

# 제 3 장

# 암호의 역사



박종혁 교수

Tel: 970-6702

Email: [jhpark1@seoultech.ac.kr](mailto:jhpark1@seoultech.ac.kr)

## [참고영상]

- 독립투사들이 "닭다리"로 은행을 턴 방법은? 역사 속 숨겨진 암호와 코드 이야기 (15m)
  - 50m full version

**1절 시저 암호**

**2절 단일 치환 암호**

**3절 다중 치환 암호**

**4절 에니그마**

**5절 전치 암호와 치환 암호**

**6절 암호 알고리즘과 키**

# 제1절 시저암호

**1.1 시저 암호란?**

**1.2 시저 암호의 암호화**

**1.3 시저 암호의 복호화**

**1.4 전사 공격에 의한 해독**

# 1.1 시저 암호란?

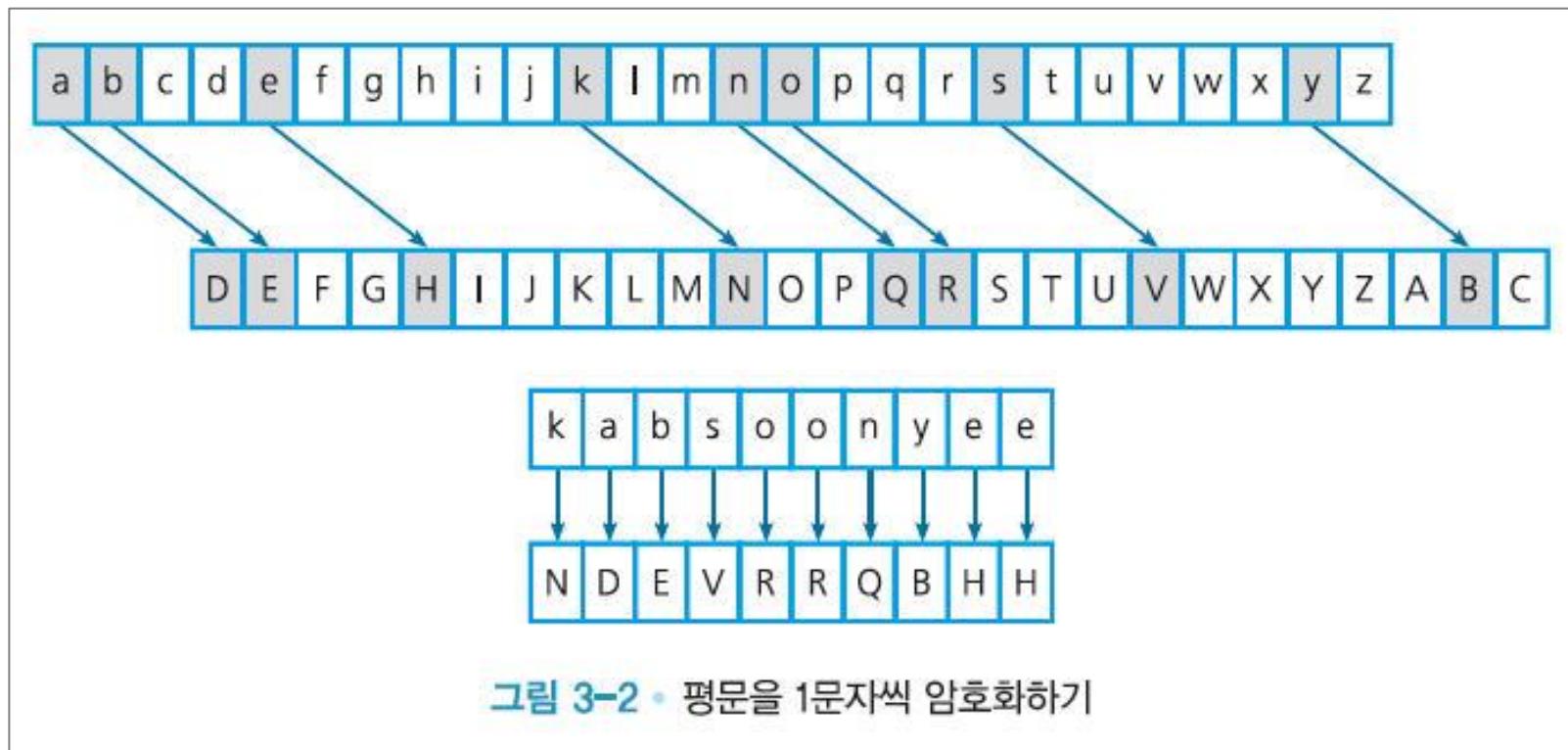
- 시저 암호(Caesar cipher)
  - 줄리어스 시저(유리우스 케사르)가 사용하였다는 암호
  - 평문으로 사용되는 알파벳을 일정한 문자 수 만큼 「평행이동」 시킴으로써 암호화

