Defeating the German Enigma

CRYPTOLOGY

Cryptology

The study of making and breaking ciphers

CRYPTOLOGY

Cryptology

The study of making and breaking ciphers

- Cryptography: The study of making ciphers.

CRYPTOLOGY

Cryptology

The study of making and breaking ciphers

- Cryptography: The study of making ciphers.
- Cryptanalysis: The study of breaking ciphers.

THE CAESAR SHIFT

LEHWBRXFDQUHDGWKLV

THE CAESAR SHIFT

LEHWBRXFDQUHDGWKLV

- Shift each letter by a fixed amount.

THE CAESAR SHIFT

LEHWBRXFDQUHDGWKLV

- Shift each letter by a fixed amount.
- Originally, Caesar shifted by 3. $A \to D$, $B \to E$, etc.

THE CAESAR SHIFT

LEHWBRXFDQUHDGWKLV

- Shift each letter by a fixed amount.
- Originally, Caesar shifted by 3. $A \to D$, $B \to E$, etc.
- What is the size of the key space?

THE CAESAR SHIFT

LEHWBRXFDQUHDGWKLV

- Shift each letter by a fixed amount.
- Originally, Caesar shifted by 3. $A \to D$, $B \to E$, etc.
- What is the size of the key space? 26.

THE CAESAR SHIFT

LEHWBRXFDQUHDGWKLV

- Shift each letter by a fixed amount.
- Originally, Caesar shifted by 3. $A \to D$, $B \to E$, etc.
- What is the size of the key space? 26.
- How hard is it to guess?

LEHWBRXFDQUHDGWKLV

LEHWBRXFDQUHDGWKLV

LEHWBRXFDQUHDGWKLV

LEHWBRXFDQUHDGWKLV

LEHWBRXFDQUHDGWKLV

MFIXCSYGERVIEHXLMW

LEHWBRXFDQUHDGWKLV

LEHWBRXFDQUHDGWKLV
MFIXCSYGERVIEHXLMW
NGJYDTZHFSWJFIYMNX

LEHWBRXFDQUHDGWKLV

LEHWBRXFDQUHDGWKLV
MFIXCSYGERVIEHXLMW
NGJYDTZHFSWJFIYMNX
OHKZEUAIGTXKGJZNOY

LEHWBRXFDQUHDGWKLV

LEHWBRXFDQUHDGWKLV	YRUJOEKSQDHUQTJXYI
MFIXCSYGERVIEHXLMW	ZSVKPFLTREIVRUKYZJ
NGJYDTZHFSWJFIYMNX	ATWLQGMUSFJWSVLZAK
OHKZEUAIGTXKGJZNOY	BUXMRHNVTGKXTWMABL
PILAFVBJHUYLHKAOPZ	CVYNSIOWUHLYUXNBCM
QJMBGWCKIVZMILBPQA	DWZOTJPXVIMZVYOCDN
RKNCHXDLJWANJMCQRB	EXAPUKQYWJNAWZPDEO
SLODIYEMKXBOKNDRSC	FYBQVLRZXKOBXAQEFP
TMPEJZFNLYCPLOESTD	GZCRWMSAYLPCYBRFGQ
UNQFKAGOMZDQMPFTUE	HADSXNTBZMQDZCSGHR
VORGLBHPNAERNQGUVF	IBETYOUCANREADTHIS
WPSHMCIQOBFSORHVWG	JCFUZPVDBOSFBEUIJT
XQTINDJRPCGTPSIWXH	KDGVAQWECPTGCFVJKU

LEHWBRXFDQUHDGWKLV

LEHWBRXFDQUHDGWKLV	YRUJOEKSQDHUQTJXYI
MFIXCSYGERVIEHXLMW	ZSVKPFLTREIVRUKYZJ
NGJYDTZHFSWJFIYMNX	ATWLQGMUSFJWSVLZAK
OHKZEUAIGTXKGJZNOY	BUXMRHNVTGKXTWMABL
PILAFVBJHUYLHKAOPZ	CVYNSIOWUHLYUXNBCM
QJMBGWCKIVZMILBPQA	DWZOTJPXVIMZVYOCDN
RKNCHXDLJWANJMCQRB	EXAPUKQYWJNAWZPDEO
SLODIYEMKXBOKNDRSC	FYBQVLRZXKOBXAQEFP
TMPEJZFNLYCPLOESTD	GZCRWMSAYLPCYBRFGQ
UNQFKAGOMZDQMPFTUE	HADSXNTBZMQDZCSGHR
VORGLBHPNAERNQGUVF	IBETYOUCANREADTHIS
WPSHMCIQOBFSORHVWG	JCFUZPVDBOSFBEUIJT
XQTINDJRPCGTPSIWXH	KDGVAQWECPTGCFVJKU

Monoalphabetic Substitution Ciphers

Use a full permutation of the alphabet.

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krusfltagzmqnbveophxjywcid
```

Monoalphabetic Substitution Ciphers

Use a full permutation of the alphabet.

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krusfltagzmqnbveophxjywcid
```

- `NOT JUST A SIMPLE SHIFT`

Monoalphabetic Substitution Ciphers

Use a full permutation of the alphabet.

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krusfltagzmqnbveophxjywcid
```

- ```
  NOT JUST A SIMPLE SHIFT
  bvx zjhx k hgneqf haglx
  ```
  ```

Monoalphabetic Substitution Ciphers

Use a full permutation of the alphabet.

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krusfltagzmqnbveophxjywcid
```

- ```
  NOT JUST A SIMPLE SHIFT
  bvx zjhx k hgneqf haglx
  ```
  ```

Monoalphabetic Substitution Ciphers

Use a full permutation of the alphabet.

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krusfltagzmqnbveophxjywcid
```

- ```
  NOT JUST A SIMPLE SHIFT
  bvx zjhx k hgneqf haglx
  ```
- What is the size of the key space?
  ```

Monoalphabetic Substitution Ciphers

Use a full permutation of the alphabet.

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krusfltagzmqnbveophxjywcid
```

- ```
  NOT JUST A SIMPLE SHIFT
  bvx zjhx k hgneqf haglx
  ```
- What is the size of the key space? $26! \approx 10^{26} = 100$ septillion.
  ```

Monoalphabetic Substitution Ciphers

Use a full permutation of the alphabet.

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krusfltagzmqnbveophxjywcid
```

- ```
  NOT JUST A SIMPLE SHIFT
  bvx zjhx k hgneqf haglx
  ```
- What is the size of the key space? $26! \approx 10^{26} = 100$ septillion.
- How do you manage so many keys?
  ```

Monoalphabetic Substitution Ciphers

Use a full permutation of the alphabet.

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krusfltagzmqnbveophxjywcid
```

- ```
  NOT JUST A SIMPLE SHIFT
  bvx zjhx k hgneqf haglx
  ```
- What is the size of the key space? $26! \approx 10^{26} = 100$ septillion.
- How do you manage so many keys? Use a keyword/phrase:

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krustyheclownpqvxzabdfgijm
```
```

Monoalphabetic Substitution Ciphers

Use a full permutation of the alphabet.

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krusfltagzmqnbveophxjywcid
```

- ```
  NOT JUST A SIMPLE SHIFT
  bvx zjhx k hgneqf haglx
  ```
- What is the size of the key space? $26! \approx 10^{26} = 100$ septillion.
- How do you manage so many keys? Use a keyword/phrase:

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krustyheclownpqvxzabdfgijm
```
```

Monoalphabetic Substitution Ciphers

Use a full permutation of the alphabet.

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krusfltagzmqnbveophxjywcid
```

- ```
  NOT JUST A SIMPLE SHIFT
  bvx zjhx k hgneqf haglx
  ```
- What is the size of the key space? $26! \approx 10^{26} = 100$ septillion.
- How do you manage so many keys? Use a keyword/phrase:

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: krustyheclownpqvxzabdfgijm
```

- Monoalphs remained secure for centuries. Arab cryptanalysts discovered *frequency analysis* around 800 A.D.
```

Frequency of Letters in English

Letter	Percentage		Letter	Percentage
A	8.2		N	6.7
B	1.5		O	7.5
C	2.8		P	1.9
D	4.3		Q	0.1
E	12.7		R	6.0
F	2.2		S	6.3
G	2.0		T	9.1
H	6.1		U	2.8
I	7.0		V	1.0
J	0.2		W	2.4
K	0.8		X	0.2
L	4.0		Y	2.0
M	2.4		Z	0.1

- (Source: H. Beker and F. Piper, *Cipher Systems: The Protection of Communication.*)

Example of Frequency Analysis and Language Modelling

LXV TWJ RXZGR KL TVSZJGBJ WJTBEZXG EX EIZN Z PJTG EIZN ZN TG

TVSZJGBJ EITE ZN WTZNJS XG EJYJMZNZXG EIJZW NETGSTWSN ITMJ KJJG

YXDJWJS XMJW EIJ LJTWN LXV HGXD EIJNJ RVLN NZE ZG AWXGE XA EIJZW

NJEN TGS EIJ RTPPT WTLN JTE EIJ DIZEJ KYXXS BJYYN XA EIJZW

KWTZGN XVE VI LXV HGXD Z FVZE

A:0.013	B:0.017	C:0.000	D:0.017
E:0.098	F:0.004	G:0.071	H:0.008
I:0.058	J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	T:0.080
U:0.000	V:0.040	W:0.058	X:0.080
Y:0.022	Z:0.093		

Example of Frequency Analysis and Language Modelling

LXV TWJ RXZGR KL TVSZJGBJ WJTBEZXG EX EIZN Z PJTG EIZN ZN TG

TVSZJGBJ EITE ZN WTZNJS XG EJYJMZNZXG EIJZW NETGSTWSN ITMJ KJJG

YXDJWJS XMJW EIJ LJTWN LXV HGXD EIJNJ RVLN NZE ZG AWXGE XA EIJZW

NJEN TGS EIJ RTPPT WTLN JTE EIJ DIZEJ KYXXS BJYYN XA EIJZW

KWTZGN XVE VI LXV HGXD Z FVZE

A:0.013	B:0.017	C:0.000	D:0.017
E:0.098	F:0.004	G:0.071	H:0.008
I:0.058	J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	T:0.080
U:0.000	V:0.040	W:0.058	X:0.080
Y:0.022	Z:0.093		

Example of Frequency Analysis and Language Modelling

LXV TWe RXZGR KL TVSZeGBe WeTBEZXG EX EIZN Z PeTG EIZN ZN TG

TVSZeGBe EITE ZN WTZNeS XG EeYeMZNZXG EIeZW NETGSTWSN ITMe KeeG

YXDeWeS XMeW EIe LeTWN LXV HGXD EIeNe RVLN NZE ZG AWXGE XA EIeZW

NeEN TGS EIe RTPPT WTLN eTE EIe DIZEe KYXXS BeYYN XA EIeZW

KWTZGN XVE VI LXV HGXD Z FVZE

A:0.013	B:0.017	C:0.000	D:0.017
E:0.098	F:0.004	G:0.071	H:0.008
I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	T:0.080
U:0.000	V:0.040	W:0.058	X:0.080
Y:0.022	Z:0.093		

Example of Frequency Analysis and Language Modelling

LXV TWe RXZGR KL TVSZeGBe WeTBEZXG EX EIZN Z PeTG EIZN ZN TG

TVSZeGBe EITE ZN WTZNeS XG EeYeMZNZXG EIeZW NETGSTWSN ITMe KeeG

YXDeWeS XMeW EIe LeTWN LXV HGXD EIeNe RVLN NZE ZG AWXGE XA EIeZW

NeEN TGS EIe RTPPT WTLN eTE EIe DIZEe KYXXS BeYYN XA EIeZW

KWTZGN XVE VI LXV HGXD Z FVZE

A:0.013	B:0.017	C:0.000	D:0.017
E:0.098	F:0.004	G:0.071	H:0.008
I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	T:0.080
U:0.000	V:0.040	W:0.058	X:0.080
Y:0.022	Z:0.093		

Example of Frequency Analysis and Language Modelling

LXV TWe RXZGR KL TVSZeGBe WeTBtZXG tX tIZN Z PeTG tIZN ZN TG

TVSZeGBe tITt ZN WTZNeS XG teYeMZNZXG tIeZW NtTGSTWSN ITMe KeeG

YXDeWeS XMeW tIe LeTWN LXV HGXD tIeNe RVLN NZt ZG AWXGt XA tIeZW

NetN TGS tIe RTPPT WTLN eTt tIe DIZte KYXXS BeYYN XA tIeZW

KWTZGN XVt VI LXV HGXD Z FVZt

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	T:0.080
U:0.000	V:0.040	W:0.058	X:0.080
Y:0.022	Z:0.093		

Example of Frequency Analysis and Language Modelling

LXV TWe RXZGR KL TVSZeGBe WeTBtZXG tX tIZN Z PeTG tIZN ZN TG

TVSZeGBe tITt ZN WTZNeS XG teYeMZNZXG tIeZW NtTGSTWSN ITMe KeeG

YXDeWeS XMeW tIe LeTWN LXV HGXD tIeNe RVLN NZt ZG AWXGt XA tIeZW

NetN TGS tIe RTPPT WTLN eTt tIe DIZte KYXXS BeYYN XA tIeZW

KWTZGN XVt VI LXV HGXD Z FVZt

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	T:0.080
U:0.000	V:0.040	W:0.058	X:0.080
Y:0.022	Z:0.093		

Example of Frequency Analysis and Language Modelling

LXV TWe RXZGR KL TVSZeGBe WeTBtZXG tX thZN Z PeTG thZN ZN TG

TVSZeGBe thTt ZN WTZNeS XG teYeMZNZXG theZW NtTGSTWSN hTMe KeeG

YXDeWeS XMeW the LeTWN LXV HGXD theNe RVLN NZt ZG AWXGt XA theZW

NetN TGS the RTPPT WTLN eTt the DhZte KYXXS BeYYN XA theZW

KWTZGN XVt Vh LXV HGXD Z FVZt

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	T:0.080
U:0.000	V:0.040	W:0.058	X:0.080
Y:0.022	Z:0.093		

Example of Frequency Analysis and Language Modelling

LXV TWe RXZGR KL TVSZeGBe WeTBtZXG tX thZN Z PeTG thZN ZN TG

TVSZeGBe thTt ZN WTZNeS XG teYeMZNZXG theZW NtTGSTWSN hTMe KeeG

YXDeWeS XMeW the LeTWN LXV HGXD theNe RVLN NZt ZG AWXGt XA theZW

NetN TGS the RTPPT WTLN eTt the DhZte KYXXS BeYYN XA theZW

KWTZGN XVt Vh LXV HGXD Z FVZt

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	T:0.080
U:0.000	V:0.040	W:0.058	X:0.080
Y:0.022	Z:0.093		

Example of Frequency Analysis and Language Modelling

LXV aWe RXZGR KL aVSZeGBe WeaBtZXG tX thZN Z PeaG thZN ZN aG

aVSZeGBe that ZN WaZNeS XG teYeMZNZXG theZW NtaGSaWSN haMe KeeG

YXDeWeS XMeW the LeaWN LXV HGXD theNe RVLN NZt ZG AWXGt XA theZW

NetN aGS the RaPPa WaLN eat the DhZte KYXXS BeYYN XA theZW

KWaZGN XVt Vh LXV HGXD Z FVZt

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	V:0.040	W:0.058	X:0.080
Y:0.022	Z:0.093		

Example of Frequency Analysis and Language Modelling

LXV aWe RXZGR KL aVSZeGBe WeaBtZXG tX thZN Z PeaG thZN ZN aG

aVSZeGBe that ZN WaZNeS XG teYeMZNZXG theZW NtaGSaWSN haMe KeeG

YXDeWeS XMeW the LeaWN LXV HGXD theNe RVLN NZt ZG AWXGt XA theZW

NetN aGS the RaPPa WaLN eat the DhZte KYXXS BeYYN XA theZW

KWaZGN XVt Vh LXV HGXD Z FVZt

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	V:0.040	W:0.058	X:0.080
Y:0.022	Z:0.093		

Example of Frequency Analysis and Language Modelling

LoV aWe RoZGR KL aVSZeGBe WeaBtZoG to thZN Z PeaG thZN ZN aG

aVSZeGBe that ZN WaZNeS oG teYeMZNZoG theZW NtaGSaWSN haMe KeeG

YoDeWeS oMeW the LeaWN LoV HGoD theNe RVLN NZt ZG AWoGt oA theZW

NetN aGS the RaPPa WaLN eat the DhZte KYooS BeYYN oA theZW

KWaZGN oVt Vh LoV HGoD Z FVZt

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	V:0.040	W:0.058	o-X:0.080
Y:0.022	Z:0.093		

Example of Frequency Analysis and Language Modelling

LoV aWe RoZGR KL aVSZeGBe WeaBtZoG to thZN Z PeaG thZN ZN aG

aVSZeGBe that ZN WaZNeS oG teYeMZNZoG theZW NtaGSaWSN haMe KeeG

YoDeWeS oMeW the LeaWN LoV HGoD theNe RVLN NZt ZG AWoGt oA theZW

NetN aGS the RaPPa WaLN eat the DhZte KYooS BeYYN oA theZW

KWaZGN oVt Vh LoV HGoD Z FVZt

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	V:0.040	W:0.058	o-X:0.080
Y:0.022	Z:0.093		

Example of Frequency Analysis and Language Modelling

LoV aWe RoiGR KL aVSieGBe WeaBtioG to thiN i PeaG thiN iN aG

aVSieGBe that iN WaiNeS oG teYeMiNioG theiW NtaGSaWSN haMe KeeG

YoDeWeS oMeW the LeaWN LoV HGoD theNe RVLN Nit iG AWoGt oA theiW

NetN aGS the RaPPa WaLN eat the Dhite KYooS BeYYN oA theiW

KWaiGN oVt Vh LoV HGoD i FVit

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	V:0.040	W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

LoV aWe RoiGR KL aVSieGBe WeaBtioG to thiN i PeaG thiN iN aG

aVSieGBe that iN WaiNeS oG teYeMiNioG theiW NtaGSaWSN haMe KeeG

YoDeWeS oMeW the LeaWN LoV HGoD theNe RVLN Nit iG AWoGt oA theiW

NetN aGS the RaPPa WaLN eat the Dhite KYooS BeYYN oA theiW

KWaiGN oVt Vh LoV HGoD i FVit

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	V:0.040	W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

LoV are RoiGR KL aVSieGBe reaBtioG to thiN i PeaG thiN iN aG

aVSieGBe that iN raiNeS oG teYeMiNioG their NtaGSarSN haMe KeeG

YoDereS oMer the LearN LoV HGoD theNe RVLN Nit iG AroGt oA their

NetN aGS the RaPPa raLN eat the Dhite KYooS BeYYN oA their

KraiGN oVt Vh LoV HGoD i FVit

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

LoV are RoiGR KL aVSieGBe reaBtioG to thiN i PeaG thiN iN aG

aVSieGBe that iN raiNeS oG teYeMiNioG their NtaGSarSN haMe KeeG

YoDereS oMer the LearN LoV HGoD theNe RVLN Nit iG AroGt oA their

NetN aGS the RaPPa raLN eat the Dhite KYooS BeYYN oA their

KraiGN oVt Vh LoV HGoD i FVit

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

LoV are RoiGR KL aVSieGBe reaBtioG to this i PeaG this is aG

aVSieGBe that is raiseS oG teYeMisioG their staGSarSs haMe KeeG

YoDereS oMer the Lears LoV HGoD these RVLs sit iG AroGt oA their

sets aGS the RaPPa raLs eat the Dhite KYooS BeYYs oA their

KraiGs oVt Vh LoV HGoD i FVit

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

LoV are RoiGR KL aVSieGBe reaBtioG to this i PeaG this is aG

aVSieGBe that is raiseS oG teYeMisioG their staGSarSs haMe KeeG

YoDereS oMer the Lears LoV HGoD these RVLs sit iG AroGt oA their

sets aGS the RaPPa raLs eat the Dhite KYooS BeYYs oA their

KraiGs oVt Vh LoV HGoD i FVit

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

Lou are RoiGR KL auSieGBe reaBtioG to this i PeaG this is aG

auSieGBe that is raiseS oG teYeMisioG their staGSarSs haMe KeeG

YoDereS oMer the Lears Lou HGoD these RuLs sit iG AroGt oA their

sets aGS the RaPPa raLs eat the Dhite KYooS BeYYs oA their

KraiGs out uh Lou HGoD i Fuit

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

Lou are RoiGR KL auSieGBe reaBtioG to this i PeaG this is aG

auSieGBe that is raiseS oG teYeMisioG their staGSarSs haMe KeeG

YoDereS oMer the Lears Lou HGoD these RuLs sit iG AroGt oA their

sets aGS the RaPPa raLs eat the Dhite KYooS BeYYs oA their

KraiGs out uh Lou HGoD i Fuit

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are RoiGR Ky auSieGBe reaBtioG to this i PeaG this is aG

auSieGBe that is raiseS oG teYeMisioG their staGSarSs haMe KeeG

YoDereS oMer the years you HGoD these Ruys sit iG AroGt oA their

sets aGS the RaPPa rays eat the Dhite KYooS BeYYs oA their

KraiGs out uh you HGoD i Fuit
```

