충남대학교
CHUNGNAM NATIONAL UNIVERSITY

고전암호

2022년 9월 14일 수요일

정보보호

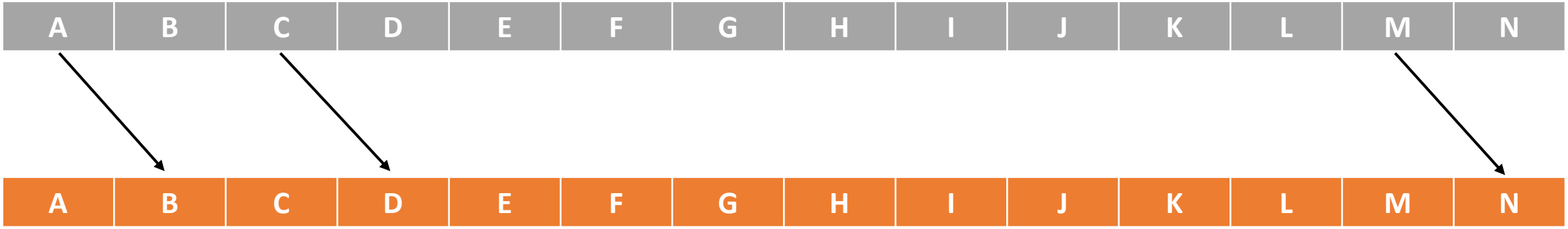
충남대학교 정보보호연구실 허강준

Julius Caesar

시저암호(카이사르 암호)

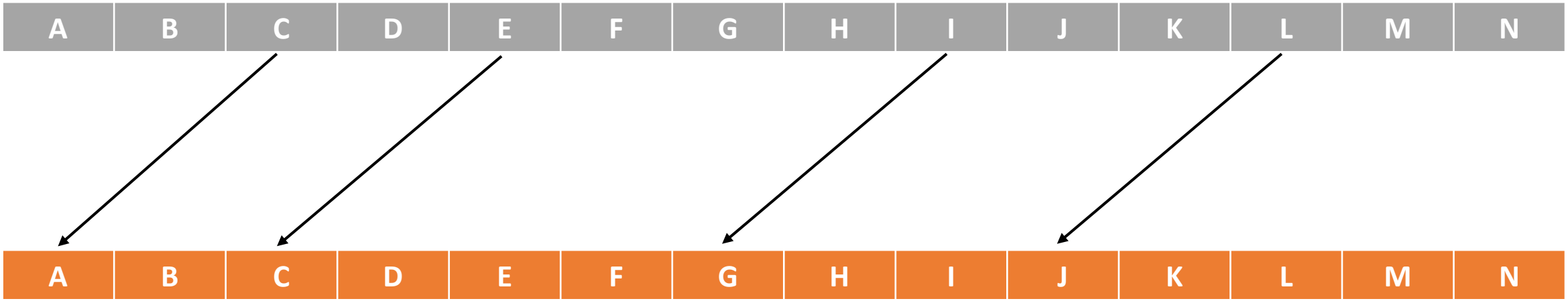
- 로마 황제 율리우스 카이사르(줄리어스 시저)가 전쟁 수행을 위해 사용한 암호
- 이동암호(Shift cipher code)의 일종
- “암호키” -> 문자를 얼마나 밀어낼 것인가?
- Caesar(P, K) P: 평문, K: 암호키

Caesar(“CAM”, 1) = “DBN”



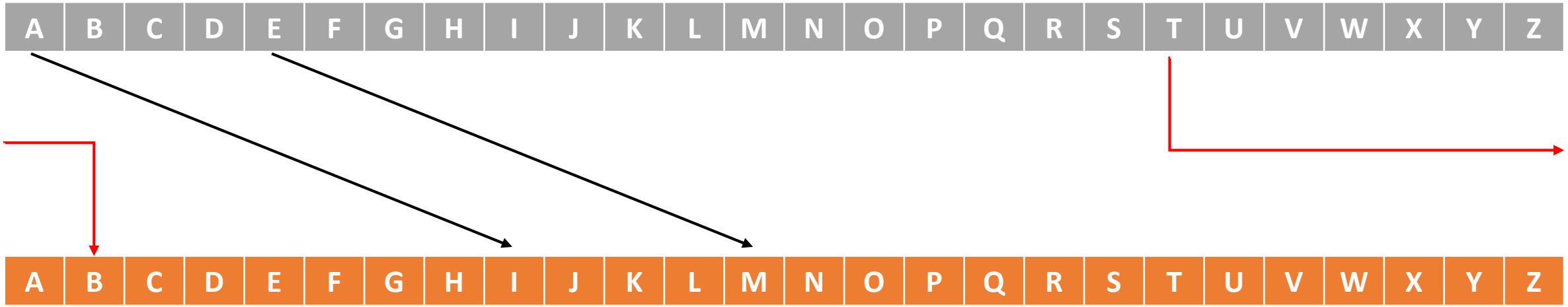
시저암호(카이사르 암호)

Caesar(“CEIL”, -2) = “ACGL”



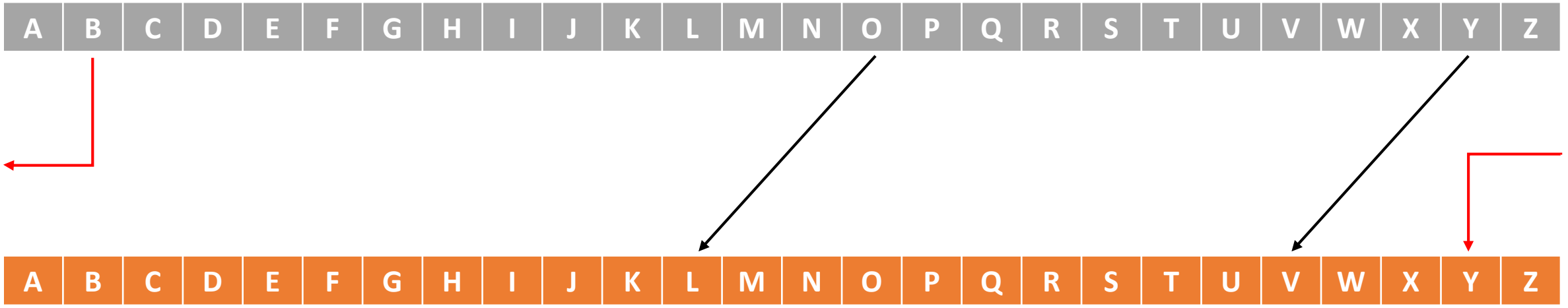
시저암호(카이사르 암호)

Caesar(“TEA”, 8) = “BIM”



시저암호(카이사르 암호)

Caesar(“BOY”, -3) = “YLV”



시저암호의 해독 – 취약점?

시저암호의 특성:

- 적은 경우의 수:

  암호키의 경우의 수 = 알파벳의 개수 = 26

- 단일치환암호의 한계:

  같은 문자일 경우? – 같은 암호문이 나옴 Caesar(“ABCABCABC”, 3) = DEFDEFDEF

시저암호의 해독 – Brute Forcing

- 암호키의 경우의 수 = 알파벳의 개수 = 26
- 상당히 적은 경우의 수: 시도해 볼 만함

뭐라는 걸까

시저암호의 해독 – Brute Forcing

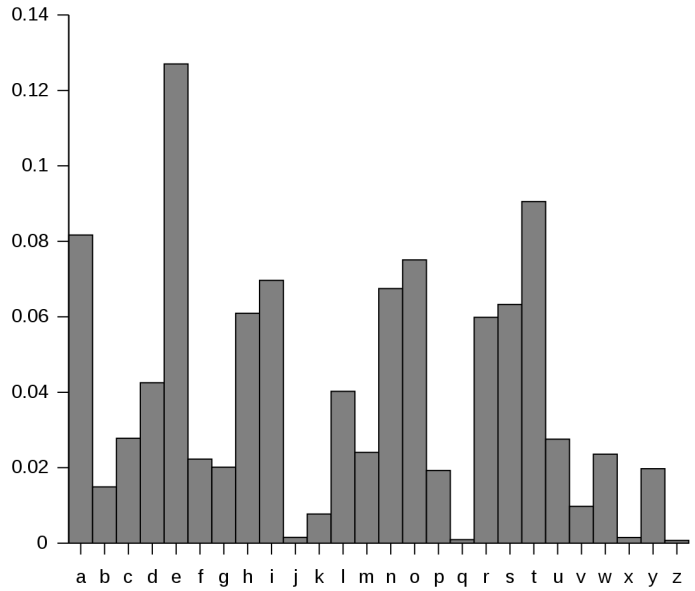
- 암호문: W, OA MCIF TOHVSF

+1	V, NZ LBHE SNGURE
+2	U, MY KAGD RMFTQD
+3	T, LX JZFC QLESPC
+4	S, KW IYEB PKDROB
+5	R, JV HXDA OJCQNA
+6	Q, IU GWCZ NIBPMZ
+7	P, HT FVBY MHAOLY
+8	O, GS EUAX LGZNKX
+9	N, FR DTZW KFYMJW
+10	M, EQ CSYV JEXLIV
+11	L, DP BRXU IDWKHU
+12	K, CO AQWT HCVJGT
+13	J, BN ZPVS GBUIFS
+14	I, AM YOUR FATHER
+15	H, ZL XNTQ EZSGDQ
+16	G, YK WMSP DYRFCP
+17	F, XJ VLRO CXQEBO
+18	E, WI UKQN BWPDAN
+19	D, VH TJPM AVOCZM
+20	C, UG SIOL ZUNBYL
+21	B, TF RHNK YTMAXK
+22	A, SE QGMJ XSLZWJ
+23	Z, RD PFLI WRKYVI
+24	Y, QC OEKH VQJXUH
+25	X, PB NDJG UPIWTG

시저암호의 해독 – Brute Forcing

시저암호의 해독 – Frequency Analysis

- 같은 문자일 경우? – 같은 암호문이 나옴 Caesar("ABCABCABC", 3) = DEFDEFDEF
- 영문의 글자수 빈도



Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

시저암호의 해독 – Frequency Analysis

- 너무 짧으면 시도하기 어렵다

너무 짧다

시저암호의 해독 – Frequency Analysis

Tq lzak laew eq hslawfuw osk wpzsmklwv, twusmkw A osk af s zmjjq lg klsjl lscafy eq wfyafw shsjl. Kg A lgkkwv gxx lzak vjsoafy. Sfv A lzjwo gml sf wphdsfslagf oalz al.

"Lzak ak gfdq zak tgp. Lzw kzwwh qgm skcwv xgj ak afkavw."

A osk nwjq kmjhjakwv lg kww s dayzl tjwsc gnwj lzw xsuw gx eq qgmfy bmvyw

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A	23	G	14	M	8	S	20	Y	6
B	1	H	5	N	2	T	4	Z	12
C	3	I	0	O	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K	21	Q	9	W	26		
F	13	L	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq lzak laee eq hslaefue osk epzsmklev, teusmke A osk af s zmjjq lg klsjl lscafy eq efyafe shsjl. Kg A lgkkev gxx lzak vjsoafy. Sfv A lzjeo gml sf ephdsfslagf oalz al.

"Lzak ak gfdq zak tgp. Lze kzeeh qgm skcev xgj ak afkave."

A osk nejq kmjhjakev lg kee s dayzl tjesc gnej lze xsue gx eq qgmfy bmvye

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A	23	G	14	M	8	S	20	Y	6
B	1	H	5	N	2	T	4	Z	12
C	3	I	0	O	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K	21	Q	9	W->E	26		
F	13	L	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq lzak laee eq hslaefue osk epzsmklev, teusmke A osk af s zmjjq lg klsjl lscafy eq efyafe shsjl. Kg A lgkkev gxx lzak vjsoafy. Sfv A lzjeo gml sf ephdsfslagf oalz al.

"Lzak ak gfdq zak tgp. Lze kzeeh qgm skcev xgj ak afkave."

A osk nejq kmjhjakev lg kee s dayzl tjesc gnej lze xsue gx eq qgmfy bmvye

Tee, Aee, Oee, lee, Nee, See: K=>S?

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A	23	G	14	M	8	S	20	Y	6
B	1	H	5	N	2	T	4	Z	12
C	3	I	0	O	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K	21	Q	9	W->E	26		
F	13	L	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq lzas laee eq hslaefue oss epzsmslev, teusmse A oss af s zmjjq lg slsjl lscafy eq efyafe shsjl. Sg A lgssev gxx lzas vjsoafy. Sfv A lzjeo gml sf ephdsfslagf oalz al.

"Lzas as gfdq zas tgp. Lze szeeh qgm skcev xgj as afsave."

A oss nejq smjhjasev lg see s dayzl tjesc gnej lze xsue gx eq qgmfy bmvye

Letter	Frequency	Letter	Frequency
~~e~~	~~12.7020%~~	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
~~s~~	~~6.3270%~~	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A	23	G	14	M	8	S	20	Y	6
B	1	H	5	N	2	T	4	Z	12
C	3	I	0	O	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq lzas laee eq hslaefue oss epzsmslev, teusmse A oss af s zmjjq lg slsjl lscafy eq efyafe shsjl. Sg A lgssev gxx lzas vjsoafy. Sfv A lzjeo gml sf ephdsfslagf oalz al.

"Lzas as gfdq zas tgp. Lze szeeh qgm sscev xgj as afsave."

as (x), os, is, ns, …

A oss nejq smjhjasev lg see s dayzl tjesc gnej lze xsue gx eq qgmfy bmvye

Letter	Frequency	Letter	Frequency
~~e~~	~~12.7020%~~	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
~~s~~	~~6.3270%~~	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A	23	G	14	M	8	S	20	Y	6
B	1	H	5	N	2	T	4	Z	12
C	3	I	0	O	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq lzis liee eq hsliefue oss epzsmslev, teusmse I oss if s zmjjq lg slsjl lscify eq efyife shsjl. Sg I lgssev gxx lzis vjsoify. Sfv I lzjeo gml sf ephdsfsligf oilz il.

"Lzis is gfdq zis tgp. Lze szeeh qgm sscev xgj is ifsive."

I oss nejq smjhjisev lg see s diyzl tjesc gnej lze xsue gx eq qgmfy bmvye

Letter	Frequency	Letter	Frequency
~~e~~	~~12.7020%~~	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
~~i~~	~~6.9660%~~	y	1.9740%
n	6.7490%	p	1.9290%
~~s~~	~~6.3270%~~	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G	14	M	8	S	20	Y	6
B	1	H	5	N	2	T	4	Z	12
C	3	I	0	O	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq lzis liee eq hsliefue oss epzsmslev, teusmse I oss if s zmjjq lg slsjl lscify eq efyife shsjl. Sg I lgssev gxx lzis vjsoify. Sfv I lzjeo gml sf ephdsfsligf oilz il.

"Lzis is gfdq zis tgp. Lze szeeh qgm sscev xgj is ifsive."

This is?

I oss nejq smjhjisev lg see s diyzl tjesc gnej lze xsue gx eq qgmfy bmvye

Letter	Frequency	Letter	Frequency
~~e~~	~~12.7020%~~	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
~~i~~	~~6.9660%~~	y	1.9740%
n	6.7490%	p	1.9290%
~~s~~	~~6.3270%~~	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G	14	M	8	S	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq this liee eq hsliefue oss epzsmslev, teusmse I oss if s zmjjq lg slsjl lscify eq efyife shsjl. Sg I lgssev gxx this vjsoify. Sfv I lzjeo gml sf ephdsfsligf oilz il.

“This is gfdq zis tgp. Lze szeeh qgm sscev xgj is ifsive."

I oss nejq smjhjisev lg see s diyzl tjesc gnej lze xsue gx eq qgmfy bmvye

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G	14	M	8	S	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq this tiee eq hstiefue oss ephsmstev, teusmse I oss if s hmjjq tg stsjt tscify eq efyife shsjt. Sg I tgssev gxx this vjsoify. Sfv I thjeo gmt sf ephdsfstigf oith it.

“This is gfdq his tgp. The sheeh qgm sscev xgj is ifsive."

I oss nejq smjhjisev tg see s diyht tjesc gnej the xsue gx eq qgmfy bmvye

see a?

Letter	Frequency	Letter	Frequency
~~e~~	~~12.7020%~~	m	2.4060%
~~t~~	~~9.0560%~~	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
~~i~~	~~6.9660%~~	y	1.9740%
n	6.7490%	p	1.9290%
~~s~~	~~6.3270%~~	b	1.4920%
~~h~~	~~6.0940%~~	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G	14	M	8	S->A	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq this tiee eq hatiefue oas ephamstev, teuamse I oas if a hmjjq tg stajt tacify eq efyife ahajt. Sg I tgssev gxx this vjaoify. Afv I thjeo gmt af ephdafatigf oith it.

“This is gfdq his tgp. The sheeh qgm ascev xgj is ifsive."