# 알파벳 3문자 평행 이동

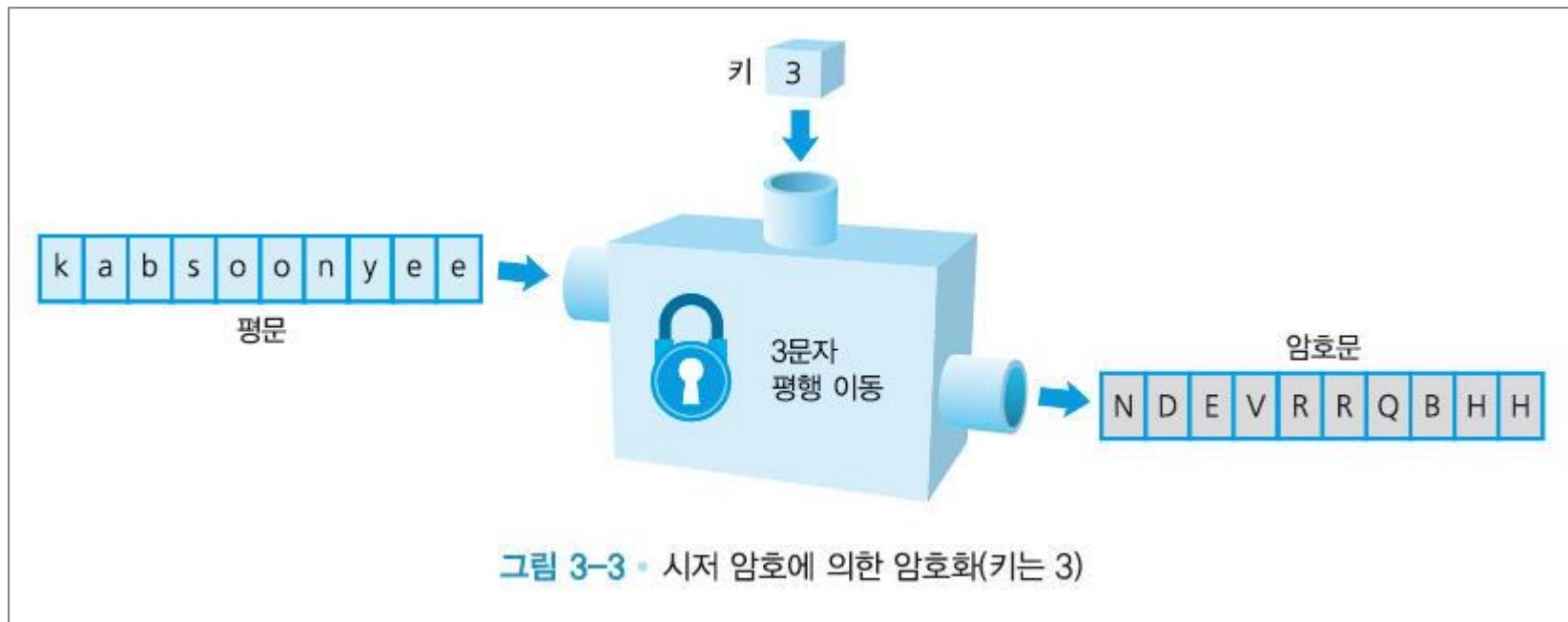


## 1.2 시저 암호의 암호화

- 평문: kabsoonyee
- 암호문: NDeVRRQBHH

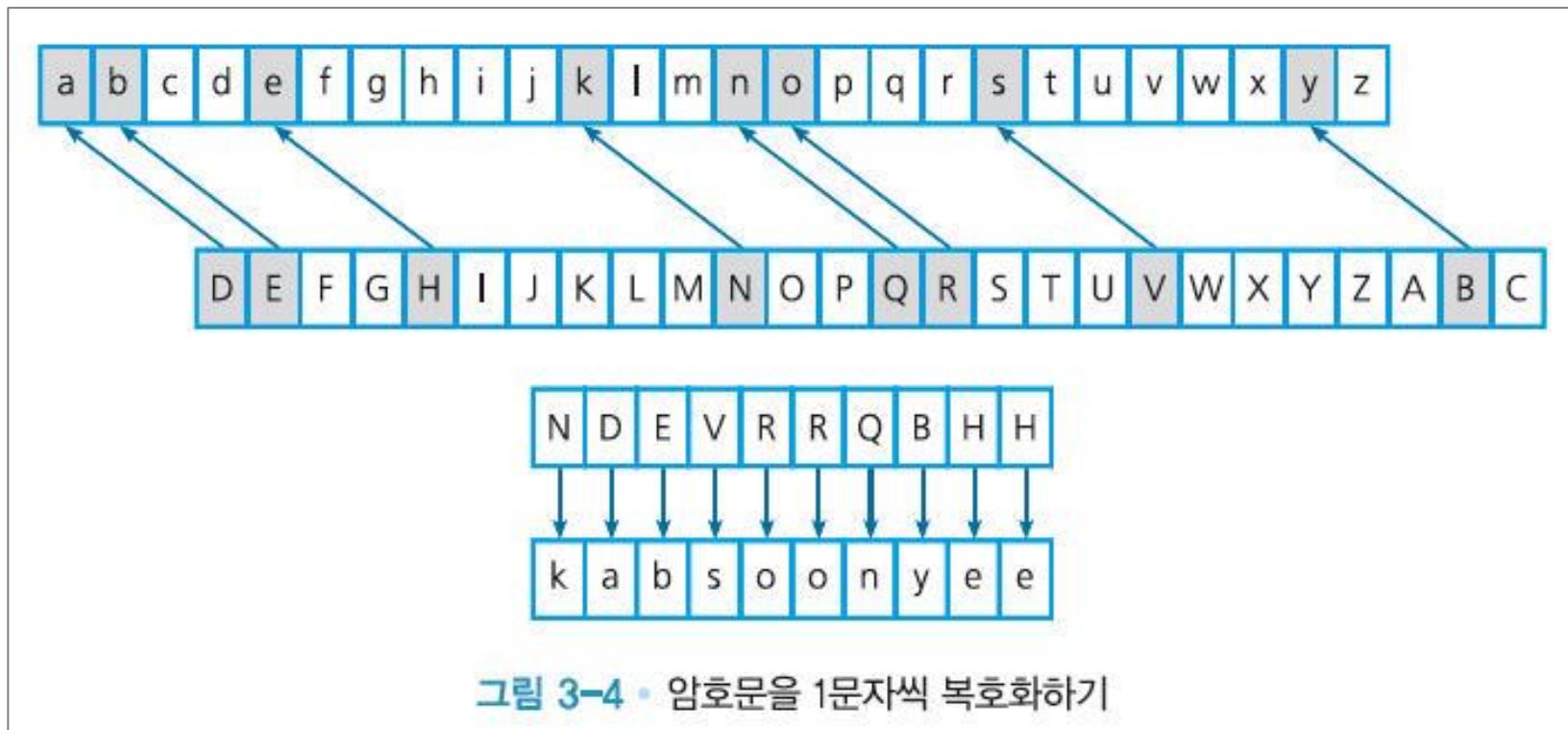


# 시저 암호에 의한 암호화

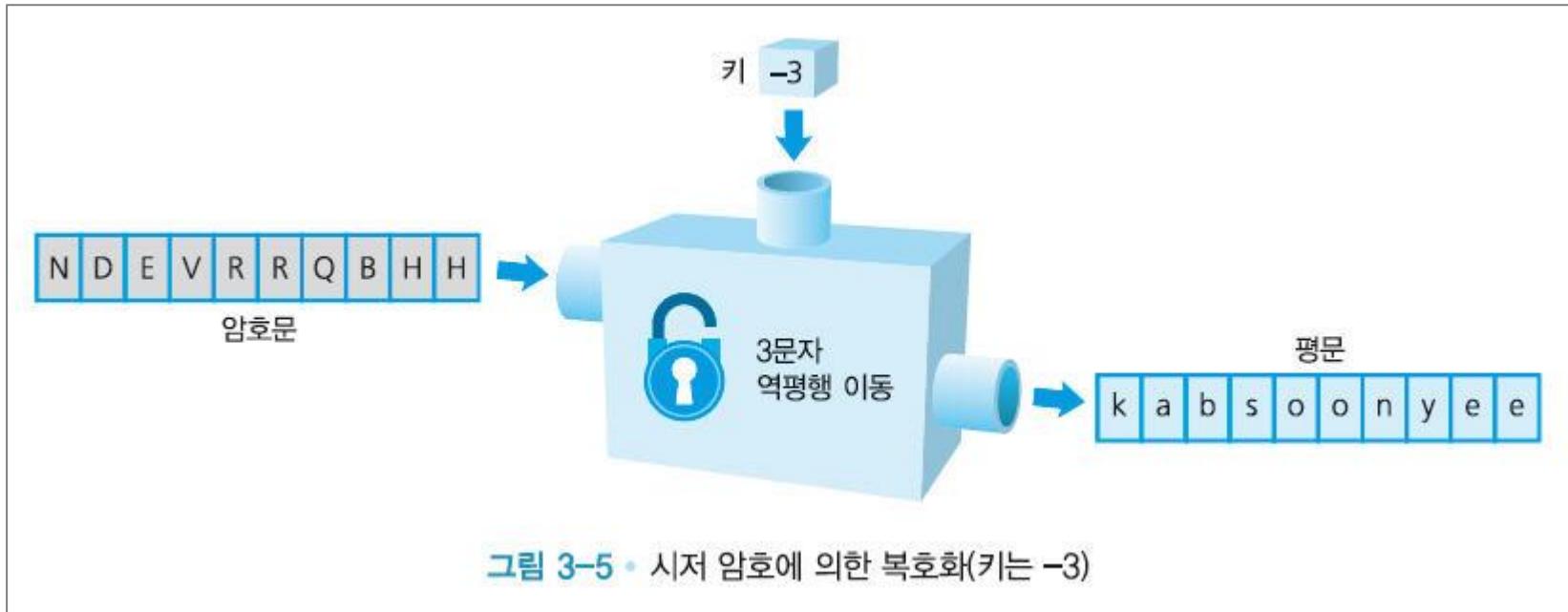


## 1.3 시저 암호의 복호화

- 암호화 때와 동일한 크기의 역방향 평행이동



# 시저 암호에 의한 복호화



## 1.4 전사 공격에 의한 해독

- 암호문 NDeVRRQBHH 을 보고 다른 정보 없이도 kabsoonyee 라는 메시지를 맞출 수는 없을까?
- 영어 알파벳은 26 문자이므로 암호화 키는 0에서 25까지 26가지
- 전사공격(brute-force attack)
  - 키가 될 수 있는 모든 가능한 후보들을 시도해 보는 방법

# 시저 암호문에 대한 전사 공격



- 철자의 빈도와 자주 사용되는 단어와 형태를 이용하는 등 전사공격에 취약함

# 제2절 단일 치환 암호

**2.1 단일 치환 암호란 무엇인가?**

**2.2 단일 치환 암호의 암호화**

**2.3 단일 치환 암호의 복호화**

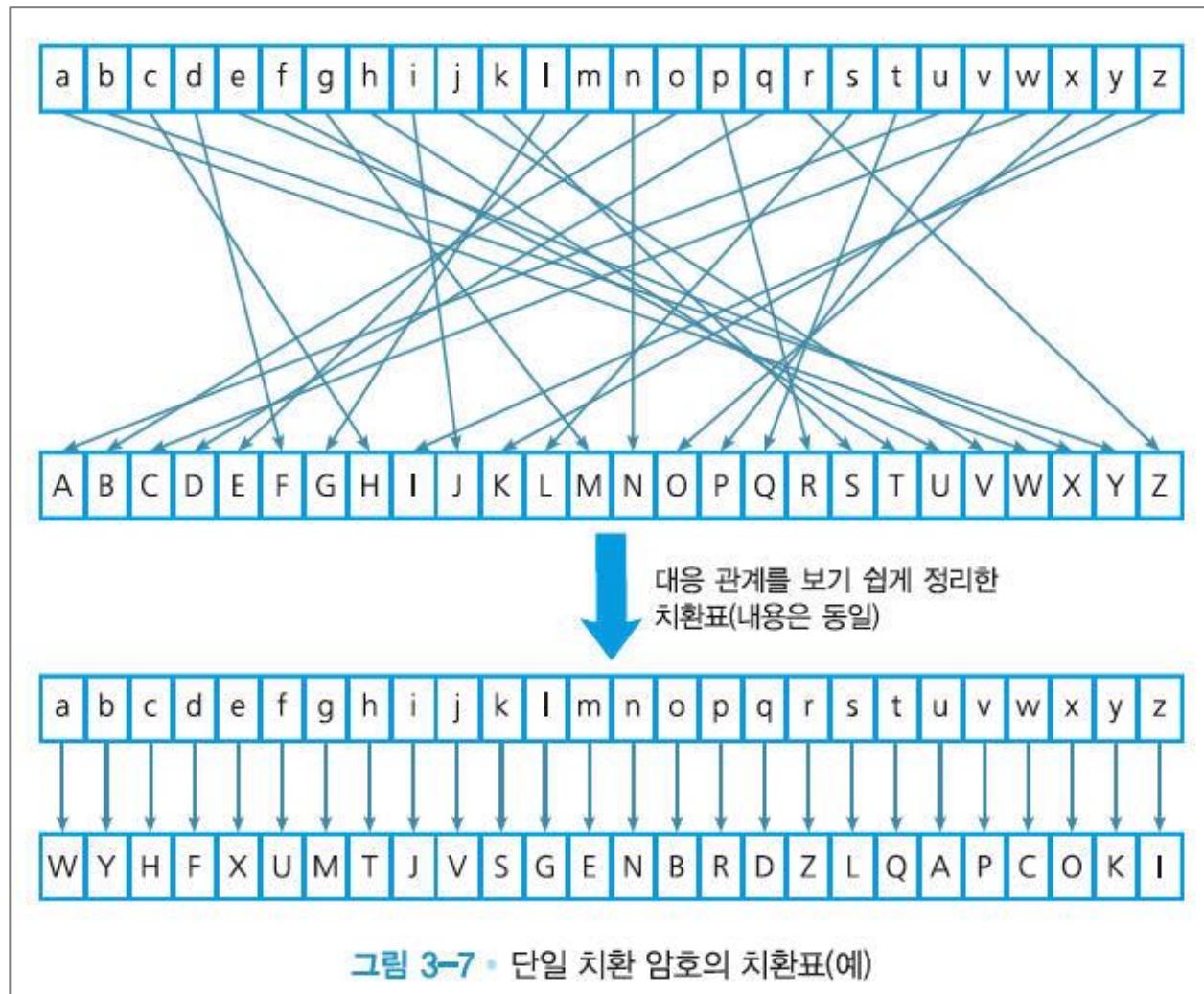
**2.4 단일 치환 암호의 키 공간**

**2.5 빈도 분석에 의한 해독**

## 2.1 단일치환 암호란 무엇인가?

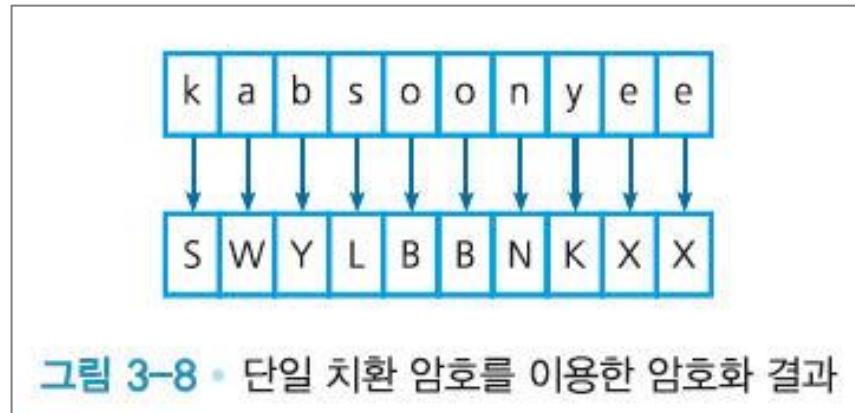
- 단일 치환 암호(simple substitution cipher)
  - 평문을 구성하는 알파벳을 다른 알파벳으로 변환하는 암호
  - 시저 암호는 단일 치환 암호