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

you are RoiGR Ky auSieGBe reaBtioG to this i PeaG this is aG

auSieGBe that is raiseS oG teYeMisioG their staGSarSs haMe KeeG

YoDereS oMer the years you HGoD these Ruys sit iG AroGt oA their

sets aGS the RaPPa rays eat the Dhite KYooS BeYYs oA their

KraiGs out uh you HGoD i Fuit

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are RoinR Ky auSienBe reaBtion to this i Pean this is an

auSienBe that is raiseS on teYeMision their stanSarSs haMe Keen

YoDereS oMer the years you HnoD these Ruys sit in Aront oA their

sets anS the RaPPa rays eat the Dhite KYooS BeYYs oA their

Krains out uh you HnoD i Fuit
```

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

you are RoinR Ky auSienBe reaBtion to this i Pean this is an

auSienBe that is raiseS on teYeMision their stanSarSs haMe Keen

YoDereS oMer the years you HnoD these Ruys sit in Aront oA their

sets anS the RaPPa rays eat the Dhite KYooS BeYYs oA their

Krains out uh you HnoD i Fuit

A:0.013	B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are RoinR Ky auSience reaction to this i Pean this is an

auSience that is raiseS on teYeMision their stanSarSs haMe Keen

YoDereS oMer the years you HnoD these Ruys sit in Aront oA their

sets anS the RaPPa rays eat the Dhite KYooS ceYYs oA their

Krains out uh you HnoD i Fuit
```

A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

you are RoinR Ky auSience reaction to this i Pean this is an

auSience that is raiseS on teYeMision their stanSarSs haMe Keen

YoDereS oMer the years you HnoD these Ruys sit in Aront oA their

sets anS the RaPPa rays eat the Dhite KYooS ceYYs oA their

Krains out uh you HnoD i Fuit

A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are RoinR Ky audience reaction to this i Pean this is an

audience that is raised on teYeMision their standards haMe Keen

YoDered oMer the years you HnoD these Ruys sit in Aront oA their

sets and the RaPPa rays eat the Dhite KYood ceYYs oA their

Krains out uh you HnoD i Fuit
```

A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

you are RoinR Ky audience reaction to this i Pean this is an

audience that is raised on teYeMision their standards haMe Keen

YoDered oMer the years you HnoD these Ruys sit in Aront oA their

sets and the RaPPa rays eat the Dhite KYood ceYYs oA their

Krains out uh you HnoD i Fuit

A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are RoinR Ky audience reaction to this i Pean this is an

audience that is raised on teleMision their standards haMe Keen

loDered oMer the years you HnoD these Ruys sit in Aront oA their

sets and the RaPPa rays eat the Dhite Klood cells oA their

Krains out uh you HnoD i Fuit
```

A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

you are RoinR Ky audience reaction to this i Pean this is an

audience that is raised on teleMision their standards haMe Keen

loDered oMer the years you HnoD these Ruys sit in Aront oA their

sets and the RaPPa rays eat the Dhite Klood cells oA their

Krains out uh you HnoD i Fuit

A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are RoinR Ky audience reaction to this i Pean this is an

audience that is raised on television their standards have Keen

loDered over the years you HnoD these Ruys sit in Aront oA their

sets and the RaPPa rays eat the Dhite Klood cells oA their

Krains out uh you HnoD i Fuit
```

A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

you are RoinR Ky audience reaction to this i Pean this is an

audience that is raised on television their standards have Keen

loDered over the years you HnoD these Ruys sit in Aront oA their

sets and the RaPPa rays eat the Dhite Klood cells oA their

Krains out uh you HnoD i Fuit

A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are RoinR Ky audience reaction to this i Pean this is an

audience that is raised on television their standards have Keen

loDered over the years you HnoD these Ruys sit in front of their

sets and the RaPPa rays eat the Dhite Klood cells of their

Krains out uh you HnoD i Fuit
```

f-A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

you are RoinR Ky audience reaction to this i Pean this is an

audience that is raised on television their standards have Keen

loDered over the years you HnoD these Ruys sit in front of their

sets and the RaPPa rays eat the Dhite Klood cells of their

Krains out uh you HnoD i Fuit

f-A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are going Ky audience reaction to this i Pean this is an

audience that is raised on television their standards have Keen

loDered over the years you HnoD these guys sit in front of their

sets and the gaPPa rays eat the Dhite Klood cells of their

Krains out uh you HnoD i Fuit
```

f-A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	g-R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are going Ky audience reaction to this i Pean this is an

audience that is raised on television their standards have Keen

loDered over the years you HnoD these guys sit in front of their

sets and the gaPPa rays eat the Dhite Klood cells of their

Krains out uh you HnoD i Fuit
```

f-A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	P:0.013
Q:0.000	g-R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are going Ky audience reaction to this i mean this is an

audience that is raised on television their standards have Keen

loDered over the years you HnoD these guys sit in front of their

sets and the gamma rays eat the Dhite Klood cells of their

Krains out uh you HnoD i Fuit
```

f-A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	m-P:0.013
Q:0.000	g-R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

you are going Ky audience reaction to this i mean this is an

audience that is raised on television their standards have Keen

loDered over the years you HnoD these guys sit in front of their

sets and the gamma rays eat the Dhite Klood cells of their

Krains out uh you HnoD i Fuit

f-A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	m-P:0.013
Q:0.000	g-R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are going by audience reaction to this i mean this is an

audience that is raised on television their standards have been

loDered over the years you HnoD these guys sit in front of their

sets and the gamma rays eat the Dhite blood cells of their

brains out uh you HnoD i Fuit
```

f-A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	b-K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	m-P:0.013
Q:0.000	g-R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

you are going by audience reaction to this i mean this is an

audience that is raised on television their standards have been

loDered over the years you HnoD these guys sit in front of their

sets and the gamma rays eat the Dhite blood cells of their

brains out uh you HnoD i Fuit

f-A:0.013	c-B:0.017	C:0.000	D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	b-K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	m-P:0.013
Q:0.000	g-R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are going by audience reaction to this i mean this is an

audience that is raised on television their standards have been

lowered over the years you Hnow these guys sit in front of their

sets and the gamma rays eat the white blood cells of their

brains out uh you Hnow i Fuit
```

f-A:0.013	c-B:0.017	C:0.000	w-D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	b-K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	m-P:0.013
Q:0.000	g-R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are going by audience reaction to this i mean this is an

audience that is raised on television their standards have been

lowered over the years you Hnow these guys sit in front of their

sets and the gamma rays eat the white blood cells of their

brains out uh you Hnow i Fuit
```

f-A:0.013	c-B:0.017	C:0.000	w-D:0.017
t-E:0.098	F:0.004	n-G:0.071	H:0.008
h-I:0.058	e-J:0.129	b-K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	m-P:0.013
Q:0.000	g-R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are going by audience reaction to this i mean this is an

audience that is raised on television their standards have been

lowered over the years you know these guys sit in front of their

sets and the gamma rays eat the white blood cells of their

brains out uh you know i Fuit
```

f-A:0.013	c-B:0.017	C:0.000	w-D:0.017
t-E:0.098	F:0.004	n-G:0.071	k-H:0.008
h-I:0.058	e-J:0.129	b-K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	m-P:0.013
Q:0.000	g-R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are going by audience reaction to this i mean this is an

audience that is raised on television their standards have been

lowered over the years you know these guys sit in front of their

sets and the gamma rays eat the white blood cells of their

brains out uh you know i Fuit
```

f-A:0.013	c-B:0.017	C:0.000	w-D:0.017
t-E:0.098	F:0.004	n-G:0.071	k-H:0.008
h-I:0.058	e-J:0.129	b-K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	m-P:0.013
Q:0.000	g-R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Example of Frequency Analysis and Language Modelling

```
you are going by audience reaction to this i mean this is an

audience that is raised on television their standards have been

lowered over the years you know these guys sit in front of their

sets and the gamma rays eat the white blood cells of their

brains out uh you know i quit
```

f-A:0.013	c-B:0.017	C:0.000	w-D:0.017
t-E:0.098	q-F:0.004	n-G:0.071	k-H:0.008
h-I:0.058	e-J:0.129	b-K:0.017	y-L:0.031
v-M:0.013	s-N:0.075	O:0.000	m-P:0.013
Q:0.000	g-R:0.017	d-S:0.035	a-T:0.080
U:0.000	u-V:0.040	r-W:0.058	o-X:0.080
l-Y:0.022	i-Z:0.093		

Polyalphabetic Ciphers

- Vigenère cipher: Use a keyword to interleave several Caesar shifts.

```
homerhomerhomerho
WELCOMETOILLINOIS
dsxgftsfszszurfpq
```

Polyalphabetic Ciphers

- Vigenère cipher: Use a keyword to interleave several Caesar shifts.

```
homerhomerhomerho
WELCOMETOILLINOIS
dsxgftsfszszurfpq
```

- KWUMZESWIZOBKIUPQEZKEDMAOBIAVTABHUAIYMAZBHUAIEINMCDU
  MNOMTTITUARMQSQLOZBEXMVUAIAVTTMIDATMVDMZDEPAHMBQMNXW
  WQZEPWVQZTTMYQIREGOGSNAETTMSQOUKASUBIZNRAVTANTTMIDAE
  FAAZLTTMGMUMMZAKAEMBTTMWTQTQJLAWDOMLXAORBHQQRNZAUVSA
  CTGPYACKZWWUYUUB

Polyalphabetic Ciphers

- Vigenère cipher: Use a keyword to interleave several Caesar shifts.

```
homerhomerhomerho
WELCOMETOILLINOIS
dsxgftsfszszurfpq
```

- KWUMZESWIZOBKIUPQEZKEDMAOBIAVTABHUAIYMAZBHUAIEINMCDU
  MNOMTTITUARMQSQLOZBEXMVUAIAVTTMIDATMVDMZDEPAHMBQMNXW
  WQZEPWVQZTTMYQIREGOGSNAETTMSQOUKASUBIZNRAVTANTTMIDAE
  FAAZLTTMGMUMMZAKAEMBTTMWTQTQJLAWDOMLXAORBHQQRNZAUVSA
  CTGPYACKZWWUYUUB
- Look how the frequency distribution is flattened out:

A:0.0577	B:0.0222	C:0.0088	D:0.0355	E:0.0888
F:0.0622	G:0.0222	H:0.0222	I:0.0711	J:0.0044
K:0.0355	L:0.0044	M:0.0711	N:0.0266	O:0.0266
P:0.0577	Q:0.0622	R:0.0222	S:0.0488	T:0.0577
U:0.0577	V:0.0266	W:0.0488	X:0.0088	Y:0.0088
Z:0.0400				

Vigenère Cipher (Cont.)

- The Vigenère cipher remained unbroken for about three hundred years. Babbage discovered the following weakness:

```
KWUMZESWIZOBKIUPQEZKEDMAOBIAVTABHUAIYMAZBHUAIEINMCDU
MNOMTTITUARMQSQLOZBEXMVUAIAVTTMIDATMVDMZDEPAHMBQMNXW
WQZEPWVQZTTMYQIREGOGSNAETTMSQOUKASUBIZNRAVTANTTMIDAE
FAAZLTTMGMUMMZAKAEMBTTMWTQTQJLAWDOMLXAORBHQQRNZAUVSA
CTGPYACKZWWUYUUB
```

Vigenère Cipher (Cont.)

- The Vigenère cipher remained unbroken for about three hundred years. Babbage discovered the following weakness:

```
KWUMZESWIZOBKIUPQEZKEDMAOBIAVTABHUAIYMAZBHUAIEINMCDU
MNOMTTITUARMQSQLOZBEXMVUAIAVTTMIDATMVDMZDEPAHMBQMNXW
WQZEPWVQZTTMYQIREGOGSNAETTMSQOUKASUBIZNRAVTANTTMIDAE
FAAZLTTMGMUMMZAKAEMBTTMWTQTQJLAWDOMLXAORBHQQRNZAUVSA
CTGPYACKZWWUYUUB
```

- Common letter blocks spaced apart by a multiple of the keyword will encrypt identically.

Vigenère Cipher (Cont.)

- The Vigenère cipher remained unbroken for about three hundred years. Babbage discovered the following weakness:

```
KWUMZESWIZOBKIUPQEZKEDMAOBIAVTABHUAIYMAZBHUAIEINMCDU
MNOMTTITUARMQSQLOZBEXMVUAIAVTTMIDATMVDMZDEPAHMBQMNXW
WQZEPWVQZTTMYQIREGOGSNAET<-----   21   ----->TTMIDAE
FAAZLTTMGMUMMZAKAEMBTTMWTQTQJLAWDOMLXAORBHQQRNZAUVSA
CTGPYACKZWWUYUUB
```

- Common letter blocks spaced apart by a multiple of the keyword will encrypt identically.
- Key length divides GCD of identical spacings.

Vigenère Cipher (Cont.)

- The Vigenère cipher remained unbroken for about three hundred years. Babbage discovered the following weakness:

```
KWUMZESWIZOBKIUPQEZKEDMAOBIAVTABHUAIYMAZBHUAIEINMCDU
MNOMTTITUARMQSQLOZBEXMVUAIAVTTMIDATMVDMZDEPAHMBQMNXW
WQZEPWVQZTTMYQIREGOGSNAETTMSQOUKASUBIZNRAVTANTTMIDAE
FAAZLT<---- 15 ---->TTMWTQTQJLAWDOMLXAORBHQQRNZAUVSA
CTGPYACKZWWUYUUB
```

- Common letter blocks spaced apart by a multiple of the keyword will encrypt identically.
- Key length divides GCD of identical spacings.

Vigenère Cipher (Cont.)

- The Vigenère cipher remained unbroken for about three hundred years. Babbage discovered the following weakness:

```
KWUMZESWIZOBKIUPQEZKEDMAOBIAVTABHUAIYMAZBHUAIEINMCDU
MNOMTTITUARMQSQLOZBEXMVUAIAVTTMIDATMVDMZDEPAHMBQMNXW
WQZEPWVQZTTMYQIREGOGSNAETTMSQOUKASUBIZNRAVTANTTMIDAE
FAAZLTTMGMUMMZAKAEMBTTMWTQTQJLAWDOMLXAORBHQQRNZAUVSA
CTGPYACKZWWUYUUB
```

- Common letter blocks spaced apart by a multiple of the keyword will encrypt identically.
- Key length divides GCD of identical spacings. Here $\gcd(15, 21) = 3$.

Vigenère Cipher (Cont.)

- The Vigenère cipher remained unbroken for about three hundred years. Babbage discovered the following weakness:

```
KWUMZESWIZOBKIUPQEZKEDMAOBIAVTABHUAIYMAZBHUAIEINMCDU
MNOMTTITUARMQSQLOZBEXMVUAIAVTTMIDATMVDMZDEPAHMBQMNXW
WQZEPWVQZTTMYQIREGOGSNAETTMSQOUKASUBIZNRAVTANTTMIDAE
FAAZLTTMGMUMMZAKAEMBTTMWTQTQJLAWDOMLXAORBHQQRNZAUVSA
CTGPYACKZWWUYUUB
```

- Common letter blocks spaced apart by a multiple of the keyword will encrypt identically.
- Key length divides GCD of identical spacings. Here $\gcd(15, 21) = 3$.
- Once key length is discovered, perform multiple frequency counts.

A:0.1200	A:0.1333	A:0.0811
B:0.0000	B:0.1067	B:0.0270
C:0.0000	C:0.0400	C:0.0000
D:0.0400	D:0.0000	D:0.0541
E:0.0400	E:0.0133	E:0.0946
F:0.0133	F:0.0000	F:0.0000
G:0.0267	G:0.0133	G:0.0135
H:0.0133	H:0.0000	H:0.0405
I:0.0000	I:0.0533	I:0.1081
J:0.0000	J:0.0133	J:0.0000
K:0.0533	K:0.0133	K:0.0135
L:0.0000	L:0.0267	L:0.0270
M:0.1067	M:0.1867	M:0.0135
N:0.0133	N:0.0267	N:0.0541
O:0.0400	O:0.0267	O:0.0405
P:0.0267	P:0.0267	P:0.0000
Q:0.1067	Q:0.0533	Q:0.0000
R:0.0133	R:0.0000	R:0.0541
S:0.0133	S:0.0133	S:0.0541
T:0.1067	T:0.0000	T:0.1757
U:0.1200	U:0.0133	U:0.0541
V:0.0000	V:0.0667	V:0.0270
W:0.0000	W:0.0800	W:0.0405
X:0.0400	X:0.0000	X:0.0000
Y:0.0133	Y:0.0133	Y:0.0270
Z:0.0933	Z:0.0800	Z:0.0000

o-A:0.1200	A:0.1333	A:0.0811
p-B:0.0000	B:0.1067	B:0.0270
q-C:0.0000	C:0.0400	C:0.0000
r-D:0.0400	D:0.0000	D:0.0541
s-E:0.0400	E:0.0133	E:0.0946
t-F:0.0133	F:0.0000	F:0.0000
u-G:0.0267	G:0.0133	G:0.0135
v-H:0.0133	H:0.0000	H:0.0405
w-I:0.0000	I:0.0533	I:0.1081
x-J:0.0000	J:0.0133	J:0.0000
y-K:0.0533	K:0.0133	K:0.0135
z-L:0.0000	L:0.0267	L:0.0270
a-M:0.1067	M:0.1867	M:0.0135
b-N:0.0133	N:0.0267	N:0.0541
c-O:0.0400	O:0.0267	O:0.0405
d-P:0.0267	P:0.0267	P:0.0000
e-Q:0.1067	Q:0.0533	Q:0.0000
f-R:0.0133	R:0.0000	R:0.0541
g-S:0.0133	S:0.0133	S:0.0541
h-T:0.1067	T:0.0000	T:0.1757
i-U:0.1200	U:0.0133	U:0.0541
j-V:0.0000	V:0.0667	V:0.0270
k-W:0.0000	W:0.0800	W:0.0405
l-X:0.0400	X:0.0000	X:0.0000
m-Y:0.0133	Y:0.0133	Y:0.0270
n-Z:0.0933	Z:0.0800	Z:0.0000

o-A:0.1200
p-B:0.0000
q-C:0.0000
r-D:0.0400
s-E:0.0400
t-F:0.0133
u-G:0.0267
v-H:0.0133
w-I:0.0000
x-J:0.0000
y-K:0.0533
z-L:0.0000
a-M:0.1067
b-N:0.0133
c-O:0.0400
d-P:0.0267
e-Q:0.1067
f-R:0.0133
g-S:0.0133
h-T:0.1067
i-U:0.1200
j-V:0.0000
k-W:0.0000
l-X:0.0400
m-Y:0.0133
n-Z:0.0933

s-A:0.1333
t-B:0.1067
u-C:0.0400
v-D:0.0000
w-E:0.0133
x-F:0.0000
y-G:0.0133
z-H:0.0000
a-I:0.0533
b-J:0.0133
c-K:0.0133
d-L:0.0267
e-M:0.1867
f-N:0.0267
g-O:0.0267
h-P:0.0267
i-Q:0.0533
j-R:0.0000
k-S:0.0133
l-T:0.0000
m-U:0.0133
n-V:0.0667
o-W:0.0800
p-X:0.0000
q-Y:0.0133
r-Z:0.0800

A:0.0811
B:0.0270
C:0.0000
D:0.0541
E:0.0946
F:0.0000
G:0.0135
H:0.0405
I:0.1081
J:0.0000
K:0.0135
L:0.0270
M:0.0135
N:0.0541
O:0.0405
P:0.0000
Q:0.0000
R:0.0541
S:0.0541
T:0.1757
U:0.0541
V:0.0270
W:0.0405
X:0.0000
Y:0.0270
Z:0.0000

o-A:0.1200
p-B:0.0000
q-C:0.0000
r-D:0.0400
s-E:0.0400
t-F:0.0133
u-G:0.0267
v-H:0.0133
w-I:0.0000
x-J:0.0000
y-K:0.0533
z-L:0.0000
a-M:0.1067
b-N:0.0133
c-O:0.0400
d-P:0.0267
e-Q:0.1067
f-R:0.0133
g-S:0.0133
h-T:0.1067
i-U:0.1200
j-V:0.0000
k-W:0.0000
l-X:0.0400
m-Y:0.0133
n-Z:0.0933

s-A:0.1333
t-B:0.1067
u-C:0.0400
v-D:0.0000
w-E:0.0133
x-F:0.0000
y-G:0.0133
z-H:0.0000
a-I:0.0533
b-J:0.0133
c-K:0.0133
d-L:0.0267
e-M:0.1867
f-N:0.0267
g-O:0.0267
h-P:0.0267
i-Q:0.0533
j-R:0.0000
k-S:0.0133
l-T:0.0000
m-U:0.0133
n-V:0.0667
o-W:0.0800
p-X:0.0000
q-Y:0.0133
r-Z:0.0800

a-A:0.0811
b-B:0.0270
c-C:0.0000
d-D:0.0541
e-E:0.0946
f-F:0.0000
g-G:0.0135
h-H:0.0405
i-I:0.1081
j-J:0.0000
k-K:0.0135
l-L:0.0270
m-M:0.0135
n-N:0.0541
o-O:0.0405
p-P:0.0000
q-Q:0.0000
r-R:0.0541
s-S:0.0541
t-T:0.1757
u-U:0.0541
v-V:0.0270
w-W:0.0405
x-X:0.0000
y-Y:0.0270
z-Z:0.0000

Vigenère Cipher (Cont.)

