# 11. 암호 역사

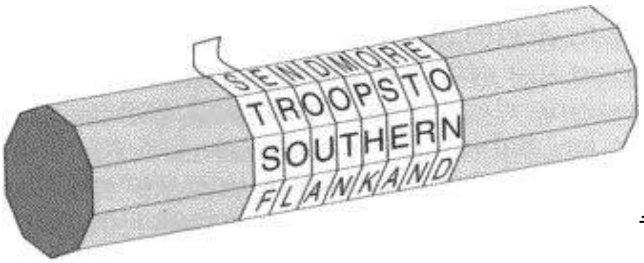
암호는 주로 군사, 외교통신에 사용되었고, 지금은 사업 등에도 많이 사용되고 있다.

| 암호 및 도구 | 설 명 |
|---|---|
| **스키탈레 암호**<br>**(Scytale cipher)** | • 알려진 최초의 암호이다.(기원전 400년, 스파르타 시대)<br>• 원통에 종이테이프를 감아 테이프 위에 메시지를 세로쓰기 방식으로 기술하였다.**(전치암호)**<br>• 테이프를 풀어서는 메시지 내용을 판독할 수 없다. |
| **시저 암호**<br>**(Caesar cipher)** | • 로마 장군인 Caesar(시저, 카이사르)가 사용한 암호이다.<br>→ 기원전 100년<br>• 시저 암호는 **대치암호의 일종**이다. |
| **베네치아 암호** | • 14~15세기, 이탈리아에서 고안, 발달하였다.<br>• 최초의 완전암호라고 한다. |
| **비지넬 암호**<br>**(Vigenere cipher)** | • 16세기, 프랑스에서 비지넬 암호표가 고안되었다.<br>• 당시에는 해독 불능 암호로 평가되었다.<br>• 현재에도 대치암호의 기본형식으로 사용되고 있다.<br>• 비지넬은 근대적 암호의 시조라고 한다. |
| **에니그마**<br>**(ENIGMA)** | • 에니그마는 암호문 작성과 해독이 가능한 기계이다.**(기계암호)**<br>• 에니그마는 자판, 램프, 반사판, 배전반 등으로 구성되었다.<br>• 문장을 입력하면 회전자가 돌면서 암호문, 평문을 만들어낸다.<br>• 보안성에 따라 여러 모델이 있다.<br>• 제2차 세계 대전 중 **독일군이 군사기밀** 암호화에 사용하였다.<br>• 2차 대전에 사용된 암호기 중에 가장 해독이 어려운 시스템이었다. |
| **Purple machine** | • 1937년부터 일본이 외교 통신 암호화를 위해 사용(기계암호) |
| **M-209**<br>**(Hagelin machine)** | • 1942년부터 미군이 암호화에 사용(기계암호) - 한국전에도 사용<br>• 기계암호는 컴퓨터 출현과 동시에 무용지물이 되었다. |
| **혼돈과 확산** | • 1948년, Shannon이 **통신의 수학적 이론** 발표 – **현대 암호** 시작<br>• 혼돈(confusion)과 확산(diffusion) 기법을 사용하면 복잡도가 높은 암호시스템 구현이 가능하다. |
| **Feistel 구조** | • 1970년 H. Feistel 등은 DES의 모체가 된 LUCIFER를 개발<br>• 블록 암호의 기본구조로 사용되는 Feistel 구조 고안 |
| **현대 암호** | • 1970년대 스탠포드 및 MIT 대학에서 본격적으로 시작<br>• 스탠포드 대학의 디페(Diffie)와 헬만(Hellman)이 논문 발표<br>→ 공개키 암호 방식의 개념 발표<br>→ 논문 이름은 New Direction in Cryptography<br>• 미국 상무성 표준국에 의해 DES 출현<br>• MIT 대학의 Rivest, Shamir, Adleman에 의해 RSA 발표<br>• 라빈(Rabin)의 **공개키 암호** 방식 발표 |