# 단일 치환 암호의 치환표(예)



## 2.2 단일 치환 암호의 암호화

- 평문: kabsoonyee 를 암호화해 보자
- 암호문: SWYLBBNKXX



- 약점
  - 평문에 등장하는 문자의 빈도가 암호문으로 바뀐 뒤에도 암호문 내에서 동일한 빈도로 나타난다

## 2.3 단일 치환 암호의 복호화

- 치환표가 단일 치환 암호의 「키」
- 암호화 때에 사용한 치환표가 필요
- 송신자와 수신자는 치환표를 공유

## 2.4 단일 치환 암호의 키 공간

- 시저 암호는 전사 공격으로 해독 가능
- 단일 치환 암호는 전사 공격으로 해독이 어렵다
  - 단일 치환 암호가 시저 암호에 비해 훨씬 많은 키 후보를 가질 수가 있기 때문

# 키 공간

- 키 공간(key space)

- 해당 암호에서 사용할 수 있는 「모든 키의 집합」
- 이 키 공간에 속하는 가능한 키의 총수를 키 공간의 크기
- 키 공간이 크면 클수록 전사공격은 어렵다
- 단일 치환 암호의 키의 총수

$$\begin{aligned} 26 \times 25 \times 24 \times 23 & \quad \cdots \quad 1 \\ & = 403291461126605635584000000 \end{aligned}$$

## 전사공격 시간

$$\begin{aligned}26 \times 25 \times 24 \times 23 \cdots \times 1 \\= 403291461126605635584000000\end{aligned}$$

- 키 수가 이렇게 많다면
- 1초에 10억 개의 키를 적용하는 속도로 조사한다고 해도, 모든 키를 조사하는 데 120억년 이상의 시간이 필요

## 2.5 빈도 분석에 의한 해독

- 빈도 분석 암호 해석법을 사용하면 단일 치환 암호도 해독할 수 있다
- 빈도 분석에서는
  - 평문에 등장하는 문자의 빈도
  - 암호문에 나오는 문자의 빈도가 일치하는 것을 이용

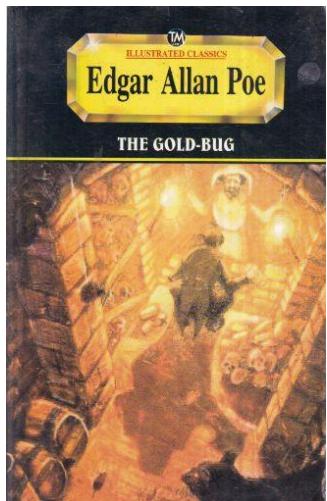
## 2.5 빈도분석을 이용한 암호해독

53†††305))6\*:4826)4†.)4†):800\*:48†8¶60))85:1†(:‡\*8  
†83(88)5\*†:48(:88\*96\*?;8)\*‡(:485):5\*†2:‡(:4956\*2(5\*-4  
):8¶8\*:4068285):)6†8)4††:1(‡9:48081:8:8‡1:48†85:4)485  
†528808\*81(‡9:48:(88:4(‡?34:48)4‡:181::188:‡?:

A good glass in the bishop's hostel in the devil's seat  
forty-one degrees and thirteen minutes northeast and by  
north main branch seventh limb east side shoot from the  
left eye of the death's-head a bee line from the tree  
through the shot fifty feet out. - 애드가 앨런 포우 『황금벌레』

# 소설에 등장한 빈도분석

- 빈도분석 방법은 여러 소설에 등장
  - 에드가 앤런 포우의 ‘황금벌레’



- 아서 코난 도일의 ‘셜록홈즈 이야기’, ‘춤추는 남자의 모험’

# 소설 속의 암호



‘셀록홈즈 이야기’ 인 ‘춤추는 남자의 모험’에 나오는 암호

## 최초의 빈도분석에 대한 자료

- 최초의 기록으로 남아있는 빈도분석에 대한 내용
    - 9세기 ‘암호문 해독에 관한 논고’에 등장하는 아랍의 현학자 알 키ndi(al-Kindi)에 의해 제안

مراد الله - ولله الحمد والحمد لله رب العالمين

لسم الله الرحمن الرحيم . وحسم الله ربكم  
سادوا سعادكم بغير الدارع استلزم العزم الراصدا  
فهي سعادكم لا يقدر علاها ثمن ، ولكنها مرضد لشدة الشدة الاستلزم بالمربي  
الكل العده والفضل والشرف والشرف ، فالله اذ ارسى سلامكم على النائم المفعم  
عندهم اسلامه اسلامه ، فلما وقع لهم الشر وعيدهم كل الشعور والخوف وفسر العذاب عليهم  
الراصد ، سعادكم داركم وسعادكم ، يفتح ، اذ لا انفك لراصدكم ناسا يحيى العزم

**팁 2-8** 알킨디의 '암호문 해독에 관한 논고' 첫 페이지

# 빈도분석을 이용한 암호해독

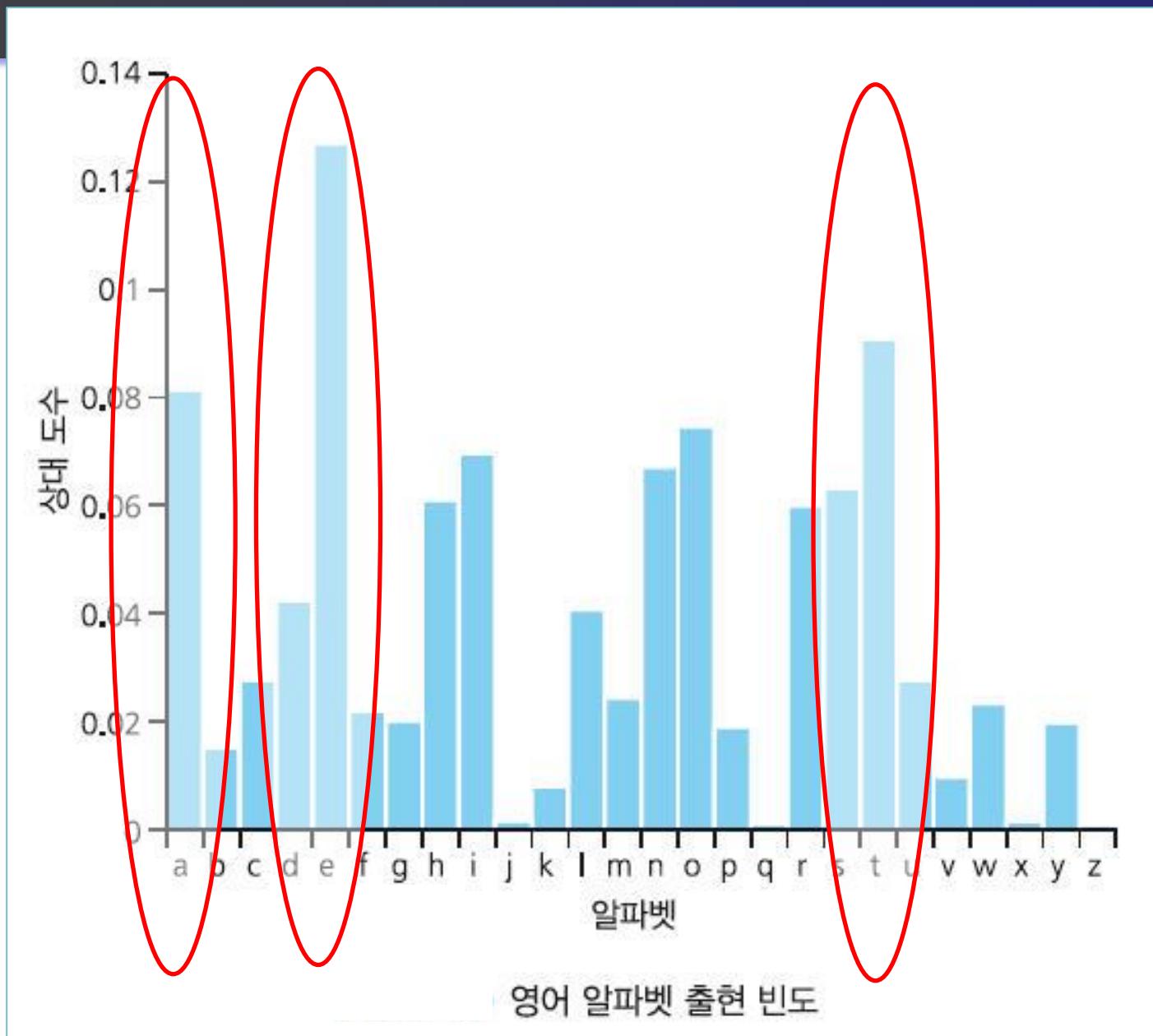
- 암호문

MeYLGVIWAMeYOPINYZGWYeGMZRUUYPZAIXILGVSIZZMPGKKD  
WOMePGROeIWGPCeIPAMDKKKeYCIUYMGIFRWCeGLOPINYZHRZM  
PDNYWDWOGWITDWYSeDCeeIAFYYWMPIDWYAGTYPPIKGLMXFPI  
WCeHRZMMMeYMeDWOMGQRYWCeUXMeDPZMQRGMeYAPISDWO  
FICJILYSNICYZeYMGGJIPRWIHRUNIWAHRZMUDZZYAMeYFRW  
CeMRPWDWOPGRWAIOIDWSDMeIGWYMSGMePYYeYHRUNYARNF  
RMSDMeWGOPYIMYPZRCCYZZIOIDWIWAIOIDWeYMPDYAILMYPM  
eYMWUNMDWOUGPZYKFRMIMKIZMeIAMGODTYDMRNIWASIKJYAI  
SIXSDMeeDZWGZYDWMeYIDPZIXDWODIUZRPYMeYXIPYZGRPDM  
DZYIZXMGAYZNDZYSeIMXGRCIWWGMOYM

# 암호문 속의 영어 알파벳 출현 빈도표

문자	개수	문자	개수	문자	개수	문자	개수	문자	개수
I	47개	G	27개	C	12개	F	7개	V	2개
Y	47개	Z	27개	S	11개	L	6개	B	0개
M	45개	P	26개	N	10개	H	5개		
W	35개	R	22개	U	10개	J	3개		
e	33개	A	17개	K	8개	T	3개		
D	30개	O	16개	X	8개	Q	2개		

