 암호 – 일회성 암호(OTP One-Time Pad)

- 일회성 암호에는 암호화하려는 메시지와 동일한 길이를 갖는 무작위 비트열로 만들어진 키가 필요
- 암호화 : 평문 $\oplus$ 키 = 암호문
- 복호화 : 암호문 $\oplus$ 키 = 평문
- 비트 x와 비트 y 간의 XOR 연산은 $x \oplus y$로 표시

- 예) 트루디가 다음과 같은 키를 사용한다고 가정

	h	e	i	l	h	i	t	l	e	r
평문(P)	001	000	010	100	001	010	111	100	000	101
키(K)	111	101	110	101	111	100	000	101	110	000
암호문(C)	110	101	100	001	110	110	111	001	110	101
	s	r	l	h	s	s	t	h	s	r

- 암호문 비트를 문자로 다시 변환하면 최종 암호문은 srlhssthsr

2.3 고전 암호 – 일회성 암호

- 예) 이브(스파이)가 이 메시지를 받게 된다면 같은 키를 이용해 암호문을 복호화해 원래의 평문을 얻음

	s	r	l	h	s	s	t	h	s	r
암호문(C)	110	101	100	001	110	110	111	001	110	101
키(K)	111	101	110	101	111	100	000	101	110	000
평문(P)	001	000	010	100	001	010	111	100	000	101
	h	e	i	l	h	i	t	l	e	r

- 예) 찰리(트루디의 적)는 트루디가 메시지를 암호화할 때 사용한 실제 키가 다음과 같다고 주장

$$K' = (101\ 111\ 000\ 101\ 111\ 100\ 000\ 101\ 110\ 000)$$

- 찰리가 준 키로 이브가 암호문을 복호화한 결과

	s	r	l	h	s	s	t	h	s	r
암호문(C)	110	101	100	001	110	110	111	001	110	101
키(K')	101	111	000	101	111	100	000	101	110	000
평문(P')	011	010	100	100	001	010	111	100	000	101
	k	i	l	l	h	i	t	l	e	r

2.3 고전 암호 – 일회성 암호

- 예) 연합군이 트루디가 제시한 키로 암호문을 복호화한 결과

	s	r	l	h	s	s	t	h	s	r
암호문(C)	110	101	100	001	110	110	111	001	110	101
키(K'')	111	101	000	011	101	110	001	011	101	101
평문(P'')	001	000	100	010	011	000	110	010	011	000
	h	e	l	i	k	e	s	i	k	e

■ 일회성 암호가 한 번밖에 사용될 수 없는 이유

- 예) 두 개의 평문 P_1, $P2$가 $C_1 = P_1 \oplus K$, $C_2 = P_2 \oplus K$로 각각 암호화되었다고 가정
  - 두 개의 메시지가 같은 '일회성' 암호인 K로 암호화되어 있는데 암호 분석 분야에서는 이것을 깊이(depth)가 있다고 표현
  - 깊이가 있는 일회성 암호에서는 두 개의 암호문을 더하면 키가 사라짐

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

2.3 고전 암호 – 일회성 암호

■ 깊이가 있는 일회성 암호

- [표 2-1]과 같은 비트 문자 변경표를 사용해 얻은 결과
  - P_1 = like = (100 010 011 000) and P_2 = kite = (011 010 111 000)
- 같은 키인 K=(110 011 101 111)로 암호화한다고 가정하면 두 가지 암호문이 만들어짐

	l	i	k	e
P_1	100	010	011	000
K	110	011	101	111
C_1	010	001	110	111
	i	h	s	t

	k	i	t	e
P_2	011	010	111	000
K	110	011	101	111
C_2	101	001	010	111
	r	h	i	t

- C_1과 C_2만을 알고 있는 트루디가 P_1 = kill = (011 010 100 100)으로 추측했다고 가정하면 트루디는 다음과 같은 대응 추정키를 얻음

		k	i	l	l
추정	P_1	011	010	100	100
	C_1	010	001	110	111
추정	K	001	011	010	011

2.3 고전 암호 – 일회성 암호

- 트루디는 이렇게 추정된 키 K를 다시 이용해 다음과 같이 C_2를 복호화

	C_2	101	001	010	111
추정	K	001	011	010	011
추정	P_2	100	010	000	100
		l	i	e	L

2.3 고전 암호 – 일회성 암호 실습

- (1) 일회성 암호 암호화
  - 일회성 암호의 암호화 복호화 원리 이해

1. 평문을 비트열로 변환하는 방법 이해
2. 키와 평문 비트열을 XOR연산 암호문 생성
3. 이를 복호화 하는 과정 실습

- 평문 문자 -> 비트 변환 테이블

e	h	i	k	l	r	s	t
000	001	010	011	100	101	110	111

- 순서

1. 평문(heilhitler) -> 비트열
2. 키를 준비(랜덤)
3. 암호화 (XOR 연산)
4. 복호화

2.3 고전 암호 – 코드북 암호

- 코드북 암호는 단어와 해당 단어에 할당된 코드가 수록된 사전과 같음
- 가장 중요한 점은 코드북 자체를 잃어버리지 않는 것
- 코드북은 제2차 세계대전 당시에 널리 사용됨

