

알기 쉬운

정보보호개론

3판

흥미로운 암호 기술의 세계

INFORMATION SECURITY and CRYPTOGRAPHY





INFORMATION SECURITY and CRYPTOGRAPHY

CHAPTER 3 암호의 역사

Section 01 시저 암호

Section 02 단일 치환 암호

Section 03 다중 치환 암호

Section 04 에니그마

Section 05 암호 알고리즘과 키



Section 01

시저 암호

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 수만큼 「평행이동」 시킴으로써 암호화

알파벳 3문자 평행 이동

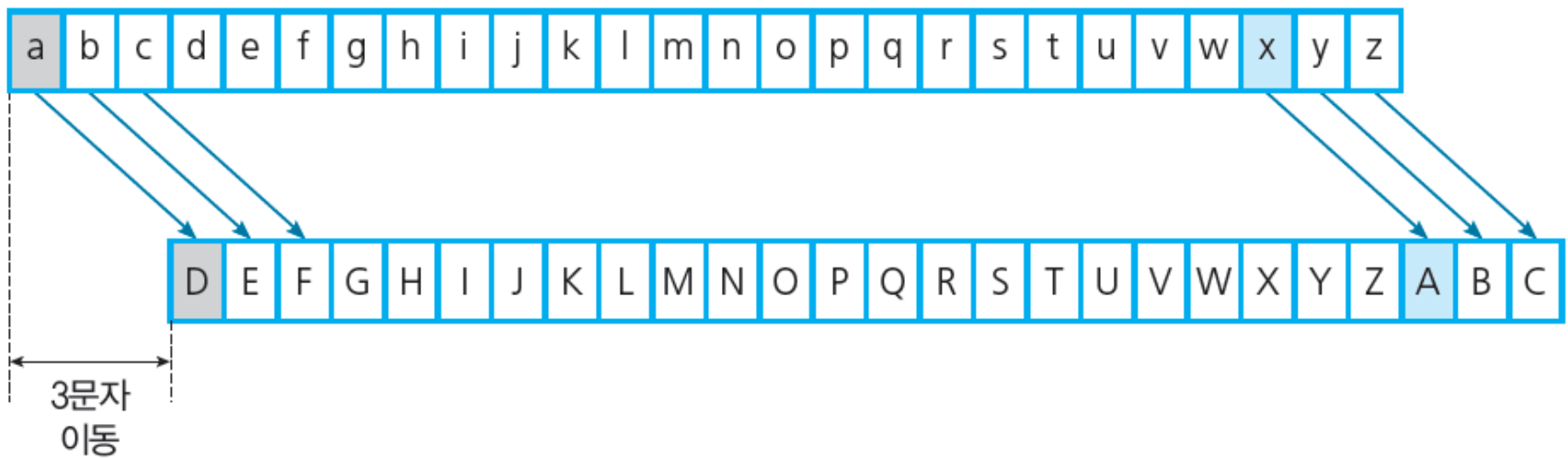


그림 3-1 • 시저 암호에서는 알파벳을 「평행 이동」시킨다

1.2 시저 암호의 암호화

- 평문: kabsoonyee
- 암호문: NDEVRRQBHH

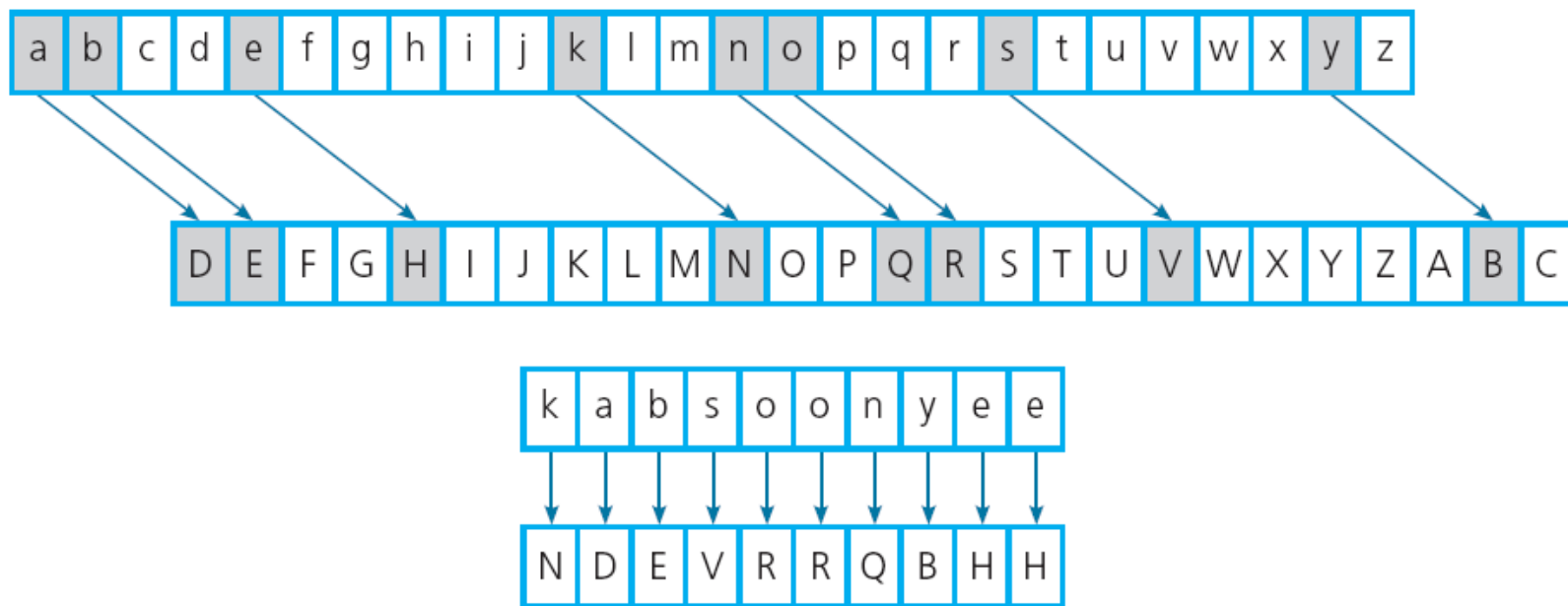


그림 3-2 • 평문을 한 문자씩 암호화하기

시저 암호에 의한 암호화

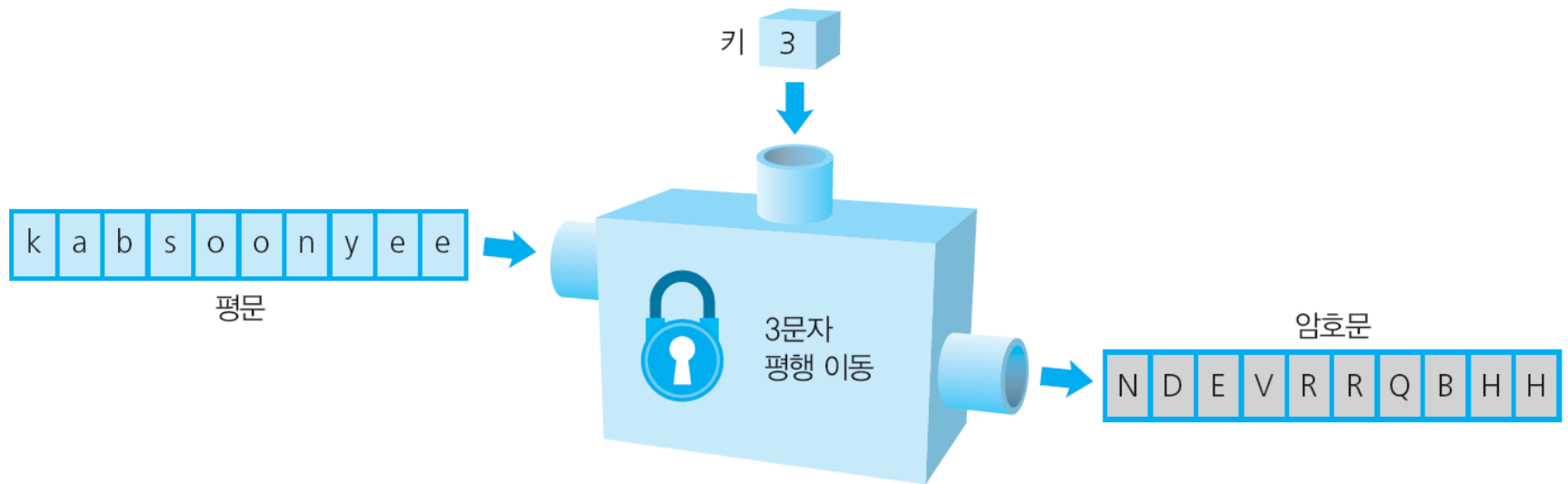


그림 3-3 • 시저 암호에 의한 암호화(키는 3)