I oas nejq smjhjisev tg see a diyht tjeac gnej the xaue gx eq qgmfy bmvye

To see?

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G	14	M	8	S->A	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq this tiee eq hatiefue oas ephamstev, teuamse I oas if a hmjjq to stajt tacify eq efyife ahajt. So I tossev oxx this vjaoify. Afv I thjeo omt af ephdafatiof oith it.

“This is ofdq his top. The sheeh qom ascev xoj is ifsive."

I oas nejq smjhjisev to see a diyht tjeac onej the xaue ox eq qomfy bmvye

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M	8	S->A	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq this tiee eq hatiefue oas ephamstev, teuamse I oas if a hmjjq to stajt tacify eq efyife ahajt. So I tossev oxx this vjaoify. Afv I thjeo omt af ephdafatiof oith it.

with?

"This is ofdq his top. The sheeh qom ascev xoj is ifsive."

was?

I oas nejq smjhjisev to see a diyht tjeac onej the xaue ox eq qomfy bmvye

Letter	Frequency	Letter	Frequency
~~e~~	~~12.7020%~~	m	2.4060%
~~t~~	~~9.0560%~~	w	2.3600%
~~a~~	~~8.1670%~~	f	2.2280%
~~o~~	~~7.5070%~~	g	2.0150%
~~i~~	~~6.9660%~~	y	1.9740%
n	6.7490%	p	1.9290%
~~s~~	~~6.3270%~~	b	1.4920%
~~h~~	~~6.0940%~~	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M	8	S->A	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq this tiee eq hatiefue was ephamstev, teuamse I was if a hmjjq to stajt tacify eq efyife ahajt. So I tossev oxx this vjawify. Afv I thjew omt af ephdafatiof with it.

“This is ofdq his top. The sheeh qom ascev xoj is ifsive."

I was nejq smjhjisev to see a diyht tjeac onej the xaue ox eq qomfy bmvye

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3680%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M	8	S->A	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O->W	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

start?

Tq this tiee eq hatiefue was ephamstev, teuamse I was if a hmjjq to stajt tacify eq efyife ahajt. So I tossev oxx this vjawify. Afv I thjew omt af ephdafatiof with it.

threw?

“This is ofdq his top. The sheeh qom ascev xoj is ifsive."

I was nejq smjhjisev to see a diyht tjeac onej the xaue ox eq qomfy bmvye

Letter	Frequency	Letter	Frequency
~~e~~	~~12.7020%~~	m	2.4060%
~~t~~	~~9.0560%~~	~~w~~	~~2.3680%~~
~~a~~	~~8.1670%~~	f	2.2280%
~~o~~	~~7.5070%~~	g	2.0150%
~~i~~	~~6.9660%~~	y	1.9740%
n	6.7490%	p	1.9290%
~~s~~	~~6.3270%~~	b	1.4920%
~~h~~	~~6.0940%~~	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M	8	S->A	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O->W	6	U	3		
D	3	J	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq this tiee eq hatiefue was ephamstev, teuamse I was if a hmrrq to start tacify eq efyife ahart. So I tossev oxx this vrawify. Afv I threw omt af ephdafatiof with it.

“This is ofdq his top. The sheeh qom ascev xor is ifsive."

I was nerq smrhrisev to see a diyht treac oner the xaue ox eq qomfy bmvye

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3680%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M	8	S->A	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O->W	6	U	3		
D	3	J->R	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq this tiee eq hatiefue was ephamstev, teuamse I was if a hmrrq to start tacify eq efyife ahart. So I tossev oxx this vrawify. Afv I threw omt af ephdafatiof with it.

And? inside?

"This is ofdq his top. The sheeh qom ascev xor is ifsive."

I was nerq smrhrisev to see a diyht treac oner the xaue ox eq qomfy bmvye

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3680%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M	8	S->A	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O->W	6	U	3		
D	3	J->R	12	P	3	V	8		
E	4	K->S	21	Q	9	W->E	26		
F	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Tq this tiee eq hatienue was ephamsted, teuamse I was in a hmrrq to start taciny eq enyine ahart. So I tossed oxx this drawiny. And I threw omt an ephdanation with it.

“This is ondq his top. The sheeh qom asced xor is inside."

I was nerq smrhrised to see a diyht treac oner the xaue ox eq qomny bmdye

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3680%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M	8	S->A	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O->W	6	U	3		
D	3	J->R	12	P	3	V->D	8		
E	4	K->S	21	Q	9	W->E	26		
F->N	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

in a hurry?

Tq this tiee eq hatienue was ephamsted, teuamse I was in a hmrrq to start taciny eq enyine ahart. So I tossed oxx this drawiny. And I threw omt an ephdanation with it.

threw out?

“This is ondq his top. The sheeh qom asced xor is inside."

I was nerq smrhrised to see a diyht treac oner the xaue ox eq qomny bmdye

Letter	Frequency	Letter	Frequency
~~e~~	~~12.7020%~~	m	2.4060%
~~t~~	~~9.0560%~~	~~w~~	~~2.3680%~~
~~a~~	~~8.1670%~~	f	2.2280%
~~o~~	~~7.5070%~~	g	2.0150%
~~i~~	~~6.9660%~~	y	1.9740%
~~n~~	~~6.7490%~~	p	1.9290%
~~s~~	~~6.3270%~~	b	1.4920%
~~h~~	~~6.0940%~~	v	0.9780%
~~r~~	~~5.9870%~~	k	0.7720%
~~d~~	~~4.2530%~~	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M	8	S->A	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O->W	6	U	3		
D	3	J->R	12	P	3	V->D	8		
E	4	K->S	21	Q	9	W->E	26		
F->N	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Ty this tiee ey hatienue was ephausted, teuause I was in a hurry to start taciny ey enyine ahart. So I tossed oxx this drawiny. And I threw out an ephdanation with it.

“This is ondy his top. The sheeh you asced xor is inside."

I was nery surhrised to see a diyht treac oner the xaue ox ey youny budye

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3680%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M->U	8	S->A	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O->W	6	U	3		
D	3	J->R	12	P	3	V->D	8		
E	4	K->S	21	Q->Y	9	W->E	26		
F->N	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Ty this tiee ey hatienue was ephausted, teuause I was in a hurry to start taciny ey enyine ahart. So I tossed oxx this drawiny. And I threw out an ephdanation with it.

This is only! You asked for!

"This is ondy his top. The sheeh you asced xor is inside."

I was nery surhrised to see a diyht treac oner the xaue ox ey youny budye

Very surprised

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M->U	8	S->A	20	Y	6
B	1	H	5	N	2	T	4	Z->H	12
C	3	I	0	O->W	6	U	3		
D	3	J->R	12	P	3	V->D	8		
E	4	K->S	21	Q->Y	9	W->E	26		
F->N	13	L->T	21	R	0	X	5		

시저암호의 해독 – Frequency Analysis

Ty this tiee ey patienue was ephausted, teuause I was in a hurry to start takiny ey enyine apart. So I tossed off this drawiny. And I threw out an epplanation with it.

“This is only his top. The sheep you asked for is inside."

I was very surprised to see a liyht treak over the faue of ey youny budye

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3680%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M->U	8	S->A	20	Y	6
B	1	H->P	5	N->V	2	T	4	Z->H	12
C->K	3	I	0	O->W	6	U	3		
D->L	3	J->R	12	P	3	V->D	8		
E	4	K->S	21	Q->Y	9	W->E	26		
F->N	13	L->T	21	R	0	X->F	5		

시저암호의 해독 – Frequency Analysis

Ty this tiee ey patienue was ephausted, teuause I was in a hurry to start takiny ey enyine apart. So I tossed off this drawiny. And I threw out an epplanation with it.

“This is only his top. The sheep you asked for is inside."

I was very surprised to see a liyht treak over the faue of ey youny budye

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3680%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M->U	8	S->A	20	Y	6
B	1	H->P	5	N->V	2	T	4	Z->H	12
C->K	3	I	0	O->W	6	U	3		
D->L	3	J->R	12	P	3	V->D	8		
E	4	K->S	21	Q->Y	9	W->E	26		
F->N	13	L->T	21	R	0	X->F	5		

시저암호의 해독 – Frequency Analysis

By this time my patience was exhausted, because I was in a hurry to start taking my engine apart. So I tossed off this drawing. And I threw out an explanation with it.

“This is only his box. The sheep you asked for is inside."