# 영어 알파벳 출현 빈도



# 최빈도를 갖는 문자를 e로 변환

I와 Y중 하나를 e라고 가정. Y → e라고 가정하고 변경

ME<sub>e</sub>LGVIWAMEeOPINeZGWeEGMZRUUePZAIXILGVSIZZMPGKKDWO  
MEPGROEIWGPCEIPAMDKEeCIUeMGIFRWCEGLOPINeZHRZMPDN  
eWDWOGWITDWeSEDCEEIAFeeWMPIDWeAGTePIKGLMXFPIWCEHR  
ZMMEeMEDWOMGQReWCEUXMEDPZMQRGMEEeAPISDWOFICJILeS  
NICeZEeMGGJIPRWIWAIRUNIWAHRZMUDZZeAMEeFRWCEMRPWD  
WOPGRWAIOIDWSDMEIGWeMSGMEPeEeHRUNeARNFRMSDMEWG  
OPeIMePZRCCeZZOIDWIWAIOIDWEeMPDeAILMePMEEeMWUNMDWO  
UGPZeKFRMIMKIZMEIAMGODTeDMRNIWASIKJeAISIXSDMEEDZWGZ  
eDWMEeIDPZIXDWODIUZRPeMEeXIPeZGRPDMZelZXMGAeZNDZe  
SEIMXGRCIWWGMOeM

# 영어의 ‘the’ 점검

theLGVIWAtheOPINeZGWehGtZRUUePZAIXILGVSI~~Z~~tPGKKDW~~O~~thPG  
ROhIWGPChIPAtDKKheCIUetGIFRWChGLOPINeZHRZtPDNeWDWOG  
WITDWeShDChhIAFeeWtPIDWeAGTePIKGLtXFPIWChHRZtthethDW~~O~~t  
GQReWChUXthDPZtQRGthheAPISDWOFICJILeSNICeZhetGGJIPRWI  
WAIHRUNIWAHRZtUDZZeAtheFRWchtRPWDWOPGRWAIOIDWSDthIG  
WetSG Pee |heHRUNeARNFRtSDthWGOPeltePZRCCeZZIOIDWIWAIOI  
DWhetPDeAILtePthetWUNtDWOUGPZeKFRtItKIZthIAtGODTeDtRN~~I~~WA  
SIKJeAISIXSDthhDZWGZeDWtheIDPZIXDWODIUZRPetheXIPeZGRP~~D~~t  
DZeIZXtGAeZNDZeShltXGRCIWWGtOet

thPee → three

P→r ??

# 익숙한 단어 추측

theLGVIWAtheOrINeZGWehGtZRUUerZAIXILGVSIZZtrGKKDWOthrGR  
OhIWGrChIrAtDKKheCIUetGIFRWChGLOrINeZHRZtrDNeWDWOGWIT  
DWeShDChhIAFeeWtrIDWeAGTerIKGLtXFrlWChHRZtthethDWotGQRe  
WChUXthDrZtQRGthheArISDWOFICJILeSNICeZhetGGJlrRWIWAIRU  
NIWAHRZtUDZZeAtheFRWChtrWDWOrGRWAIOIDWSDthIGWetSG  
eeheHRUNeARNFRtSDthWGOrelterZRCCeZZIOIDWIWAIOIDWhetrDeA  
ILterhetWUNtDWOUGrZeKFRtlkIZthlAtGODTeDtRNIWASIKJeAISIXSD  
thhDZWGZeDWthelDrZIXDWODIUZRretheXlreZGRrDtDZeIZXtGAeZND  
ZeShltXGRCIWWGtOet

Oet → bet, get, set ,⋯ 중 하나.

get이라고 가정: O→g

# 단어 패턴

- theDWg라는 패턴이 보인다. 이것은 the thing일지도 모른다  
 $D \rightarrow i$ ,  $W \rightarrow n$  ??
- grlNe라는 패턴이 보인다. 사전을 찾아보았더니  
grace, grade, grape, grate, grave, ripe, grofe, …처럼 많은 후보가 있다. 이것으로는 결정을 할 수 없다.
  - I $\rightarrow$ a를 가정해 보면 greater라는 패턴이 나오므로 I $\rightarrow$ a는 맞는 것 같다.
  - 하지만, N $\rightarrow$ c를 가정하면 tricening라는 패턴이 나왔다.  
이런 단어는 영어 단어에 없는 것 같다. 따라서 N $\rightarrow$ c는 잘못일지도 모른다

# 빈도 추측

- 빈도가 높은 문자 중 아직 가정에 등장하지 않은 문자는 o이다
- 한편 암호문 중에 등장하는 빈도가 높은 문자로서 아직 모르는 것은 G와 Z
- $G \rightarrow o$ 를 가정

theLoVanAthegraNeZonehotZRUUerZAaXaLoVSaZZtroKKingthroRgha  
norCharAtiKKheCaUetoaFRnChoLgraNeZHRZtriNeningonaTineShiChh  
aAFeeentraineAoTeraKoLtXFranChHRZtthethingtoQRenChUXthirZtQRo  
thheAraSingFaCJaLeSNaCeZhetoJarRnanAaHRUNanAHRZtUiZZeAt  
heFRnChtRrningroRnAagainSithaonetSothreeheHRUNeARNFRtSithno  
greaterZRCCEZZagainanAagainhetrieAaLterthetnUNtingUorZeKFRtat  
KaZthaAtogiTeitRNanASaKJeAaSaXSithhiZnoZeintheairZaXingiaUZRr  
etheXareZoRritiZeaZXtoAeZNiZeShatXoRCannotget

- 끝에 Cannotget이라는 패턴이 등장했다.  $C \rightarrow c$ 가 틀림없다.  
 $C \rightarrow c$ 라는 것을 통해 조금 전에 생각한  $N \rightarrow c$ 는 역시 잘못이라는 것을 알 수 있다

theLoVanAthegraNeZonehotZRUUerZAaXaLoVSaZZtro  
KKingthroRghanorcharAtiKKhecaUetoaFRnchoLgraNeZ  
HRZtriNeningonaTineShichhaAFeentraineAoTeraKoLtX  
FranchHRZtthethingtoQRenchUXthirZtQRothheAraSing  
FacJaLeSNaceZhetoJarRnanAaHRUNanAHRZtUiZZeA  
theFRnchtRrningroRnAagainSithaonetSothreeheHRUNe  
ARNFRtSithnogreaterZRcceZZagainanAagainhetrieAaLt  
erthetnUNtingUorZeKFRtatKaZthaAtogiTeitRNanASaKJ  
eAaSaXSithhiZnoZeintheairZaXingiaUZRretheXareZoRri  
tiZeaZXtoAeZNiZeShatXoRcannotget

- Shich라는 패턴이 보인다. 이것은 which일 것이다 (S→w)

# 빈도가 낮은 문자 추측

- `the thing to QRench`라는 패턴이 찾아졌다.  
이것은 분명히 `the thing to QRench`이다.  
사전을 찾아보니 `quench`라는 단어가 있었다( $Q \rightarrow q$ ,  $R \rightarrow u$ ).  
– `quench`라는 것은 「갈증을 해소하다」라는 의미이다. 마시는 것에 관한 이야기가 아닐까?
- `hotZuUUer`라는 패턴이 찾아졌다.  
이것은 `hot summer`일 것이다( $Z \rightarrow s$ ,  $U \rightarrow m$ ).  
U가 두 개 연속해 있다는 것이 큰 실마리였다.  
「갈증을 해소하다」라는 문맥과도 일치한다.

# 단어와 내용 추측

theLoVanAthebraNesonehotsummersAaXaLoVwasstroKKingthrougha  
norcharAtiKKhecame to a FunchoLgraNesHustriNeningonaTinewhichha  
AFeentraineAoTeraKoLtXFanchHustthe thing to quenchmXthirstquothh  
eArawingFacJaLewNaceshetooJarunanAaHumNanAHustmisseAtheFu  
nchturningrounAagainwithaonetwothreeheHumNeAuNFutwithnogreat  
erssuccessagainanAagainhtrieAaLterthetnmNtingmorseKFutatKastha  
AtogiTeituNanAwakJeAawaXwithhisnoseintheairsaXingiamsuretheXar  
esouritiseasXtoAesNisewhatYoucannotget

- sucessagainanAagain라는 패턴이 있다. 이것은 success again and again일 것이다(A→d). triedaLter라는 패턴이 보인다. 이것은 틀림없이 tried after이다(L→f). whatYoucannotget라는 패턴이 보인다. 이것은 what you cannot get일 것이다(X→y).

# 정리

the fox and the grapes one hot summer's day a fox was stroking through a  
richard tick he came to a bunch of grapes but ripening on a tree which had been  
trained onto a rocky branch but the thing to quench my thirst quota hedra  
wing face a few paces he too jarun and a hump and but missed the bunch turn  
ing round again with a one two three he humped up but with no greater success  
again and again he tried after the attempt morse but at last had to give it up  
and walk away with his nose in the air saying i am sure they are sour it is  
as you deserve what you cannot get

- foxwassstroKKing
  - fox was strolling
  - (K → l)
- hetooJarunandaHumpandHustmissed
- he took a run and a jump and just missed
  - (H → j)
  - (J → k)
- hejumpedupFutwithnogreatersuccess
- he jumped up but with no greater success
  - (F → b)
- butatlasthadtogiTeitup
- but at last had to give it up
  - (T → v)
- 이 암호문에 나오지 않은 마지막 1문자
  - (B → z)
- 암호문이 전부 해독됨!!!

# 치환표

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
I	F	C	A	Y	L	O	E	D	H	J	K	U	W	G	N	Q	P	Z	M	R	T	S	V	X	B

# 해독된 평문

the fox and the grapes one hot summer's day a fox was strolling through a no  
r hard till he came to a bunch of grapes just ripening on a vine which had been tra  
ined over a lofty branch just then to quench my thirst quo the drawing back a fe  
wpaces he took a run and a jump and just missed the bunch turning around aga  
in with honetwo three he jumped up but with no greater success again and agai  
n he tried after the tempting morsel but at last had to give it up and walked away  
with his nose in the air saying i am sure they are sour it is easy to despise what y  
ou cannot get

# 띄어쓰기

- 『이솝우화』에 나오는 「여우와 포도」 이야기

"The Fox and the Grapes"

One hot summer's day, a Fox was strolling through an orchard till he came to a bunch f grapes just ripening on a vine which had been trained over a lofty branch. "Just the to quench my thirst, "quoth he. Drawing back a few paces, he took a run and a jump, and just missed the bunch. Turning round again with one , two, three, he jumped up, but with no greater success. Again and again he tried after the tempting morsel, but at last had to give it up, and walked away with his nose in the air, saying: "I am sure they are sour." It is easy to despise what you cannot get.

# 해독작업

- 빈도가 높은 문자뿐만 아니라 빈도가 낮은 문자도 단서가 된다.
- 처음과 끝을 아는 것은 단서가 된다. 단어의 단락을 알면 그것도 단서가 될 수 있다.
- 암호문이 길면 해독이 쉬워진다.
- 같은 문자가 연속해서 나타나면 그것은 단서가 된다.
  - 단일 치환 암호에서는 어떤 문자 어느 문자로 암호화되는지는 정해져 있기 때문
- 해독의 속도가 점점 빨라진다.