1.3 시저 암호의 복호화

- 암호화 때와 동일한 크기의 역방향 평행 이동

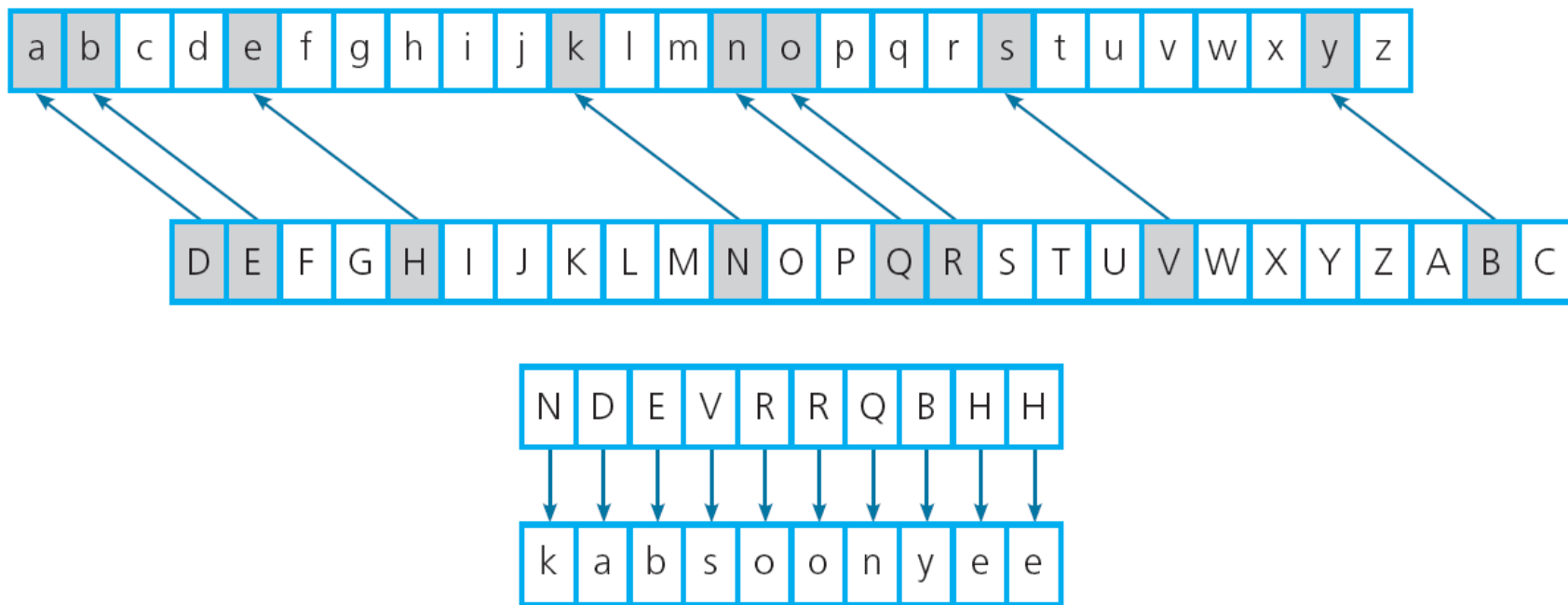


그림 3-4 • 암호문을 1문자씩 복호화하기

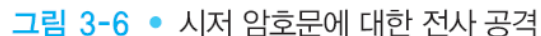
시저 암호에 의한 복호화



그림 3-5 • 시저 암호에 의한 복호화(키는 -3)

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
 - 힘 닿는 데까지 공격
 - 전수탐색(exhaustive search), 라운드로빈법 : 모든 키 중에서 바른 키를 찾는 것



Quiz 1 시저암호

- 시저암호로 암호화된 다음과 같은 암호문이 당신의 손에 들어왔다고 하자. 키 (평행 이동된 문자 수)는 알 수 없다. 이 암호문을 해독해 보시오.

PELCGBTENCUL

Quiz 1 시저암호

PELCGBTENCUL 키 0으로 복호화 pelcgbtencul
PELCGBTENCUL 키 1로 복호화 odkbfasdmdbtk
PELCGBTENCUL 키 2로 복호화 ncjaezrcclasj
PELCGBTENCUL 키 3으로 복호화 mbizdyqbkzri
PELCGBTENCUL 키 4로 복호화 lahycxpajyqh
PELCGBTENCUL 키 5로 복호화 kzgxbwozixpg
PELCGBTENCUL 키 6으로 복호화 jyfwavnyhwof
PELCGBTENCUL 키 7로 복호화 ixevzumxgvne
PELCGBTENCUL 키 8로 복호화 hwduytlwfumd
PELCGBTENCUL 키 9로 복호화 gvctxskvetlc
PELCGBTENCUL 키 10으로 복호화 fubswrjudskb
PELCGBTENCUL 키 11로 복호화 etarvqitcrja
PELCGBTENCUL 키 12로 복호화 dszquphsbqiz
PELCGBTENCUL 키 13으로 복호화 **cryptography**

Section 02

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)

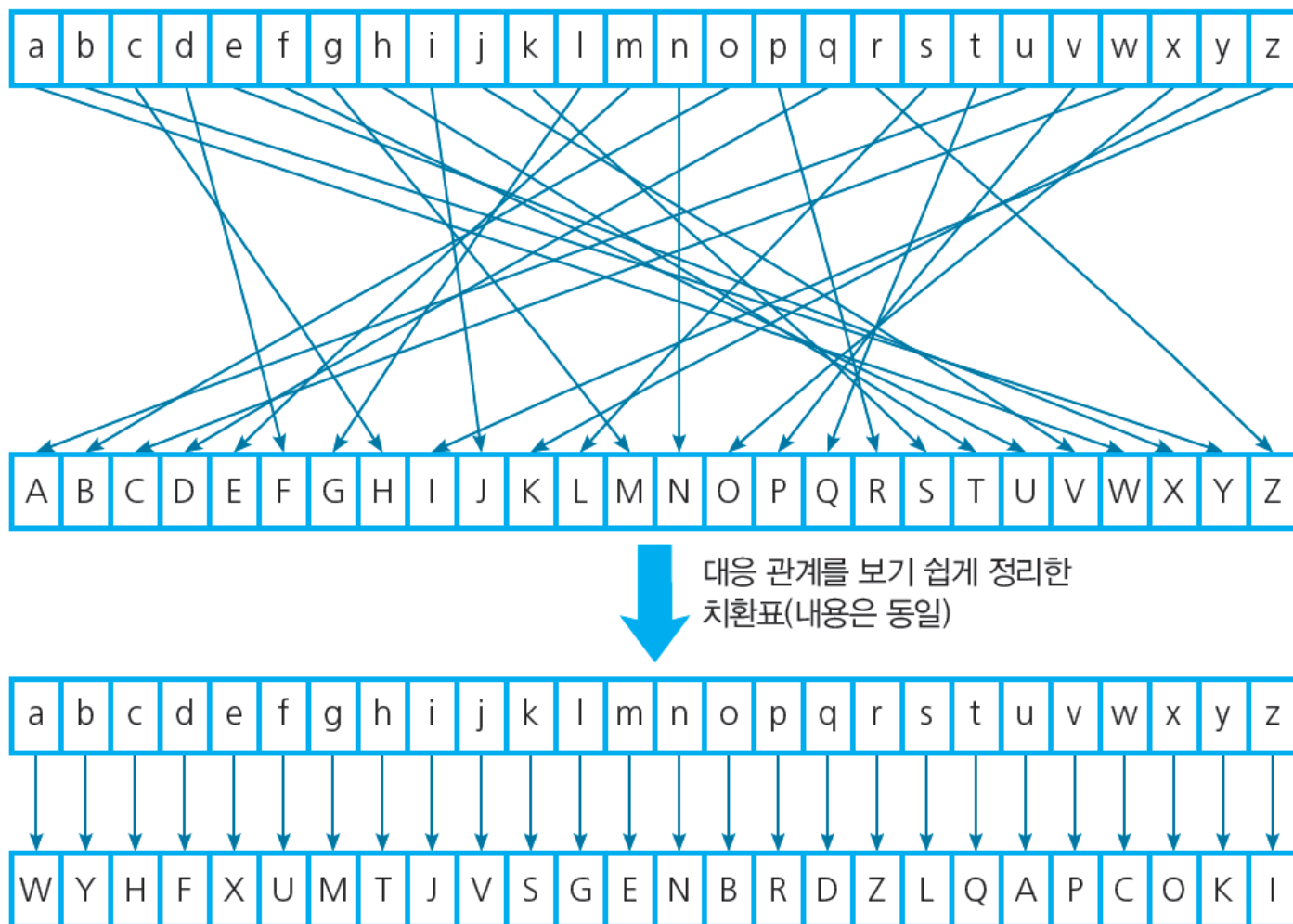
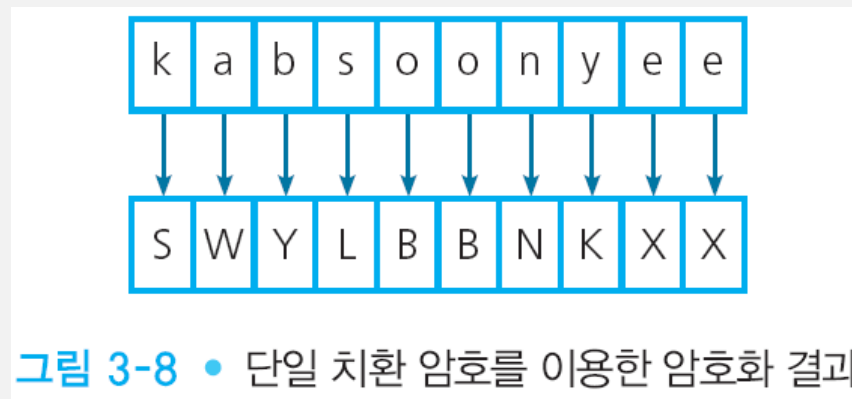