I was very surprised to see a light break over the face of my young judge

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3680%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

A->I	23	G->O	14	M->U	8	S->A	20	Y	6
B	1	H->P	5	N->V	2	T	4	Z->H	12
C->K	3	I	0	O->W	6	U	3		
D->L	3	J->R	12	P	3	V->D	8		
E	4	K->S	21	Q->Y	9	W->E	26		
F->N	13	L->T	21	R	0	X->F	5		

비즈네르 암호

- 치환암호 (Substitution Cipher)
- 하지만 더 복잡한 다중치환암호(Polyalphabetic substitution cipher)
- Vigenere(P, K)

- 같은 문자에 대해서 매번 다른 암호문이 나옴 Vigenere(“AAA”, “ABC”) = ABC
- 앞서 사용한 빈도분석법(Frequency Analysis) 사용 불가

비즈네르 암호

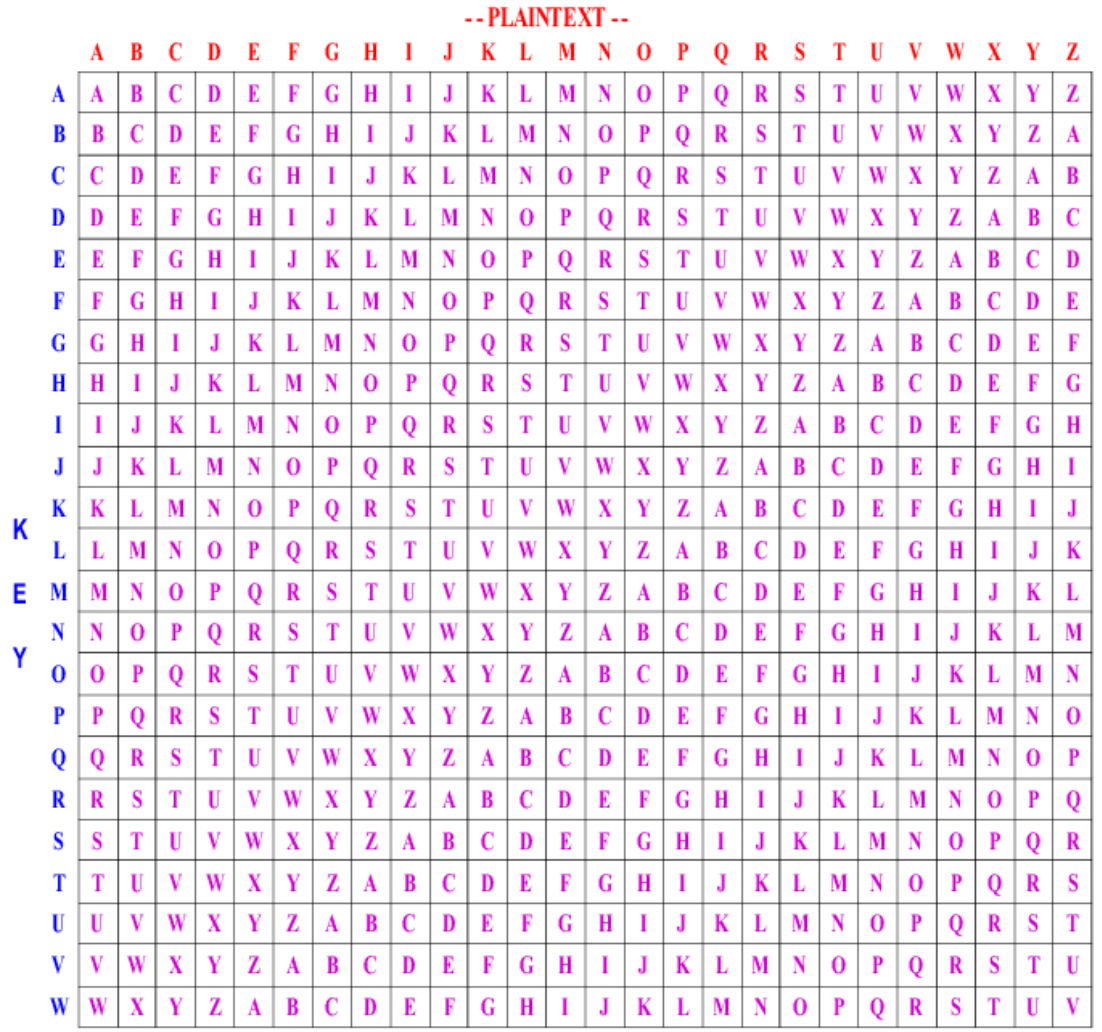
Vigenere(“HELLO”, “CNU”)

= JRFNB

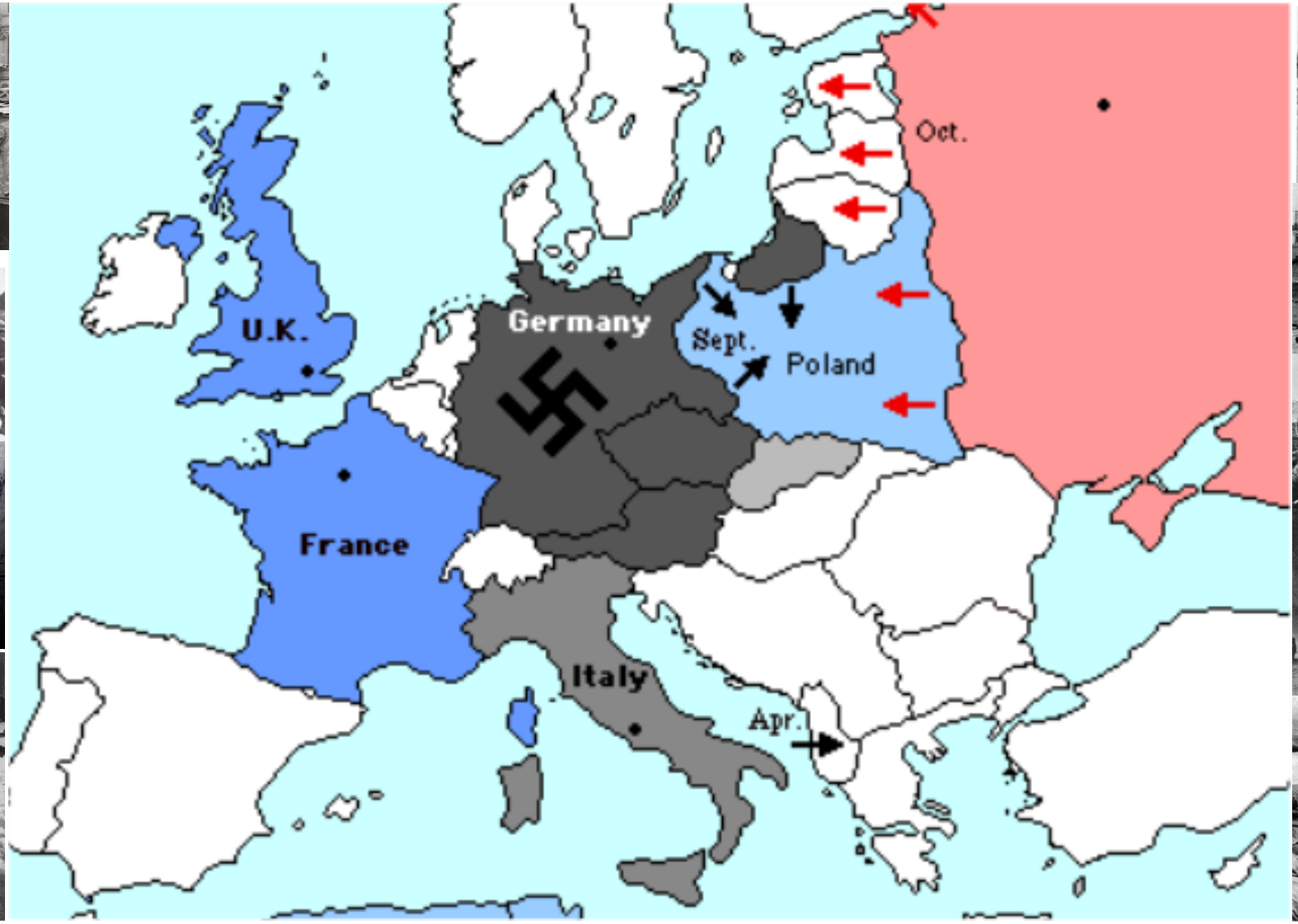
(H-C = J) (E-N = R) (L-U = F) (L-C = N) (O-N = B)

Viegenere(“GOOD MORNING”, “INFOSEC”)