### 3. 다중 치환 암호

- 단일 치환암호의 약점
  - 평문과 암호문간의 단순 대응을 사용하기 때문에 평문의 단일 문자에 대한 빈도가 그대로 암호문에 반영된다.
- 따라서 암호해독자로 하여금 빈도분석을 어렵게 하기 위해서는 암호문에 나타나는 문자들의 빈도를 거의 균등하게 만드는 암호를 이용하는 것이 바람직하다.  
→ 다중 치환을 이용하여 문자의 발생빈도를 균일화 한다.

### 3.1 빙도 분석이 가능한가?

- 빙도분석이 가능했던 이유는 평문에 등장하는 문자의 빙도와 암호문에 등장하는 문자의 빙도가 일치하기 때문
- 다중치환암호(polyalphabetic substitution cipher)
  - 평문에 등장하는 문자의 빙도와 암호문에 등장하는 문자의 빙도를 다르게 만드는 암호 알고리즘
  - 힐암호
  - 비장느르 암호 / 비제네르 (Vigenere) 암호
  - 에니그마 기계(Enigma machine)
  - 빙도분석을 이용한 공격방법이 무용지울

# 치환 기법

- Hill 암호 기법
  - 각 문자에 정수 값을 부여하고 m개의 문자를 치환
    - M=3개는 3개의 문자를 치환하는 방법

$$C_1 = (k_{11} p_1 + k_{12} p_2 + k_{13} p_3) \bmod 26$$

$$C_2 = (k_{21} p_1 + k_{22} p_2 + k_{23} p_3) \bmod 26$$

$$C_3 = (k_{31} p_1 + k_{32} p_2 + k_{33} p_3) \bmod 26$$

C: 암호문

P: 평문

k: 키

# 치환 기법

- 암호문 형식을 열 벡터와 행렬로 표현

$$\begin{vmatrix} C_1 \\ C_2 \\ C_3 \end{vmatrix} = \begin{vmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{vmatrix} \begin{vmatrix} P_1 \\ P_2 \\ P_3 \end{vmatrix}$$

- 암호화 사례

- 평문: PAYMOREMONEY

- 암호 키

$$K = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix}$$

# 치환 기법

- 암호문 계산

$$\begin{vmatrix} C1 \\ C2 \\ C3 \end{vmatrix} = \begin{vmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{vmatrix} \begin{vmatrix} P1 \\ P2 \\ P3 \end{vmatrix}$$

- 평문을 숫자변환

→ PAYMOREMONEY : P → 15, A → 0, Y → 24, ...

- 숫자 대입 암호문 치환

$$\begin{vmatrix} C1 \\ C2 \\ C3 \end{vmatrix} = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix} \begin{vmatrix} 15 \\ 0 \\ 24 \end{vmatrix} \text{ mod } 26 \rightarrow \begin{vmatrix} 11 \\ 13 \\ 18 \end{vmatrix} \begin{vmatrix} L \\ N \\ S \end{vmatrix}$$

- $K(15 0 24) + (375 819 486) \text{ mod } 26 = (11 13 18) = \text{LNS}$ 
  - $C1 = 17 \times 15 + 17 \times 0 + 5 \times 24 = 375 \text{ mod } 26 = 14 \dots \dots 11$
  - $C2 = 21 \times 15 + 18 \times 0 + 21 \times 24 = 819 \text{ mod } 26 = 31 \dots \dots 13$
  - $C3 = 2 \times 15 + 2 \times 0 + 19 \times 24 = 486 \text{ mod } 26 = 18 \dots \dots 18$

# 치환 기법

- 복호문 계산

- 암호문 계산 형식  $C = E_k(P) = KP$ 에서
- 평문  $P = D_k(C) = K^{-1}C = K^{-1}KP = P$ ; (여기서,  $K^{-1}$ 은 역행렬:  $K^{-1}K = I$ )

$$\begin{vmatrix} P1 \\ P2 \\ P3 \end{vmatrix} = \begin{vmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 7 \end{vmatrix} \begin{vmatrix} 11 \\ 13 \\ 18 \end{vmatrix} \mod 26 \rightarrow \begin{vmatrix} 15 \\ 0 \\ 24 \end{vmatrix} \begin{vmatrix} P \\ A \\ Y \end{vmatrix}$$

- 역행렬 계산

$$\begin{vmatrix} 17 & 17 & 15 \\ 21 & 18 & 2 \\ 2 & 2 & 19 \end{vmatrix} \begin{vmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 7 \end{vmatrix} = \begin{vmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{vmatrix} \mod 26 \rightarrow \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}$$

# 치환 기법

- 다중 단일 문자 치환 암호 기법
  - 관련된 단일 문자 치환 규칙들의 집합을 사용함
  - 주어진 변환에 사용될 특정 규칙은 키에 의해 결정됨
- 대표적인 Vigeneré 암호 방식
  - 행렬표를 구성
  - 키 문자 x와 평문자 y가 주어지면 암호 문자는 x행 y 열의 암호문 V
  - 키 : deceptive
  - 평문 : we are discovered save yourself
  - 암호화

키	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e
평문	w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s	a	v
암호문	Z	I	C	V	T	W	Q	N	G	R	Z	G	V	T	W	A	V	Z

- 복호화 ?

# 현대 VIGENRE 표

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

# 제4절 에니그마

## 영화 “이미테이션 게임” (2014)



이미테이션 게임 (The Imitation Game)은  
엘런 튜닝의 암호 해독기에 관한 내용

알고리즘과 계산 개념을 튜링머신 (Turing machine)이라는 추상 모델을 통해 형식화한  
잉글랜드의 천재 (수학자) 암호학자

# 제4절 에니그마

4.1 에니그마란 무엇인가?

4.2 에니그마에 의한 암호 통신

4.3 에니그마의 구조

4.4 에니그마의 암호화

4.5 날자별 키와 통신 키

4.6 통신 오류의 회피

4.7 에니그마의 복호화

4.8 에니그마의 약점

4.9 에니그마의 해독

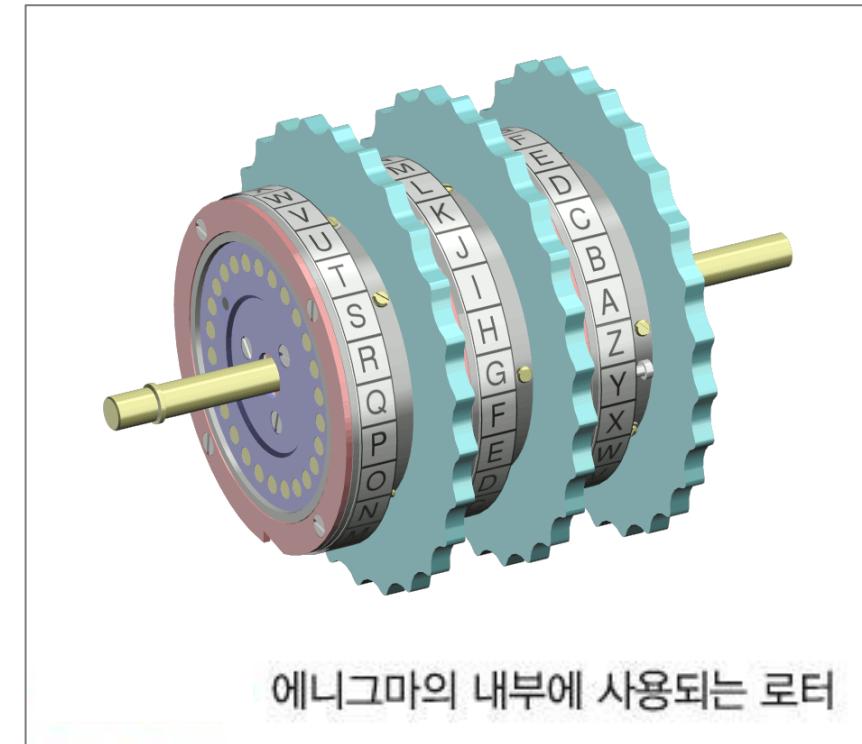
## 4.1 에니그마란 무엇인가?

- 에니그마(enigma)
  - 독일의 세르비우스(Arthur Scherbius)가 20세기 초에 발명한 암호화/복호화를 수행하는 기계
  - 에니그마는 독일어로 「수수께끼」 를 의미
  - 회전하는 원반과 전기회로를 써서 강력한 암호를 만들고자 시도
  - 발명 당시에는 에니그마를 상용으로 사용
  - 나치독일 시대에는 군용으로 사용하려고 개량

# 에니그마와 로터



독일군이 사용하던 에니그마의 전형적 모습



## 4.2 에니그마에 의한 암호 통신

- 타이프라이터, 텁니바퀴, 전지, 전구를 조합한 기계
- 암호화와 복호화를 1 대의 기계로 수행
- 송신자와 수신자는 각각 에니그마를 1 대씩 소유