■ 덧셈(additive)

- 기존 코드북을 오래 사용하는 방법
- 메시지를 암호화하고 복호화하려면 덧셈북과 코드북이 모두 필요

2.3 고전 암호 – 코드북 암호 실습

- (1) 코드북 암호 암호화
  - 코드북 암호의 암호화 복호화 원리 이해
  - 코드북 암호 : 단어 <-> 코드 값 매핑
  - 덧셈열(Additive Sequence) : 임의의 숫자열을 코드 값에 더해서 보안을 강화하는 방식 -> 같은 평문이라도 매번 다른 암호문 생성

- 순서
  1. 코드북 생성(단어 <-> 코드값 매핑)
  2. 평문 메시지 입력
  3. 랜덤 덧샘열 생성
  4. 암호화 : 코드값 + 덧셈열
  5. 복호화 : 암호문 – 덧셈열

attack	dawn	meet	secret
1234	5678	9101	1121

2.4 고전 암호의 역사

- 고전 암호가 역사적 사건에 개입된 세 가지 경우
  - 1876년 미국 대통령 선거에서 보안이 취약한 암호가 사용
  - 제1차 세계대전에서 사용된 짐머맨 전보에 관한 이야기
  - VENONA 메시지로 미국에 있는 소련 스파이들이 일회성 암호를 사용하여 전송한 메시지

2.4 고전 암호의 역사 – 1876년 선거에서의 암호

- 특정 후보자의 지지자들이 해당 주의 고위 공무원에게 많은 양의 암호화 메시지를 전송
- [표 2-2]는 이때 사용한 코드북의 일부

표 2-2 1876년 선거 코드북

평문	암호문
Greenbacks	Copenhagen
Hayes	Greece
votes	Rochester
Tilden	Russia
telegram	Warsaw
⋮	⋮

- 10개 단어로 된 메시지의 순열: 9, 3, 6, 1, 10, 5, 2, 7, 4, 8
- 실제 사용된 암호문 중 하나

  Warsaw they read all unchanged last are idiots can't situation
- 전위와 치환을 원위치로 하여 앞의 메시지를 해독한 '바르샤바' 전문

  Can't read last telegram.

  Situation unchanged.

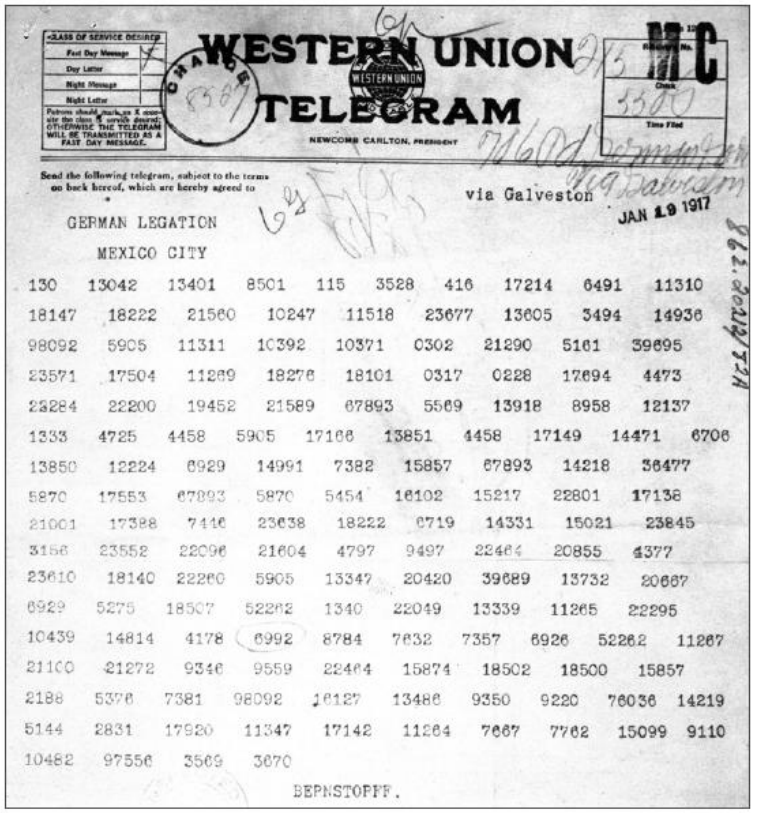
  They are all idiots.