- Keyword = MIA

youaregoingbyaudiencereactiontothisimeanthisisanaudi
KWUMZESWIZOBKIUPQEZKEDMAOBIAVTABHUAIYMAZBHUAIEINMCDU

encethatisraisedontelevisiontheirstandardshavebeenlo
MNOMTTITUARMQSQLOZBEXMVUAIAVTTMIDATMVDMZDEPAHMBQMNXW

weredovertheyearsyouknowtheseguyssitinfrontoftheirse
WQZEPWVQZTTMYQIREGOGSNAETTMSQOUKASUBIZNRAVTANTTMIDAE

tsandthegammarayseatthewhitebloodcellsofthierbrainso
FAAZLTTMGMUMMZAKAEMBTTMWTQTQJLAWDOMLXAORBHQQRNZAUVSA

utuhyouknowiquit
CTGPYACKZWWUYUUB

Vigenère Cipher (Cont.)

- Keyword = MIA

```
  u  e  i  b  u  e  e  a  i  t  h  i  a  h  i  n  d
  U  E  I  B  U  E  E  A  I  T  H  I  A  H  I  N  D

 n  t  t  r  s  o  e  v  i  t  i  t  d  d  a  b  n
 N  T  T  R  S  O  E  V  I  T  I  T  D  D  A  B  N

w  e  v  t  y  r  o  n  t  s  u  s  i  r  t  t  i  e
W  E  V  T  Y  R  O  N  T  S  U  S  I  R  T  T  I  E

  a  t  g  m  a  e  t  w  t  l  d  l  o  h  r  a  s
  A  T  G  M  A  E  T  W  T  L  D  L  O  H  R  A  S

 t  y  k  w  u
 T  Y  K  W  U
```

Vigenère Cipher (Cont.)

- Keyword = MIA

youaregoingbyaudiencereactiontothisimeanthisisanaudi
KWUMZESWIZOBKIUPQEZKEDMAOBIAVTABHUAIYMAZBHUAIEINMCDU

encethatisraisedontelevisiontheirstandardshavebeenlo
MNOMTTITUARMQSQLOZBEXMVUAIAVTTMIDATMVDMZDEPAHMBQMNXW

weredovertheyearsyouknowtheseguyssitinfrontoftheirse
WQZEPWVQZTTMYQIREGOGSNAETTMSQOUKASUBIZNRAVTANTTMIDAE

tsandthegammarayseatthewhitebloodcellsofthierbrainso
FAAZLTTMGMUMMZAKAEMBTTMWTQTQJLAWDOMLXAORBHQQRNZAUVSA

utuhyouknowiquit
CTGPYACKZWWUYUUB

Perfecting the Vigenère Cipher

- What if the keyword in a Vigenère cipher is chosen to be long enough that it never cycles?

Perfecting the Vigenère Cipher

- What if the keyword in a Vigenère cipher is chosen to be long enough that it never cycles?

ONE-TIME PADS

Vigenère ciphers whose keyword is as long as the message itself.

Perfecting the Vigenère Cipher

- What if the keyword in a Vigenère cipher is chosen to be long enough that it never cycles?

ONE-TIME PADS

Vigenère ciphers whose keyword is as long as the message itself.

- Are unbreakable because any message of the same length is a possible decryption. For example:

Perfecting the Vigenère Cipher

- What if the keyword in a Vigenère cipher is chosen to be long enough that it never cycles?

ONE-TIME PADS

Vigenère ciphers whose keyword is as long as the message itself.

- Are unbreakable because any message of the same length is a possible decryption. For example:

`message: IDECRYPTEDIT`

Perfecting the Vigenère Cipher

- What if the keyword in a Vigenère cipher is chosen to be long enough that it never cycles?

ONE-TIME PADS

Vigenère ciphers whose keyword is as long as the message itself.

- Are unbreakable because any message of the same length is a possible decryption. For example:

```
message: IDECRYPTEDIT
keyword: XIJLWAMBOCEK
```

Perfecting the Vigenère Cipher

- What if the keyword in a Vigenère cipher is chosen to be long enough that it never cycles?

ONE-TIME PADS

Vigenère ciphers whose keyword is as long as the message itself.

- Are unbreakable because any message of the same length is a possible decryption. For example:

```
message: IDECRYPTEDIT
keyword: XIJLWAMBOCEK
cipher : FLNNNYBUSFMD
```

Perfecting the Vigenère Cipher

- What if the keyword in a Vigenère cipher is chosen to be long enough that it never cycles?

ONE-TIME PADS

Vigenère ciphers whose keyword is as long as the message itself.

- Are unbreakable because any message of the same length is a possible decryption. For example:

```
          message: IDECRYPTEDIT
          keyword: XIJLWAMBOCEK
          cipher : FLNNNYBUSFMD
guessed keyword: REAZPKHRKCZK
```

Perfecting the Vigenère Cipher

- What if the keyword in a Vigenère cipher is chosen to be long enough that it never cycles?

ONE-TIME PADS

Vigenère ciphers whose keyword is as long as the message itself.

- Are unbreakable because any message of the same length is a possible decryption. For example:

```
            message: IDECRYPTEDIT
            keyword: XIJLWAMBOCEK
            cipher : FLNNNYBUSFMD
  guessed keyword: REAZPKHRKCZK
incorrect decrypt: OHNOYOUDIDNT
```

One-time Pads (Cont.)

- One-time pads provide perfect secrecy, but present a large key distribution problem.

One-time Pads (Cont.)

- One-time pads provide perfect secrecy, but present a large key distribution problem.
- One-time pads can only be used once.

XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT

QHNNFIJNWSSOTGUJRNOXFMHRESMHVP

OERZTOHXANSASLKWELZBAOJVUSOUOV

One-time Pads (Cont.)

- One-time pads provide perfect secrecy, but present a large key distribution problem.
- One-time pads can only be used once.

```
XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT

QHNNFIJNWSSOTGUJRNOXFMHRESMHVP

OERZTOHXANSASLKWELZBAOJVUSOUOV
```

- This is vulnerable to *cribbing*.

One-time Pads (Cont.)

Guess the location of "the".

XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT

QHNNFIJNWSSOTGUJRNOXFMHRESMHVP

OERZTOHXANSASLKWELZBAOJVUSOUOV

One-time Pads (Cont.)

Guess the location of "the".

```
          XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT


crib--> the
          QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
key --> xaj

          OERZTOHXANSASLKWELZBAOJVUSOUOV
```

One-time Pads (Cont.)

Find corresponding decrypts. Guess again.

```
          att
          XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
          xaj

 crib--> the
          QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
 key --> xaj

          rei
          OERZTOHXANSASLKWELZBAOJVUSOUOV
          xaj
```

One-time Pads (Cont.)

Find corresponding decrypts.

```
crib--> attack
        XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
key --> xajtqr

        the
        QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
        xaj

        rei
        OERZTOHXANSASLKWELZBAOJVUSOUOV
        xaj
```

One-time Pads (Cont.)

A wrong assumption.

```
attack
XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
xajtqr

theupr
QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
xajtqr

reigdx
OERZTOHXANSASLKWELZBAOJVUSOUOV
xajtqr
```

One-time Pads (Cont.)

Back up.

```
att
XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
xaj

the
QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
xaj

rei
OERZTOHXANSASLKWELZBAOJVUSOUOV
xaj
```

One-time Pads (Cont.)

Crib again. Looks good!

```
crib--> atthe
        XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
key --> xajmo

        thebr
        QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
        xajmo

        reinf
        OERZTOHXANSASLKWELZBAOJVUSOUOV
        xajmo
```

One-time Pads (Cont.)

Crib again.

```
          atthebrea
          XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
          xajmoaqvw

          thebritsa
          QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
          xajmoaqvw

crib--> reinforce
          OERZTOHXANSASLKWELZBAOJVUSOUOV
          xajmoaqvw
```

One-time Pads (Cont.)

... which leads to ...

```
crib--> atthebreak
        XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
        xajmoaqvwb

        thebritsar
        QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
        xajmoaqvwb

        reinforcem
        OERZTOHXANSASLKWELZBAOJVUSOUOV
        xajmoaqvwb
```

One-time Pads (Cont.)

... which leads to ...

```
        atthebreakofda
        XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
        xajmoaqvwbonzt

        thebritsarebun
        QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
        xajmoaqvwbonzt

crib--> reinforcements
        OERZTOHXANSASLKWELZBAOJVUSOUOV
        xajmoaqvwbonzt
```

One-time Pads (Cont.)

... which leads to ... ??? Back up and try again.

```
crib--> atthebreakofday
        XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
        xajmoaqvwbonzti

        thebritsarebunm
        QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
        xajmoaqvwbonzti

        reinforcementsc
        OERZTOHXANSASLKWELZBAOJVUSOUOV
        xajmoaqvwbonzti
```

One-time Pads (Cont.)

Much better! Keep going ...

```
crib--> atthebreakofdawn
        XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
        xajmoaqvwbonztkf

        thebritsarebunke
        QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
        xajmoaqvwbonztkf

        reinforcementsar
        OERZTOHXANSASLKWELZBAOJVUSOUOV
        xajmoaqvwbonztkf
```

One-time Pads (Cont.)

Keep going ...

```
          atthebreakofdawnsei
          XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
          xajmoaqvwbonztkfajl

crib--> thebritsarebunkered
          QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
          xajmoaqvwbonztkfajl

          reinforcementsareco
          OERZTOHXANSASLKWELZBAOJVUSOUOV
          xajmoaqvwbonztkfajl
```

One-time Pads (Cont.)

Almost there ...

```
crib--> atthebreakofdawnseize
        XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
        xajmoaqvwbonztkfajlps

        thebritsarebunkeredin
        QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
        xajmoaqvwbonztkfajlps

        reinforcementsarecomi
        OERZTOHXANSASLKWELZBAOJVUSOUOV
        xajmoaqvwbonztkfajlps
```

One-time Pads (Cont.)

Almost there ...

```
        atthebreakofdawnseizeth
        XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
        xajmoaqvwbonztkfajlpsbd

        thebritsarebunkeredinle
        QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
        xajmoaqvwbonztkfajlpsbd

crib--> reinforcementsarecoming
        OERZTOHXANSASLKWELZBAOJVUSOUOV
        xajmoaqvwbonztkfajlpsbd
```

One-time Pads (Cont.)

Almost there ...

```
crib--> atthebreakofdawnseizethe
        XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
        xajmoaqvwbonztkfajlpsbdu

        thebritsarebunkeredinlex
        QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
        xajmoaqvwbonztkfajlpsbdu

        reinforcementsarecomingb
        OERZTOHXANSASLKWELZBAOJVUSOUOV
        xajmoaqvwbonztkfajlpsbdu
```

One-time Pads (Cont.)

... got it!

```
         atthebreakofdawnseizetheharbor
         XTCTSBHZWLCSCTGSSNTOWUKYDFXPVT
         xajmoaqvwbonztkfajlpsbduwfgohc

crib--> thebritsarebunkeredinlexington
         QHNNFIJNWSSOTGUJRNOXFMHRESMHVP
         xajmoaqvwbonztkfajlpsbduwfgohc

         reinforcementsarecomingbynight
         OERZTOHXANSASLKWELZBAOJVUSOUOV
         xajmoaqvwbonztkfajlpsbduwfgohc
```

Background of Enigma

- After the French cracked the ADFGVX cipher in WWI, Arthur Scherbius set out to create an improved cipher machine.

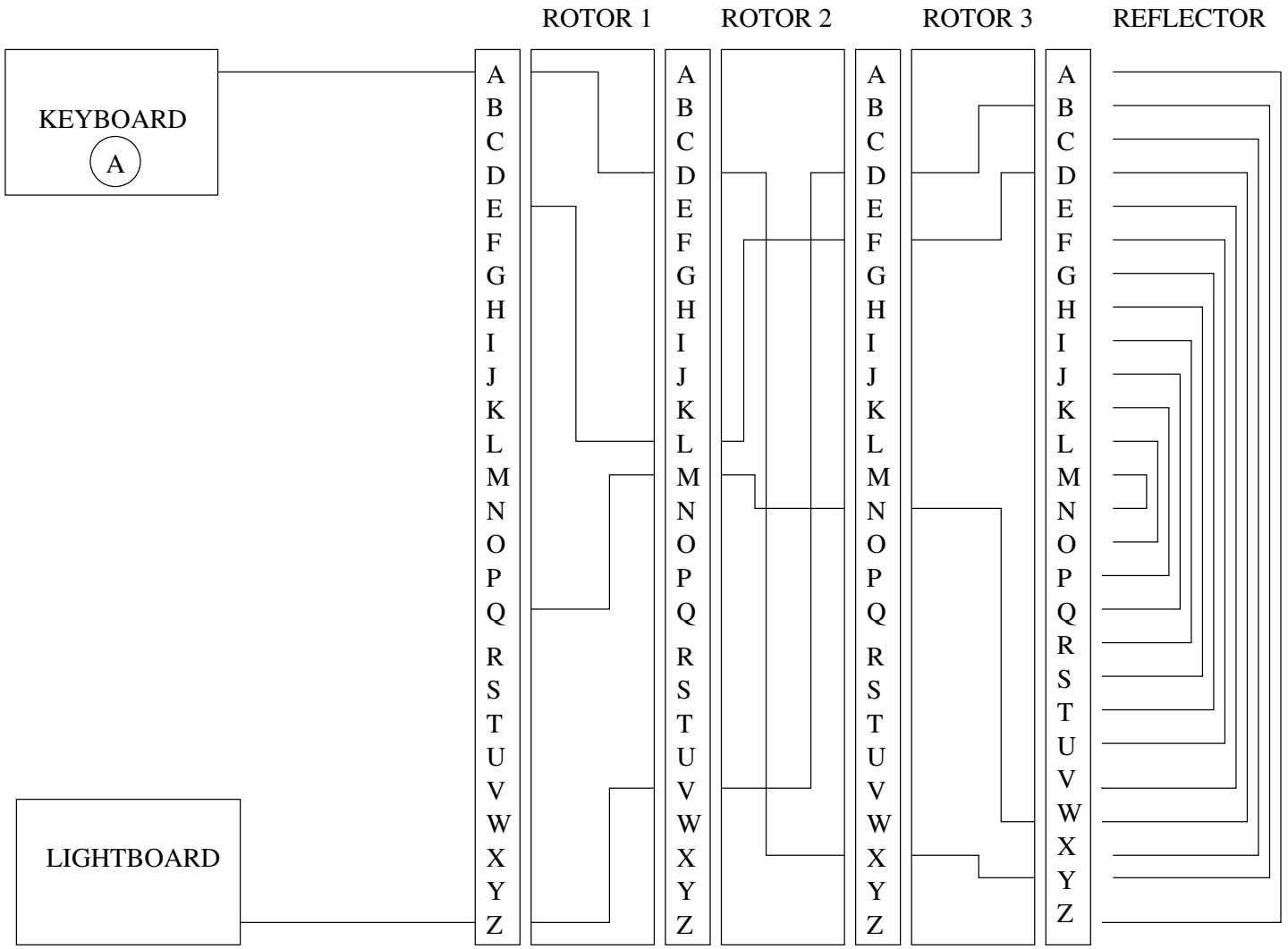
Background of Enigma

- After the French cracked the ADFGVX cipher in WWI, Arthur Scherbius set out to create an improved cipher machine.
- He generalized and automated a Vigenère cipher by having a changeable substitution cipher.

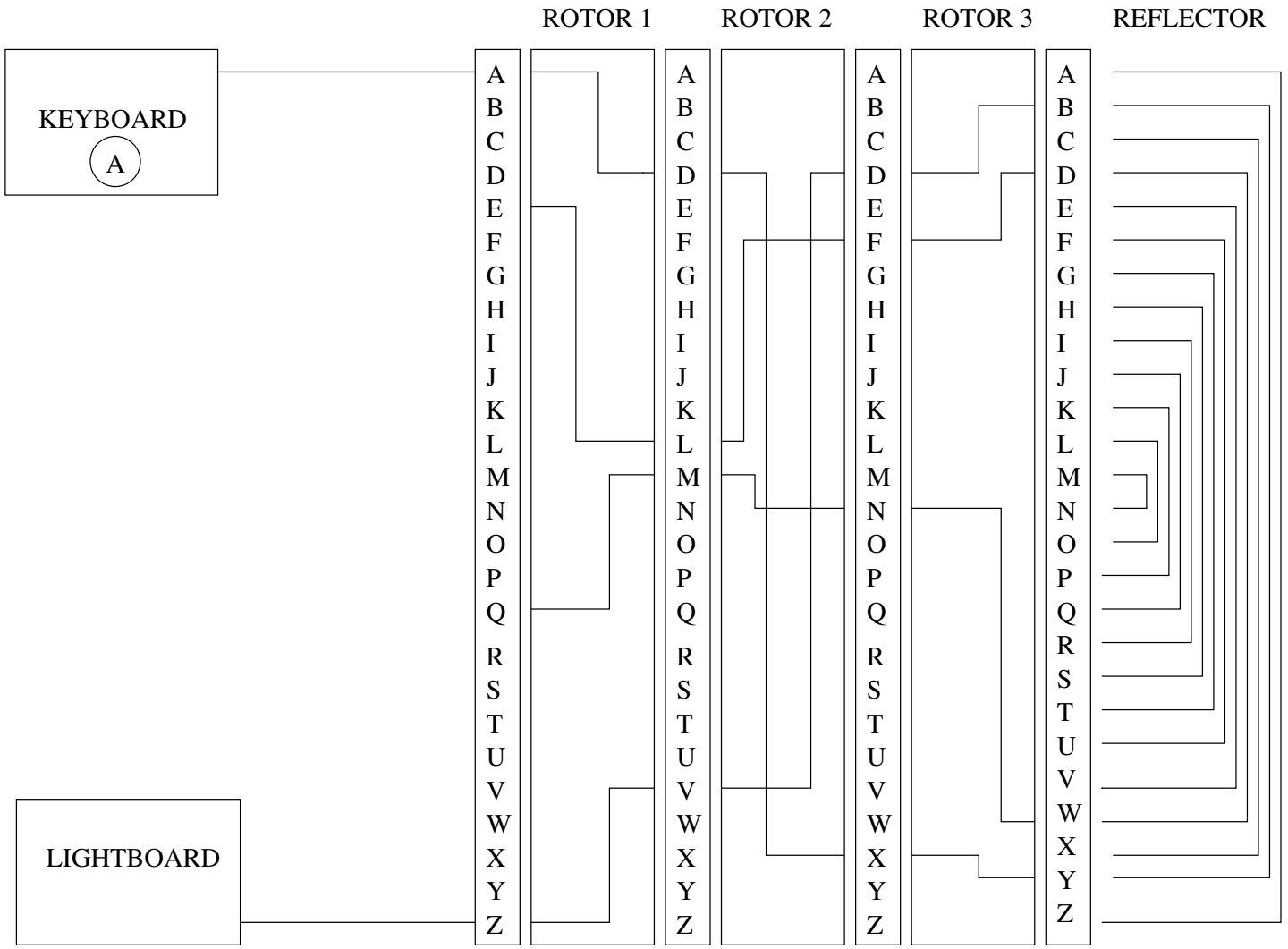
Background of Enigma

- After the French cracked the ADFGVX cipher in WWI, Arthur Scherbius set out to create an improved cipher machine.
- He generalized and automated a Vigenère cipher by having a changeable substitution cipher.