그림 3-7 • 단일 치환 암호의 치환 표(예)

2.2 단일 치환 암호의 암호화

- 평문 **kabsoonyee** 를 암호화
- 암호문: **SWYLBBNKXX**



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

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 어려움**
 - 이유 : 단일 치환 암호가 시저 암호에 비해 훨씬 많은 키 후보를 가질 수가 있기 때문임

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 전사 공격은 어렵다.
 - 단일 치환 암호의 키의 총수

$$\begin{aligned} & 26 \times 25 \times 24 \times 23 \cdots \times 1 \\ & = 403,291,461,126,605,635,584,000,000 \\ & = 4 \times 10^{26} \end{aligned}$$

약 4조의 1000조배 되는 값

전사공격 시간

$$26 \times 25 \times 24 \times 23 \cdot \cdot \cdot \times 1$$

$$= 403291461126605635584000000$$

- 키 수가 이렇게 많다면 1초에 10억 개의 키를 적용하는 속도로 조사한다고 해도, 모든 키를 조사하는데 120억년 이상의 시간이 필요
- 바른 키를 찾아내는데 평균 약 60억년

2.5 빈도 분석에 의한 해독

- 단일 치환 암호는 안전할까?
- 전사 공격에서 단일 치환 암호를 해독하는 것은 어렵다.
- **그러나, 빈도 분석 암호 해석법을 사용하면 단일 치환 암호도 해독할 수 있다.**

빈도분석을 이용한 암호해독

- 암호문
- 단일치환 암호로 암호화 되었다는 가정

MEYLGVIWAMEYOPINYZGWYEGMZRUUY PZAIXILGVSIZZMPGKKDWOME P
GROEIWGPCEIPAMDKKEYCIUYMGIFRWCEGLOPINYZHRZMPDNYWDWOG
WITDWYSEDCEEIAFYWWMPIDWYAGTYPIKGLMXFPIWCEHRZMMEYMEDW
OMGQRYWCEUXMEDPZMQRGMEYAPISDWOFICJILYSNICYZEYMGGJIPR
WIWAIHRUNIWAHRZMUDZZYAMEYFRWCCEMRPWDWOPGRWAIOIDWSD
MEIGWYMSGMEPYEYHRUNYARNFRMSDMEWGOPYIMYPZRCCYZZIOID
WIWAIOIDWEYMPDYAILMYPM_eYMWUNMDWOUGPZYKFRMIMKIZMEIA
MGODTYDMRNIWASIKJYASIXSDMEEDZWGZYDWMYIDPZIXDWODIUZR
PYMEYXIPYZGRPDMDZYIZXMGAYZNDZYSEIMXGRCIWWGMOYM

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

- 애드거 앨런 포의 황금벌레에 등장하는 영문자의 빈도수 나열

– e t a o l n s h r d l u c m f w g y p b v k x j q z

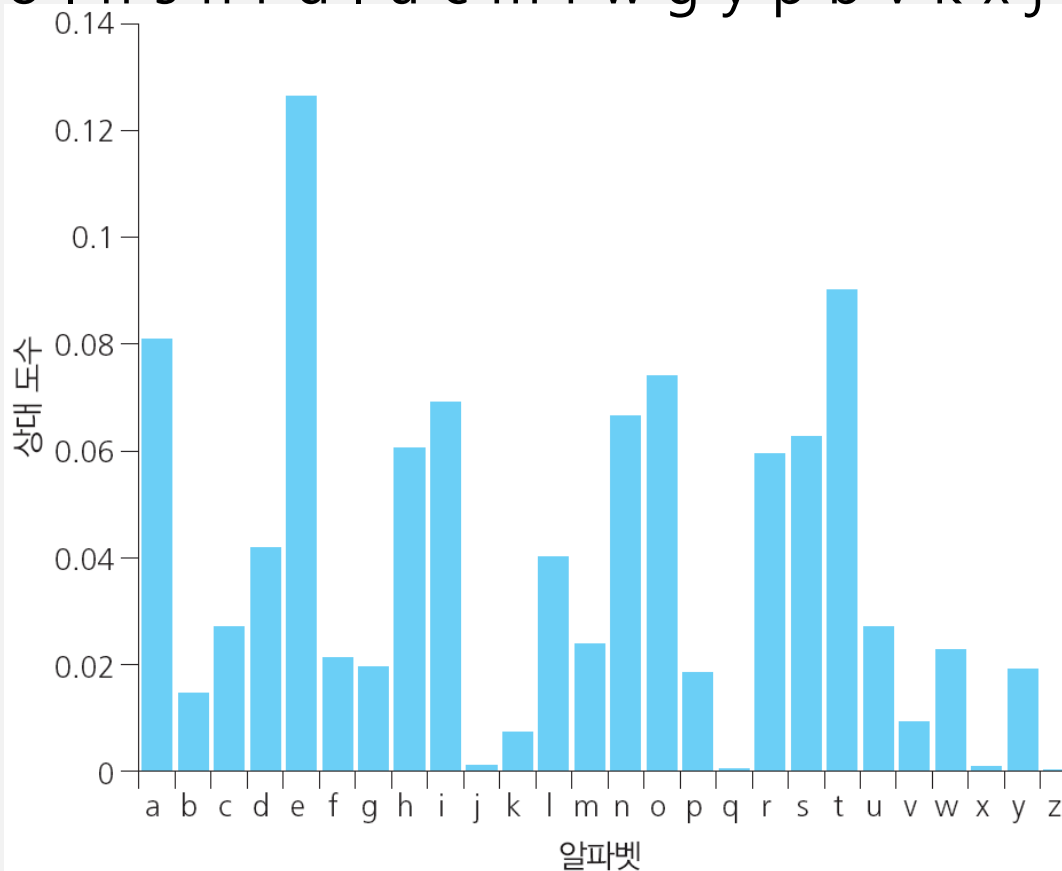


그림 3-9 • 영어 알파벳 출현 빈도

최빈도를 갖는 문자를 e로 변환

- I나 Y중 하나를 e라고 가정
 - Y를 e로 변환

MEeLGVIWAMEeOPINeZGWeEGMZRUUePZAIXILGVSI ZZMPGKKDWO
 MEPGROEIWGPCEIPAMDKKEeCIUeMGIFRWCEGLOPINeZHRZMPDNe
 WDWOGWITDWeSEDCEEIAFeeWMPIDWeAGTePIKGLMXFPIWCEHRZ
 MMEeMEDWOMGQReWCEUXMEDPZMQRGMEEEeAPISDWOFICJILESN
 ICeZEeMGGJIPRWIWAHRUNIWAHRZMUDZZeAMEeFRWCCEMRPWDW
 OPGRWAI OIDWSDMEIGWeMSGMEPeEeHRUNEARNFRMSDMEWGO
 PeIMePZRCCeZZIOIDWIWAI OIDWEeMPDeAILMePMEeMWUNMDWO
 UGPZeKFRMIMKIZMEIAMGODTeDMRNIWASIKJeAISIXSDMEEDZWGZ
 eDWMEeIDPZIXDWODIUZRPeMEeXIPeZGRPDMDZeIZXMGAeZNDZeS
 EIMXGRCIWWGMOeM

M~~E~~e가 the가 아닐까?

- 영어에 자주 등장하는 the 검색
 - M~~E~~e를 the로 추정

M~~E~~eLGVIWAM~~E~~eOPINeZGWeEGMZRUUePZAIXILGVSIZZMPGKKDWO
 MEPGROEIWGPCEIPAMDKKEeCIUeMGIFRWCEGLOPINeZHRZMPDNe
 WDWOGWITDWeSEDCEEIAF~~e~~eWMPIDWeAGTePIKGLMXFPIWCEHRZ
 M~~E~~eMEDWOMGQReWCEUXMEDPZMQRGME~~E~~eAPISDWOFICJILeSN
 ICeZEeMGGJIPRWIWAHRUNIWAHRZMUDZZeA~~M~~~~E~~eFRWCEMRPWDW
 OPGRWAIOIDWSDMEIGWeMSGMEP~~ee~~EeHRUNeARNFRMSDMEWGO
 PeIMePZRCCeZZIOIDWIWAIOIDWeeMPDeAILMeP~~M~~~~E~~eMWUNMDWO
 UGPZeKFRMIMKIZMEIAMGODTeDMRNIWASIKJeAISIXSDMEEDZWGZ
 eDWMEeIDPZIXDWODIUZRPeMEeXI~~P~~eZGRPDMDZeIZXMGAeZNDZeS
 EIMXGRCIWWGMOeM

$M \rightarrow t$, $E \rightarrow h$ 로 변경

theLGVIWatheOPINeZGWeEGMZRUUePZAIXILGVSIZZMPGKKDWOME
 PGROEIWGPCEIPAMDKKEeCIUeMGIFRWCEGLOPINeZHRZMPDNeWD
 WOGWITDWeSEDCEEIAFeeWMPIDWeAGTePIKGLMXFPIWCEHRZMthe
 MEDWOMGQReWCEUXMEDPZMQRGMEeEAPISDWOFICJILESNICEZEe
 MGGJIPRWIWAHRUNIWAHRZMUDZZeAtheFRWCEMRPWDWOPGRW
 AOIDWSDMEIGWeMSGMEPeEeHRUNeARNFRMSDMEWGOPeIMeP
 ZRCCeZZIOIDWIWAIOIDWeeMPDeAILMePtheMWUNMDWOUGPZeKF
 RMIMKIZMEIAMGODTeDMRNIWASIKJeAISIXSDMEEDZWGZeDWMeel
 DPZIXDWODIUZRPeMEeXIPeZGRPDMDZeIZXMGaeZNDZeSEIMXGRCI
 WWGMOeM