= OBTR ESTVVSU

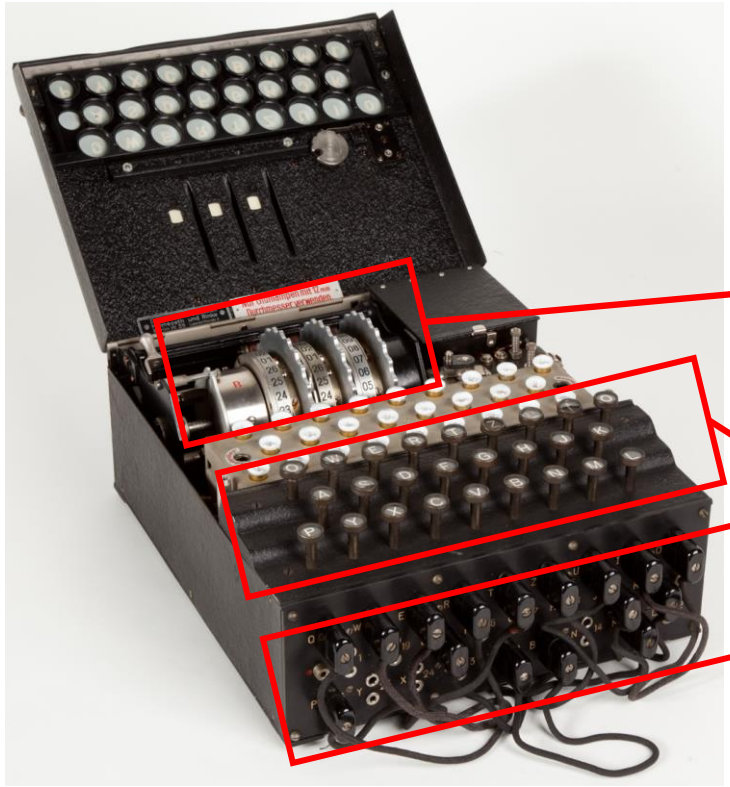


썰



썰

- How does it work?



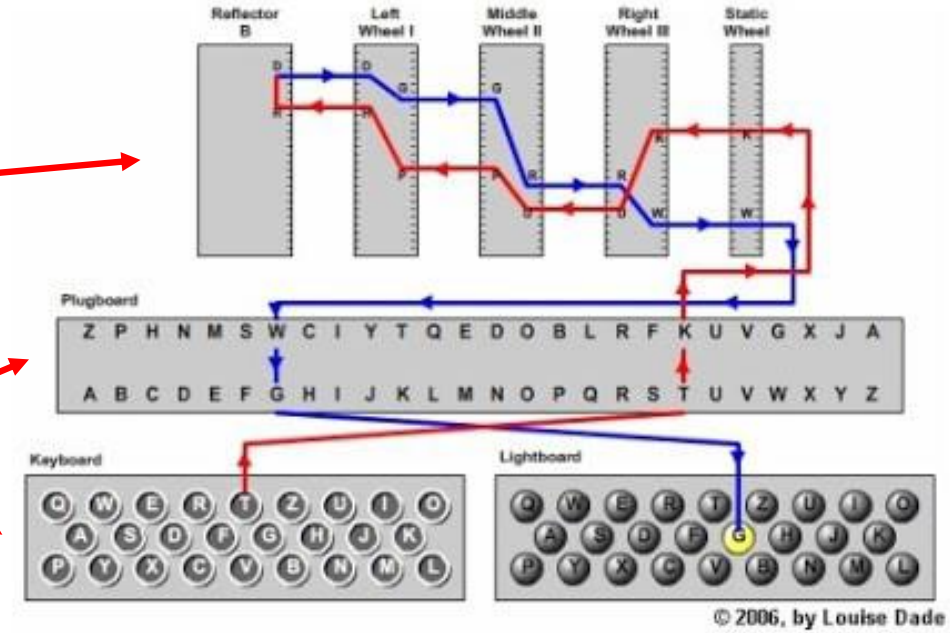
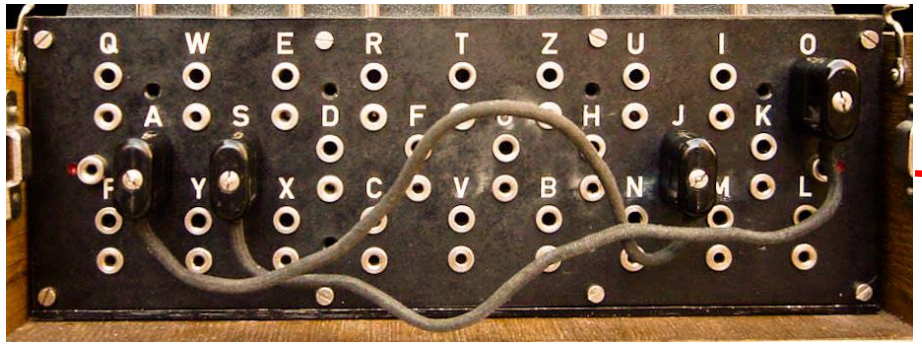


Figure 1: How one letter is changed into another letter at each stage as it passes through an Enigma machine.

- How does it work?



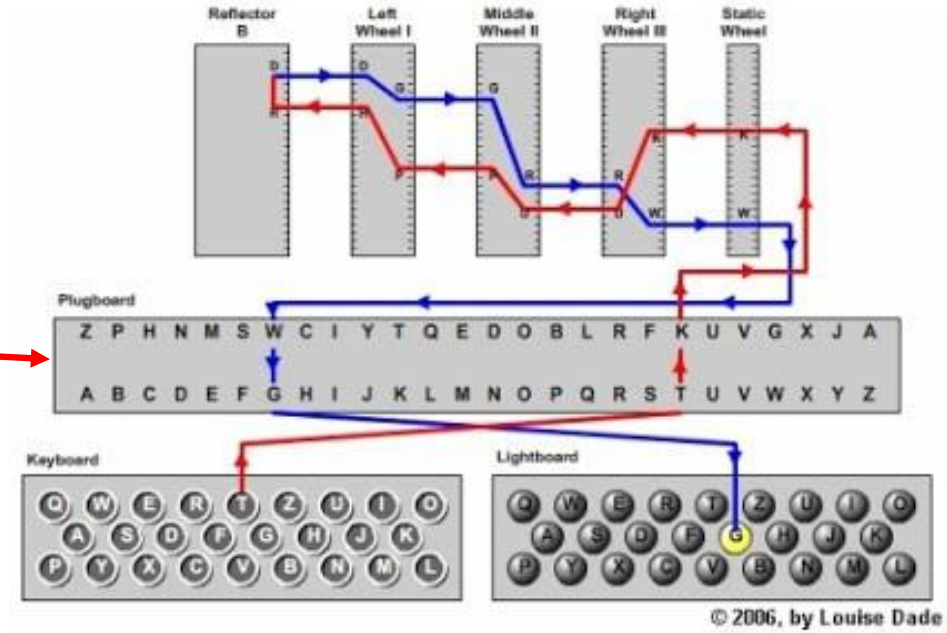


Figure 1: How one letter is changed into another letter at each stage as it passes through an Enigma machine.

- How does it work?