탐구

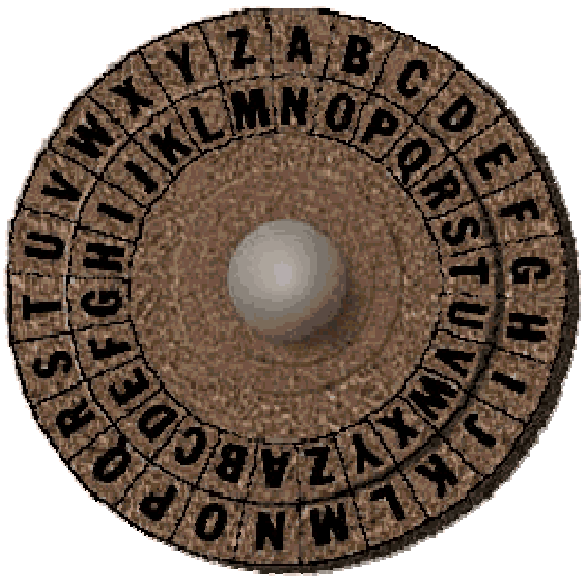
## 스키탈레 암호(scytale cipher) / 시저 암호(caesar cipher)

- 스키탈레 암호는 일정한 너비의 종이테이프를 원통에 서로 겹치지 않도록 감아서, 그 테이프 위에 세로쓰기로 메시지를 기술하는 방식이다.
- 테이프가 풀어진 상태에서는 기록된 내용을 판독할 수 없지만,
- 메시지를 기록할 때 사용한 것과 동일한 지름의 원통에 감아보면 내용을 읽을 수 있다.




스키탈레 암호(전치암호)

- 시저 암호는 알파벳 문자를 다른 알파벳 문자로 바꾸는 방식이다.




시저 암호(대치암호)


## 우리나라 암호 역사

• 1948년 12월 육군이 창설되면서 미군의 도움을 받아 암호를 만들어 전군에 배포
• 1950년 6월 육군 전파감시소는 북한의 암호문을 해독함(암호해독의 첫걸음)

• 1995년 3월 국내에서 많이 사용 중이던 '아래아한글 2.1'용 암호 해독

• 1998년 부가형 전자서명방식(KCDSA)을 한국정보통신단체 표준으로 확정
→ Korean Certificate-based Digital Signature Algorithm

• 1998년 Hash algorithm HAS-160을 한국정보통신단체 표준으로 확정

• 1999년 한국 민간용 표준암호 **SEED** 제정 - SEED는 정보보호의 씨앗이 되라는 뜻

• 2003년 국가기관용 표준암호 NES(National Encryption Standard) 제정

• 2004년 12월 행정업무용 표준암호 **ARIA**(Academy-Research Institute-Agency) 제정
• 2004년 지식경제부의 국가표준(KS)으로 지정, 표준번호 KS X 1213:2004

◈ **LEA(Lightweight Encryption Algorithm) 주요 특징**
• 개발연도 : 2010년-2012년(2013년 공개)
• 알고리즘 구분 : 128비트 **블록암호**
• 키 길이 : 128비트, 192비트, 256비트
• 구조 : ARX(Addition, Rotation, Xor) 기반 GFN(Generalized Feistel Network)
• 성능 : 다양한 SW 환경에서 국제표준암호 AES 대비 1.5배~2배 성능

◈ **LSH(Lightweight Secure Hash) 주요 특징**
• 개발연도 : 2014년
• 알고리즘 구분 : **해시함수**
• 출력 길이 : 224비트, 256비트, 384비트, 512비트
• 구조 : Wide-pipe Merkle Damgård 구조
• 성능 : 다양한 SW 환경에서 국제 표준(SHA2/3) 대비 2배 이상 성능

## 기출문제 분석

### 1. 다음에서 설명하는 것은? [2017 경기 추가 9급]

---

**평문을 암호화하거나 암호화된 문장을 복호화하는 전기, 기계 장치로 자판에 문장을 입력하면 회전자가 돌아가면서 암호화된 문장, 복호화된 평문을 만들어낸다.**

---

① 스키테일(scytale)　② 아핀(affine)
③ 에니그마(enigma)　④ 비제니어(vigenere)