Enigma Schematic

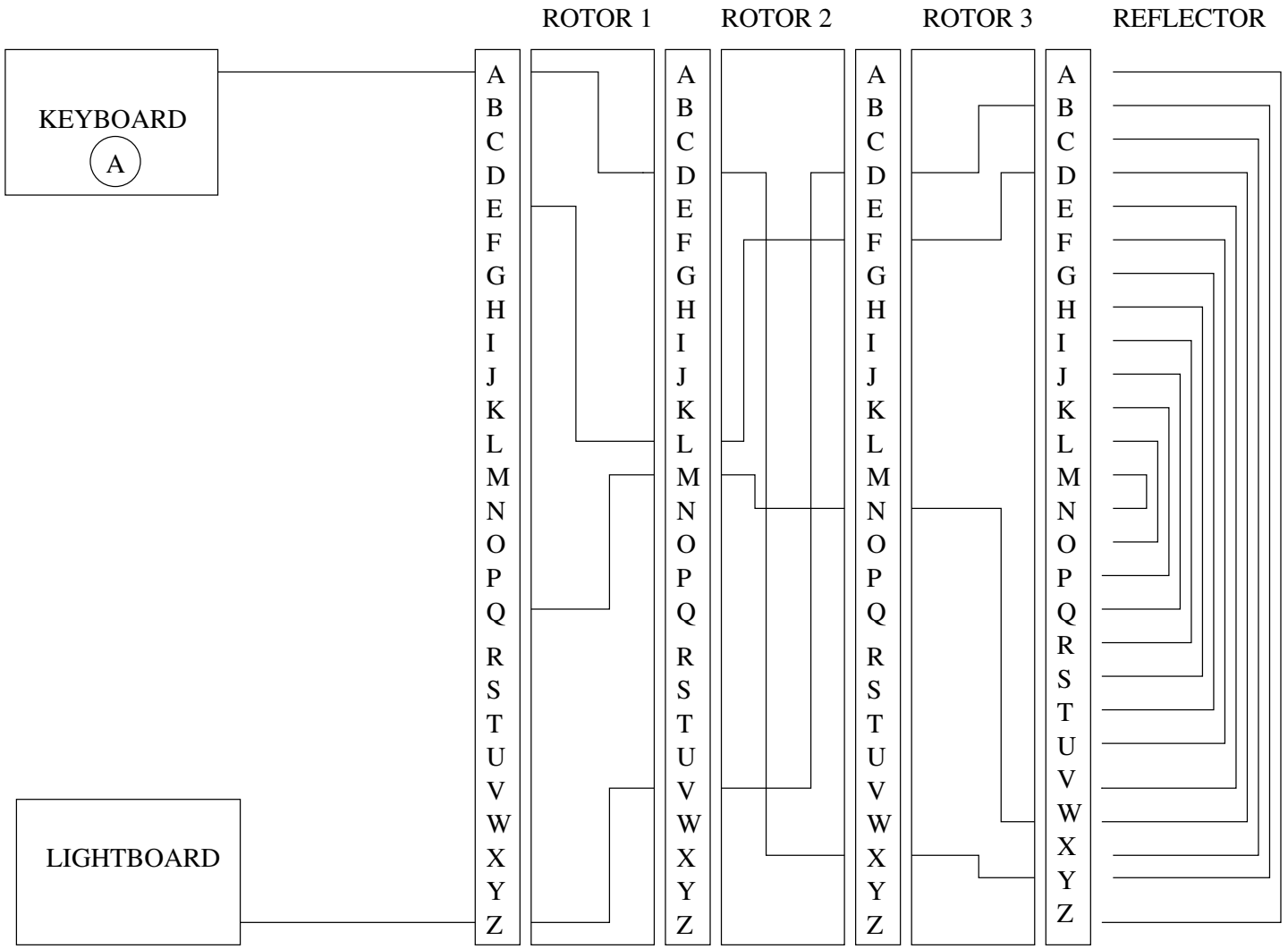


Enigma Schematic



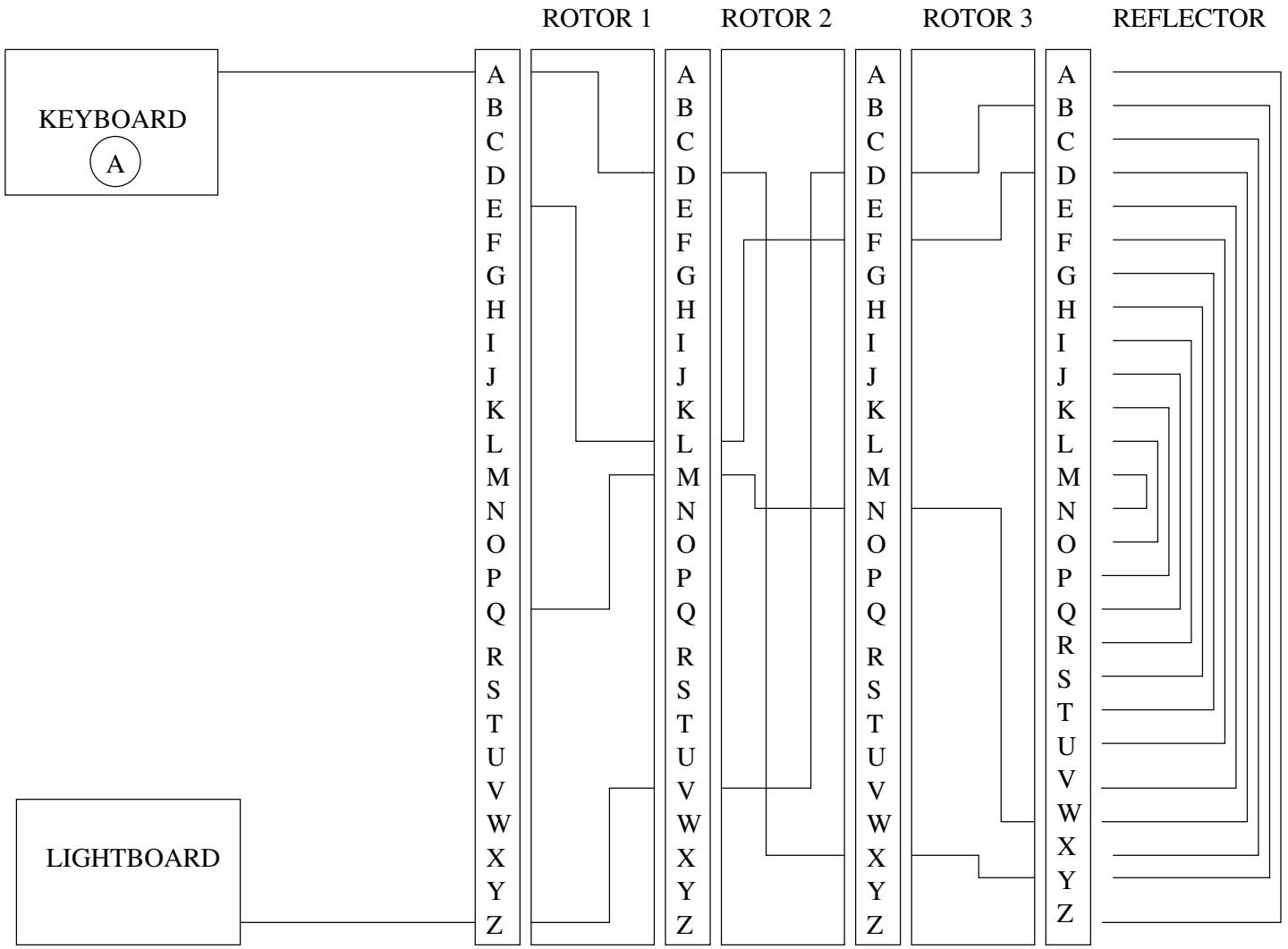
- Rotors start in any one of 26 positions.

Enigma Schematic



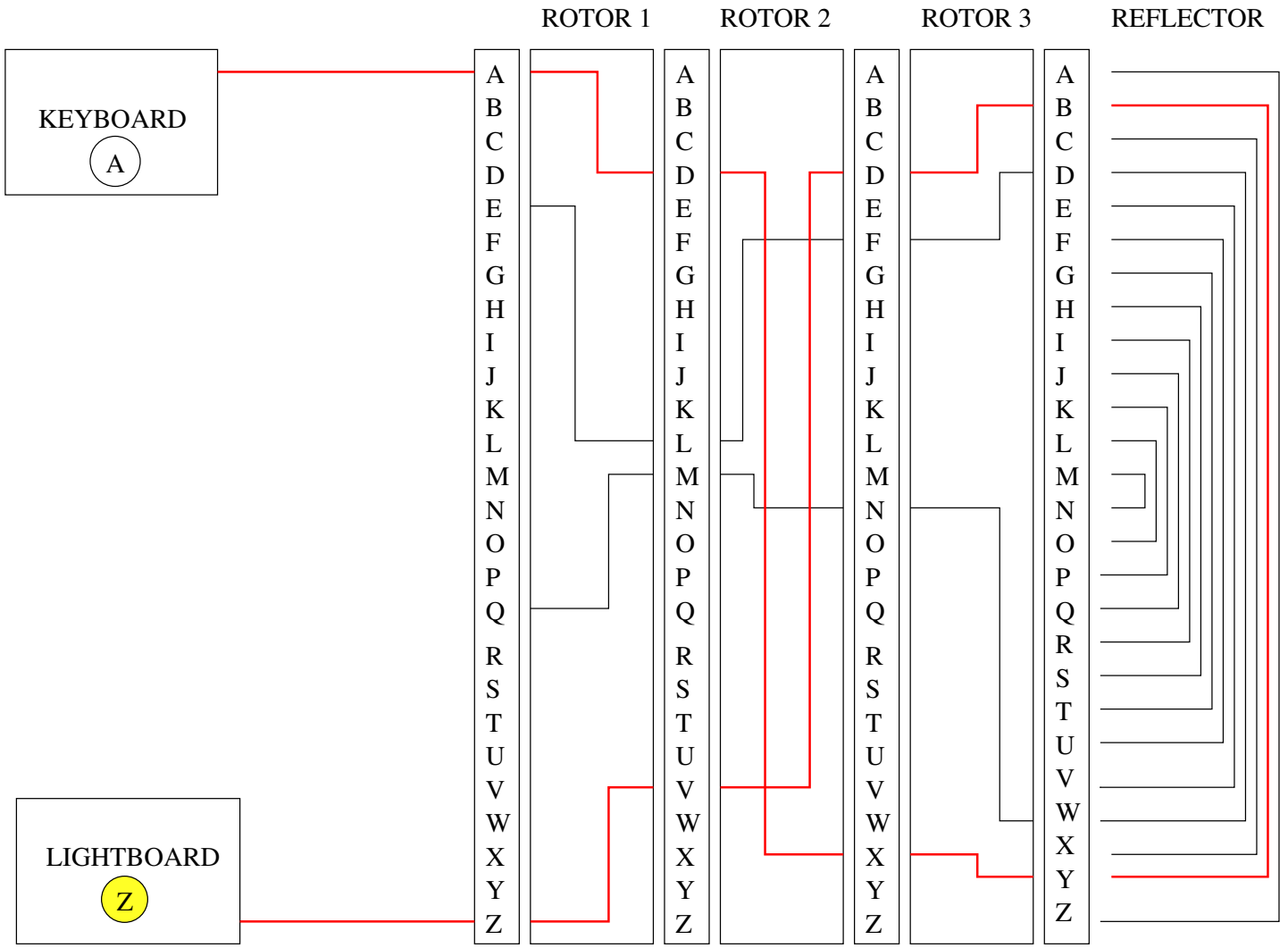
- Rotors start in any one of 26 positions.
- Rotors start in any one of $3! = 6$ orders.

Enigma Schematic



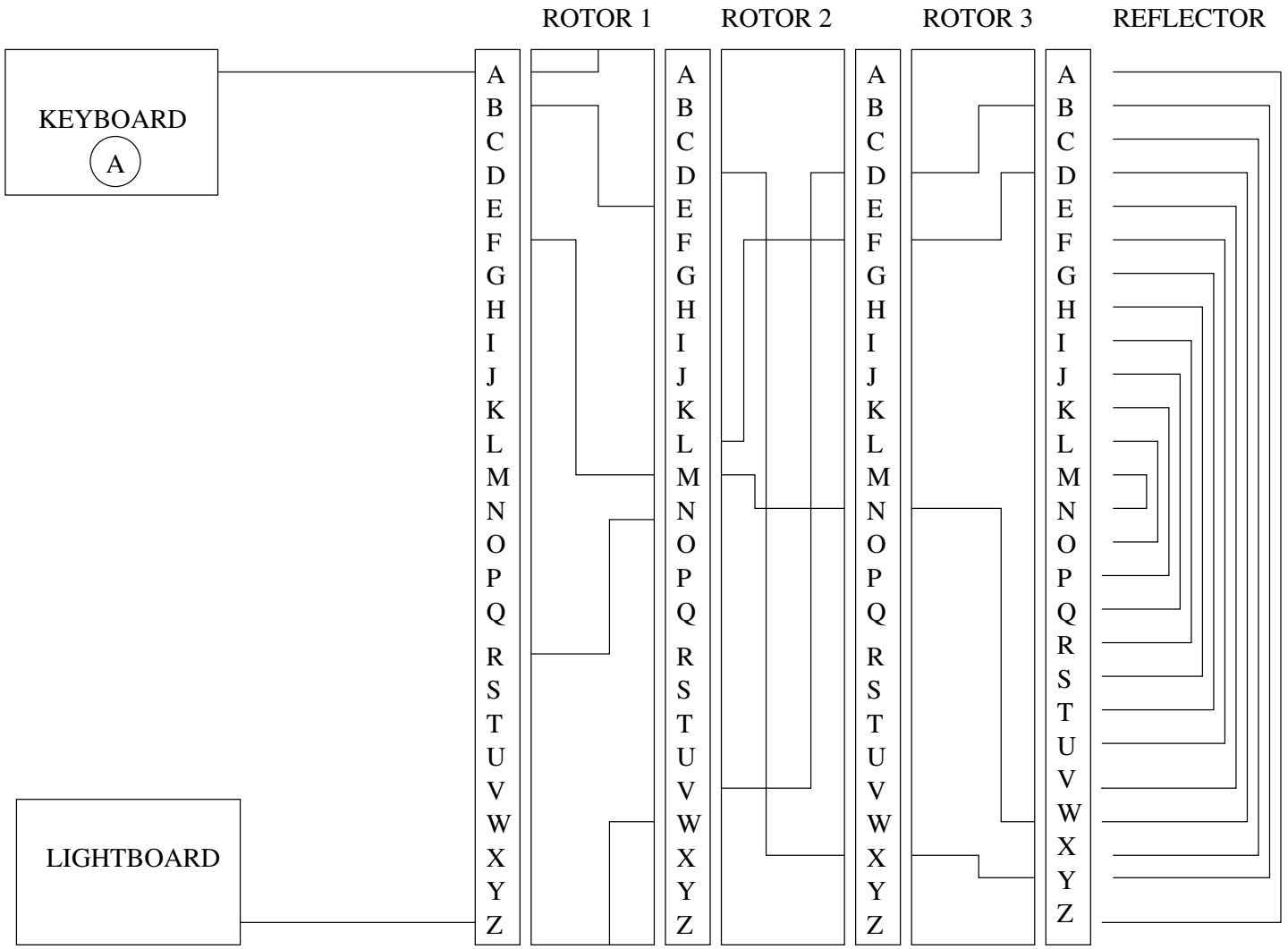
- Rotors start in any one of 26 positions.
- Rotors start in any one of $3! = 6$ orders.
- Reflector is fixed.

Enigma Schematic



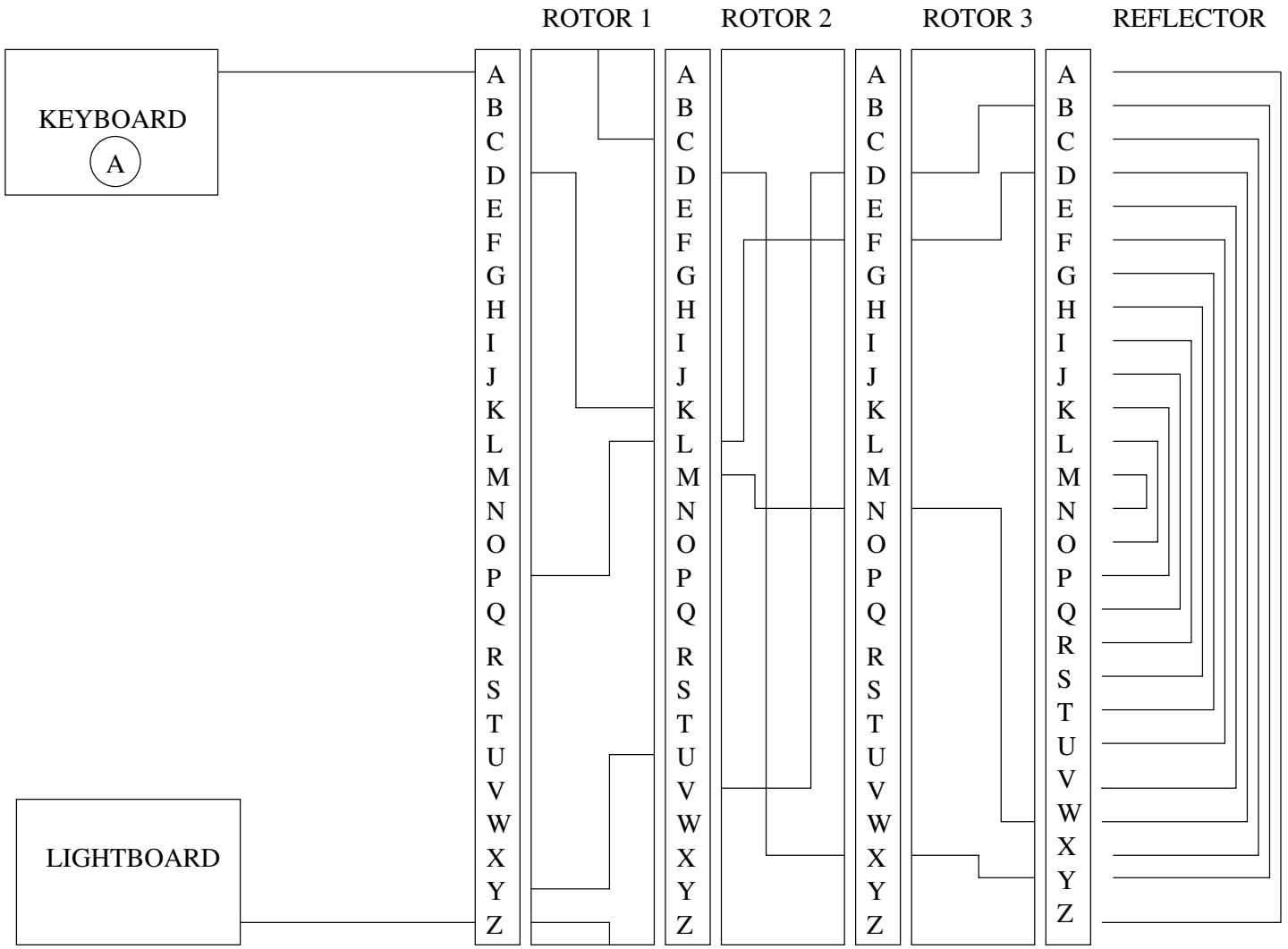
- A encrypts to Z.

Enigma Schematic



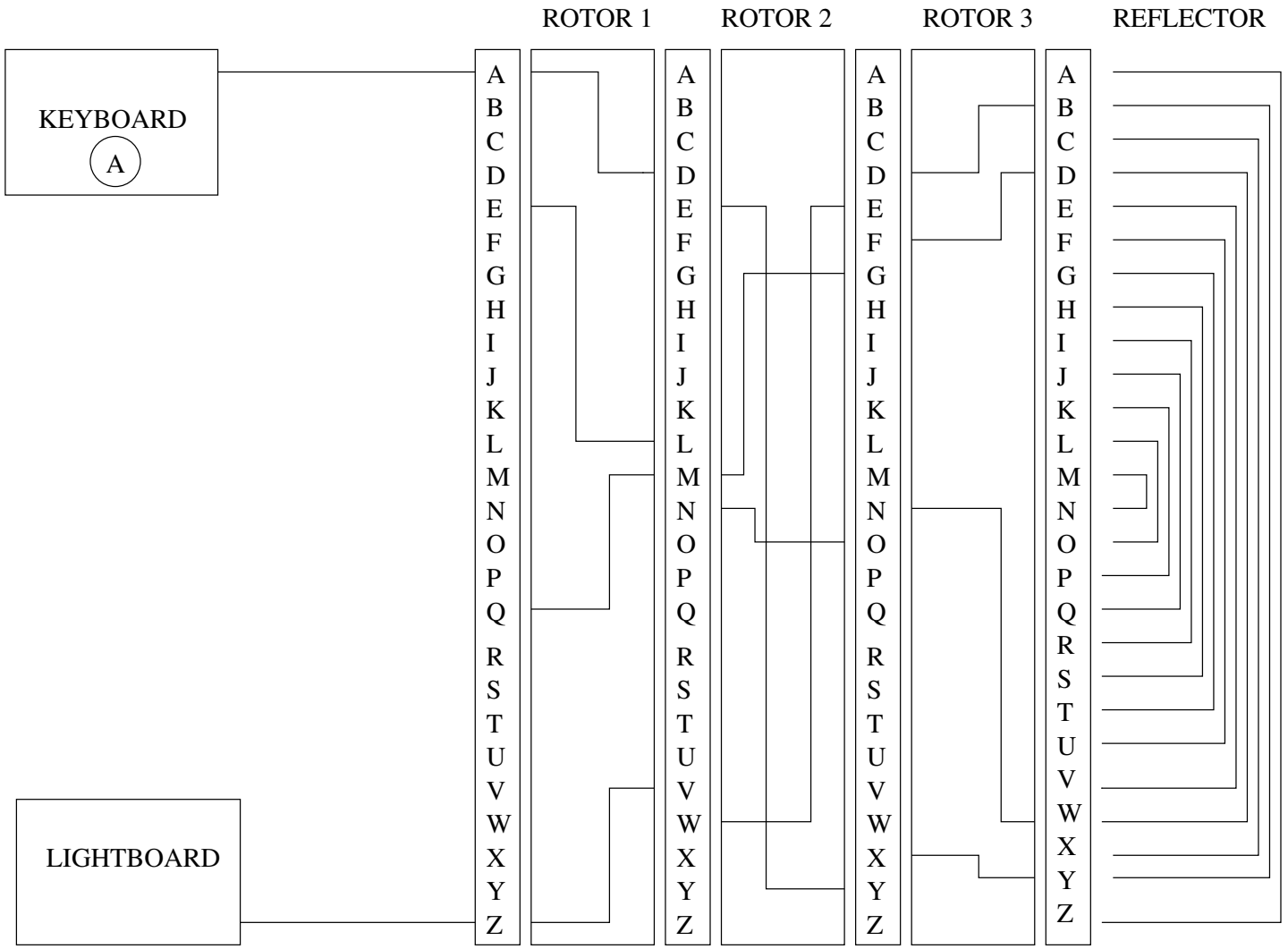
- A encrypts to Z.
- Rotor 1 moves after each letter is encrypted.