# 코드북과 코드북의 내부



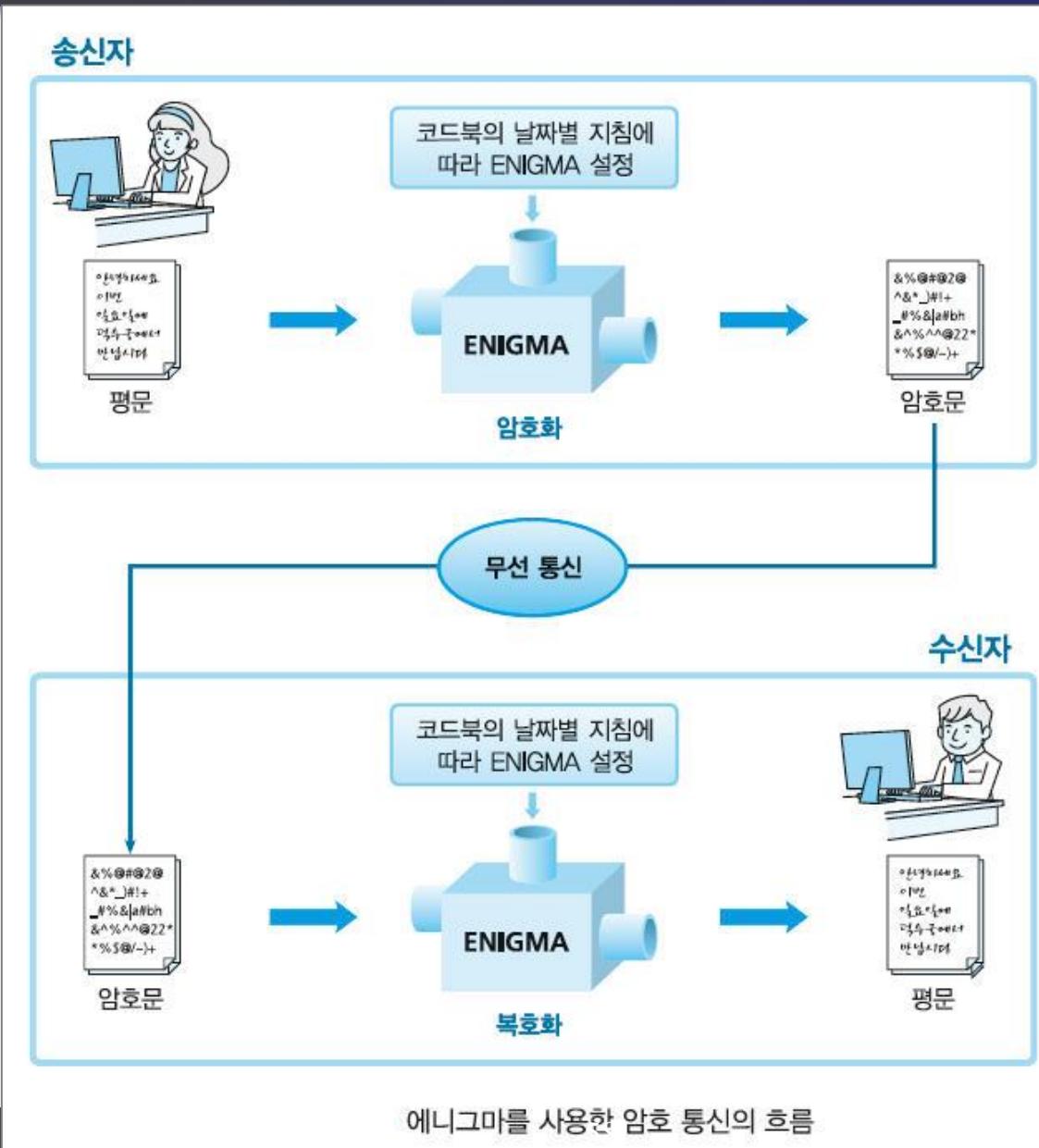
GEHEIM				SONDER-MASCHINEN-Schlüssel: WOLFPACK LEAGUE												FEBRUAR 1942				
				Tug. (UKW)	Wellenlage	(Ringstellung)	Stachelschweinbindungen								Kenngruppen					
19	B	II	VII	IV	IV	18 25 24	AB	BD	CY	DK	FT	HE	HQ	LH	ME	PX	IHS	WDE	RQJ	QDQ
20	B	IV	II	I	I	07 22 12	AO	CP	EI	GK	HE	JT	LS	HF	QT	RX	ARY	ADG	ETQ	WEP
21	C	VII	III	VIII	III	03 02 17	AZ	BT	CF	DX	FU	GL	HO	JK	JV	SZ	TUJ	LSY	FED	WQA
22	C	V	VIII	II	II	18 16 20	AC	DQ	IG	EH	FR	HE	JT	JF	KT	MF	PGC	SAL	GRT	WPO
23	C	IV	V	VII	VII	01 12 05	BP	CE	EJ	EO	FQ	GT	KR	LX	JU	SY	ETV	OMS	LET	FFF
24	B	VII	VII	VI	III	09 08 10	AB	BJ	CH	DE	FT	JH	LE	ME	QE	QR	VZB	GRO	FIS	AID
25	C	V	VII	II	II	08 10 03	AZ	BQ	CB	HR	JU	KF	ME	OP	TY	VW	EGR	LUT	RQB	WVQ
26	C	III	IV	VII	VII	18 05 17	AB	BU	CH	DE	HQ	FT	GO	IS	JL	LX	MLO	GLO	RVB	HEE
27	C	V	II	VII	VII	04 21 21	AO	BY	FB	GS	HT	JL	KF	LW	ME	PX	REN	DDP	HEX	GAM
28	C	IV	VI	VIII	VIII	19 11 26	DE	CX	DE	FE	GB	IL	JG	KH	QP	VW	KTR	FET	QQT	QEE
29	C	VII	I	IV	IV	04 08 17	AJ	BF	CT	HR	JQ	KH	LU	OV	PS	XV	SAG	CTG	ARK	GHY
30	C	VII	III	IV	IV	02 11 18	AB	BF	CT	DQ	EF	HE	JL	KR	OP	UY	ENB	JRY	TUJ	VAK
31	C	VI	III	V	V	07 22 11	AD	BV	CF	EJ	FT	GH	KE	LH	MW	QR	ZBI	FEI	PAI	DAQ
32	B	VII	IV	III	III	18 16 03	AB	DO	CG	DT	EF	FF	IE	JX	LB	UY	HTJ	QED	WQT	AHS
33	C	VI	II	IV	IV	07 07 05	AL	DV	CJ	DI	EF	GY	HE	KR	NU	QE	DIX	CDO	RFS	HRX
34	B	IV	II	VI	VI	06 19 09	BD	CL	EH	FR	GG	IU	KU	OX	ST	TH	AJR	BRD	VLI	CWV
35	B	VIII	VI	III	III	18 23 21	AF	EF	BT	EH	GW	HD	HT	OQ	RV	SZ	XOG	COG	LGJ	EIG
36	B	VII	VI	VIII	VIII	01 08 13	AL	DI	FX	GR	HF	IK	OF	RS	TE	UY	JUF	PCX	RNG	DNV