2.4 고전 암호의 역사 – 짐머맨 전보

- [표 2-3]은 제1차 세계대전에서 많이 사용된 코드북 암호의 일부 내용
- 예) [표 2-3]의 코드북을 사용해 Februar이라는 독일어를 암호화
  - 이 단어는 5자리 숫자 코드 13605로 대치

표 2-3 독일 코드북 일부

평문	암호문
Februar	13605
fest	13732
finanzielle	13850
folgender	13918
Frieden	17142
Friedenschluss	17149
⋮	⋮



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7416 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3070

BEPNSTORFF.

그림 2-4 짐머맨 전보[95]

2.4 고전 암호의 역사 – VENONA 프로젝트

- 일회용 암호를 실세계에서 사용한 흥미로운 사례
- 1940년대까지 미국에 입국하는 소련 스파이들은 일회용 암호키로 메시지를 암호화해서 모스크바에 있는 상사에게 보고
- 당시 미국 정부의 기밀 정보가 이러한 방식으로 암호화되어 유출
- 미국 암호 분석자들은 도청한 많은 암호 메시지를 해독
- 약 3,000개의 VENONA 메시지를 성공적으로 분석

2.5 현대 암호의 역사

- 1929년에 미국은 '신사는 타인의 우편물을 읽지 않는다'라는 문구와 함께 정부의 공식적인 암호 분석 활동을 종료
  - ↳ 일본의 진주만 공격을 겪으며 이것이 실수였음이 증명
- 1941년 12월 7일 일본의 공격에 앞서, 미국은 암호 분석 프로그램을 다시 시작
  - ↳ 암호 분석의 황금시대
- 태평양 지역 전장에서는 '퍼플(purple)암호'라고 불리는 암호체계를 일본 정부 고위급이 통신할 때 사용
- 유럽에서는 독일군의 이니그마 암호체계(코드명 ULTRA)로부터 해독한 정보가 전쟁 중인 연합군에게 아주 중요한 정보가 됨
- 이니그마 암호는 폴란드 암호학자가 최초로 해독

2.5 현대 암호의 역사

■ 이니그마 암호체계의 '배선도'

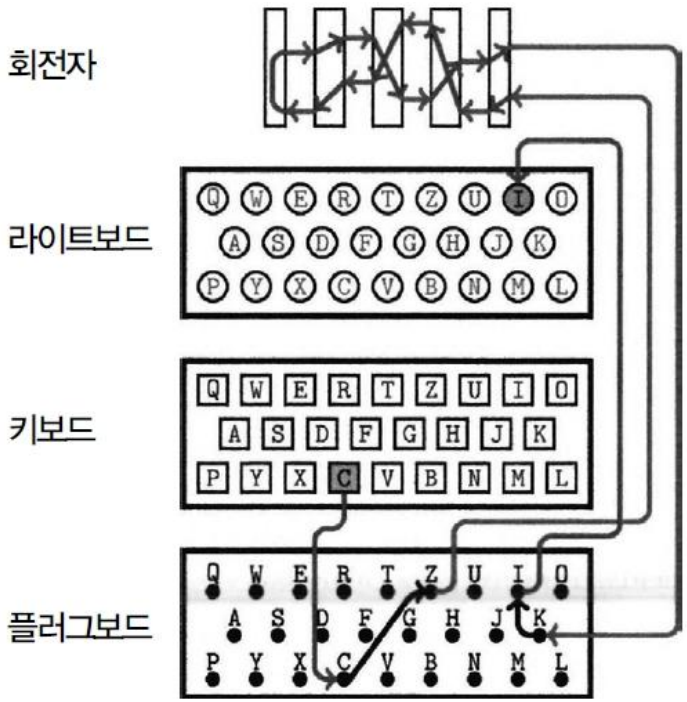


그림 2-5 이니그마 암호장비 및 사용된 회전자

▪ 동작원리

1. 사용자가 A 키를 누름.전기 신호가 플러그 보드를 거쳐 일부 글자가 교환됨.(예: A ↔ G)
2. 신호가 여러 개의 회전자(rotor)를 통과하며 복잡하게 치환됨.
    1. 각 회전자는 26개의 입력 → 26개의 출력 배선을 가짐.
    2. 매번 키를 누를 때마다 회전자가 한 칸 회전 → 매번 다른 치환이 이루어짐.
3. 신호가 반사판(reflector)에 도달 → 다시 반대로 회전자를 거쳐 되돌아옴.
    1. 이때 또 다른 경로로 신호가 섞임.
4. 최종적으로 램프 보드에 불이 들어와 암호문 글자가 출력됨.
    1. 예: A를 눌렀는데 Q가 불이 켜짐.

