you

Furino

|

you

Dickey

|

Furino

|

you

Crowe

|

Dickey

|

Furino

|

you

Coxeter

Crowe

Dickey

Furino

you

Baker

Coxeter

Crowe

Dickey

Furino

you

Cayley

Baker

Coxeter

Crowe

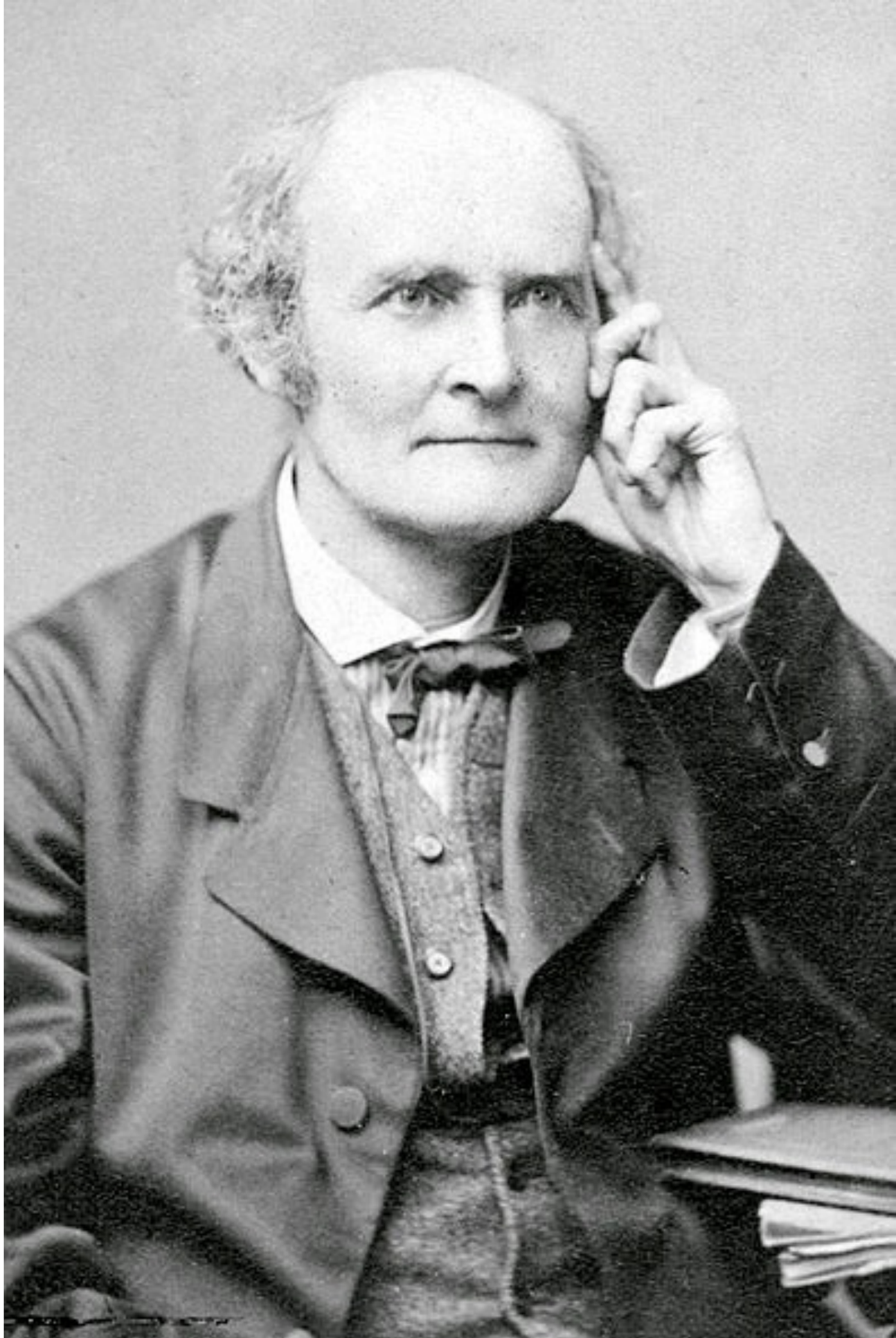
Dickey

Furino

you

Sir Arthur Cayley (1821 – 1895)