코드북에는 송/수신자가 사용하는 날짜별 키가 기록되어 있고,  
송신자/수신자는 이 책자의 지시에 따라 앤리그마를 설정

## 4.3 에니그마의 구조

- 에니그마는 알파벳 26 문자를 암호화/복호화할 수 있지만, 그림이 복잡하기 때문에 여기서는 알파벳의 수를 4 문자로 가정

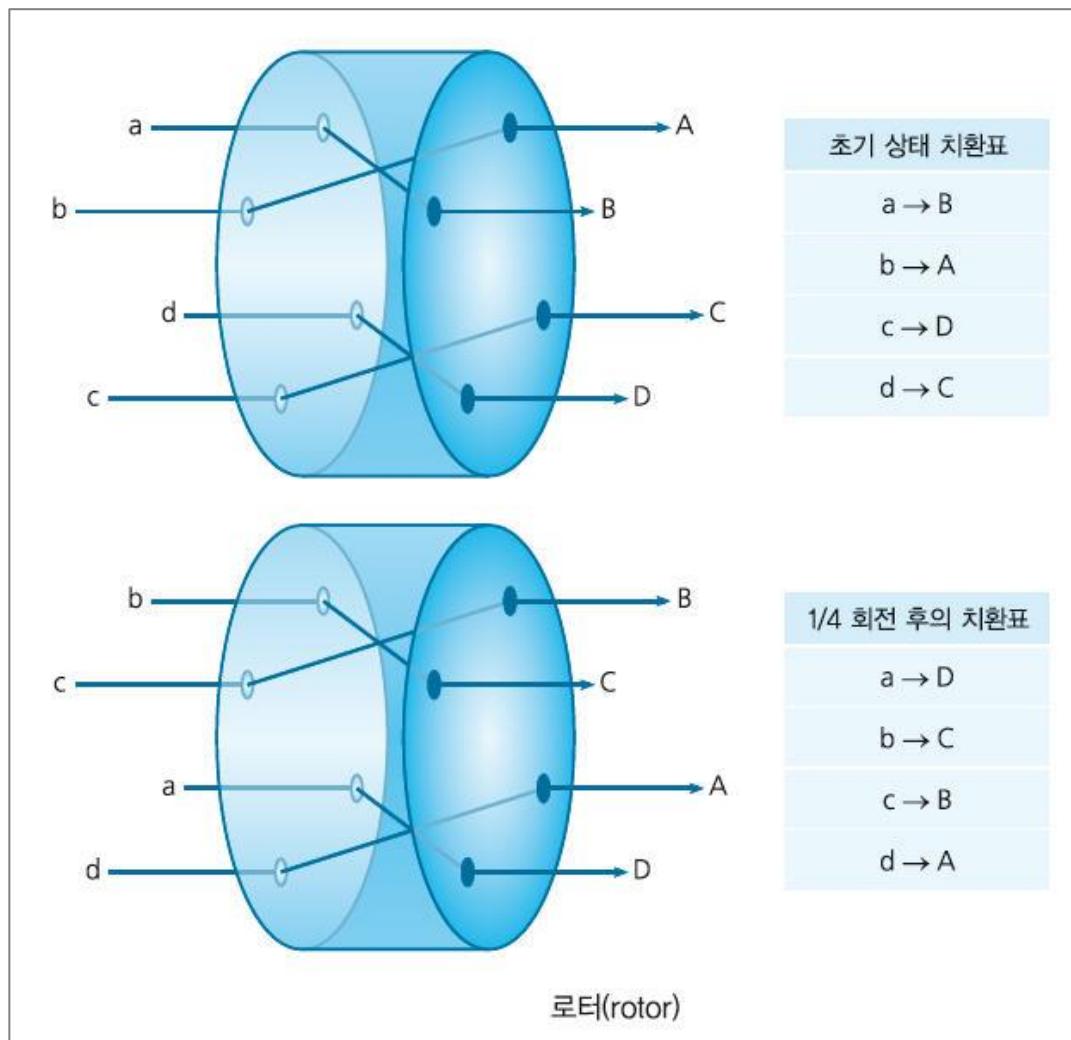
# 에니그마 암호통신 흐름



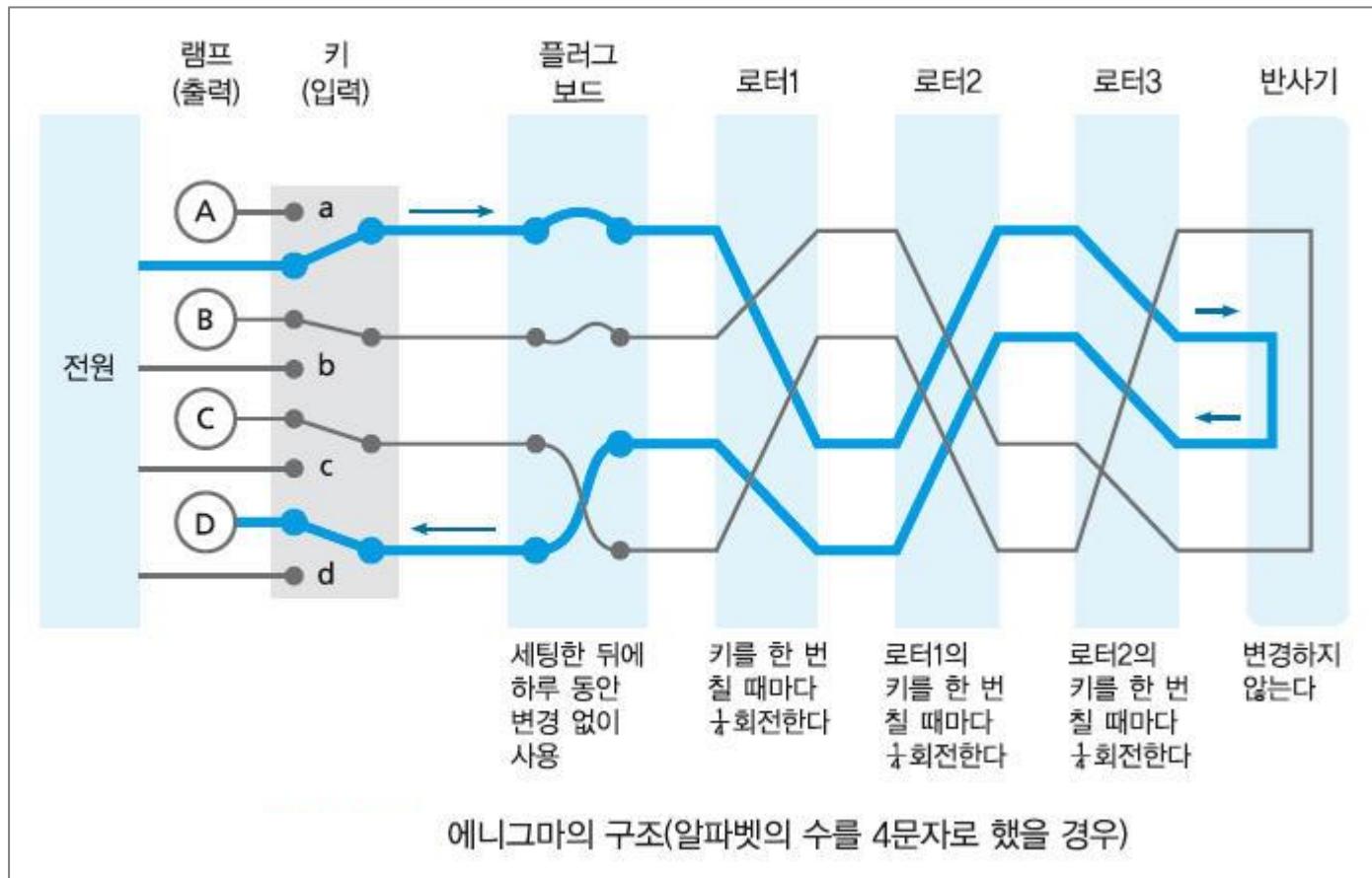
# 로터

- 로터(rotor)
  - 로터는 앞과 뒤의 단자가 전선으로 연결되어 있는 원반 모양의 부품
  - 로터 하나하나의 연결선은 바꿀 수는 없지만, 문자를 입력할 때마다 자동으로 회전
  - 하나의 문자를 입력하면 로터1이  $1/4$  회전 한다(알파벳의 수를 4 문자로 했을 경우). 로터1이 1 회전 하면 로터2가  $1/4$  회전 하고, 로터2 가 1 회전 하면 로터3이  $1/4$  회전

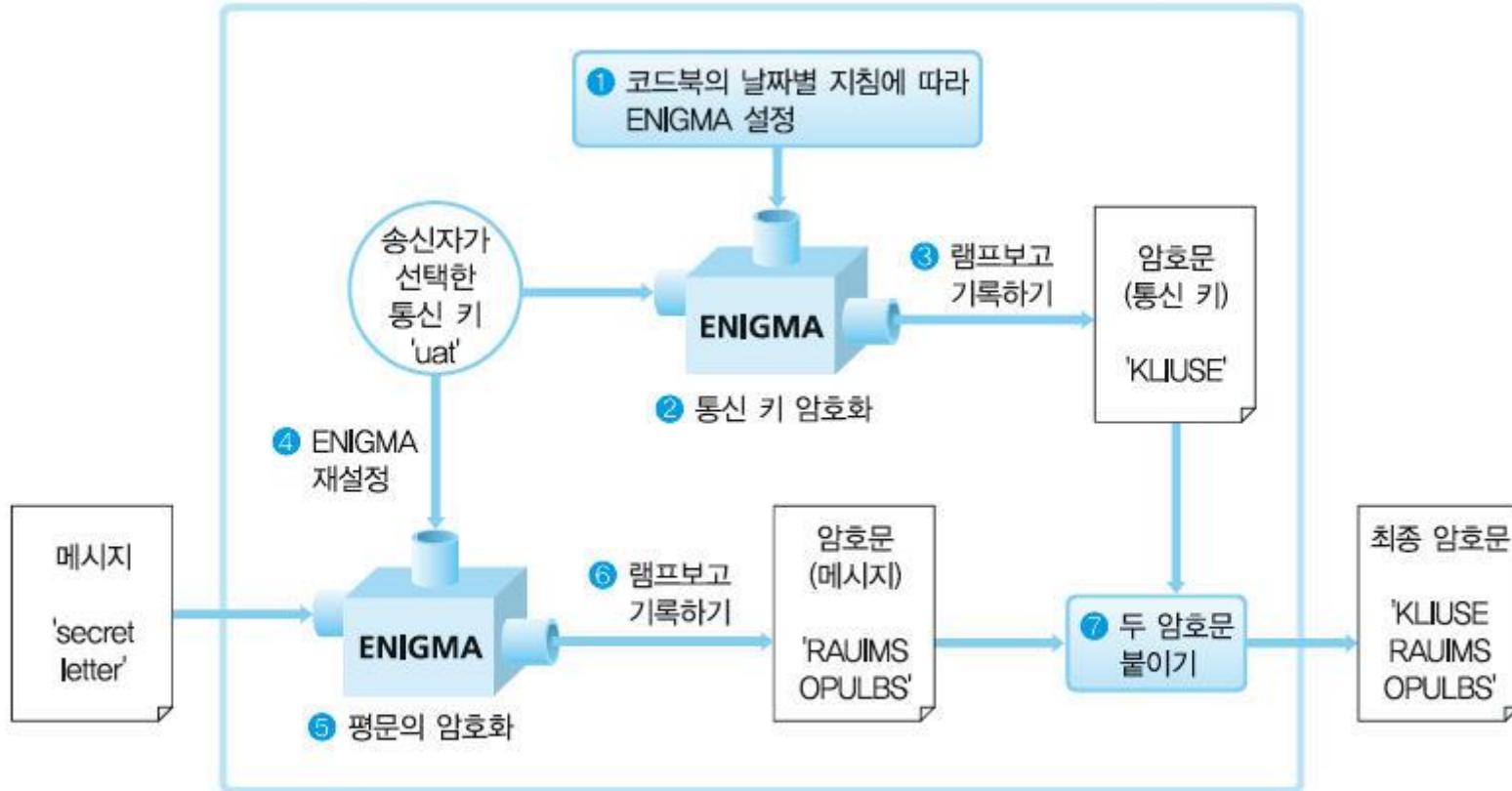
# 로터



# 에니그마의 구조(4문자)



# secretletter 를 암호화하기



에니그마를 사용한 암호화(에니그마를 사용하여 'secretletter' 를 암호화한다)

## 4.4 에니그마 암호화

- 평문: secretletter 를 암호화하여 송신하기
  - 에니그마 설정
  - 통신키의 암호화
  - 암호화된 통신키 메모
  - 에니그마의 재설정
  - 메시지의 암호화
  - 결합

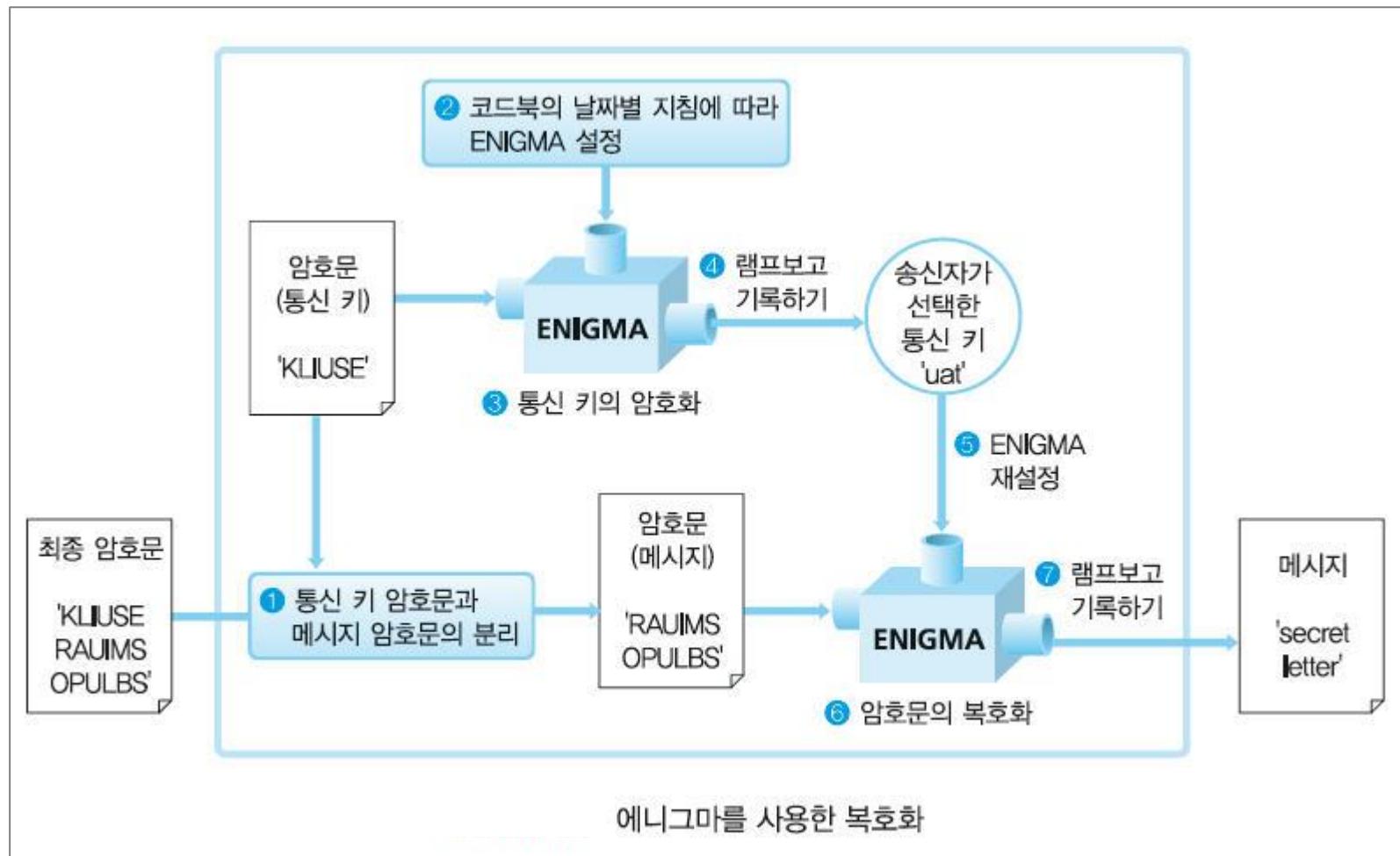
## 4.5 날짜별 키와 통신 키

- 날짜별 키는 메시지의 암호화가 아니라 통신키의 암호화에 사용
- 날짜별 키는 「키를 암호화하기 위한 키」
  - 이와 같은 키를 키 암호 키(key encrypting key; KEK)라 한다
- 메시지를 통신키로 암호화하고, 통신키를 날짜별 키로 암호화하는 2단 구조