Enigma Schematic



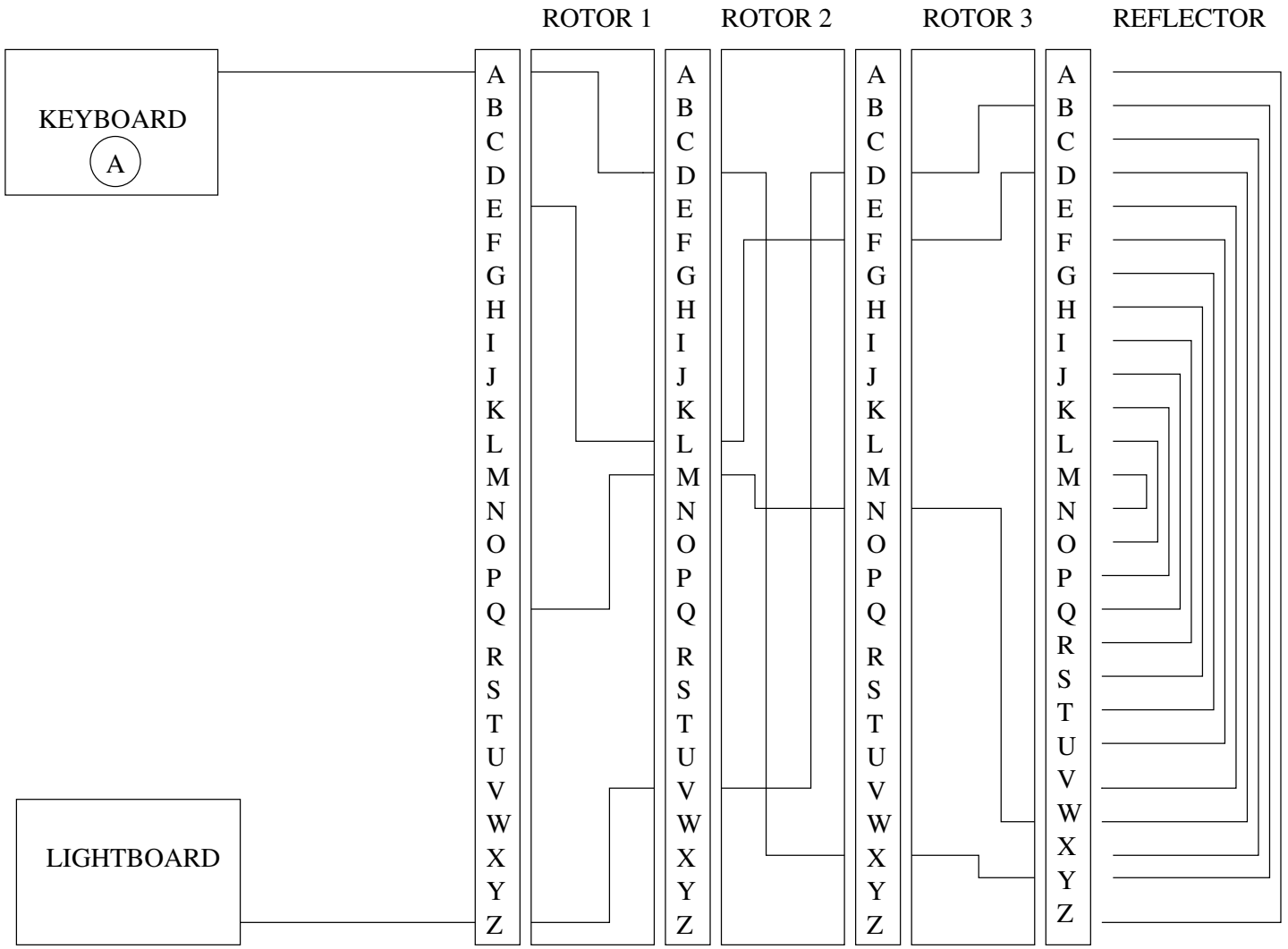
- A encrypts to Z.
- Rotor 1 moves after each letter is encrypted.
- After 25 encryptions ...

Enigma Schematic



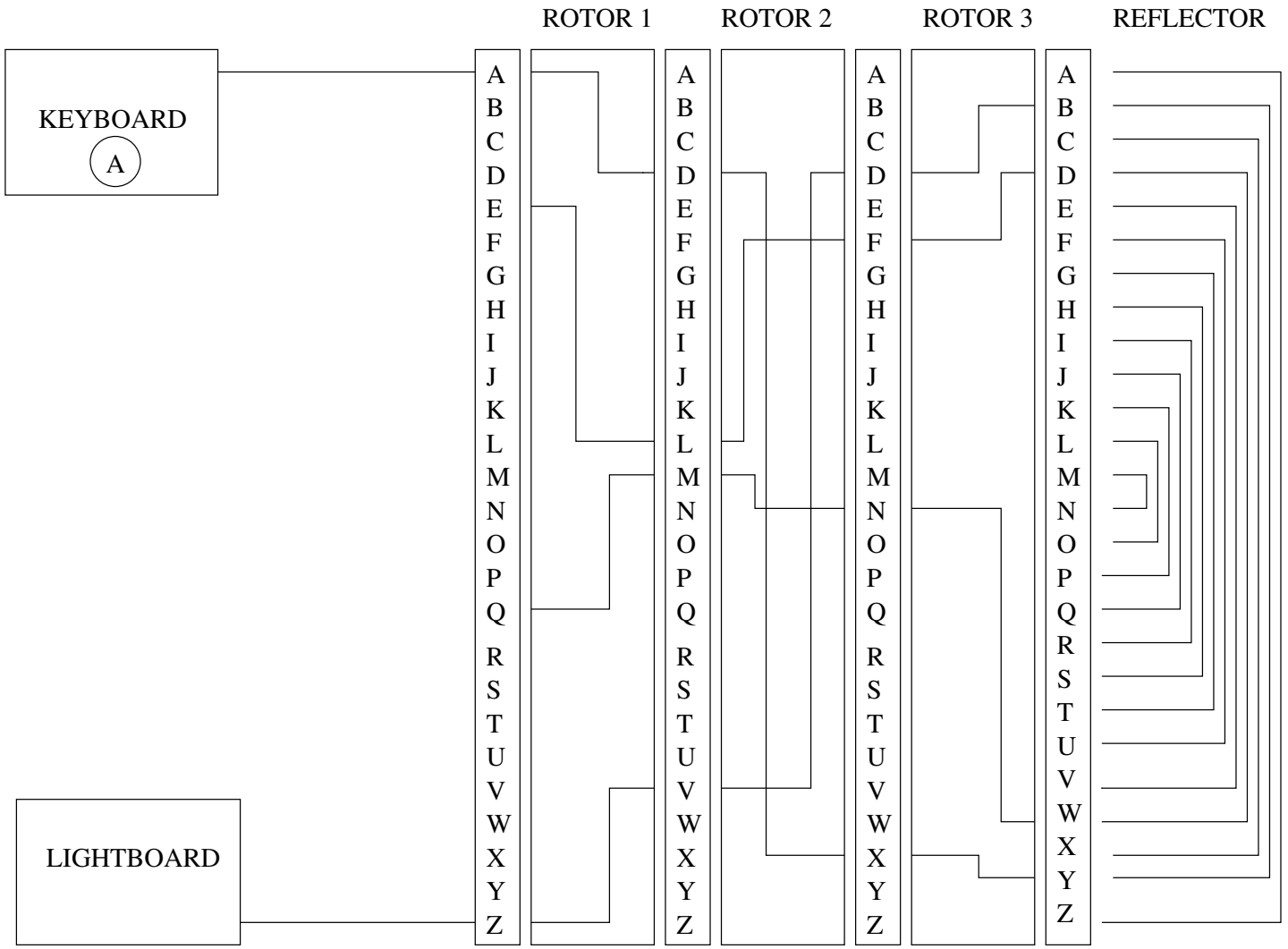
- Rotor 2 moves when Rotor 1 returns to starting position.

Enigma Schematic



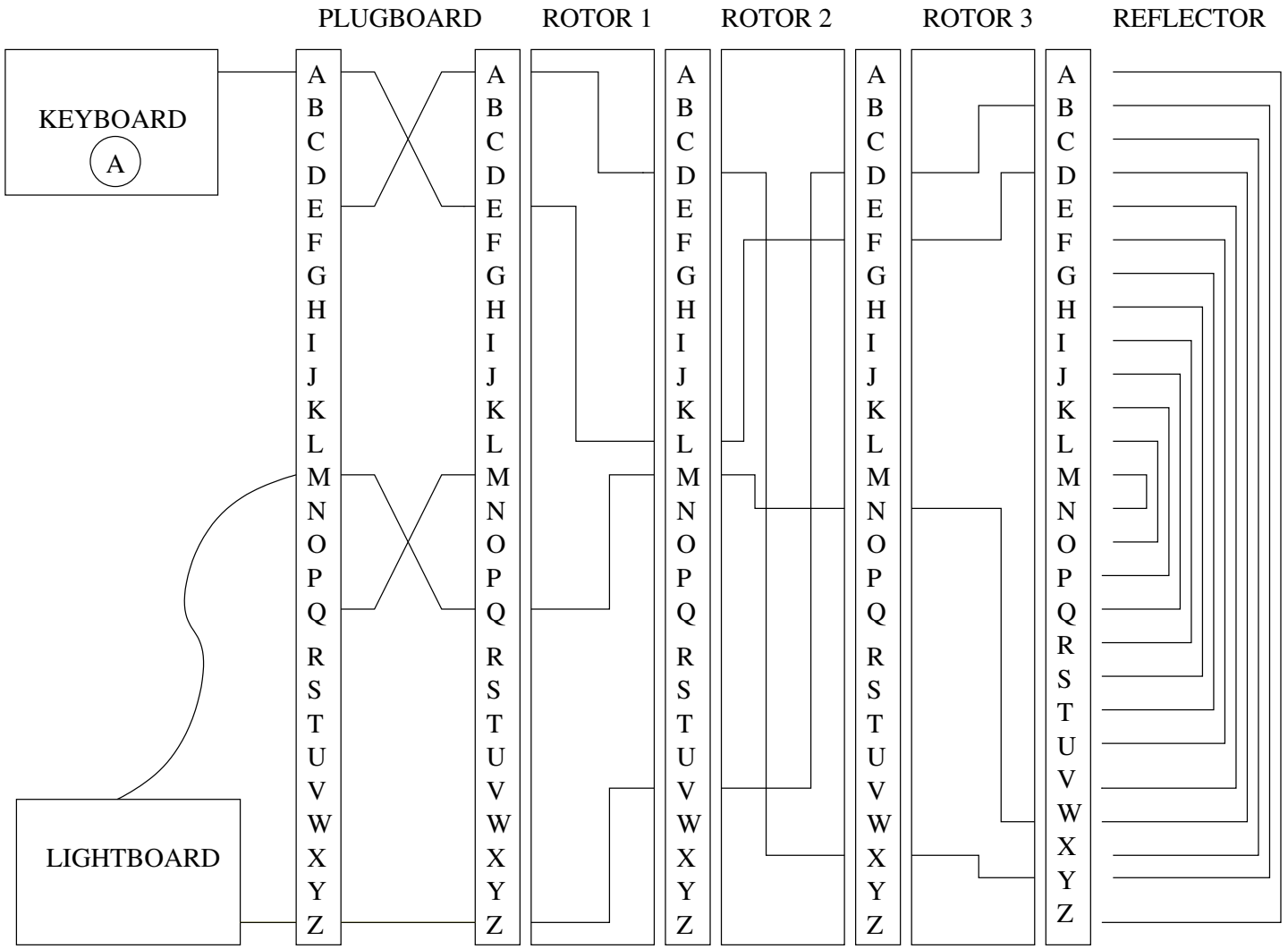
- Keysize is $26^3 \times 6 = 105,456$.

Enigma Schematic



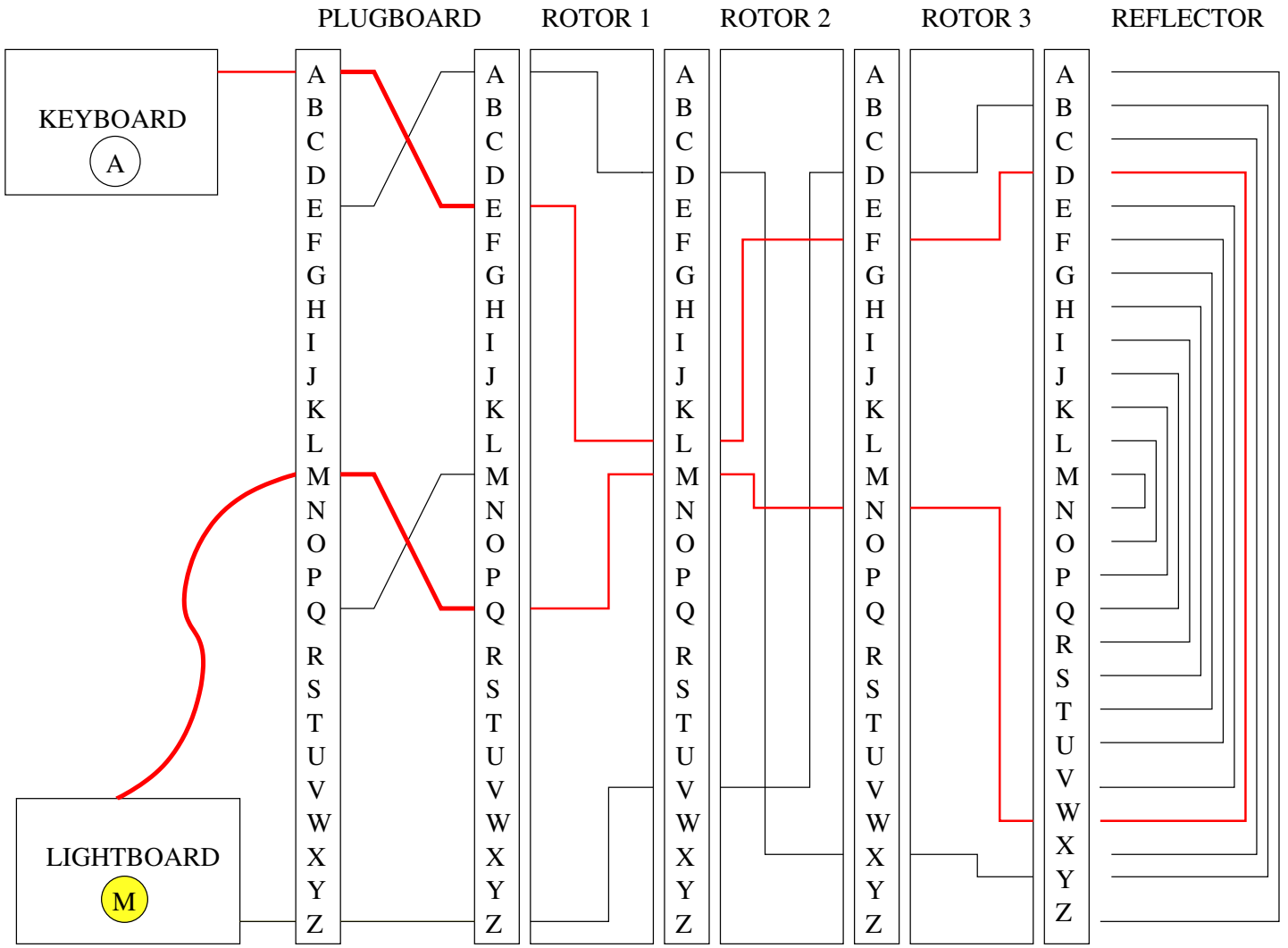
- Keysize is $26^3 \times 6 = 105,456$.
- Doesn't repeat until $26^3 = 17,576$ letters.

Enigma Schematic



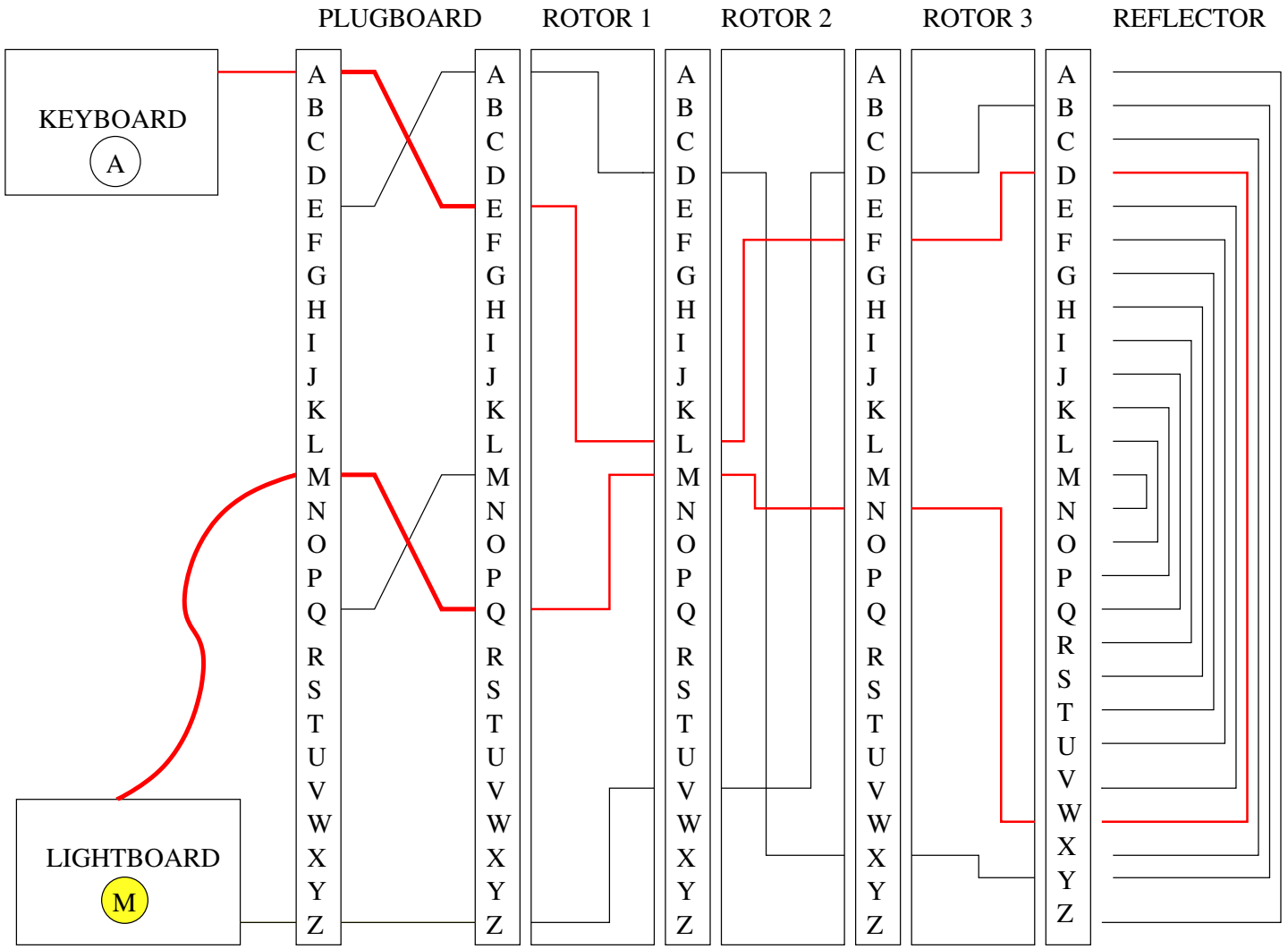
- Plugboard: 6 pairs of letter swaps.