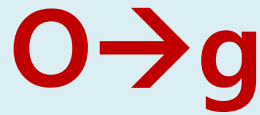
thPee가 three가 아닐까?

theLGVIWatheOPINeZGWehGtZRUEPZAIXILGVSIZZtPGKKDWothPGR
 OhIWGPChIPAtDKKheCIUetGIFRWChGLOPINeZHRZtPDNeWDWOGWI
 TDWeShDChhIAFeeWtPIDWeAGTePIKGLtXFPIWChHRZtthethDWOtGQ
 ReWChUXthDPZtQRGthheAPISDWOFICJILeSNICeZhetGGJIPRWIWAH
 RUNIWAHRZtUDZZeAtheFRWChRPWDWOPGRWAIOIDWSDthIGWetS
 GheHRUNeARNFRtSDthWGOPeltePZRCCeZZIOIDWIWAIOIDWh
 etPDeAILtePthetWUNtDWOUGPZeKFRtltKIZthIAAtGODTeDtRNIWASIKJe
 AISIXSDthhDZWGZeDWtheIDPZIXDWODIUZRPetheXIPeZGRPDtDZeIZ
 XtGAeZNDZeShltXGRCIWWGtOet

P → **r**

Oet는 get 이 아닐까?

theLGVIWAtheOrlNeZGWehGtZRUUerZAIxILGVsIZZtrGKKDWothrGRO
hIWGrChlrAtDKKheCIUetGIFRWChGLOrIneZHRZtrDNeWDWOGWITD
WeShDChhIAFeeWtrIDWeAGTerIKGLtXFrIWChHRZtthethDWOtGQReW
ChUXthDrZtQRGthheArISDWOFICJILeSNICeZhetGGJlrRWIWAiHRUNI
WAHRZtUDZZeAtheFRWChtrRWDWOrGRWAIOIDWSDthIGWetSG^{thre}
^eheHRUNeARNFRtSDthWGOrelterZRCCeZZIOIDWIWAIOIDWhetrDeAI
LterthetWUNtDWOUGrZeKFRTltKIZthlAtGODTeDtRNIWASIKJeAISIXSDt
hhDZWGZeDWtheIDrZIXDWODIUZRretheXlreZGRrDtDZeIZXtGAeZND
ZeShltXGRCIWWGtOet



theLGVIWAthe^grlNeZGWehGtZRUUerZAIXILGVSI ZZtrGKKDW^gthrGR^gh
IWGrChlrAtDKKheCIUetGIFRWChGL^grlNeZHRZtrDNeWDW^gGWITDW
eShDChhIAFeeWtrIDWeAGTerIKGLtXFrIWChHRZtthethDW^gtGQReWC
hUXthDrZtQRGthheArISDW^gFICJILeSNICeZhetGGJlrRWIWAHRUNIWA
HRZtUDZZeAtheFRWChtrRrWDW^grGRWAI^gIDWSDthIGWetSG^{three}he
HRUNeARNFRtSDthWG^grelderZRCCeZZI^gIDWIWAI^gIDWhetrDeAILtert
hetWUNtDW^gUGrZeKFRtltKIZthlAtG^gDTeDtRNIWASIKJeAISIXSDthhDZ
WGZeDWtheIDrZIXDW^gDIUZRretheXlreZGRrDtDZelZXtGAeZNDZeShlt
XGRCIWWGt^get

thethDWg는 thething 이 아닐까?

theLGVIWAthegrINeZGWehGtZRUUerZAIXILGVSIZZtrGKKDWgthrGRgh
 IWGrChlrAtDKKheCIUetGIFRWChGLgrINeZHRZtrDNeWDWgGWITDW
 eShDChhIAFeeWtrIDWeAGTerIKGLtXFrIWChHRZt**thethDWg**tGQReWC
 hUXthDrZtQRGthheArISDWgFICJILeSNICeZhetGGJlrRWIWAHRUNIWA
 HRZtUDZZeAtheFRWChtrRrWDWgrGRWAlglDWSDthIGWetSGthreehe
 HRUNeARNFRtSDthWGgrelderZRCCeZZIglDWIWAAlglDWhetrDeAILtert
 hetWUNtDWgUGrZeKFRtltKIZthlAtGgDTeDtRNIWASIKJeAISIXSDthhDZ
 WGZeDWtheIDrZIXDWgDIUZRretheXlreZGRrDtDZeIZXtGAeZNDZeShlt
 XGRCIWWGtget

D→i, W→n

$D \rightarrow i, W \rightarrow n$

theLGVInAthe**grlNe**ZGnehGtZRUUerZAIxILGVsIZZtrGKK**ing**thrGRghIn
 GrChlrAtiKKheCIUetGIFR**n**ChGL**grlNe**ZHRZtriNen**ing**GnITineShiChhIAF
 een**n**trlineAGTerIKGLtXFrInChHRZttheth**ing**tGQRenChUXthirZtQRGthhe
 Arl**Sing**FICJILeSNICeZhetGGJlrR**n**InAIHRUNInAHRZtUiZZeAtheFR**n**Cht
 Rr**n**ingrGR**n**Algli**n**SithIG**n**etSGthreeheHRUNeARNFRtSith**n**G**gre**lterZR
 CCeZZIgli**n**InAlgli**n**hetrieAlLterthet**n**UNt**ing**UGrZeKFRtltKIZthlAtGgiTeit
 RNI**n**ASIKJeAISIXSithhi**n**GZe**n**thelirZIX**ing**iIUZRretheXlreZGRritiZelZX
 tGAeZNiZeShltXGRCl**nn**Gtget

단어 패턴

- **grlNe**라는 패턴이 보인다. 사전을 찾아보았더니, **grace, grade, grape, grate, grave, gripe, grofe, ...**처럼 많은 후보가 있다. 이것으로는 결정을 할 수 없다.

l→a를 가정해 보면 **greater**라는 패턴이 나오므로 l→a는 맞는 것 같다.

I → a 가 맞는 것 같다

theLGVInAthe**grlNe**ZGnehGtZRUErZAIXLGVSI ZZtrGKKingthrGRghIn
 GrChlrAtiKKheCIUetGIFRnChGL**grlNe**ZHRZtriNeningGnlTineShiChhIAF
 eent**trline**AGTerIKGLtXFrInChHRZtthethingtGQRenChUXthirZtQRGthhe
 ArlSingFICJILeSNICeZhetGGJlrRnInAIHRUNInAHRZtUiZZeAtheFRnCh
 RrningrGRnAlglinSithIGnetSGthreeheHRUNeARNFRtSithnG**grelder**ZRC
 CeZZIglinInAlglinhetrieAILterthetnUNtingUGrZeKFRtltKIZthlAtGgiTeitR
 NInASIKJeAISIXSithhiZnGZeinthelirZIXingilUZRretheXlreZGRritiZelZXt
 GAeZNiZeShltXGRClInnGtget

I → a 라고 가정하면 **grelder** → **greater**



theLGVanAtheGraNeZGnehGtZRUErZAaXaLGVSaZZtrGKKingthrGRgh
anGrCharAtiKKheCaUetGaFRnChGLgraNeZHRZtriNeningGnaTineShiC
hhAFeentraineAGTerKGLtXFranchHRZtthethingtGQRenChUXthirZtQ
RGthheArSingFaCJaLeSNaCeZhetGGJarRnaaHRUNaAHRZtUiZZe
AtheFRnChtrRningrGRnAagainSithaGnetSGthreeheHRUNeARNFRtSith
nGgreaterZRCCeZZagainanAagainhetrieAalterthetnUNtingUGrZeKFRt
atKaZthaAtGgiTeitRNanASaKJeAaSaXSithhiZnGZeintheairZaXingiaUZR
retheXareZGRritiZeZXtGAeZNiZeShatXGRCannGtget


$N \rightarrow c$ 가 아닌 것 같다

theLGVanAthe**graNe**ZGnehGtZRUErZAaXaLGVSaZZtrGKKingthrGRgh
 anGrCharAtiKKheCaUetGaFRnChGLgraNeZHRZ**triNening**GnaTineShiC
 hhaAFeentraineAGTeraKGLtXFranChHRZtthethingtGQRenChUXthirZtQ
 RGthheAraSingFaCJaLeSNaCeZhetGGJarRnanAaHRUNanAHRZtUiZZeA
 theFRnChRrningrGRnAagainSithaGnetSGthreeheHRUNeARNFRtSithn
 GgreaterZRCCeZZagainanAagainhetrieAaLterthetnUNtingUGrZeKFRtat
 KaZthaAtGgiTeitRNanASaKJeAaSaXSithhiZnGZeintheairZaXingiaUZRre
 theXareZGRritiZeaZXtGAeZNiZeShatXGRCannGtget

$N \rightarrow c$ 라고 가정하면 **triNening** \rightarrow **tricening**

Tricening이라는 단어는 없는 것 같다.