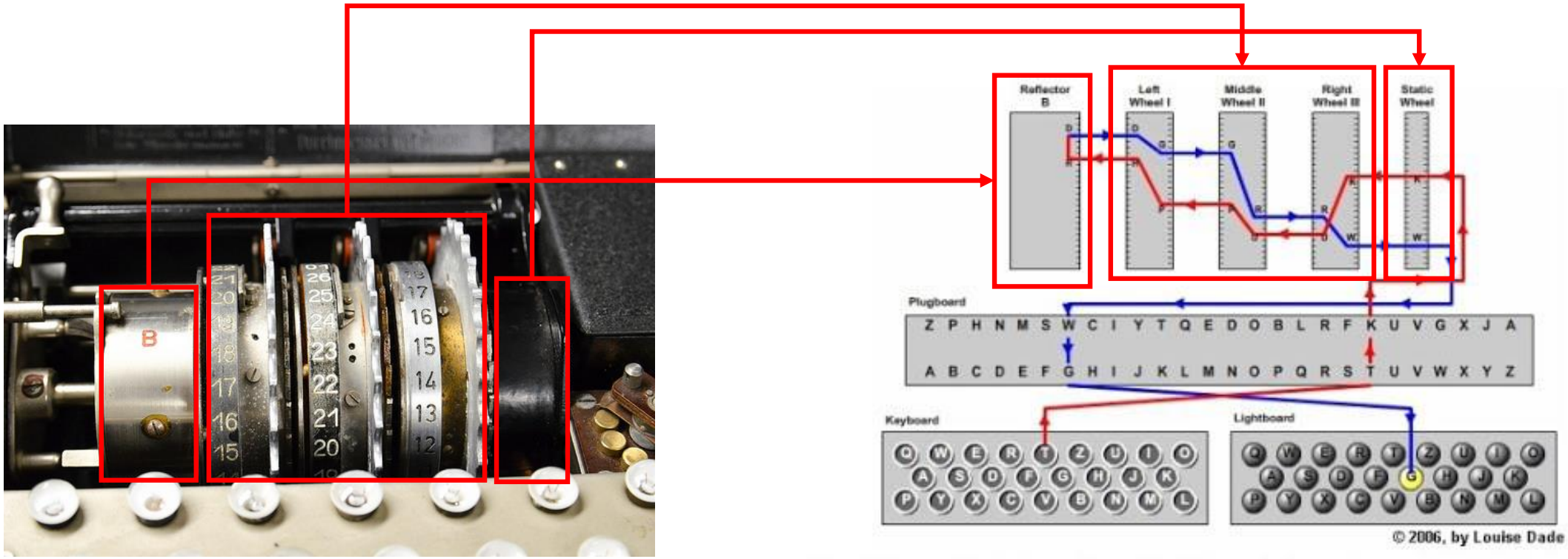
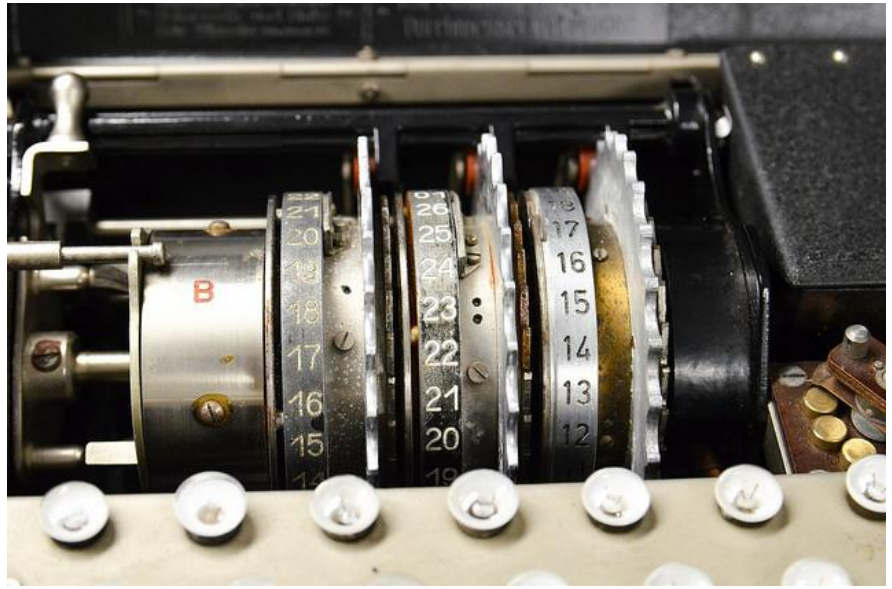
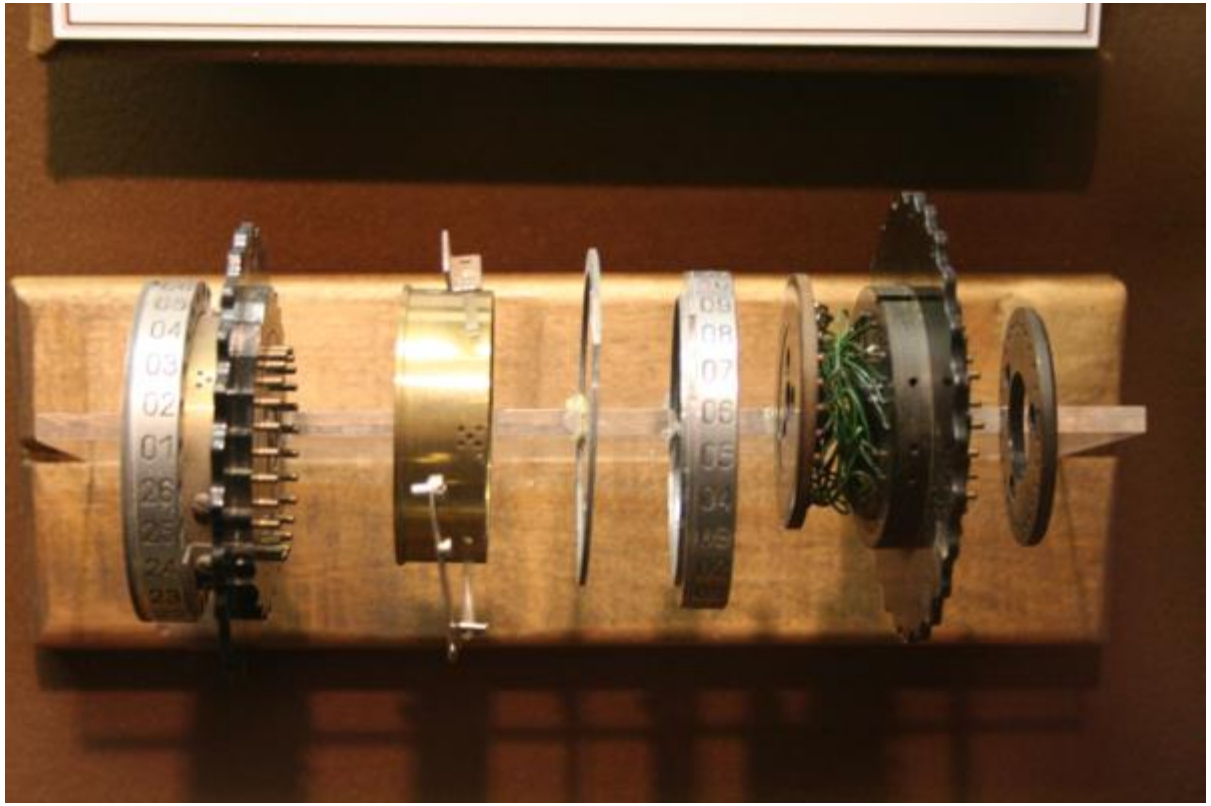


Figure 1: How one letter is changed into another letter at each stage as it passes through an Enigma machine.

- How does it work?

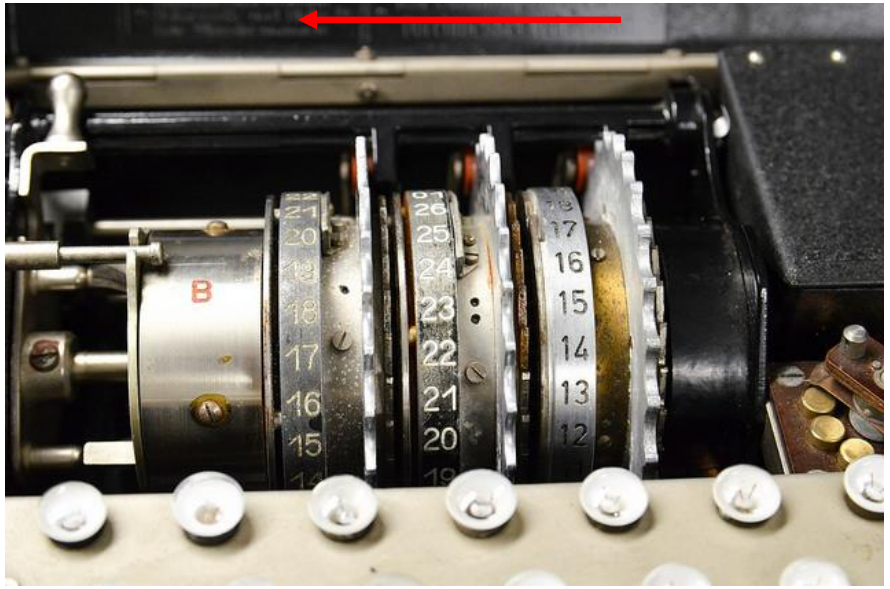


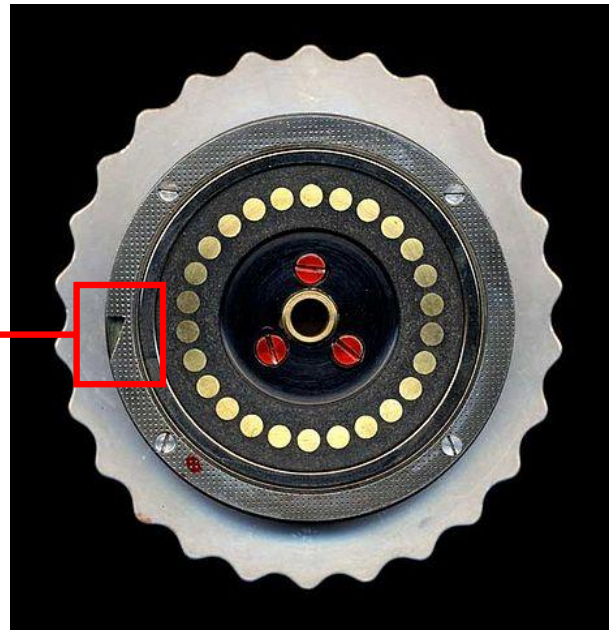


- How does it work?