♤ 에니그마(enigma)

| | |
|---|---|
| 에니그마<br>(enigma) | • 에니그마는 암호문 작성과 해독이 가능한 기계이다.(기계암호)<br>→ 에니그마는 자판, 램프, 반사판, 배전반 등으로 구성되었다.<br>• 문장을 입력하면 회전자가 돌면서 암호문, 평문을 만들어낸다.<br>→ 보안성에 따라 여러 모델이 있다.<br>• 제2차 세계 대전 중 독일군이 군사기밀 암호화에 사용하였다.<br>→ 2차 대전에 사용된 암호기 중에 가장 해독이 어려운 시스템이었다. |
| 아핀 암호<br>(affine cipher) | • 덧셈과 곱셈 암호 두 가지를 합친 암호이다.<br>→ 비밀키가 2개 필요하다.<br>• 암호화 : C = (P × K1 + K2) mod 26<br>• 복호화 : P = {(C − K2) × 1 / K1)} mod 26 |

정답 : ③

### 2. 국내 기관에서 주도적으로 개발한 암호 알고리즘은? [2014년 지방 9급]

① IDEA　② ARIA
③ AES　④ Skipjack

♤ ARIA(Academy-Research Institute-Agency)

• 아리아(ARIA)는 우리나라 국가보안기술연구소에서 개발한 블록 암호 알고리즘이다.
• 아리아(ARIA)는 2004년 12월 행정업무용 표준암호 제정

정답 : ②

**3. 우리나라 국가 표준으로 지정되었으며 경량 환경 및 하드웨어 구현에서의 효율성 향상을 위해 개발된 128비트 블록암호 알고리즘은? [2017년 국가 9급]**

① IDEA ② 3DES
③ HMAC ④ ARIA

♤ **ARIA(Academy Research Institute Agency) – 아리아**

- ARIA는 우리나라 국가보안기술연구소에서 개발한 블록 암호 알고리즘이다.
- ARIA라는 이름은 Academy(학계)-Research Institute(연구소)-Agency(정부기관)의 첫 글자를 딴 것이다. 이들의 공동 개발 노력을 함축적으로 나타낸 것이다.
- ARIA는 2004년 12월부터 우리나라 행정업무용 국가표준암호로 사용되고 있다.
  → 2004년 지식경제부의 국가표준(KS)으로 지정, 표준번호 KS X 1213:2004
  → ARIA 문의 및 보급신청 : aria@ensec.re.kr
- ARIA는 경량 환경 및 하드웨어에서 효율성 있도록 개발되었다.

정답 : ④

**4. 다음 중 한국에서 개발한 암호화 알고리즘이 아닌 것은? [2022년 군무원 7급]**

① AES ② ARIA
③ SEED ④ LEA

♤ **한국에서 개발한 암호 알고리즘**

| 년도 | 이름 | 비고 |
|---|---|---|
| 1999년 | SEED | 128bit 블록암호, **민간용** 표준암호, Feistel 구조 |
| 2004년 | ARIA | 128bit 블록암호, **행정업무용** 표준암호, SPN 구조 |
| 2005년 | HIGHT | 64bit **초경량** 블록암호, **RFID/사물인터넷** 등에 적용 가능 |
| 2013년 | LEA | 128bit **블록암호**, 국제표준암호 AES 대비 1.5배~2배 성능 |
| 2014년 | LSH | **해시함수**(224bit, 256bit, 384bit, 512bit) |

- **AES** : 2001년 **미국표준기술연구소**(NIST)에 의해 제정된 암호

정답 : ①

## 5. ROT13 암호로 info를 암호화한 결과는? [2016년 서울 9급]

① jvxv ② foin
③ vasb ④ klmd

### ♤ ROT13(Rotate by 13) 암호

- ROT13은 단순한 카이사르 암호의 일종으로 영어 알파벳을 13글자씩 밀어서 만든다.
- ROT-13 혹은 rot13이라고도 쓴다.

**// 예를 들어,**

- ROT13으로 'LOVE'를 암호화하면 'YBIR'가 된다.
- ROT13으로 info를 암호화하면 vasb가 된다.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| n | o | p | q | r | **s** | t | u | **v** | w | x | y | z | **a** | **b** | c | d | e | f | g | h | i | j | k | l | m |

정답 : ③