아직 변환하지 못한 문자

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		

G와 Z가 빈도가 높다

- 빈도가 높은 문자 순서는 e>t>a>o 순이다.
- 아직 가정에 등장하지 않은 문자는 o 이다.
- 한편 암호문 중에 등장하는 빈도가 높은 문자로서 아직 모르는 것은 G와 Z

G→o라고 가정하자

G → O

theL○VanAtheGraNeZ○neh○tZRUUerZAaXaL○VSaZZtr○KKingthroRgha
n○rCharAtiKKheCaUet○aFRnCh○LgraNeZHRZtriNening○naTineShiChh
aAFeentraineA○TeraK○LtXFranChHRZtthethingt○QRenChUXthirZtQR○
thheAraSingFaCJaLeSNaCeZhet○○JarRnanAaHRUNanAHRZtUiZZeAthe
FRnChtrningr○RnAagainSitha○netS○threeheHRUNeARNFRtSithn○gr
eaterZRCCeZZagainanAagainhetrieAaLterthetnUNtingU○rZeKFRtatKaZ
thaAt○giTeitRNanASaKJeAaSaXSithhiZn○ZeintheairZaXingiaUZRretheX
areZ○RritiZeaZXt○AeZNiZeShatX○RCann○tget

C→c 가 확실하다

theLoVanAtheGraNeZonehotZRUUerZAaXaLoVSaZZtroKKingthroRgha
 norCharAtiKKheCaUetoaFRnChoLgraNeZHRZtriNeningonaTineShiChh
 aAFeentraineAoTeraKoLtXFranChHRZtthethingtoQRenChUXthirZtQRot
 hheAraSingFaCJaLeSNaCeZhetooJarRnanAaHRUNanAHRZtUiZZeAthe
 FRnChtrRningroRnAagainSithaonetSothreeheHRUNeARNFRtSithnogre
 aterZRCCeZZagainanAagainhetrieAaLterthetnUNtingUorZeKFRtatKaZt
 haAtogiTeitRNanASaKJeAaSaXSithhiZnoZeintheairZaXingiaUZRretheX
 areZoRritiZeaZXtoAeZNiZeShatXoR**Cannotget**

끝에 **Cannotget**이라는 패턴이 등장했다. C→c가 틀림없다.
 C→c라는 것을 통해 조금 전에 생각한 N→c는 역시 잘못된
 라는 것을 알 수 있다.

패턴

theLoVanAtheGraNeZonehotZRUErZAaXaLoVsaZZtr
oKKingthroRghanorcharAtiKKhecaUetoaFRnchoLgraN
eZHRZtriNeningonaTineShichhaAFeentraineAoTeraKo
LtXFranchHRZtthethingtoQRenchUXthirZtQRothheAr
aSingFacJaLeSNaceZhetooJarRnanAaHRUNanAHRZtU
iZZeAtheFRnchtRrningroRnAagainSithaonetSothreehe
HRUNeARNFRtSithnogreaterZRcceZZagainanAagainh
etrieAaLterthetnUNtingUorZeKFRtatKaZthaAtogiTeitR
NanASaKJeAaSaXSithhiZnoZeintheairZaXingiaUZRret
heXareZoRritiZeaZXtoAeZNiZeShatXoRcannotget

빈도가 낮은 문자 추측

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

패턴

- hotZRUEr → hotsummer 같다
($Z \rightarrow s, R \rightarrow u, U \rightarrow m$)
- Shich → which 일 것 같다
($S \rightarrow w$)
- thethingtoQRench → hethingtoQuench
(the thing to quench) 같다
($Q \rightarrow q$)

빈도가 낮은 문자 추측

theLoVanAtheGraNesonehotsummersAaXaLoVwasstroKKingthrougha
norcharAtiKKhecametoaFunchoLgraNesHustriNeningonaTinewichh
aAFeentraineAoTeraKoLtXFranchHustthethingtoquenchmXthirstquot
hheArawingFacJaLewNaceshetooJarunanAaHumNanAHustmisseAthe
FunchturningrounAagainwithaonetwothreeheHumNeAuNFutwithno
greatersuccessagainanAagainhetrieAaLterthetnmNtingmorseKFuta
tKasthaAtogiTeituNanAwaKJeAawaXwithhishnoseintheairsaXingiamsur
etheXaresouritiseasXtoAesNisewhatXoucannotget

단어와 내용 추측

- successagainanAagain라는 패턴이 있다. 이것은 success again and again일 것이다
(**A**→**d**)
- trieAaLter라는 패턴이 보인다. 이것은 틀림없이 tried after이다
(**L**→**f**).
- whatXoucannotget라는 패턴이 보인다. 이것은 what you cannot get일 것이다
(**X**→**y**).

단어와 내용 추측

thefoVandthegraNesonehotsummersdayafoVwasstroK
 KingthroughanorchardtKKhecametoaFunchofgraNesHu
 striNeningonaTinewhichhadFeentrainedoTeraKofTyFranc
 hHustthethingtoquenchmythirstquothhedrawingFacJafe
 wNaceshetooJarunandaHumNandHustmissedtheFuncht
 urningroundagainwithaonetwothreeheHumNeduNFutwi
 thnogreatersuccessagainandagainhetriedafterthetnmNti
 ngmorseKFutatKasthadtogiTeituNandwaKJedawaywithhi
 snoseintheairsayingiamsuretheyaresouritiseasytodesNis
 ewhatyoucannotget

단어와 내용 추측

- thefoVandthegraNesonehotsummersday

the foV and the graNes one hot summers day

$V \rightarrow x$

$N \rightarrow p$

정리

the fox and the grapes one hot summers day a fox was strok King through an orchard ti KK he came to a Funchof grapes Hustripening on a Tinewhich had Fe entrained o Tera Kofty Franch Hust the thing to quench my thirst quo thhedra wing Fac Ja few paces hetoo Jarunanda Hump and Hust missed the Funchtu rning round again with a one two three he Humped up Fut with no greater success again and again he tried after the tnmpting morse K Futat Kast had togi Te itup and wa K Jed away with his nose in the air saying i am sure they are sour itise asy to despise what you cannot get

정리

- foxwasstroKKing = fox was strolling
 - $(K \rightarrow I)$
- hetooJarunandaHumpandHustmissed = he took a run and a jump and just missed
 - $(H \rightarrow j)$
 - $(J \rightarrow k)$
- hejumpedupFutwithnogreatersuccess
- he jumped up but with no greater success
 - $(F \rightarrow b)$
- utatKasthadtogiTeitup = but at last had to give it up
- but at last had to give it up
 - $(T \rightarrow v)$
- 이 암호문에 나오지 않은 마지막 1문자
 - $(B \rightarrow z)$

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

403291461126605635584000000 가지 중의 한 개

해독된 평문

the fox and the grapes one hot summers day a fox was strolling through a
norchard till he came to a bunch of grapes just ripening on a vine which had
been trained over a lofty branch just that to quench my thirst quoth he dra
wing back a few paces he took a run and a jump and just missed the bunch t
urning round again with one two three he jumped up but with no greater s
uccess again and again he tried after the tempting morsel but at last had t
o 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

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 of 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 단서
- 처음과 끝을 아는 것은 단서
- 단어의 단락을 알면 그것도 단서
- 암호문이 길면 해독이 용이
- 같은 문자가 연속해서 나타나면 그것은 단서(단일 치환 암호에서는 어떤 문자가 어느 문자로 암호화 되는지 정해져 있기 때문)
- 해독의 속도가 점점 빨라짐

퀴즈 2 단일치환 암호의 개선

- 위의 예에서는 $c \rightarrow C$, $q \rightarrow Q$ 와 같이 평문의 문자가 동일 문자로 암호화되는 경우가 있었다. 이를 보고 앨리스는 동일 문자로 변환되지 않는 치환표를 사용하면 해독하기 어려워질 것이라고 생각한다. 이 생각은 맞는 것일까?

빈도분석에
강한
암호는 없을까?

Section 03

다중 치환 암호

3.1 빈도 분석이 가능한가?

3.1 빈도 분석이 가능한가?

- 빈도분석이 가능했던 이유는 평문에 등장하는 문자의 빈도와 암호문에 등장하는 문자의 빈도가 일치하기 때문
- **다중치환암호**(polyalphabetic substitution cipher)
 - 평문에 등장하는 문자의 빈도와 암호문에 등장하는 문자의 빈도를 다르게 만드는 암호 알고리즘
 - 비장느르 암호(Vigenere Cipher)
 - 에니그마 기계(Enigma machine)
 - 빈도분석을 이용한 공격방법이 무용지물

비장르 암호(Vigenere Cipher)

	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

비장느르 암호(Vigenere Cipher)

- SECURITY를 암호화하는 방법
 - 키워드를 정함(예 LOVE로 정함) 맨 앞줄을 기준으로 숫자 12 15 22 5와 매핑이 됨
 - S : 12행에 매핑되는 알파벳은 H
 - E : 15행에 매핑되는 알파벳은 Q
 - C : 22행에 매핑되는 알파벳은 H
 - U : 5행에 매핑되는 알파벳은 Q
 - R : 12행에 매핑되는 알파벳은 G
 - I : 15행에 매핑되는 알파벳은 U
 - T : 22행에 매핑되는 알파벳은 Y
 - Y : 5행에 매핑되는 알파벳은 U

Section 04

에니그마

- 4.1 에니그마란 무엇인가?
- 4.2 에니그마에 의한 암호 통신
- 4.3 에니그마의 구조
- 4.4 에니그마의 암호화
- 4.5 날짜별 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 만들려고 시도
- 발명 당시에는 에니그마를 상용으로 사용
- 나치독일 시대에는 군용으로 사용하려고 개량