"Notch"
다음 로터 회전

회전 전달 방향





- How does it work?

GEHEIM! **SONDER MASCHINENSCHLÜSSEL** ~~DECEMBER~~ 1939 May 1941

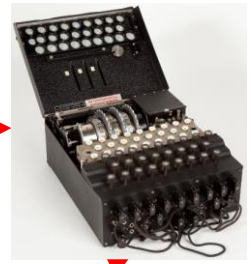
Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31	I V IV	01 13 04	AV BI CJ DP EM FK GQ HU SZ TY	REJ RFP DNM OAM
30	V III IV	09 01 03	BV CE DY FM GS HU IR JZ KP TW	VIV EKX GMA VPG
29	III IV I	10 08 26	AV BG CT EY FH IW LM NS OP QR	OFR QWB EQR NNN
28	II III I	02 05 01	AN BT CL ES FK HM IR JW QV YZ	BCP ABF GLV ZYR
27	III I IV	08 01 03	AH BV DR FT JL MN PX QS UY WZ	MYI OTU FZK HKG
26	I III IV	15 23 19	AJ CG DF EI KO LM PZ QV RX SW	AOT HYC NAX HDB
25	II V I	10 12 07	AY BK DN FI GM HU OW QV RT XZ	FHB UMD VVV DDH
24	III II IV	17 05 11	AB CT DL FO GW HV IU JX MR NP	RIJ SCN LPE IGW
23	III IV I	13 23 10	AH BG CK DV FZ JO LW NP SX TU	LPA FKH HJN SBH
22	II IV V	13 07 18	AR BX CO EN FL GQ HZ KS TY UV	MTT DUP OEO XVR
21	II IV V	15 12 20	AH BK DS EP FG IX JU LO QT WZ	MHJ EFR VBW XLI
20	I IV III	03 24 26	AO BU CJ DE GQ HP KW MX NV ST	KPF LJA JBQ EHM
19	II I III	22 04 24	AY BX FZ GJ HW IU KT LV OR QS	OFV PSZ GHZ CGU
18	III I II	15 14 08	AV CI DO ES FK HY JT MR PW QX	VOH VXM JHM CTR

- How does it work?

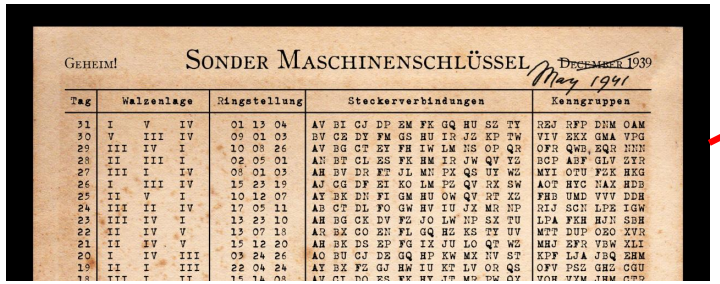
“swdgf uscyd sw fmyigoft”

- How does it work?

"swdgf uscyd sw fmyigoft"



"lunch today is sandwich"



GEHEIM! SONDER MASCHINENSCHLÜSSEL ~~DECEMBER~~ May 1941

Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31	I V IV	01 13 04	AV BI CJ DP EM FK GQ HU SZ TY	REJ RFP DNM OAM
30	V III IV	09 01 03	BV CE DY FM GS HU IR JZ KP TW	VIV EKX GMA VPG
29	III IV I	10 08 26	AY BG CT EY FH IW LM NS OP QR	OFR QWB ZQR NNN
28	II III I	02 05 01	AN BT CL ES FK HM IR JW QV YZ	BCP ABF GLV ZYR
27	III I IV	08 01 03	AH BV DR FT JL MN PX QS UY WZ	MYI OTU FZK HKG
26	I III IV	15 23 19	AJ CG DF EI KO LM PZ QV RX SW	AOT HYC NAX HDB
25	II V I	10 12 07	AY BK DN FI GM HU OW QV RT XZ	FHB UMD VVV DDH
24	III II IV	17 05 11	AB CT DL FO GW HV IU JX MR NP	RIJ SCN LPE IGW
23	III IV I	13 23 10	AH BG CK DV FZ JO LW NP SX TU	LPA FKH HJN SBH
22	II IV V	13 07 18	AR BX CO EV FL GQ HZ KS TY UV	MTT DUP OZO XYR
21	II IV V	15 12 20	AH BK DS EP FG IX JU LO QP WZ	MHJ EFR VBW XLI
20	I IV III	03 24 26	AO BU CJ DZ GQ HP KW MX NV ST	KPF LJA JBQ ZHM
19	II I III	22 04 24	AY BX FZ GJ HW IU KT LV OR QS	OFV PSZ GHZ CGU

UKW C, Rotor III-I-II (Y-B-B), Ring 1-1-1, A-V / F-T

- 그래서 얼마나 강력한가?

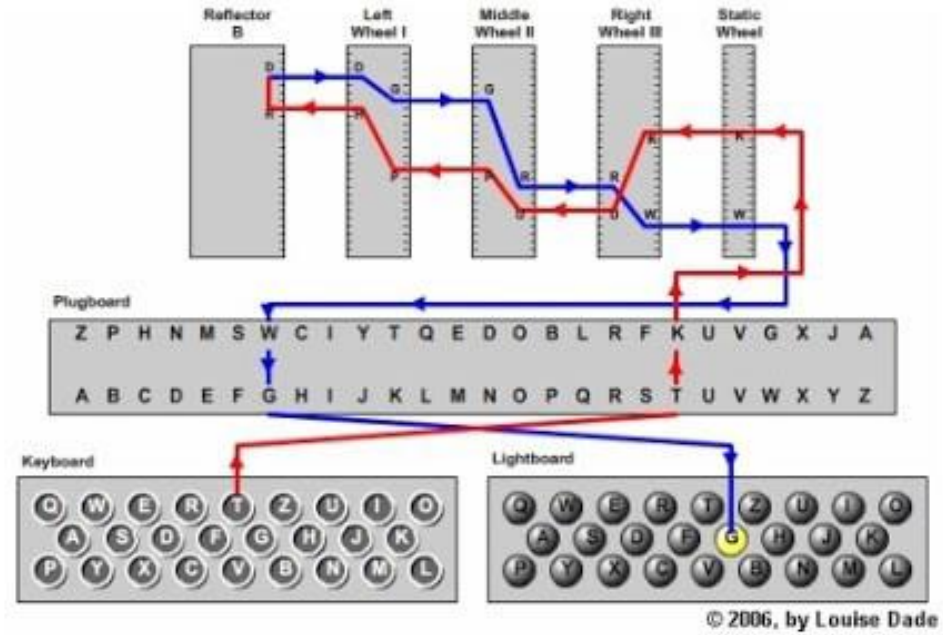


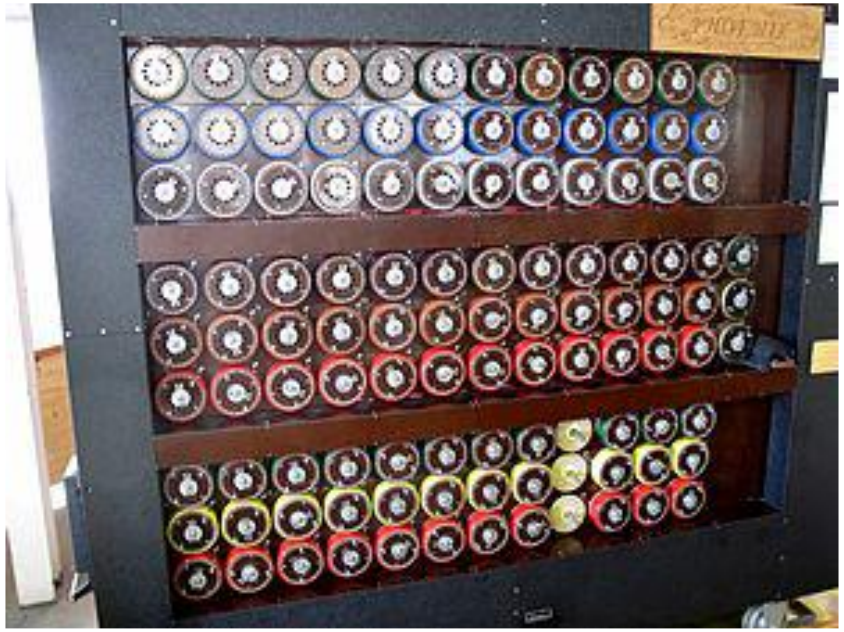
Figure 1: How one letter is changed into another letter at each stage as it passes through an Enigma machine.