## 4.6 통신 오류의 회피

- 통신키 uat를 2회 연속해서 uatuat라고 입력
- 당시 무선 기술수준이 낮아서 통신이 제대로 되지 않는 경우가 많이 있었기 때문

## 4.7 에니그마의 복호화



## 4.8 에니그마의 약점

- 「통신키를 2회 반복한 것을 암호화 한다」
- 「통신키를 선택한 것이 사람이다」
- 「코드북을 배송하지 않으면 안 된다」

## 4.9 에니그마의 해독

- 에니그마의 설계는 「숨기는 것에 의한 보안」(security by obscurity)에 의존하지 않음
- 폴란드의 암호 해독자 르예프스키
  - 날짜별 키에 의한 암호문으로부터 날짜별 키를 간파하는 방법을 고안
- 영국의 암호 해독팀은 블레츨리 파크에 모여 에니그마의 해독

# [참고영상] – 에니그마, 앤런튜링

- 컴퓨팅 시대 서막 연 독일 전설급 암호기, 에니그마 – CNET (영어 버전, 자막포함) (4m)
- 2차 세계 대전 연합군 승리의 숨은 공신! 세계를 구한 천재 수학자 앤런 튜링 - 방구석1열 - JTBC (24m)

# 제5절 전치 암호와 치환 암호

## 5.1 전치 암호

## 5.2 치환 암호

## 5.1 전치 암호

- 전치 암호(transposition cipher)
  - 전치란 평문에서 사용하는 문자의 집합과 암호문에서 사용하는 문자의 집합이 동일
  - 문자집합 내부에서 「자리를 바꾸는 규칙」
  - 평문에 사용된 문자와 암호문에 사용된 문자가 일대일 대응 규칙
  - 시저 암호

## 5.2 치환 암호

- 치환 암호(substitution cipher)
  - 치환 암호의 엄밀한 의미는 평문에서 사용하는 문자의 집합과 암호문에서 사용하는 집합이 다를 수 있다
  - 평문 문자를 다른 문자로 「교환하는 규칙」
  - 교환규칙이 일대일 대응이 아니어도 무방
  - 비장느르 암호
  - 모든 전치 암호는 치환 암호

# 제6절 암호 알고리즘과 키

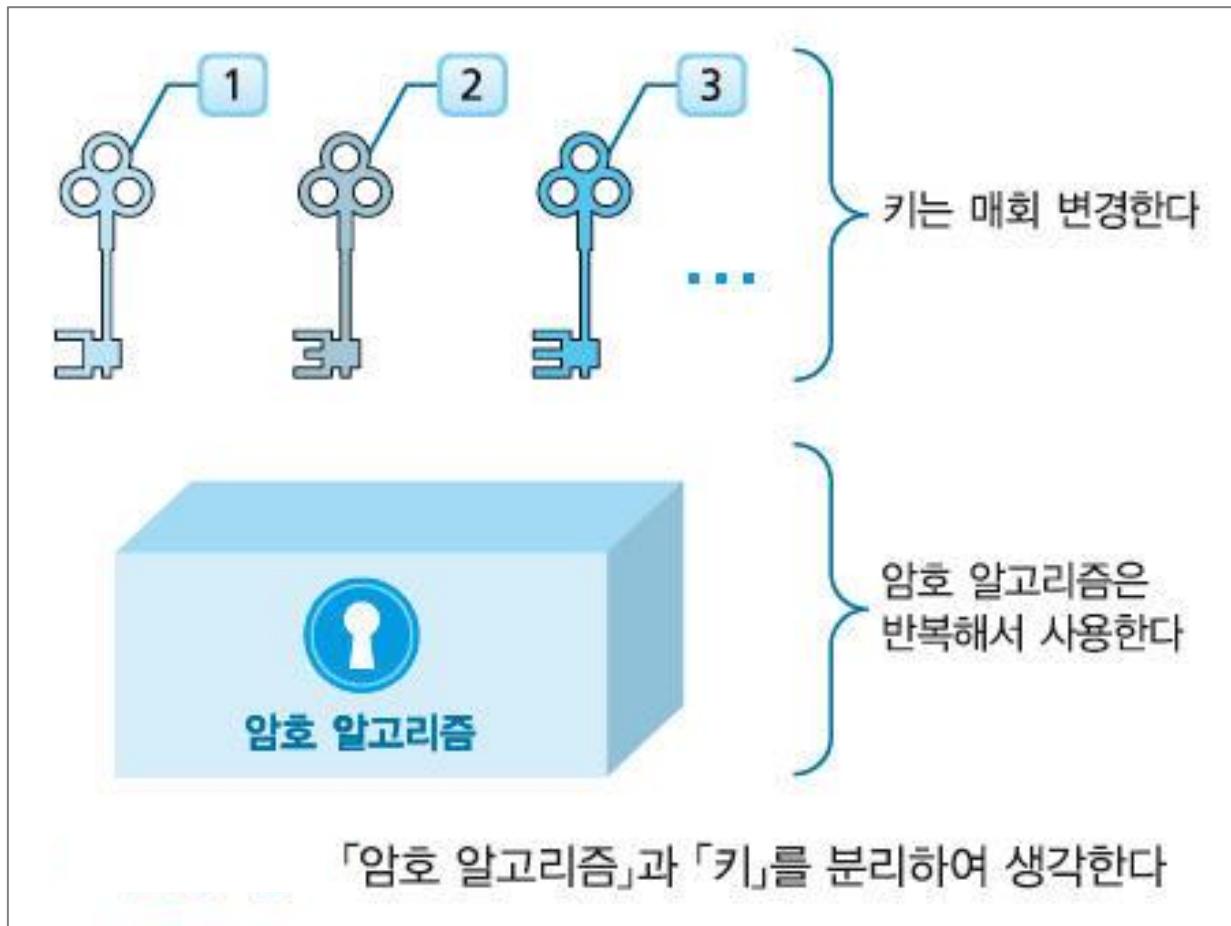
## 6.1 암호 알고리즘과 키를 분리하는 이유

- 암호알고리즘과 키의 조합을 분석
  - . 알고리즘내의 변경가능한 부분이 반드시 포함 → 키
- 암호알고리즘과 키를 반복해서 사용하면?
  - .해독 가능성?
  - .변경가능한 부분을 미리 준비해두고 사용시 매번 바꾸는것이 바람직

# 암호알고리즘과 키

암호명	암호 알고리즘	키
시저 암호	평문의 각 문자를 ‘지정한 문자 수’만큼 평행 이동한다.	평행 이동하는 문자 수
단일 치환 암호	치환표에 따라 알파벳을 변환한다.	치환표
에니그마 (통신키의암호화)	에니그마의 기계를 써서 『플러그 보드의 연결선, 3장의 로터의 순서, 각 로터의 설치 각도』에 따라 알파벳을 변환한다.	<ul style="list-style-type: none"><li>• 플러그 보드의 연결선</li><li>• 3장의 로터 순서</li><li>• 각 로터의 설치 각도</li></ul>
에니그마 (통신문의암호화)	플러그 보드의 연결선과 3장의 로터의 순서를 고정한 에니그마 기계를 사용하여 『각 로터의 설치 각도』에 따라 알파벳을 변환한다.	각 로터의 설치 각도

# 「암호 알고리즘」과 「키」를 분리



- 키는 비밀중에서 가장 중요
- 암호기술에서 키의 관리가 매우 중요(12장)

# 연습문제

# 연습문제

Q1. 시저암호에 대한 전사공격을 할 경우 키공간의 크기는 얼마인가?

A: 26

# 연습문제

Q2. 다중 치환암호에 대한 설명으로 맞는 것은?

- ① 단일 치환암호를 중복해서 적용한 암호이다.
- ② 시저 암호에서 사용한 암호방법이다.
- ③ 암호문에서는 문자의 빈도수가 거의 동일하게 나타난다.
- ④ 키 공간의 크기는 단순 치환암호의 키 공간과 동일하다.
- ⑤ 공개 키 암호의 일종이다.

# 연습문제

Q3. ( ) 암호는 하나의 문자를 다른 문자로 교환한다.

- ① 치환
- ② 전치
- ③ 대칭 암호
- ④ 공개 키 암호

# 연습문제

Q4. ( ) 암호는 가장 간단한 단일 치환 암호이다. 이는 26의 계수를 가지는 모듈러(modular) 연산을 사용한다.

- ① 시저암호
- ② 에니그마
- ③ 일회용 패드
- ④ 비장느르

# 연습문제

Q5. ( ) 암호란 평문에 사용하는 문자의 집합과 암호문에 사용하는 문자의 집합이 동일하고 이 두 집합 사이의 일대일 대응 규칙이다.

- ① 첨가
- ② 이동
- ③ 단일치환
- ④ 비장느르

# 연습문제

Q6. ( ) 암호는 암호문에 나타나는 문자의 빈도가 평문에 나타나는 문자의 빈도와 다르도록 문자들을 다른 문자들로 교체한다.

- ① 시저
- ② 다중치환
- ③ 이동
- ④ 단일치환

# 연습문제

Q7. 다음중 성격이 다른 암호는?

- ① 시저암호
- ② 비장르암호
- ③ 힐암호
- ④ 에니그마

# 연습문제

Q8. 암호시스템의 4가지 구성요소와 가장 중요한 요소를 설명하시오.

A: 평문, 암호문, 암호화알고리즘, 복호화알고리즘, 키공간(집합)

A: 가장중요한 요소는 키공간

# Thank You!

# Q & A