에니그마와 로터



그림 3-10 • 독일군이 사용하던 에니그마의 외형적 모습

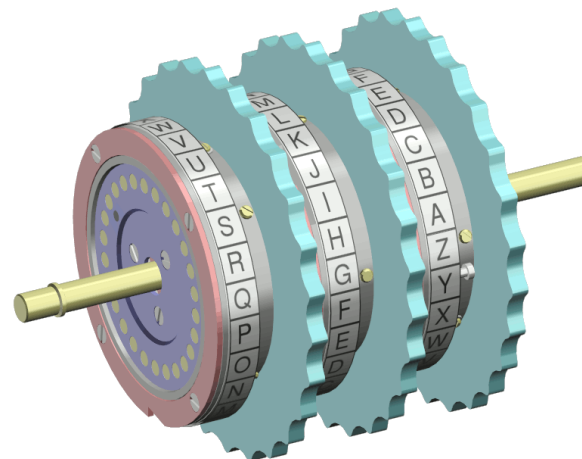


그림 3-11 • 에니그마의 내부에 사용되는 로터

4.2 에니그마에 의한 암호 통신

- 타이프라이터와 톱니바퀴와 전지와 전구를 조합한 기계
- 암호화와 복호화를 1대의 기계로 수행
- 송신자와 수신자는 각각 에니그마를 1대씩 소유

코드북과 코드북의 내부



GEHEIM! SONDER-MASCHINENSCHLÜSSEL: WOLFFACK-LEAGUE FEBRUAR 1942

Tag (HKU)	Salzenlage	Ringstellung	Stichwortverbindungen	Kenngruppen	
29	B	II VI V	26 23 24	AN BU CY DK FT HS JU LN ME FX	LES WDS KQJ QIQ
26	B	IV II I	07 22 12	AO CB EI GK HU JY LS NF QT RK	ANY AGG BTQ VHF
27	C	VII III VIII	03 02 17	AI BT CF DX EU GL HO IK NV SH	TUI LSY FZD KQA
26	C	V VIII II	26 26 20	AC DQ DG EH FR HS IY JP KT NY	PGC SAL GHT WVO
23	C	IV V VII	01 12 05	BP CE DJ EO FQ GT KR LX NU SY	ETE GHS LET FFF
24	B	VII VI III	09 06 10	AN BJ CH DE FT HU LI NF OS QR	VXD GRO TIS XID
22	C	V VII II	06 19 03	AI DQ CE HS JU KS NX OP TY VW	EGX LUT RQB BTQ
22	C	III IV VI	16 05 17	AN BU CH DH EQ FT GO IS JI LX	HLO GLO RVE UEE
21	C	V II VII	04 21 23	AO BY FH GS HT II KU LV NX FX	RSH DGR HXG GAN
20	C	IV VI VIII	19 11 26	BE CE DE FG GH IL JO KH QR VW	KYH FEF QQT QEE
19	C	VII I IV	04 09 17	AJ BF CT HR IQ KM LU OV PS XY	SAG CCG ARX GRY
18	C	VII III IV	02 11 16	AN BF CT DQ EV HS JL KR OP UY	ENH JRY TUI VAK
17	C	VI III V	07 21 11	AD EV CF EI FT GH KE LU NU QR	EMI JFI RUD ZAQ
16	B	VII IV III	15 16 02	AN DO OG PT ES FF IV JX LS UY	SVI GED WQY AUS
15	C	VI II IV	07 07 05	AL BV CJ DI EF GY HS KR NU OS	DIX CDO RPH BRK
14	B	IV II VI	06 19 09	BD CL EH FR GQ IM NN OX ST TS	AJR HKD VLE CVV
13	B	VIII VI III	15 21 11	AP EF FY EH GV HU IT OQ PV SX	WGG CGG LCI ZIG
12	B	VII VI VIII	01 06 12	AL DI FX GH IF IK OV RS TZ UY	JUP PCX RNC DGV

코드북에는 송/수신자가 사용하는 **날짜별 키**가 기록되어 있고, 송신자/수신자는 이 책자의 지시에 따라 에니그마를 설정

4.3 에니그마의 구조

- 에니그마는 알파벳 26 문자를 암호/복호화할 수 있지만, 그림이 복잡해지므로 여기서는 알파벳의 수를 4 문자로 가정

에니그마 암호통신 흐름

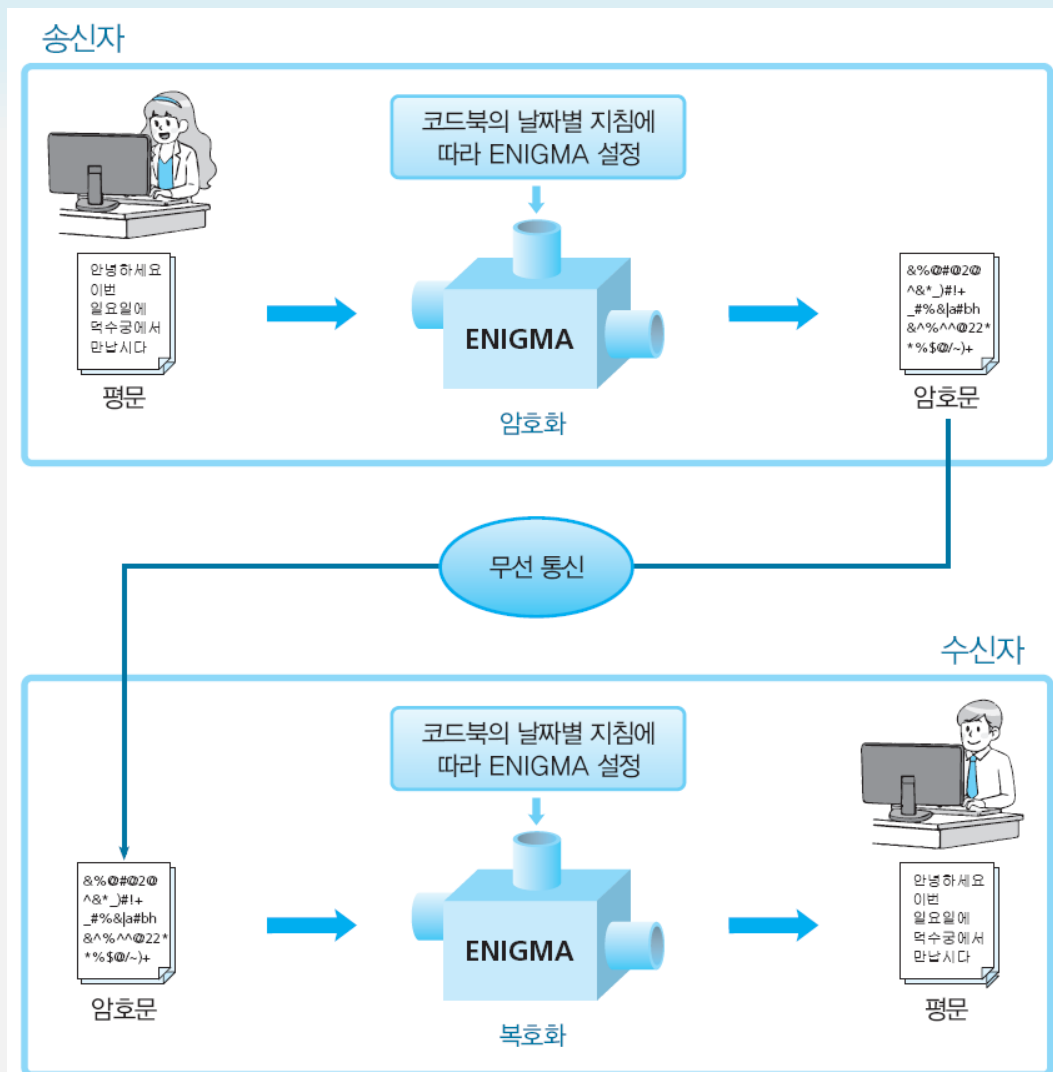


그림 3-13 • 에니그마를 사용한 암호 통신의 흐름

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, 로터2가 1 회전 하면 로터3이 $1/4$ 회전

에니그마의 구조(4문자)