2.5 현대 암호의 역사

- 제2차 세계대전 후 암호학은 감춰진 예술에서 현실 세계 과학으로 전환
- 클로드 섀넌 Claude Shannon의 논문[109]이 전환점이 됨
  - 일회성 암호체계가 안전함을 증명
  - 암호체계 설계의 두 가지 기본 원칙인 혼돈(confusion)과 확산(diffusion) 이론을 제시
    - 혼돈 : 하나의 문자를 전혀 다른 문자로 바꾸기, 확산 : 문자 한자리 위치 바꾸기

- 정부나 군대에서 주로 사용된 암호학은 1970년대에 컴퓨터에 엄청난 혁신이 생기면서 극적인 변화를 맞게 됨 (안전한 데이터 보호의 필요성)
- 미국 국가표준국(NBS)이 암호 알고리즘 개발을 맡음
- 잘못된 절차로 데이터 암호화 표준(DES)으로 불리는 암호가 만들어짐
- 공개키 암호가 등장(정확히 말하면 재발견)
- 암호(CRYPTO) 학술대회가 매년 개최
- 국가 차원에서 비밀리에 관리하는 영역에서 벗어나 민간 부분에 깊숙이 파고든 암호

2.6 암호학의 분류

- 암호학은 크게 세가지로 나눌 수 있음
  - 대칭키 암호 (Symmetric-key Cryptography)
  - 공개키 암호 (Public-key Cryptography)
  - 해시 함수 (Hash Function)
- 고전 암호는 모두 대칭키 암호
  - 송신자와 수신자가 같은 키를 공유하여 암호화 복호화
- 현대의 대칭키 암호는 스트림 암호(stream cipher)와 블록 암호(block cipher)로 나뉨
  - 제2차 세계대전 직후에는 스트림 암호가 절대적으로 많이 사용
  - 오늘날에는 블록 암호가 대칭키 암호의 대표가 됨
  - 블록 암호는 소프트웨어 구현에 최적화
  - 스트림 암호는 하드웨어 구현에 최적화

2.6 암호학의 분류

■ 공개키 암호

- 각 공개키에는 복호화에 사용하는 개인키가 항상 같이 존재
- 공개키 암호체계는 대칭키 암호가 수행하는 모든 기능을 수행 가능
- 효율성이 없어서 공개키 암호체계를 사용하지 않음

  ↳ 오늘날 암호문을 만들 때는 대칭키 암호를 주로 사용
- 개인키로 서명 -> 공개키로 복호화

■ 해시 함수

- 길이에 상관없이 값을 입력 받아 고정된 길이의 출력 값을 만들어냄
- 암호화 해시 함수는 몇 가지 매우 엄격한 요구사항을 충족해야 함
  - 입력 받은 값이 한 비트 이상 변경되면 출력 값은 전체 비트의 절반 정도 변경되어야 함
  - 입력 받은 두 값이 다르면 동일한 출력 값을 만들어낼 수 없어야 함

2.7 암호 분석의 분류

■ 암호 분석의 목표

- 평문이나 키, 또는 두 가지를 모두 찾아내는 것
- 암호문과 알고리즘을 알고 있다면 트루디(암호 분석자)는 암호문 공격(ciphertext only attack)을 할 수 있음

■ 알려진 평문(known plaintext)

- 공격에 성공할 가능성은 훨씬 높음
- 공격자가 일부 평문과 그에 해당하는 암호문을 알고 있을 때, 이를 바탕으로 키나 다른 평문 추론

■ 선택된 평문(chosen plaintext)공격

- 트루디는 평문을 임의로 선택해 이에 해당하는 암호문을 볼 수도 있음
- 공격자에게 유리한 것은 적응적으로 선택된 평문(adaptively chosen plaintext) 공격
- 암호체계에 임시 접근 가능할 때 사용

2.7 암호 분석의 분류

■ 공개키 암호체계에 적용되는 특별한 공격 방법

- 순방향 탐색 공격(forward search attack)
  - 모든 경우를 암호화 해보고 암호문과 비교
  - 대칭키 암호에서는 사용할 수 없지만 일부 응용 프로그램의 해시 함수를 공격하는 데에는 사용할 수 있음
  - 순방향 탐색 공격을 대비하여 공개키 암호에서 공격자가 모든 가능한 평문 메시지를 암호화할 수 없도록 하려면 평문 메시지 공간이 충분히 커야 함

2.8 요약

- 다양한 고전 암호체계를 살펴봄
  - 단순 치환, 이중 전위, 코드북, 일회성 암호
- 암호학과 암호 분석에 관한 기본 요소 논의함
- 다음 장에서 살펴볼 내용
  - 현대 대칭키 암호, 공개키 암호체계, 해시 함수 등