”Thus the possible cryptvariables space Allied cryptanalysts were typically faced with during the second world war when attempting to read Enigma traffic is the product of the above five values which is approximately 1×10^{23}.”

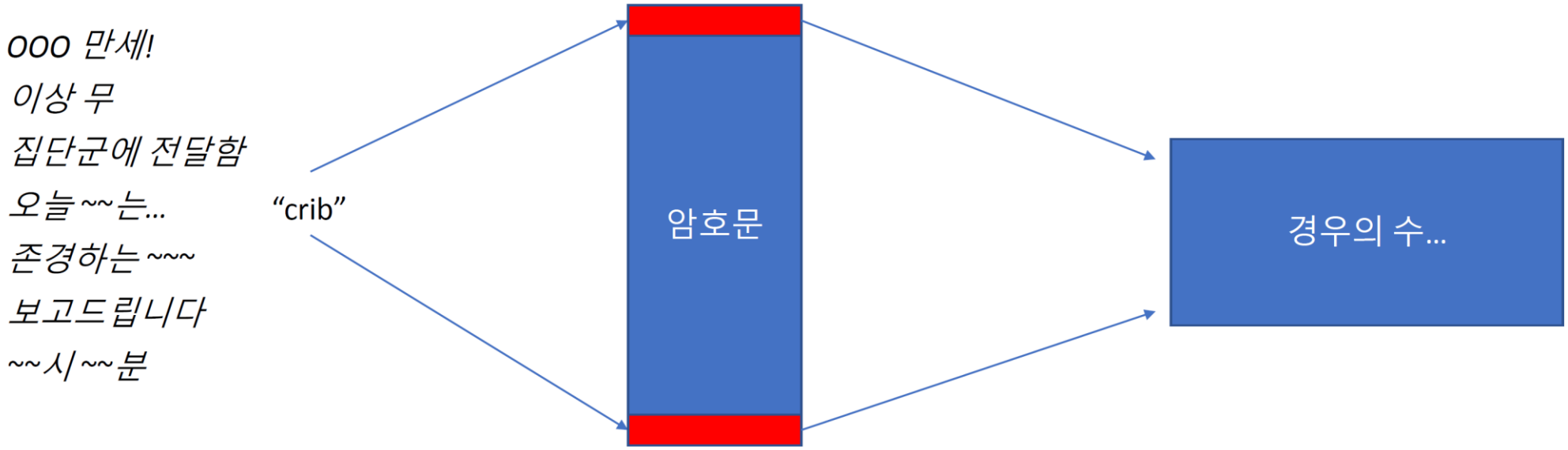
MILLER, A. R. The cryptographic mathematics of enigma. Cryptologia 19, 1 (1995), 65–80

- 하지만…


2015년 아카데미
8개부문 노미네이트
24시간 마다 바뀌는
완벽한 암호
인류의 역사를 바꾼 천재 수학자
이 미 테 이 션 게 임
암호를 해독하고
전쟁에서 이겨라
2015.02.17



- 상용구 사용에 의한 기지평문공격(Known-Plaintext Attack)



- 취약한 키 사용 / 사용한 키 재사용
  - *보안의 가장 약한 고리는 “사람”*
- 취약한 암호 생성 규칙
- 기계 자체의 설계상 결함(?)
  - 키보드로 입력한 문자는 절대 나오지 않음
  - 의미 없이 반복하는 문자들로 조합 추측
    - e.g.) AAAAAAAAAA…

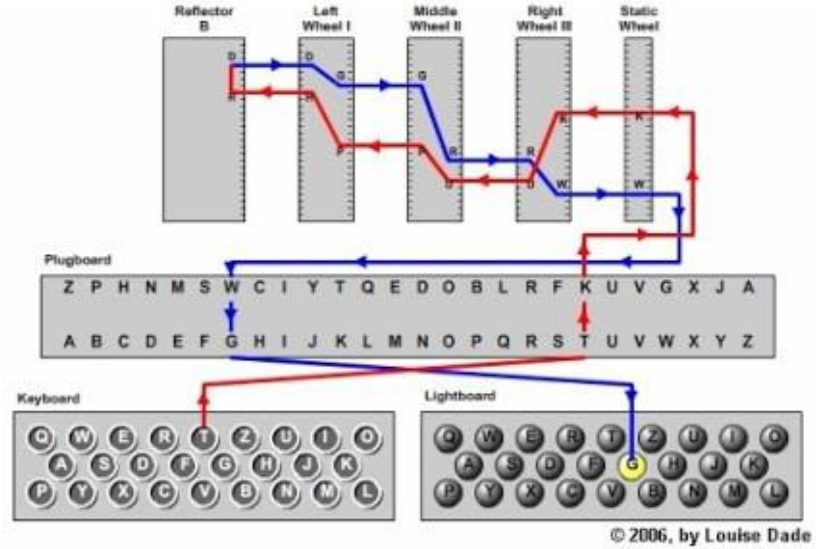


Figure 1: How one letter is changed into another letter at each stage as it passes through an Enigma machine.

- 그 이후는…

Adolf Hitler, 1889~1945

금주 과제

- Enigma I 구현하기
  - 로터: I, II, III
  - 반사판(UKW): A, B, C

  - 로터 회전, 신호 통과 부분 구현
  - 9월 21일 09:59까지

  - 필요하다면 다른 코드 수정 가능

```python
# Enigma Logics Start

# Plugboard
def pass_plugboard(input):
    for plug in SETTINGS["PLUGBOARD"]:
        if str.startswith(plug, input):
            return plug[1]
        elif str.endswith(plug, input):
            return plug[0]

    return input

# ETW
def pass_etw(input):
    return SETTINGS["ETW"][ord(input) - ord('A')]

# Wheels
def pass_wheels(input, reverse = False):
    # Implement Wheel Logics
    # Keep in mind that reflected signals pass wheels in reverse order
    return input

# UKW
def pass_ukw(input):
    return SETTINGS["UKW"][ord(input) - ord('A')]

# Wheel Rotation
def rotate_wheels():
    # Implement Wheel Rotation Logics
    pass
```

이후 일정

주차	실습 주제	과제	날짜
1	오리엔테이션 & 썰풀기	과제를 위한 GitHub 설정	9/7
2	카이사르&비즈네르 암호	ENIGMA	9/14
3	XOR과 블록암호	Simplified DES 구현하기	9/21
4	여러가지 블록암호	블록암호를 이용하여 암호통신기 완성하기	9/28
5	블록암호 운용모드	S-DES-CBC, S-DES-ECB 구현하기	10/5
6	RSA	RSA 구현하기, 저강도 RSA 크랙하기	10/12
7	해시	암호통신기에 무결성 검증 기능 추가하기	10/19
8	중 간 고 사 (10/24)		공강
9	메세지 인증코드(MAC)	HMAC 구현하기	11/2
10	디지털 서명	사설인증서 생성 및 프로그램 코드 서명	11/9
11	하이브리드 암호	하이브리드 기반 암호 통신기	11/16
12	난수	시드값 추측을 이용한 암호문 크랙	11/23
13	블록체인과 머클 트리	머클트리 구현하기	11/30
14	TLS와 PGP(GPG)	GPG를 이용하여 암호 메일 보내기	12/7
15	기 말 고 사 (12/12)		종강

질문?

- 없으면 자리에서 일어나셔도 좋습니다 :)
- 대학원 입학 문의는 언제나 환영
  - 블록체인, Web 3, 해킹 관심있거나 유경험자 우대

입학문의

- 류재철 교수님 (jcryou [at] cnu.ac.kr)
- 허강준 조교 (knowledge [at] o.cnu.ac.kr)