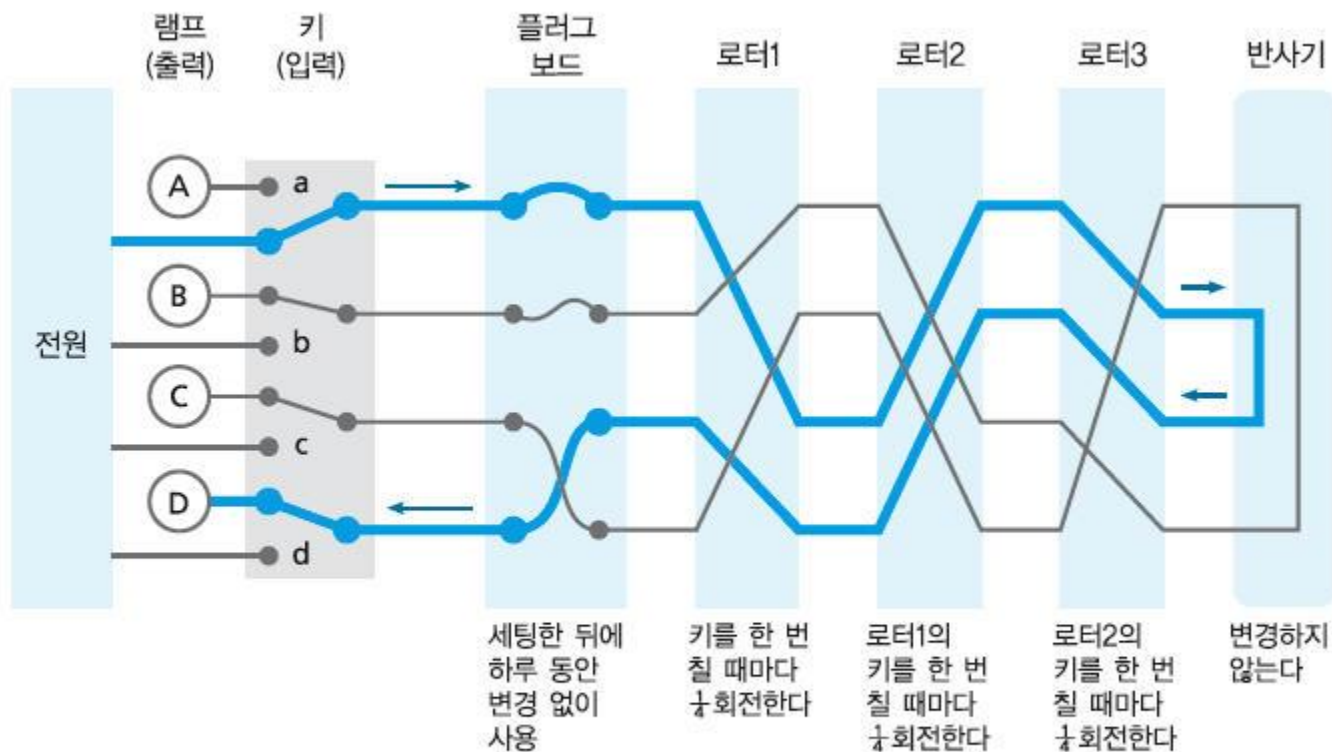
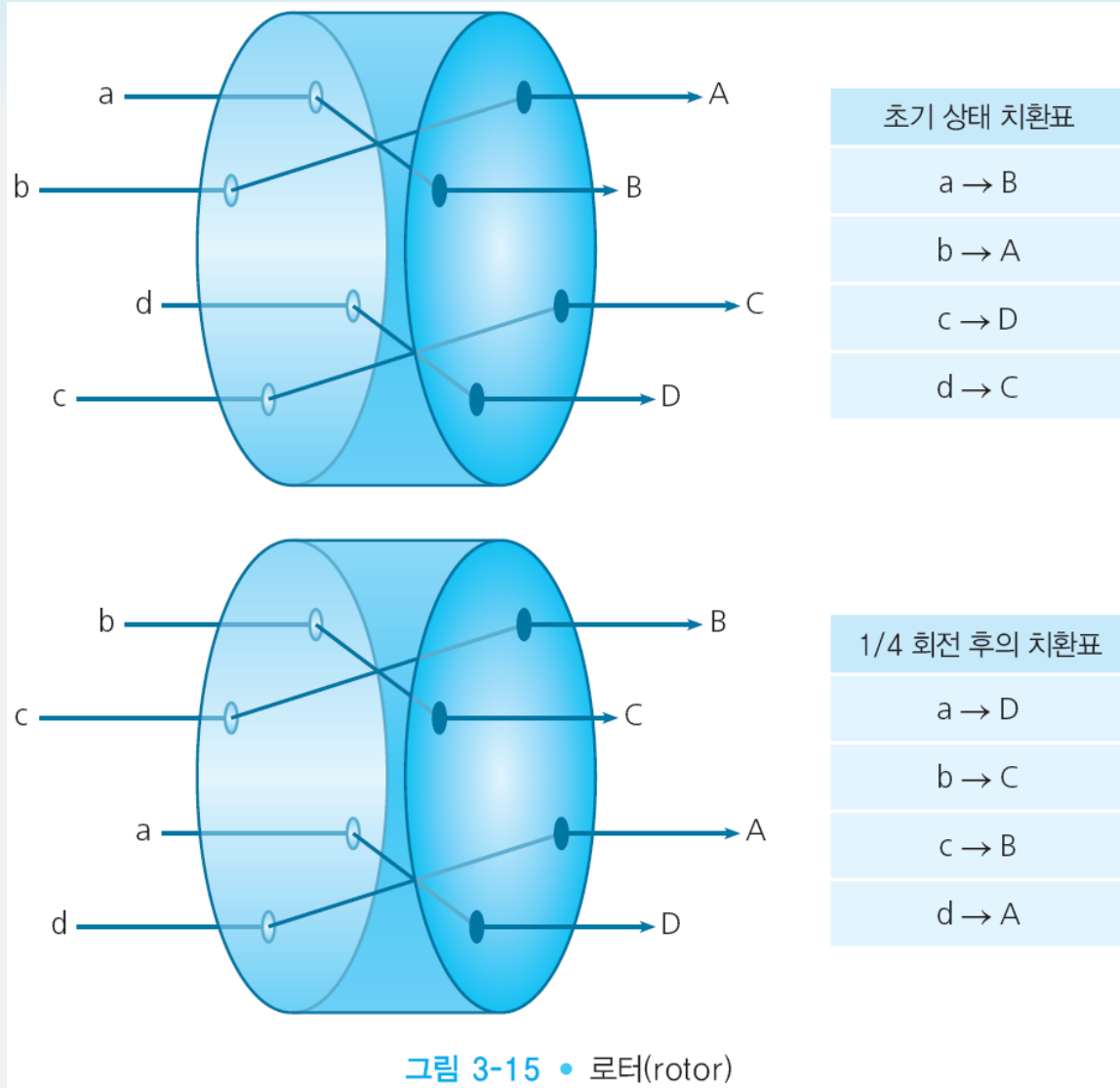


그림 3-14 · 에니그마의 구조(알파벳의 수를 4문자로 했을 경우)

로터



secretletter 를 암호화하기

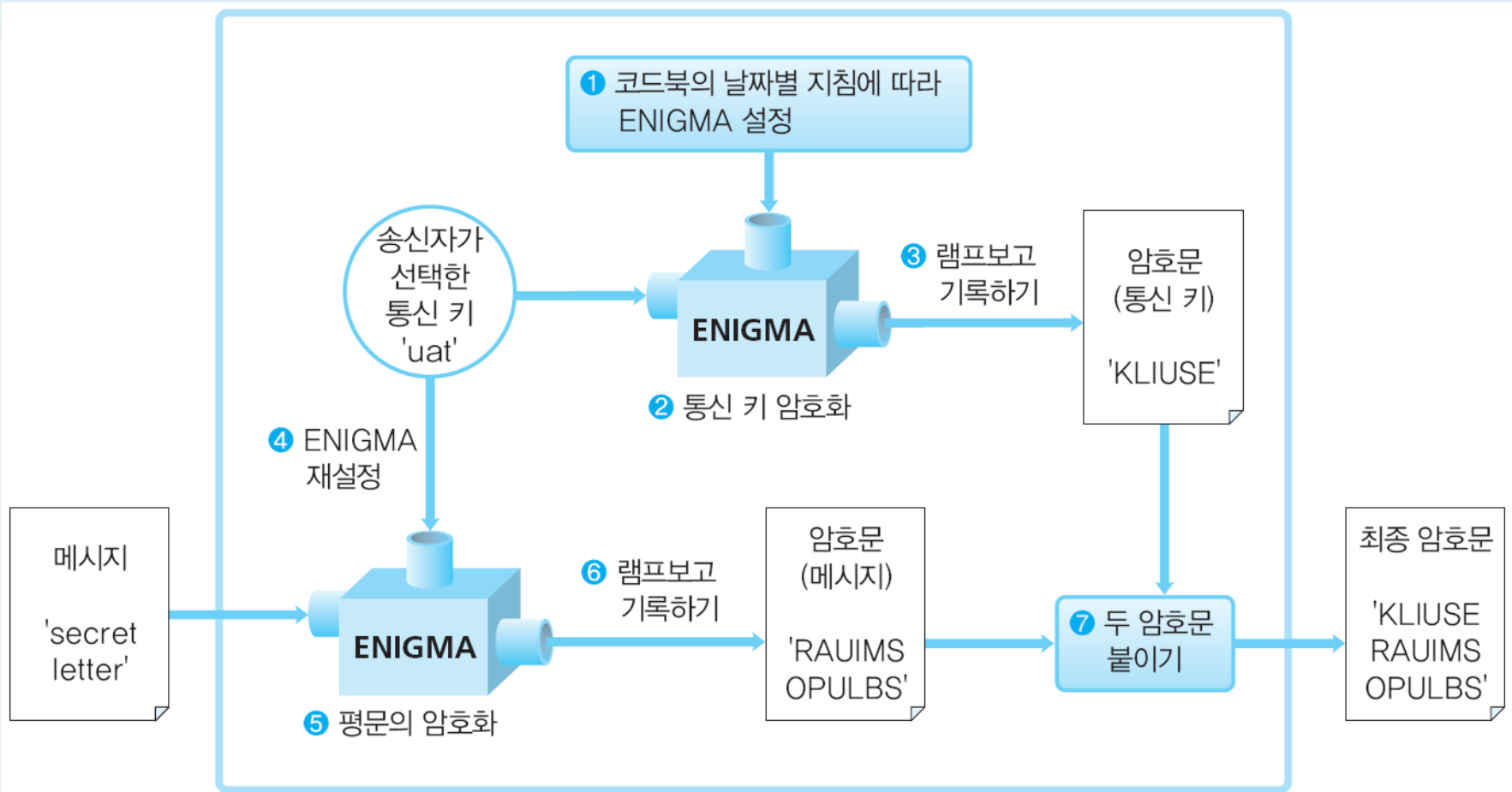


그림 3-16 • 에니그마를 사용하여 'secretletter'를 암호화 한다

4.4 에니그마 암호화

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

4.5 낱씨별 키와 통신 키

- 낱씨별 키는 메시지의 암호화가 아니라 통신키의 암호화에 사용
- 낱씨별 키는 「키를 암호화하기 위한 키」
 - 이와 같은 키를 **키 암호 키**(key encrypting key; KEK)라 한다
- 메시지를 통신키로 암호화하고, 통신키를 낱씨별 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