Enigma Schematic



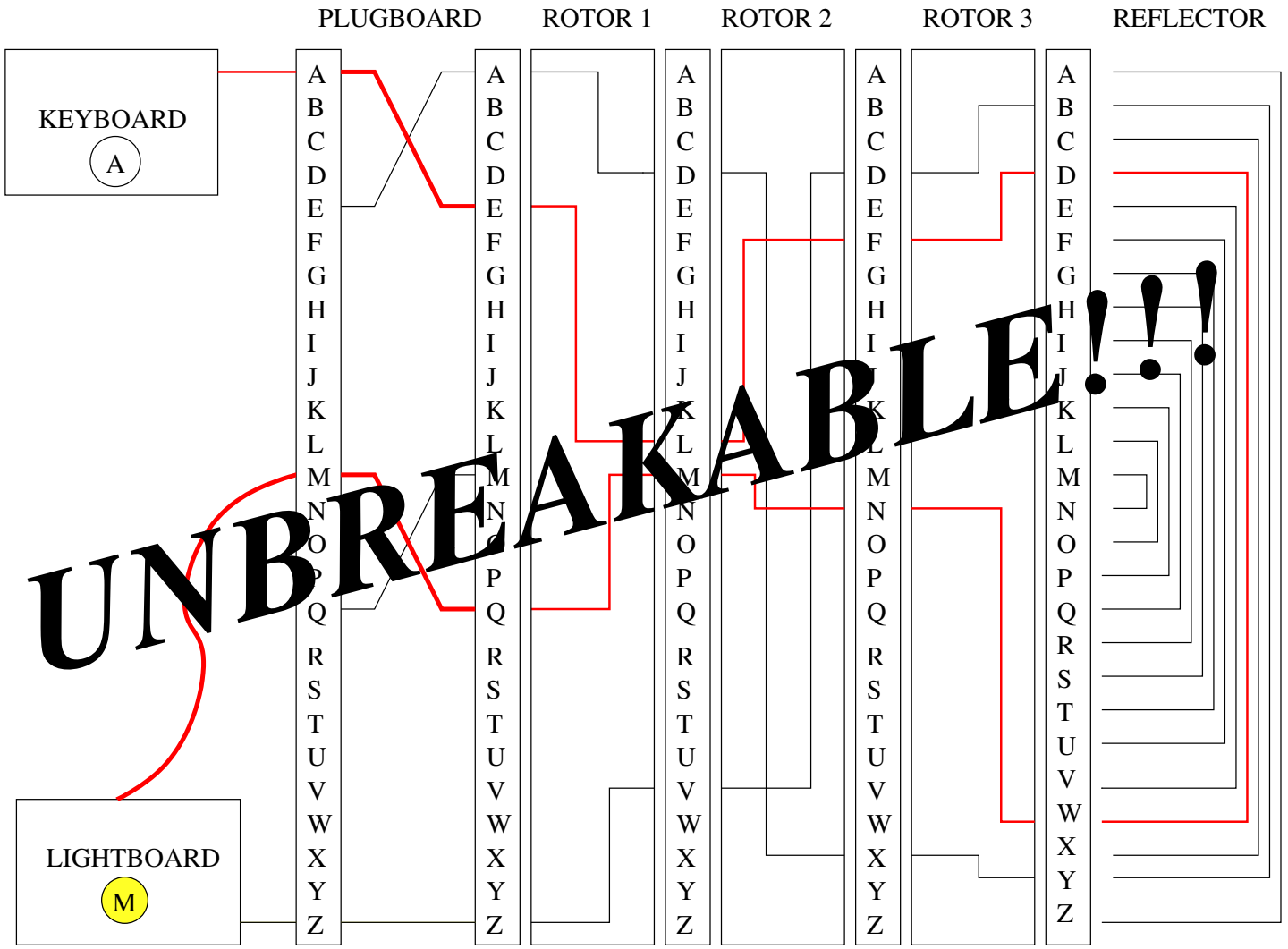
- A encrypts to M.
- Plugboard: 6 pairs of letter swaps.

Enigma Schematic



- A encrypts to M.
- Keysize is $26^3 \times 6 \times (100, 391, 791, 500) \approx 10^{16}$.
- Plugboard: 6 pairs of letter swaps.

Enigma Schematic



- A encrypts to M.
- Keysize is $26^3 \times 6 \times (100, 391, 791, 500) \approx 10^{16}$.
- Plugboard: 6 pairs of letter swaps.

Background of Enigma

- After the French cracked the ADFGVX cipher in WWI, Arthur Scherbius set out to create an improved cipher machine.
- He generalized and automated a Vigenère cipher by having a changeable substitution cipher.

Background of Enigma

- After the French cracked the ADFGVX cipher in WWI, Arthur Scherbius set out to create an improved cipher machine.
- He generalized and automated a Vigenère cipher by having a changeable substitution cipher.
- Built commercial and military versions with different internal wirings.

Background of Enigma

- After the French cracked the ADFGVX cipher in WWI, Arthur Scherbius set out to create an improved cipher machine.
- He generalized and automated a Vigenère cipher by having a changeable substitution cipher.
- Built commercial and military versions with different internal wirings.
- Due to post-war depression, widespread public use did not come to pass. Military sees no need for added expense.

Background of Enigma

- After the French cracked the ADFGVX cipher in WWI, Arthur Scherbius set out to create an improved cipher machine.
- He generalized and automated a Vigenère cipher by having a changeable substitution cipher.
- Built commercial and military versions with different internal wirings.
- Due to post-war depression, widespread public use did not come to pass. Military sees no need for added expense.
- 1923: Britain publishes official history of WWI, boasting of great cryptographic triumphs.

Background of Enigma

- After the French cracked the ADFGVX cipher in WWI, Arthur Scherbius set out to create an improved cipher machine.
- He generalized and automated a Vigenère cipher by having a changeable substitution cipher.
- Built commercial and military versions with different internal wirings.
- Due to post-war depression, widespread public use did not come to pass. Military sees no need for added expense.
- 1923: Britain publishes official history of WWI, boasting of great cryptographic triumphs.
- 1925: German military begins use of Enigma. Decade of unparalleled security begins...

The Enigma Protocol

- Daily Codebook contains **Day key,** consisting of:
  1. Rotor Order: 2-1-3
  2. Plugboard Swaps: A/V, B/R, S/U, N/W, D/P, C/Q.
  3. Rotor Settings: X-V-F

The Enigma Protocol

- Daily Codebook contains **Day key,** consisting of:
  1. Rotor Order: 2-1-3
  2. Plugboard Swaps: A/V, B/R, S/U, N/W, D/P, C/Q.
  3. Rotor Settings: X-V-F
- A **Message key** is used per message to avoid depths during encryption:

$$\underbrace{\textbf{ANFANF}}_{\text{Use 1,2,3}}\ \underbrace{\textbf{THISISTHEMESSAGE}}_{\text{Use 1,2, and A-N-F}}$$

Espionage

- Hans-Thilo Schmidt

Espionage

- Hans-Thilo Schmidt
- French-Polish reciprocity

Espionage

- Hans-Thilo Schmidt
- French-Polish reciprocity
- Poles acquire military wirings

Espionage

- Hans-Thilo Schmidt
- French-Polish reciprocity
- Poles acquire military wirings

Marian Rejewski

Cracking the Enigma

BOLJRVSQIGPQTMNWJRAKOBYTKMTTG
BBRQUPWLHSOLNFEQTHJOVXSWPAEWM
CWPBHKGABJOPHAXOYJIKXEGSBLZWB
QCOUMYYQGRKTNPSORSTOYHYASQGNV
IHFGFOTMINEDDXOYMKGGTXUQMJPKZ
CYDLCZZWGQAWZNHSKJSWPXNCQJZDP
VLROVJGLSDCPRLWHQTSSCHALESKFN
XIRZGYWUDJODMSPPSZBJEZJAEQAJG
PAGYOSILDHELQXKINYNYET

Cracking the Enigma

- The first six letters of every message on a given day are in depth!

Cracking the Enigma

- The first six letters of every message on a given day are in depth!
- In the same day, we have several other messages. Here are the first six characters of each of them:

BOLJRV	WKOTFI	JOSURM	EFKBOT	RBEDAP
TBHCAX	HWKSBT	YQDZNS	EBXBAB	KZXAQB
DABNUW	QFMQOF	WEOTSI	UWGMBN	WRBTJW
WLDTVS	ZYDKMS	FAREUC	XXHXKX	DGDNXS
NNSHDM	QKXQFB	CCZFLH	VCHVLX	ADPRWQ
XQUXNA	JHJUGY	TULCYV	PFYWOL	NQVHNG
YKIZFK	GGDGXS	BSXJEB	TITCTZ	SZALQR
KKDAFS	SSVLEG	IICITU	LPSYZM	OGKOXT
LXRYKC	MOXPRB	SLNLVE	KTFAID	XVAXHR
HFJSOY	JJQUCJ	DMWNPO	REJDSY	XUZXYH

Cracking the Enigma

Permutation	P_1	P_2	P_3	P_4	P_5	P_6
Plaintext	a	b	c	a	b	c
Ciphertext	B	O	L	J	R	V

Cracking the Enigma

Permutation	P_1	P_2	P_3	P_4	P_5	P_6
Plaintext	a	b	c	a	b	c
Ciphertext	B	O	L	J	R	V

- Call the first permutation defined by this Enigma setting, P_1, the second P_2, and so forth, then we can determine that:
  1. P_1: a$\Longleftrightarrow$B
  2. P_2: b$\Longleftrightarrow$O
  3. P_3: c$\Longleftrightarrow$L
  4. P_4: a$\Longleftrightarrow$J
  5. P_5: b$\Longleftrightarrow$R
  6. P_6: c$\Longleftrightarrow$V

Cracking the Enigma

Permutation	P_1	P_2	P_3	P_4	P_5	P_6
Plaintext	a	b	c	a	b	c
Ciphertext	B	O	L	J	R	V

- Call the first permutation defined by this Enigma setting, P_1, the second P_2, and so forth, then we can determine that:
  1. P_1: a$\Longleftrightarrow$B
  2. P_2: b$\Longleftrightarrow$O
  3. P_3: c$\Longleftrightarrow$L
  4. P_4: a$\Longleftrightarrow$J
  5. P_5: b$\Longleftrightarrow$R
  6. P_6: c$\Longleftrightarrow$V
- We don't know what a is, but we do know that P_1 links a to B, and P_4 links a to J. This leads to the Rejewski's breakthrough observation:

Cracking the Enigma

- The intercept BOLJRV tells us that
  1. $P_4 \circ P_1(\mathtt{B}) = \mathtt{J}$,
  2. $P_5 \circ P_2(\mathtt{O}) = \mathtt{R}$,
  3. $P_6 \circ P_3(\mathtt{L}) = \mathtt{V}$.

Cracking the Enigma

- The intercept BOLJRV tells us that
  1. $P_4 \circ P_1(\mathtt{B}) = \mathtt{J}$,
  2. $P_5 \circ P_2(\mathtt{O}) = \mathtt{R}$,
  3. $P_6 \circ P_3(\mathtt{L}) = \mathtt{V}$.
- The next intercept, WKOTFI, tells us that
  1. $P_4 \circ P_1(\mathtt{W}) = \mathtt{T}$,
  2. $P_5 \circ P_2(\mathtt{K}) = \mathtt{F}$,
  3. $P_6 \circ P_3(\mathtt{O}) = \mathtt{I}$.

Cracking the Enigma

- The intercept BOLJRV tells us that
  1. $P_4 \circ P_1(\mathtt{B}) = \mathtt{J}$,
  2. $P_5 \circ P_2(\mathtt{O}) = \mathtt{R}$,
  3. $P_6 \circ P_3(\mathtt{L}) = \mathtt{V}$.
- The next intercept, WKOTFI, tells us that
  1. $P_4 \circ P_1(\mathtt{W}) = \mathtt{T}$,
  2. $P_5 \circ P_2(\mathtt{K}) = \mathtt{F}$,
  3. $P_6 \circ P_3(\mathtt{O}) = \mathtt{I}$.
- We can use the entire set of intercepts to construct the following table of relationships:

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV` `WKOTFI` `JOSURM` `EFKBOT` `RBEDAP`

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- BOLJRV WKOTFI JOSURM EFKBOT RBEDAP

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- BOLJRV WKOTFI JOSURM EFKBOT RBEDAP

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- BOLJRV WKOTFI JOSURM EFKBOT RBEDAP

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- BOLJRV WKOTFI JOSURM EFKBOT RBEDAP

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- BOLJRV WKOTFI JOSURM EFKBOT RBEDAP

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV WKOTFI JOSURM EFKBOT RBEDAP`
- Rejewski observed cycles within this permutation.

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV WKOTFI JOSURM EFKBOT RBEDAP`
- Rejewski observed cycles within this permutation.

  `A-->R`

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV WKOTFI JOSURM EFKBOT RBEDAP`
- Rejewski observed cycles within this permutation.

  `A-->R-->D`

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV WKOTFI JOSURM EFKBOT RBEDAP`
- Rejewski observed cycles within this permutation.

  `A-->R-->D-->N`

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV WKOTFI JOSURM EFKBOT RBEDAP`
- Rejewski observed cycles within this permutation.

  `A-->R-->D-->N-->H`

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV WKOTFI JOSURM EFKBOT RBEDAP`
- Rejewski observed cycles within this permutation.

  `A-->R-->D-->N-->H-->S`

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV WKOTFI JOSURM EFKBOT RBEDAP`
- Rejewski observed cycles within this permutation.

```
A-->R-->D-->N-->H-->S-->L
```

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV WKOTFI JOSURM EFKBOT RBEDAP`
- Rejewski observed cycles within this permutation.

```
A-->R-->D-->N-->H-->S-->L-->Y
```

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV WKOTFI JOSURM EFKBOT RBEDAP`
- Rejewski observed cycles within this permutation.

```
A-->R-->D-->N-->H-->S-->L-->Y-->Z
```

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV WKOTFI JOSURM EFKBOT RBEDAP`
- Rejewski observed cycles within this permutation.

```
A-->R-->D-->N-->H-->S-->L-->Y-->Z-->K
```

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV WKOTFI JOSURM EFKBOT RBEDAP`
- Rejewski observed cycles within this permutation.

```
A-->R-->D-->N-->H-->S-->L-->Y-->Z-->K-->A
```

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- `BOLJRV WKOTFI JOSURM EFKBOT RBEDAP`
- Rejewski observed cycles within this permutation.

```
A-->R-->D-->N-->H-->S-->L-->Y-->Z-->K-->A
B-->J-->U-->M-->P-->W-->T-->C-->F-->E-->B
```

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- BOLJRV WKOTFI JOSURM EFKBOT RBEDAP
- Rejewski observed cycles within this permutation.

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

Cracking the Enigma

The permutation $P_4 \circ P_1$

$P_4 \circ P_1$	A	B	C	D	E	F	G	H	I
	R	**J**	**F**	**N**	**B**	**E**	**G**	**S**	**I**
$P_4 \circ P_1$	J	K	L	M	N	O	P	Q	R
	U	**A**	**Y**	**P**	**H**	**O**	**W**	**Q**	**D**
$P_4 \circ P_1$	S	T	U	V	W	X	Y	Z	
	L	**C**	**M**	**V**	**T**	**X**	**Z**	**K**	

- BOLJRV WKOTFI JOSURM EFKBOT RBEDAP
- Rejewski observed cycles within this permutation.

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

- We say $P_4 \circ P_1$ has cycle structure 10-10-1-1-1-1-1-1.

Cracking the Enigma

The permutation $P_5 \circ P_2$

$P_5 \circ P_2$	A	B	C	D	E	F	G	H	I
	U	**A**	**L**	**W**	**S**	**O**	**X**	**G**	**T**
$P_5 \circ P_2$	J	K	L	M	N	O	P	Q	R
	C	**F**	**V**	**P**	**D**	**R**	**Z**	**N**	**J**
$P_5 \circ P_2$	S	T	U	V	W	X	Y	Z	
	E	**I**	**Y**	**H**	**B**	**K**	**M**	**Q**	

Cracking the Enigma

The permutation $P_5 \circ P_2$

$P_5 \circ P_2$	A	B	C	D	E	F	G	H	I
	U	**A**	**L**	**W**	**S**	**O**	**X**	**G**	**T**
$P_5 \circ P_2$	J	K	L	M	N	O	P	Q	R
	C	**F**	**V**	**P**	**D**	**R**	**Z**	**N**	**J**
$P_5 \circ P_2$	S	T	U	V	W	X	Y	Z	
	E	**I**	**Y**	**H**	**B**	**K**	**M**	**Q**	

- $P_5 \circ P_2$ has cycles:

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

Cracking the Enigma

The permutation $P_5 \circ P_2$

$P_5 \circ P_2$	A	B	C	D	E	F	G	H	I
	U	**A**	**L**	**W**	**S**	**O**	**X**	**G**	**T**
$P_5 \circ P_2$	J	K	L	M	N	O	P	Q	R
	C	**F**	**V**	**P**	**D**	**R**	**Z**	**N**	**J**
$P_5 \circ P_2$	S	T	U	V	W	X	Y	Z	
	E	**I**	**Y**	**H**	**B**	**K**	**M**	**Q**	

- $P_5 \circ P_2$ has cycles:

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

- $P_5 \circ P_2$ has cycle structure 11-11-2-2.

Cracking the Enigma

The permutation $P_6 \circ P_3$

$P_6 \circ P_3$	A	B	C	D	E	F	G	H	I
	R	**W**	**U**	**S**	**P**	**D**	**N**	**X**	**K**
$P_6 \circ P_3$	J	K	L	M	N	O	P	Q	R
	Y	**T**	**V**	**F**	**E**	**I**	**Q**	**J**	**C**
$P_6 \circ P_3$	S	T	U	V	W	X	Y	Z	
	M	**Z**	**A**	**G**	**O**	**B**	**L**	**H**	

Cracking the Enigma

The permutation $P_6 \circ P_3$

$P_6 \circ P_3$	A	B	C	D	E	F	G	H	I
	R	**W**	**U**	**S**	**P**	**D**	**N**	**X**	**K**
$P_6 \circ P_3$	J	K	L	M	N	O	P	Q	R
	Y	**T**	**V**	**F**	**E**	**I**	**Q**	**J**	**C**
$P_6 \circ P_3$	S	T	U	V	W	X	Y	Z	
	M	**Z**	**A**	**G**	**O**	**B**	**L**	**H**	

- $P_6 \circ P_3$ has cycles:

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

Cracking the Enigma

The permutation $P_6 \circ P_3$

$P_6 \circ P_3$	A	B	C	D	E	F	G	H	I
	R	**W**	**U**	**S**	**P**	**D**	**N**	**X**	**K**
$P_6 \circ P_3$	J	K	L	M	N	O	P	Q	R
	Y	**T**	**V**	**F**	**E**	**I**	**Q**	**J**	**C**
$P_6 \circ P_3$	S	T	U	V	W	X	Y	Z	
	M	**Z**	**A**	**G**	**O**	**B**	**L**	**H**	

- $P_6 \circ P_3$ has cycles:

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

- $P_6 \circ P_3$ has cycle structure 9-9-4-4.

Cracking the Enigma

- Rejewski recorded that this particular setting of Enigma (rotor orders, settings and plugboards) had the mathematical signature

  (10-10-1-1-1-1-1-1, 11-11-2-2, 9-9-4-4).

Cracking the Enigma

- Rejewski recorded that this particular setting of Enigma (rotor orders, settings and plugboards) had the mathematical signature

  (10-10-1-1-1-1-1-1, 11-11-2-2, 9-9-4-4).

- This triple of cycle lengths is a fingerprint of the underlying Enigma setting, but which of the billions and billions of settings could it be?

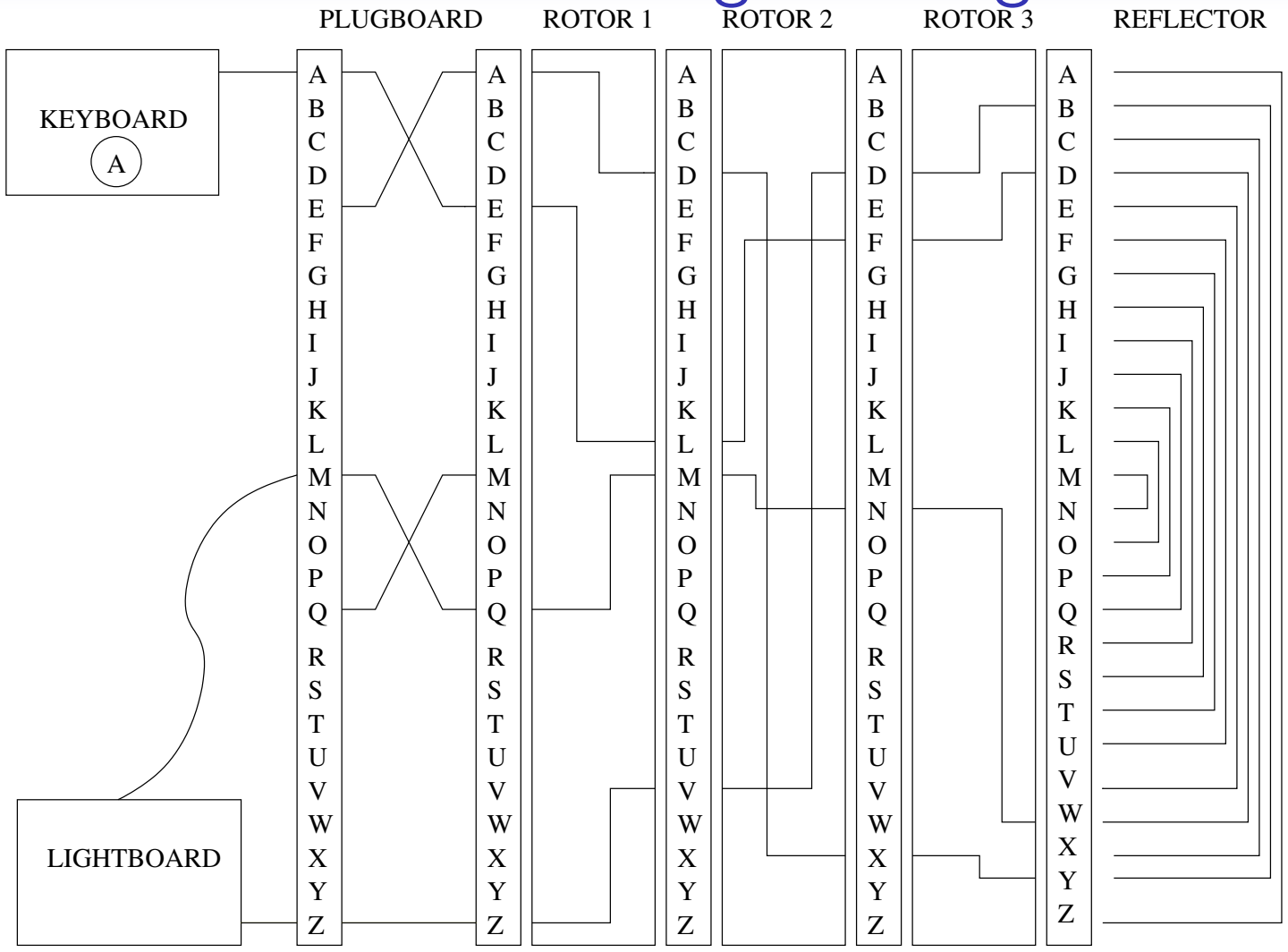
Cracking the Enigma

- Rejewski recorded that this particular setting of Enigma (rotor orders, settings and plugboards) had the mathematical signature

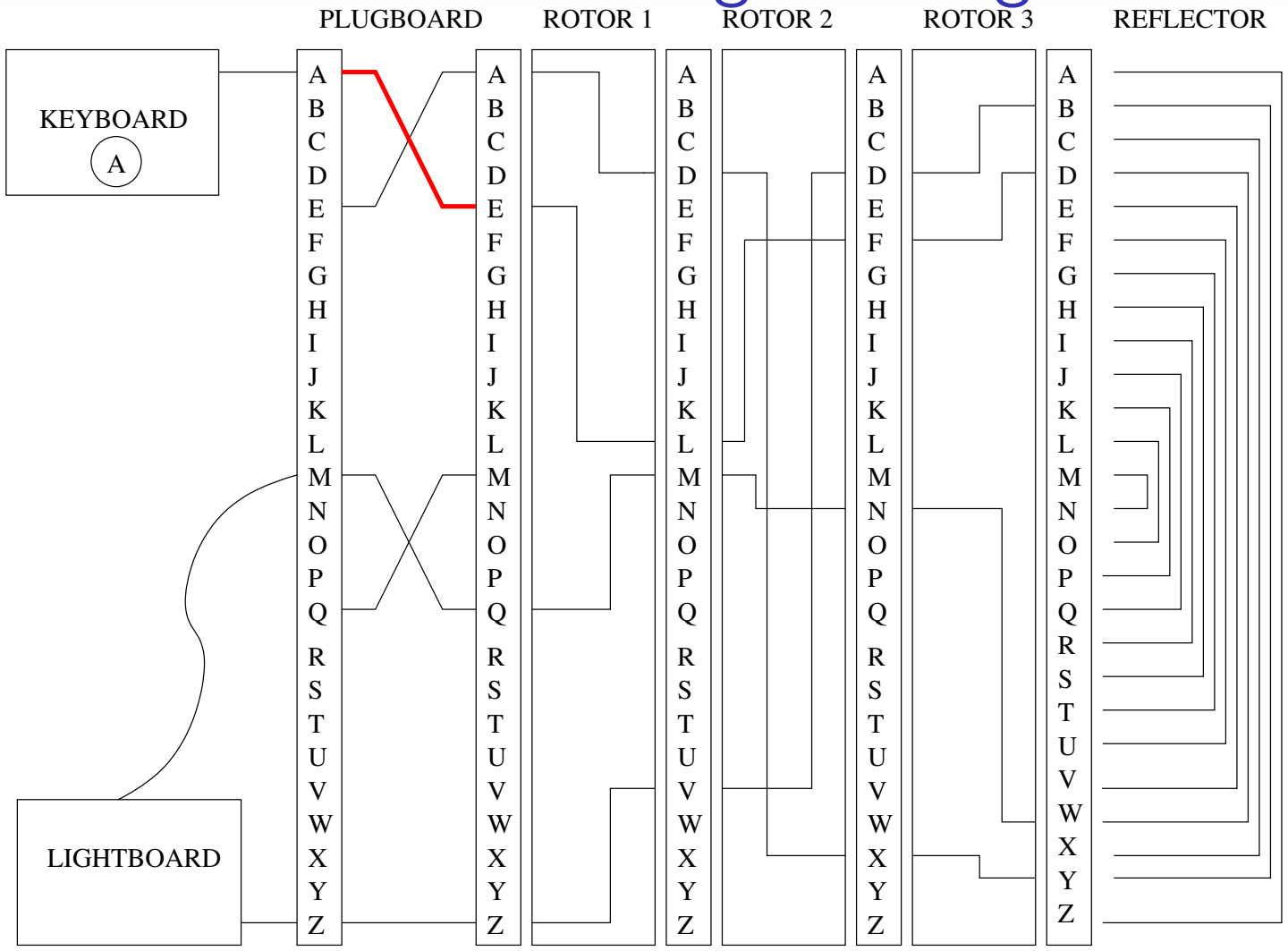
  (10-10-1-1-1-1-1-1, 11-11-2-2, 9-9-4-4).

- This triple of cycle lengths is a fingerprint of the underlying Enigma setting, but which of the billions and billions of settings could it be?
- **Recall:** $P_1 = P \circ \rho_1 \circ P$, where ρ_1 is the permutation defined by the initial rotor order and settings and P is the plugboard setting.

Cracking the Enigma

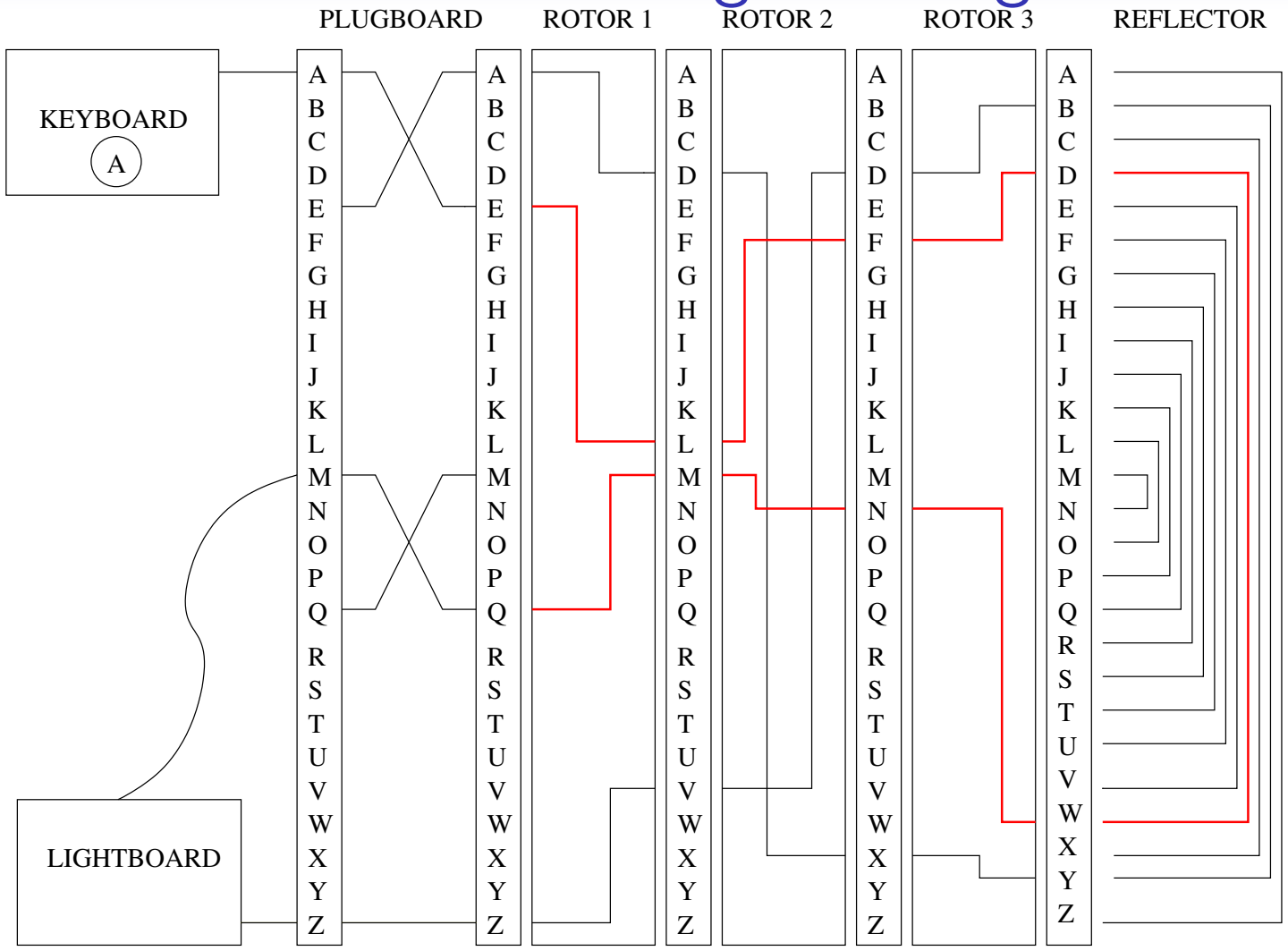


Cracking the Enigma



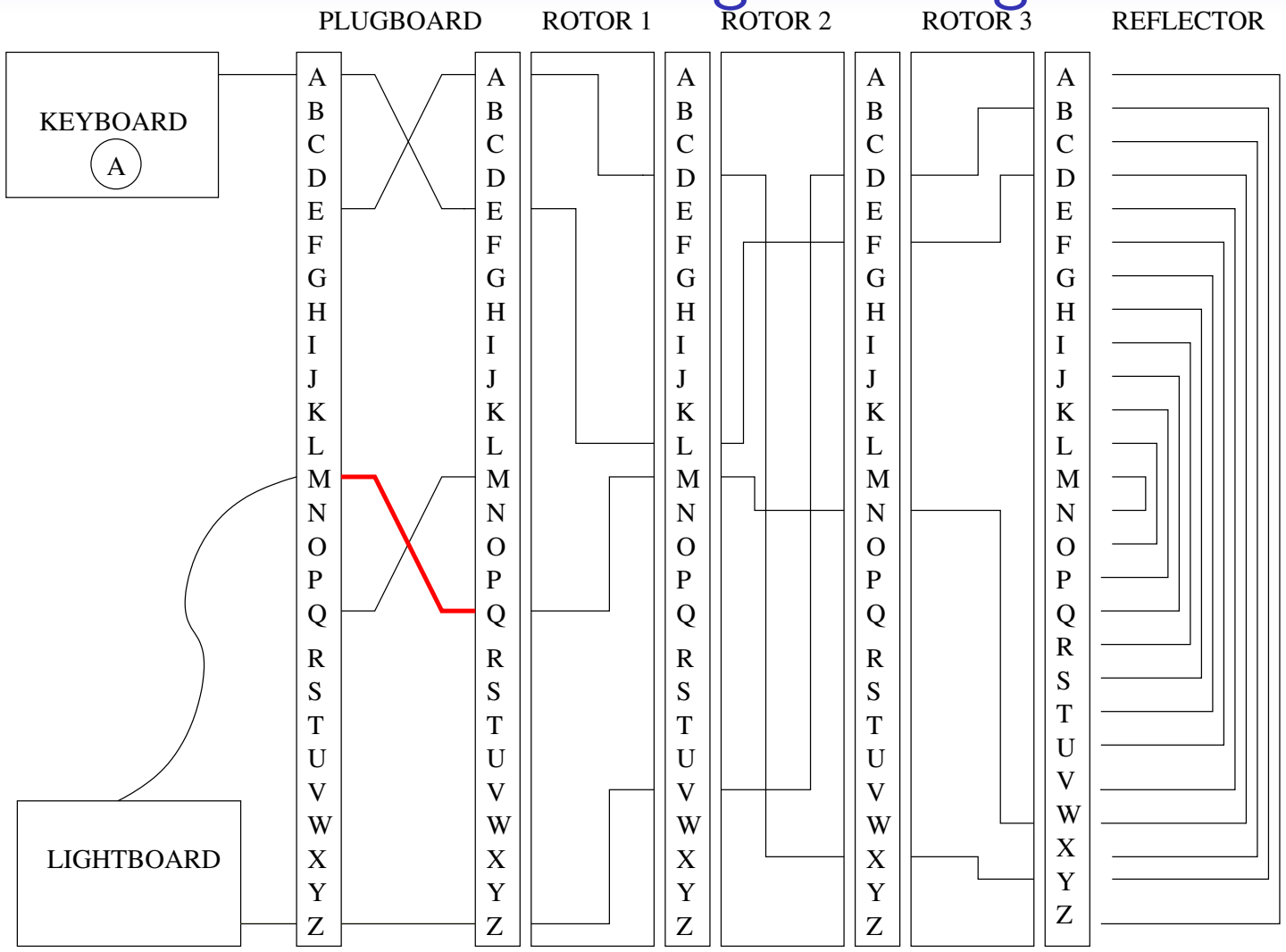
- First go through plugboard P.

Cracking the Enigma



- First go through plugboard P.
- Then pass though the rotor permutation ρ_1.

Cracking the Enigma



- First go through plugboard P.
- Then pass though the rotor permutation ρ_1.
- Pass again through $P = P^{-1}$.

Cracking the Enigma

- Rejewski recorded that this particular setting of Enigma (rotor orders, settings and plugboards) had the mathematical signature

  (10-10-1-1-1-1-1-1, 11-11-2-2, 9-9-4-4).

- This triple of cycle lengths is a fingerprint of the underlying Enigma setting, but which of the billions and billions of settings could it be?
- **Recall:** $P_1 = P \circ \rho_1 \circ P$, where ρ_1 is the permutation defined by the initial rotor order and settings and P is the plugboard setting.

Cracking the Enigma

- Rejewski recorded that this particular setting of Enigma (rotor orders, settings and plugboards) had the mathematical signature

  (10-10-1-1-1-1-1-1, 11-11-2-2, 9-9-4-4).

- This triple of cycle lengths is a fingerprint of the underlying Enigma setting, but which of the billions and billions of settings could it be?
- **Recall:** $P_1 = P \circ \rho_1 \circ P$, where ρ_1 is the permutation defined by the initial rotor order and settings and P is the plugboard setting.
- Likewise, $P_4 = P \circ \rho_4 \circ P$.

Cracking the Enigma

Key Observation

$$\begin{aligned} P_4 \circ P_1 &= (P \circ \rho_4 \circ P) \circ (P \circ \rho_1 \circ P) \\ &= P \circ \rho_4 \circ (P \circ P) \circ \rho_1 \circ P \\ &= P \circ \rho_4 \circ \rho_1 \circ P \\ &= P \circ (\rho_4 \circ \rho_1) \circ P. \end{aligned}$$

Cracking the Enigma

Key Observation

$$\begin{aligned} P_4 \circ P_1 &= (P \circ \rho_4 \circ P) \circ (P \circ \rho_1 \circ P) \\ &= P \circ \rho_4 \circ (P \circ P) \circ \rho_1 \circ P \\ &= P \circ \rho_4 \circ \rho_1 \circ P \\ &= P \circ (\rho_4 \circ \rho_1) \circ P. \end{aligned}$$

- $P_4 \circ P_1$ is the result of conjugating $\rho_4 \circ \rho_1$ by the plugboard P.

Cracking the Enigma

Key Observation

$$\begin{aligned} P_4 \circ P_1 &= (P \circ \rho_4 \circ P) \circ (P \circ \rho_1 \circ P) \\ &= P \circ \rho_4 \circ (P \circ P) \circ \rho_1 \circ P \\ &= P \circ \rho_4 \circ \rho_1 \circ P \\ &= P \circ (\rho_4 \circ \rho_1) \circ P. \end{aligned}$$

- $P_4 \circ P_1$ is the result of conjugating $\rho_4 \circ \rho_1$ by the plugboard P.
- The cycle structure of $P_4 \circ P_1$ is identical to that of $\rho_4 \circ \rho_1$.

Cracking the Enigma

Key Observation

$$\begin{aligned} P_4 \circ P_1 &= (P \circ \rho_4 \circ P) \circ (P \circ \rho_1 \circ P) \\ &= P \circ \rho_4 \circ (P \circ P) \circ \rho_1 \circ P \\ &= P \circ \rho_4 \circ \rho_1 \circ P \\ &= P \circ (\rho_4 \circ \rho_1) \circ P. \end{aligned}$$

- $P_4 \circ P_1$ is the result of conjugating $\rho_4 \circ \rho_1$ by the plugboard P.
- The cycle structure of $P_4 \circ P_1$ is identical to that of $\rho_4 \circ \rho_1$.
- But $\rho_4 \circ \rho_1$**involves only the rotors and reflector!**

Cracking the Enigma

Key Observation

$$\begin{aligned} P_4 \circ P_1 &= (P \circ \rho_4 \circ P) \circ (P \circ \rho_1 \circ P) \\ &= P \circ \rho_4 \circ (P \circ P) \circ \rho_1 \circ P \\ &= P \circ \rho_4 \circ \rho_1 \circ P \\ &= P \circ (\rho_4 \circ \rho_1) \circ P. \end{aligned}$$

- $P_4 \circ P_1$ is the result of conjugating $\rho_4 \circ \rho_1$ by the plugboard P.
- The cycle structure of $P_4 \circ P_1$ is identical to that of $\rho_4 \circ \rho_1$.
- But $\rho_4 \circ \rho_1$**involves only the rotors and reflector!**
- The cycle structure of $P_4 \circ P_1$ is **independent of the plugboard!**

Cracking the Enigma

- Recall there are only $6 \times 26^3 = 105,456$ settings determined by the rotor orders and starting positions.

Cracking the Enigma

- Recall there are only $6 \times 26^3 = 105,456$ settings determined by the rotor orders and starting positions.

- Rejewski and his colleagues spent an entire year cataloguing the signature for each of the 105,456 starting positions.

Cracking the Enigma

- Recall there are only $6 \times 26^3 = 105,456$ settings determined by the rotor orders and starting positions.
- Rejewski and his colleagues spent an entire year cataloguing the signature for each of the 105,456 starting positions.
- The beginning of this catalogue might have looked like this:

Cracking the Enigma

```
Rotor order: 1 2 3: Setting: AAA
13-13- 12-12-1-1- 12-12-1-1-

Rotor order: 1 2 3: Setting: BAA
12-12-1-1- 12-12-1-1- 11-11-2-2-

Rotor order: 1 2 3: Setting: CAA
12-12-1-1- 11-11-2-2- 12-12-1-1-

Rotor order: 1 2 3: Setting: DAA
11-11-2-2- 12-12-1-1- 13-13-

Rotor order: 1 2 3: Setting: EAA
12-12-1-1- 13-13- 13-13-

Rotor order: 1 2 3: Setting: FAA
13-13- 13-13- 4-4-3-3-3-3-2-2-1-1-

Rotor order: 1 2 3: Setting: GAA
13-13- 4-4-3-3-3-3-2-2-1-1- 6-6-5-5-2-2-

Rotor order: 1 2 3: Setting: HAA
4-4-3-3-3-3-2-2-1-1- 6-6-5-5-2-2- 13-13-
```

The Final Assault

- Find (10-10-1-1-1-1-1-1, 11-11-2-2, 9-9-4-4) in the library.

The Final Assault

- Find (10-10-1-1-1-1-1-1, 11-11-2-2, 9-9-4-4) in the library.

- We find the following entry:

  Rotor order: 2 3 1: Setting: ZQP.

The Final Assault

- Find (10-10-1-1-1-1-1-1, 11-11-2-2, 9-9-4-4) in the library.

- We find the following entry:

  Rotor order: 2 3 1: Setting: ZQP.

- With model Enigmas, completely construct the first six permutations, $\rho_1, \cdots, \rho_6$, defined by these settings, **with no plugboard.**

The Final Assault

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
A	M	V	Q	G	L	J
B	C	O	N	I	C	F
C	B	W	M	J	B	E
D	V	F	H	V	S	V
E	N	Z	Z	L	U	C
F	I	D	X	N	T	B
G	Y	L	L	A	P	X
H	W	Q	D	T	N	K
I	F	J	U	B	R	Z
J	Z	I	T	C	W	A
K	U	U	Y	M	Y	H
L	R	G	G	E	A	Q
M	A	P	C	K	X	R

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
N	E	R	B	F	H	W
O	X	B	V	X	Z	P
P	Q	M	W	Q	G	O
Q	P	H	A	P	V	L
R	L	N	S	S	I	M
S	T	T	R	R	D	U
T	S	S	J	H	F	Y
U	K	K	I	Z	E	S
V	D	A	O	D	Q	D
W	H	C	P	Y	J	N
X	O	Y	F	O	M	G
Y	G	X	K	W	K	T
Z	J	E	E	U	O	I

The Final Assault

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
A	M	V	Q	G	L	J
B	C	O	N	I	C	F
C	B	W	M	J	B	E
D	V	F	H	V	S	V
E	N	Z	Z	L	U	C
F	I	D	X	N	T	B
G	Y	L	L	A	P	X
H	W	Q	D	T	N	K
I	F	J	U	B	R	Z
J	Z	I	T	C	W	A
K	U	U	Y	M	Y	H
L	R	G	G	E	A	Q
M	A	P	C	K	X	R

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
N	E	R	B	F	H	W
O	X	B	V	X	Z	P
P	Q	M	W	Q	G	O
Q	P	H	A	P	V	L
R	L	N	S	S	I	M
S	T	T	R	R	D	U
T	S	S	J	H	F	Y
U	K	K	I	Z	E	S
V	D	A	O	D	Q	D
W	H	C	P	Y	J	N
X	O	Y	F	O	M	G
Y	G	X	K	W	K	T
Z	J	E	E	U	O	I

- It is elementary to produce this table.