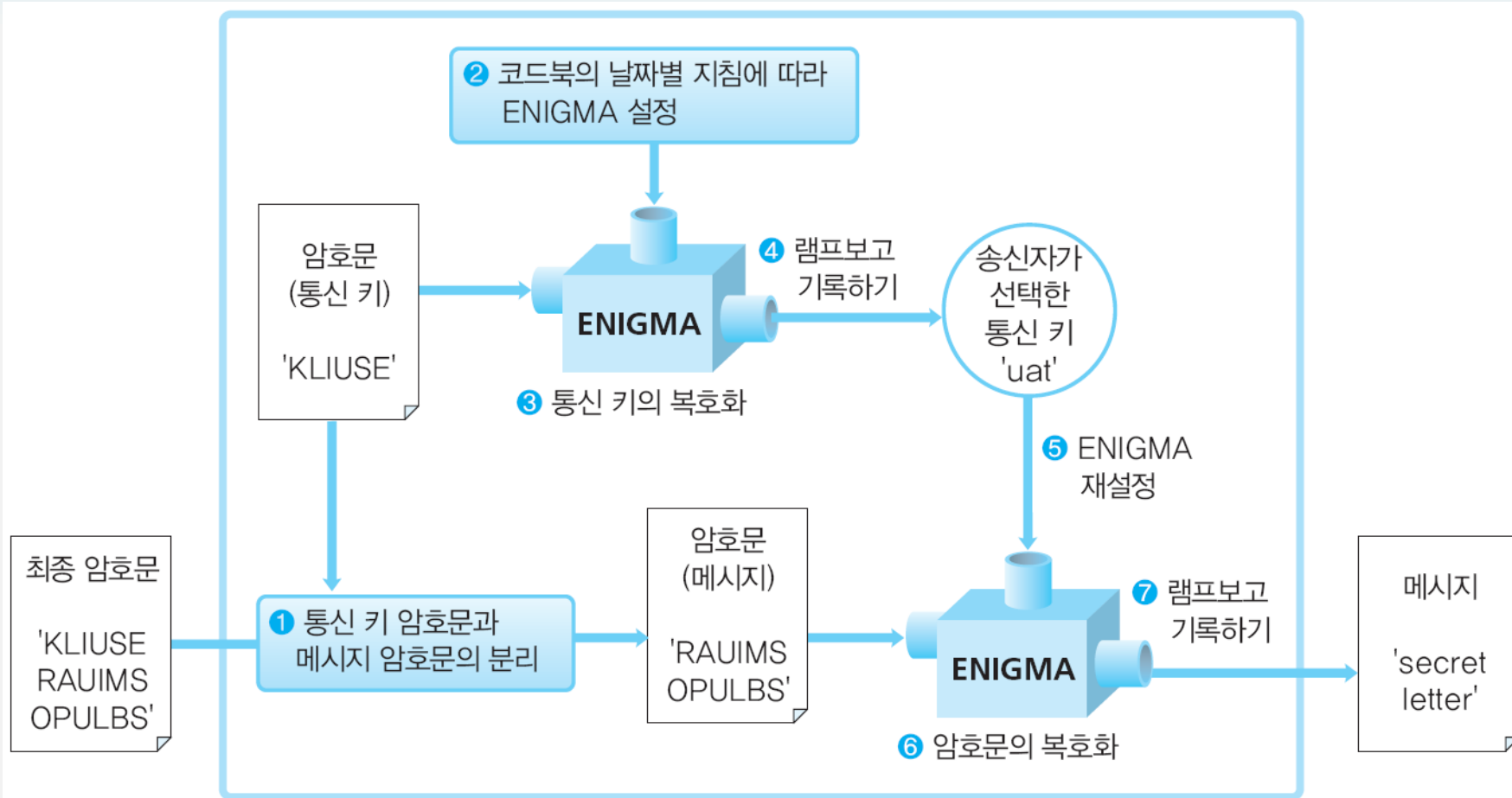


그림 3-17 • 에니그마를 사용한 복호화

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 의존하고 있지 않았다.
- 폴란드의 암호 해독자 르예프스키
 - 날짜별 키에 의한 암호문으로 부터 날짜별 키를 간파하는 방법을 고안
- 영국의 암호 해독팀은 블레츨리 파크에 모여 에니그마의 해독
 - 앨런 튜링 : 1940년에 해독하는 기계 고안

Quiz 3 L이 없는 암호문

- 제2차 세계대전 중 영국군의 암호 해독자가 에니그마의 암호문을 입수하였다. 그런데 그 암호문 중에는 문자 L이 1개도 포함되어 있지 않았다. 암호 해독자는 이 "암호문에 L이 없다"는 사실로부터 평문을 추측할 수 있었다고 한다. 과연 어떤 평문이 있을까?

Section 05

암호 알고리즘과 키

5.1 암호 알고리즘과 키를 분리하는 이유

5.1 암호 알고리즘과 키를 분리하는 이유

- 암호 알고리즘 안에는 「변경 가능한 부분」이 반드시 포함
- 「변경 가능한 부분」이 「키」에 해당

암호 알고리즘과 키

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

『암호 알고리즘』과 「키」를 분리

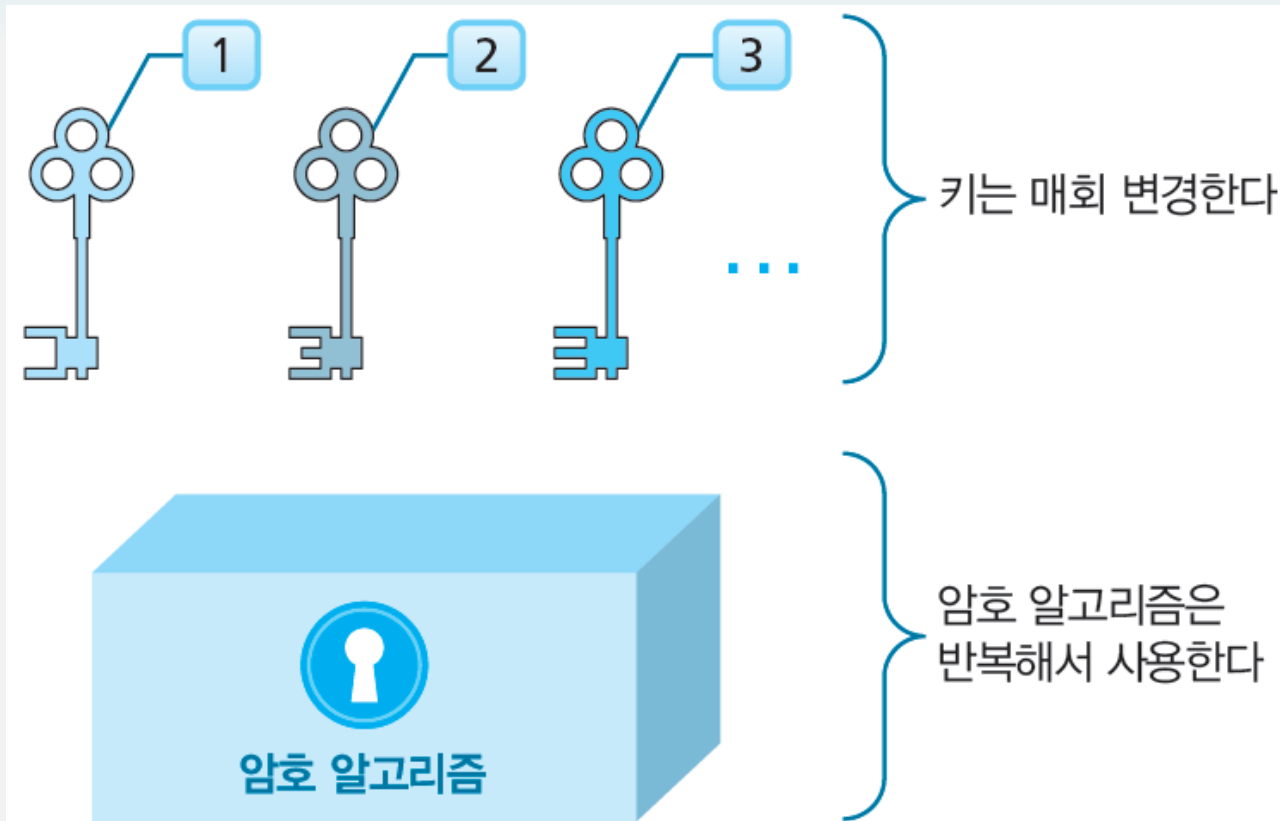


그림 3-18 • 「암호 알고리즘」과 「키」의 분리