The Final Assault

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
A	M	V	Q	G	L	J
B	C	O	N	I	C	F
C	B	W	M	J	B	E
D	V	F	H	V	S	V
E	N	Z	Z	L	U	C
F	I	D	X	N	T	B
G	Y	L	L	A	P	X
H	W	Q	D	T	N	K
I	F	J	U	B	R	Z
J	Z	I	T	C	W	A
K	U	U	Y	M	Y	H
L	R	G	G	E	A	Q
M	A	P	C	K	X	R

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
N	E	R	B	F	H	W
O	X	B	V	X	Z	P
P	Q	M	W	Q	G	O
Q	P	H	A	P	V	L
R	L	N	S	S	I	M
S	T	T	R	R	D	U
T	S	S	J	H	F	Y
U	K	K	I	Z	E	S
V	D	A	O	D	Q	D
W	H	C	P	Y	J	N
X	O	Y	F	O	M	G
Y	G	X	K	W	K	T
Z	J	E	E	U	O	I

- It is elementary to produce this table.
- Set rotors in specified position. Hit A six times to produce first row. Get two entries for each encryption!

The Final Assault

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
A	M	V	Q	G	L	J
B	C	O	N	I	C	F
C	B	W	M	J	B	E
D	V	F	H	V	S	V
E	N	Z	Z	L	U	C
F	I	D	X	N	T	B
G	Y	L	L	A	P	X
H	W	Q	D	T	N	K
I	F	J	U	B	R	Z
J	Z	I	T	C	W	A
K	U	U	Y	M	Y	H
L	R	G	G	E	A	Q
M	A	P	C	K	X	R

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
N	E	R	B	F	H	W
O	X	B	V	X	Z	P
P	Q	M	W	Q	G	O
Q	P	H	A	P	V	L
R	L	N	S	S	I	M
S	T	T	R	R	D	U
T	S	S	J	H	F	Y
U	K	K	I	Z	E	S
V	D	A	O	D	Q	D
W	H	C	P	Y	J	N
X	O	Y	F	O	M	G
Y	G	X	K	W	K	T
Z	J	E	E	U	O	I

- It is elementary to produce this table.
- Set rotors in specified position. Hit A six times to produce first row. Get two entries for each encryption!

The Final Assault

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
A	M	V	Q	G	L	J
B	C	O	N	I	C	F
C	B	W	M	J	B	E
D	V	F	H	V	S	V
E	N	Z	Z	L	U	C
F	I	D	X	N	T	B
G	Y	L	L	A	P	X
H	W	Q	D	T	N	K
I	F	J	U	B	R	Z
J	Z	I	T	C	W	A
K	U	U	Y	M	Y	H
L	R	G	G	E	A	Q
M	A	P	C	K	X	R

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
N	E	R	B	F	H	W
O	X	B	V	X	Z	P
P	Q	M	W	Q	G	O
Q	P	H	A	P	V	L
R	L	N	S	S	I	M
S	T	T	R	R	D	U
T	S	S	J	H	F	Y
U	K	K	I	Z	E	S
V	D	A	O	D	Q	D
W	H	C	P	Y	J	N
X	O	Y	F	O	M	G
Y	G	X	K	W	K	T
Z	J	E	E	U	O	I

- It is elementary to produce this table.
- Set rotors in specified position. Hit A six times to produce first row. Get two entries for each encryption!

The Final Assault

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
A	M	V	Q	G	L	J
B	C	O	N	I	C	F
C	B	W	M	J	B	E
D	V	F	H	V	S	V
E	N	Z	Z	L	U	C
F	I	D	X	N	T	B
G	Y	L	L	A	P	X
H	W	Q	D	T	N	K
I	F	J	U	B	R	Z
J	Z	I	T	C	W	A
K	U	U	Y	M	Y	H
L	R	G	G	E	A	Q
M	A	P	C	K	X	R

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
N	E	R	B	F	H	W
O	X	B	V	X	Z	P
P	Q	M	W	Q	G	O
Q	P	H	A	P	V	L
R	L	N	S	S	I	M
S	T	T	R	R	D	U
T	S	S	J	H	F	Y
U	K	K	I	Z	E	S
V	D	A	O	D	Q	D
W	H	C	P	Y	J	N
X	O	Y	F	O	M	G
Y	G	X	K	W	K	T
Z	J	E	E	U	O	I

- It is elementary to produce this table.
- Set rotors in specified position. Hit A six times to produce first row. Get two entries for each encryption!

The Final Assault

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
A	M	V	Q	G	L	J
B	C	O	N	I	C	F
C	B	W	M	J	B	E
D	V	F	H	V	S	V
E	N	Z	Z	L	U	C
F	I	D	X	N	T	B
G	Y	L	L	A	P	X
H	W	Q	D	T	N	K
I	F	J	U	B	R	Z
J	Z	I	T	C	W	A
K	U	U	Y	M	Y	H
L	R	G	G	E	A	Q
M	A	P	C	K	X	R

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
N	E	R	B	F	H	W
O	X	B	V	X	Z	P
P	Q	M	W	Q	G	O
Q	P	H	A	P	V	L
R	L	N	S	S	I	M
S	T	T	R	R	D	U
T	S	S	J	H	F	Y
U	K	K	I	Z	E	S
V	D	A	O	D	Q	D
W	H	C	P	Y	J	N
X	O	Y	F	O	M	G
Y	G	X	K	W	K	T
Z	J	E	E	U	O	I

- It is elementary to produce this table.
- Set rotors in specified position. Hit A six times to produce first row. Get two entries for each encryption!

The Final Assault

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
A	M	V	Q	G	L	J
B	C	O	N	I	C	F
C	B	W	M	J	B	E
D	V	F	H	V	S	V
E	N	Z	Z	L	U	C
F	I	D	X	N	T	B
G	Y	L	L	A	P	X
H	W	Q	D	T	N	K
I	F	J	U	B	R	Z
J	Z	I	T	C	W	A
K	U	U	Y	M	Y	H
L	R	G	G	E	A	Q
M	A	P	C	K	X	R

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
N	E	R	B	F	H	W
O	X	B	V	X	Z	P
P	Q	M	W	Q	G	O
Q	P	H	A	P	V	L
R	L	N	S	S	I	M
S	T	T	R	R	D	U
T	S	S	J	H	F	Y
U	K	K	I	Z	E	S
V	D	A	O	D	Q	D
W	H	C	P	Y	J	N
X	O	Y	F	O	M	G
Y	G	X	K	W	K	T
Z	J	E	E	U	O	I

- It is elementary to produce this table.
- Set rotors in specified position. Hit A six times to produce first row. Get two entries for each encryption!

The Final Assault

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
A	M	V	Q	G	L	J
B	C	O	N	I	C	F
C	B	W	M	J	B	E
D	V	F	H	V	S	V
E	N	Z	Z	L	U	C
F	I	D	X	N	T	B
G	Y	L	L	A	P	X
H	W	Q	D	T	N	K
I	F	J	U	B	R	Z
J	Z	I	T	C	W	A
K	U	U	Y	M	Y	H
L	R	G	G	E	A	Q
M	A	P	C	K	X	R

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
N	E	R	B	F	H	W
O	X	B	V	X	Z	P
P	Q	M	W	Q	G	O
Q	P	H	A	P	V	L
R	L	N	S	S	I	M
S	T	T	R	R	D	U
T	S	S	J	H	F	Y
U	K	K	I	Z	E	S
V	D	A	O	D	Q	D
W	H	C	P	Y	J	N
X	O	Y	F	O	M	G
Y	G	X	K	W	K	T
Z	J	E	E	U	O	I

- It is elementary to produce this table.
- Set rotors in specified position. Hit A six times to produce first row. Get two entries for each encryption!

Recovering the Plugboard

- From this table, construct the cycles for the three permutations $\rho_4 \circ \rho_1$, $\rho_5 \circ \rho_2$, and $\rho_6 \circ \rho_3$:

Recovering the Plugboard

- From this table, construct the cycles for the three permutations $\rho_4 \circ \rho_1$, $\rho_5 \circ \rho_2$, and $\rho_6 \circ \rho_3$:
  1. $\rho_4 \circ \rho_1 =$ (MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)

The Final Assault

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
A	M	V	Q	G	L	J
B	C	O	N	I	C	F
C	B	W	M	J	B	E
D	V	F	H	V	S	V
E	N	Z	Z	L	U	C
F	I	D	X	N	T	B
G	Y	L	L	A	P	X
H	W	Q	D	T	N	K
I	F	J	U	B	R	Z
J	Z	I	T	C	W	A
K	U	U	Y	M	Y	H
L	R	G	G	E	A	Q
M	A	P	C	K	X	R

Rotor order: 2 3 1 Setting: Z Q P						
Perm.	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
N	E	R	B	F	H	W
O	X	B	V	X	Z	P
P	Q	M	W	Q	G	O
Q	P	H	A	P	V	L
R	L	N	S	S	I	M
S	T	T	R	R	D	U
T	S	S	J	H	F	Y
U	K	K	I	Z	E	S
V	D	A	O	D	Q	D
W	H	C	P	Y	J	N
X	O	Y	F	O	M	G
Y	G	X	K	W	K	T
Z	J	E	E	U	O	I

- For instance $\rho_1(M) = A$ and $\rho_4(A) = G$, so $\rho_4 \circ \rho_1(M) = G$.

Recovering the Plugboard

- From this table, construct the cycles for the three permutations $\rho_4 \circ \rho_1$, $\rho_5 \circ \rho_2$, and $\rho_6 \circ \rho_3$:
  1. $\rho_4 \circ \rho_1 =$ (MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)
  2. $\rho_5 \circ \rho_2 =$ (VLPXKEOCJRH)(AQNIWBZUYMG)(FS)(DT)

Recovering the Plugboard

- From this table, construct the cycles for the three permutations $\rho_4 \circ \rho_1$, $\rho_5 \circ \rho_2$, and $\rho_6 \circ \rho_3$:
  1. $\rho_4 \circ \rho_1 =$ (MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)
  2. $\rho_5 \circ \rho_2 =$ (VLPXKEOCJRH)(AQNIWBZUYMG)(FS)(DT)
  3. $\rho_6 \circ \rho_3 =$ (QJYHVPNFG)(ALXBWODKT)(ZCRU)(ISME)

Recovering the Plugboard

- From this table, construct the cycles for the three permutations $\rho_4 \circ \rho_1$, $\rho_5 \circ \rho_2$, and $\rho_6 \circ \rho_3$:
  1. $\rho_4 \circ \rho_1 =$ (MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)
  2. $\rho_5 \circ \rho_2 =$ (VLPXKEOCJRH)(AQNIWBZUYMG)(FS)(DT)
  3. $\rho_6 \circ \rho_3 =$ (QJYHVPNFG)(ALXBWODKT)(ZCRU)(ISME)
- These cycles are intimately related to those for $P_4 \circ P_1$, $P_5 \circ P_2$, and $P_6 \circ P_3$.

Recovering the Plugboard

- From this table, construct the cycles for the three permutations $\rho_4 \circ \rho_1$, $\rho_5 \circ \rho_2$, and $\rho_6 \circ \rho_3$:
  1. $\rho_4 \circ \rho_1 =$ (MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)
  2. $\rho_5 \circ \rho_2 =$ (VLPXKEOCJRH)(AQNIWBZUYMG)(FS)(DT)
  3. $\rho_6 \circ \rho_3 =$ (QJYHVPNFG)(ALXBWODKT)(ZCRU)(ISME)
- These cycles are intimately related to those for $P_4 \circ P_1$, $P_5 \circ P_2$, and $P_6 \circ P_3$.

FACT: If $\rho_4 \circ \rho_1 : \alpha \mapsto \beta$, then $P_4 \circ P_1 : P(\alpha) \mapsto P(\beta)$.

Recovering the Plugboard

- From this table, construct the cycles for the three permutations $\rho_4 \circ \rho_1$, $\rho_5 \circ \rho_2$, and $\rho_6 \circ \rho_3$:
  1. $\rho_4 \circ \rho_1 =$ (MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)
  2. $\rho_5 \circ \rho_2 =$ (VLPXKEOCJRH)(AQNIWBZUYMG)(FS)(DT)
  3. $\rho_6 \circ \rho_3 =$ (QJYHVPNFG)(ALXBWODKT)(ZCRU)(ISME)
- These cycles are intimately related to those for $P_4 \circ P_1$, $P_5 \circ P_2$, and $P_6 \circ P_3$.

FACT: If $\rho_4 \circ \rho_1 : \alpha \mapsto \beta$, then $P_4 \circ P_1 : P(\alpha) \mapsto P(\beta)$.

Proof:

$$P_4 \circ P_1((P(\alpha)) = P \circ \rho_4 \circ \rho_1 \circ P((P(\alpha))$$

Recovering the Plugboard

- From this table, construct the cycles for the three permutations $\rho_4 \circ \rho_1$, $\rho_5 \circ \rho_2$, and $\rho_6 \circ \rho_3$:
  1. $\rho_4 \circ \rho_1 =$ (MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)
  2. $\rho_5 \circ \rho_2 =$ (VLPXKEOCJRH)(AQNIWBZUYMG)(FS)(DT)
  3. $\rho_6 \circ \rho_3 =$ (QJYHVPNFG)(ALXBWODKT)(ZCRU)(ISME)
- These cycles are intimately related to those for $P_4 \circ P_1$, $P_5 \circ P_2$, and $P_6 \circ P_3$.

FACT: If $\rho_4 \circ \rho_1 : \alpha \mapsto \beta$, then $P_4 \circ P_1 : P(\alpha) \mapsto P(\beta)$.

Proof:

$$\begin{aligned} P_4 \circ P_1((P(\alpha)) &= P \circ \rho_4 \circ \rho_1 \circ P((P(\alpha)) \\ &= P \circ \rho_4 \circ \rho_1(\alpha) \end{aligned}$$

Recovering the Plugboard

- From this table, construct the cycles for the three permutations $\rho_4 \circ \rho_1$, $\rho_5 \circ \rho_2$, and $\rho_6 \circ \rho_3$:
  1. $\rho_4 \circ \rho_1 =$ `(MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)`
  2. $\rho_5 \circ \rho_2 =$ `(VLPXKEOCJRH)(AQNIWBZUYMG)(FS)(DT)`
  3. $\rho_6 \circ \rho_3 =$ `(QJYHVPNFG)(ALXBWODKT)(ZCRU)(ISME)`
- These cycles are intimately related to those for $P_4 \circ P_1$, $P_5 \circ P_2$, and $P_6 \circ P_3$.

FACT: If $\rho_4 \circ \rho_1 : \alpha \mapsto \beta$, then $P_4 \circ P_1 : P(\alpha) \mapsto P(\beta)$.

Proof:

$$\begin{aligned} P_4 \circ P_1((P(\alpha)) &= P \circ \rho_4 \circ \rho_1 \circ P((P(\alpha)) \\ &= P \circ \rho_4 \circ \rho_1(\alpha) \\ &= P(\beta). \end{aligned}$$

Recovering the Plugboard

Corollary

If $\rho_4 \circ \rho_1$ has a cycle $(\alpha_1 \alpha_2 \ldots \alpha_n)$, then $P_4 \circ P_1$ has a cycle $(P(\alpha_1)\, P(\alpha_2)\, \ldots\, P(\alpha_n))$.

Recovering the Plugboard

Corollary

If $\rho_4 \circ \rho_1$ has a cycle $(\alpha_1 \alpha_2 \ldots \alpha_n)$, then $P_4 \circ P_1$ has a cycle $(P(\alpha_1)\, P(\alpha_2)\, \ldots\, P(\alpha_n))$.

- This establishes the fact that $\rho_4 \circ \rho_1$ and $P_4 \circ P_1$ have identical cycle structures.

Recovering the Plugboard

1. $\rho_4 \circ \rho_1 =$

   (MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)

Recovering the Plugboard

1. $\rho_4 \circ \rho_1 =$

   (MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)

2. $P_4 \circ P_1 =$

   (ARDNHSLYZK)(BJUPWTCFE)(I)(O)(Q)(V)(X)(G)

Recovering the Plugboard

1. $\rho_4 \circ \rho_1 =$

   (MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)

2. $P_4 \circ P_1 =$

   (ARDNHSLYZK)(BJUPWTCFE)(I)(O)(Q)(V)(X)(G)

- Because the plugboard has 14 fixed points, we can look for common letter groups within cycles.

Recovering the Plugboard

1. $\rho_4 \circ \rho_1 =$

   (MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)

2. $P_4 \circ P_1 =$

   (ARDNHSLYZK)(BJUPWTCFE)(I)(O)(Q)(V)(X)(G)

- Because the plugboard has 14 fixed points, we can look for common letter groups within cycles.
- The adjacency of letters in corresponding cycles suggests the proper alignment.

Recovering the Plugboard

1. $\rho_4 \circ \rho_1 =$

   (MGWTREFBJU)(AKZCINLSHY)(P)(D)(O)(Q)(V)(X)

2. $P_4 \circ P_1 =$

   (ARDNHSLYZK)(BJUPWTCFE)(I)(O)(Q)(V)(X)(G)

- Because the plugboard has 14 fixed points, we can look for common letter groups within cycles.
- The adjacency of letters in corresponding cycles suggests the proper alignment.
- For instance, consider the letters BJU in $\rho_4 \circ \rho_1$ and $P_4 \circ P_1$.

Recovering the Plugboard

$$\rho_4 \circ \rho_1 \quad \rightarrow \quad \texttt{(BJUMGWTREF)(CINLSHYAKZ)(P)(D)(O)(Q)(V)(X)}$$
$$P_4 \circ P_1 \quad \rightarrow \quad \texttt{(BJUMPWTCFE)(RDNHSLYZKA)(G)(I)(O)(Q)(V)(X)}$$

Recovering the Plugboard

$$\begin{array}{rcl} & & \downarrow \quad \downarrow\downarrow \\ \rho_4 \circ \rho_1 & \to & \texttt{(BJUMGWTREF)(CINLSHYAKZ)(P)(D)(O)(Q)(V)(X)} \\ P_4 \circ P_1 & \to & \texttt{(BJUMPWTCFE)(RDNHSLYZKA)(G)(I)(O)(Q)(V)(X)} \\ & & \uparrow \quad \uparrow\uparrow \end{array}$$

- The leftmost 11-cycles immediately yield the swaps R/C, G/P, and E/F.

Recovering the Plugboard

$$\begin{array}{rcl} & & \downarrow \\ \rho_4 \circ \rho_1 & \rightarrow & \texttt{(BJUMGWTREF)(CINLSHYAKZ)(P)(D)(O)(Q)(V)(X)} \\ P_4 \circ P_1 & \rightarrow & \texttt{(BJUMPWTCFE)(RDNHSLYZKA)(G)(I)(O)(Q)(V)(X)} \\ & & \uparrow \end{array}$$

- The leftmost 11-cycles immediately yield the swaps R/C, G/P, and E/F.
- Align the next 11-cycles of $\rho_4 \circ \rho_1$ and $P_4 \circ P_1$ using the fact that P(C)=R.

Recovering the Plugboard

$$\begin{array}{rcl} & & \downarrow\ \downarrow\quad \downarrow \\ \rho_4 \circ \rho_1 & \to & \texttt{(BJUMGWTREF)(CINLSHYAKZ)(P)(D)(O)(Q)(V)(X)} \\ P_4 \circ P_1 & \to & \texttt{(BJUMPWTCFE)(RDNHSLYZKA)(G)(I)(O)(Q)(V)(X)} \\ & & \uparrow\ \uparrow\quad \uparrow \end{array}$$

- The leftmost 11-cycles immediately yield the swaps R/C, G/P, and E/F.
- Align the next 11-cycles of $\rho_4 \circ \rho_1$ and $P_4 \circ P_1$ using the fact that P(C)=R.
- This immediately yields I/D, L/H, and A/Z. This completes the full recovery of all six letter swaps.

Recovering the Plugboard

$$\begin{aligned} \rho_4 \circ \rho_1 &\rightarrow \texttt{(BJUMGWTREF)(CINLSHYAKZ)(P)(D)(O)(Q)(V)(X)} \\ P_4 \circ P_1 &\rightarrow \texttt{(BJUMPWTCFE)(RDNHSLYZKA)(G)(I)(O)(Q)(V)(X)} \end{aligned}$$

- The leftmost 11-cycles immediately yield the swaps R/C, G/P, and E/F.
- Align the next 11-cycles of $\rho_4 \circ \rho_1$ and $P_4 \circ P_1$ using the fact that P(C)=R.
- This immediately yields I/D, L/H, and A/Z. This completes the full recovery of all six letter swaps.
- Having determined the rotor order:
  2-3-1, the settings: Z-Q-P, and the plugboard swaps: G/P, I/D, A/Z, E/F, C/R, H/L, the message can be fully decrypted.