- Collected Works published by Cambridge University Press contains 967 papers
- Cayley-Hamilton Theorem in linear algebra
- defined a group, advanced the study of abstract algebra
- contributed to non-Euclidean geometries
- contributed to study of invariants



Cayley

Baker

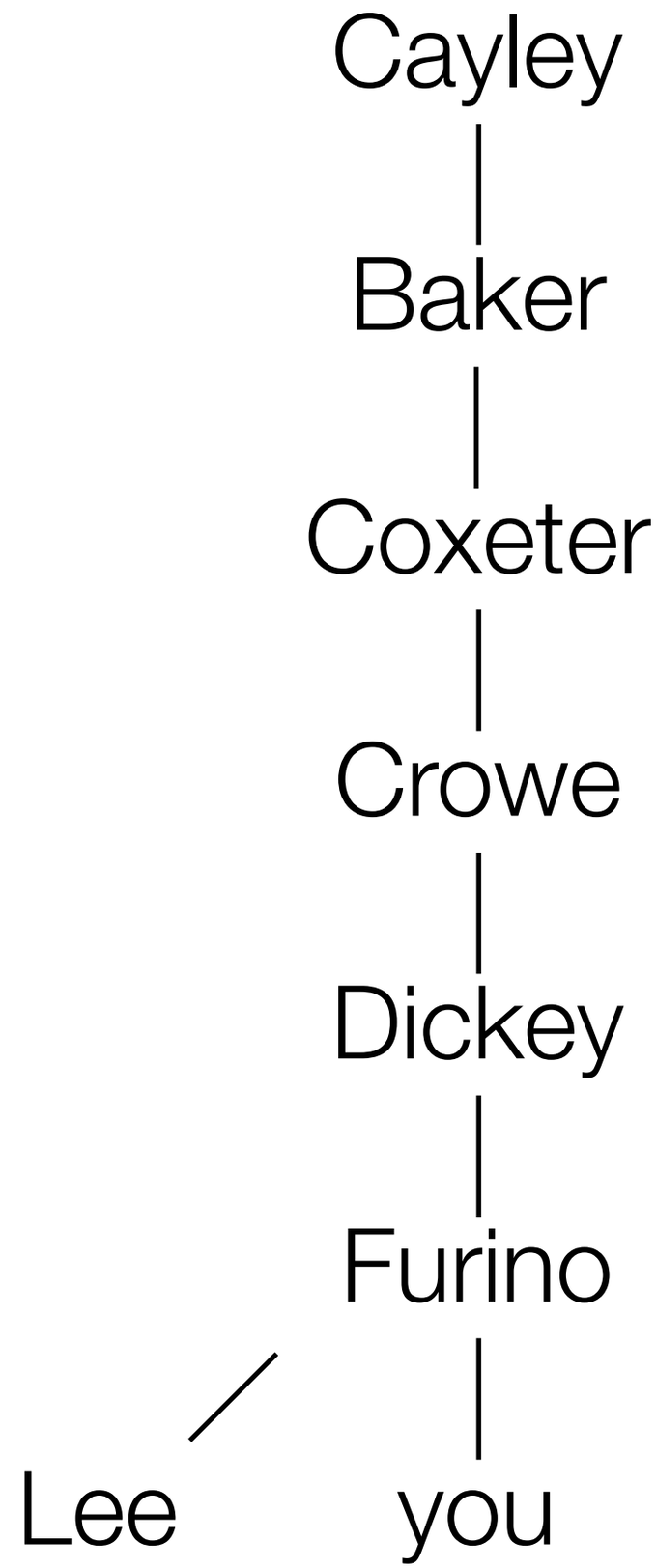
Coxeter

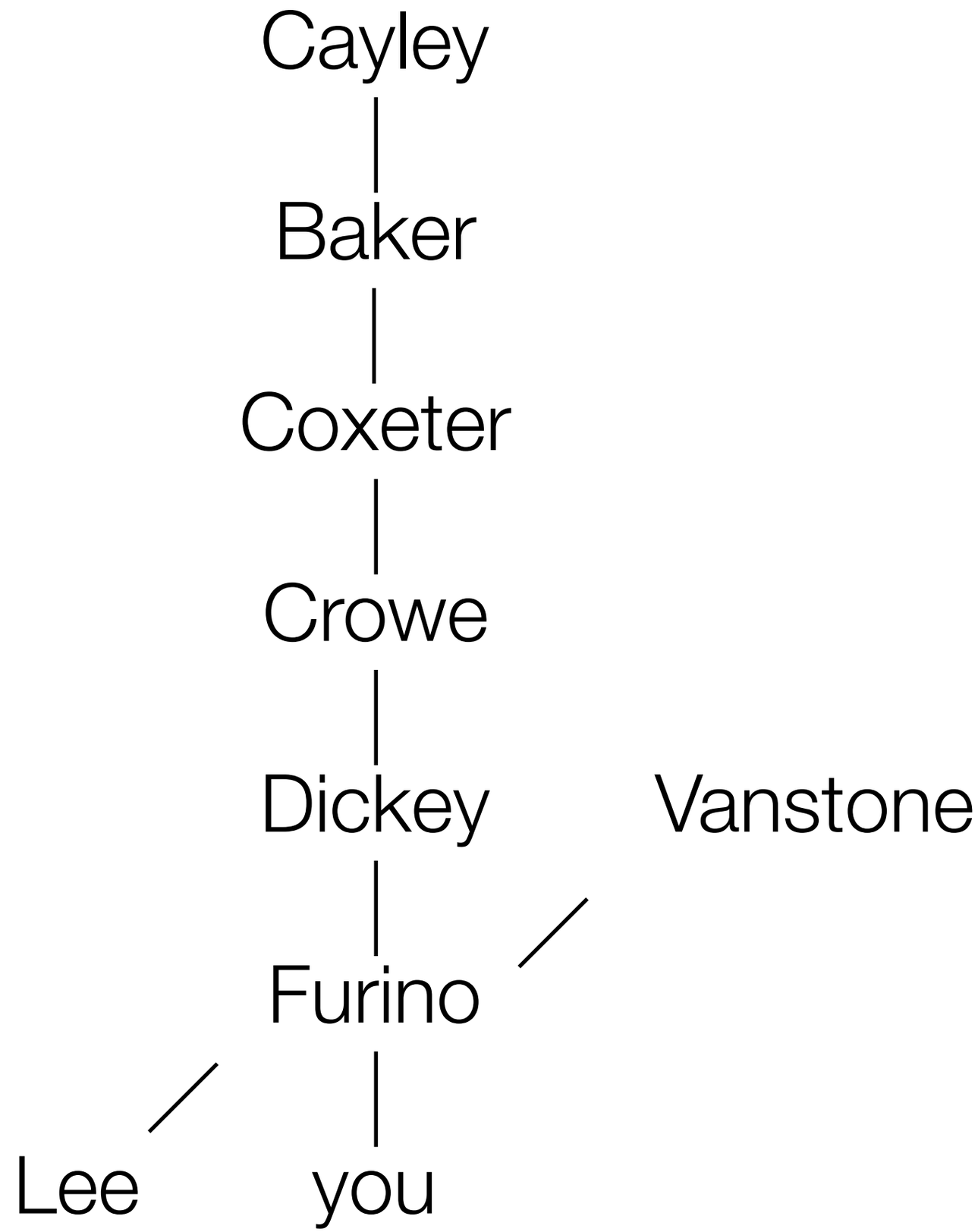
Crowe

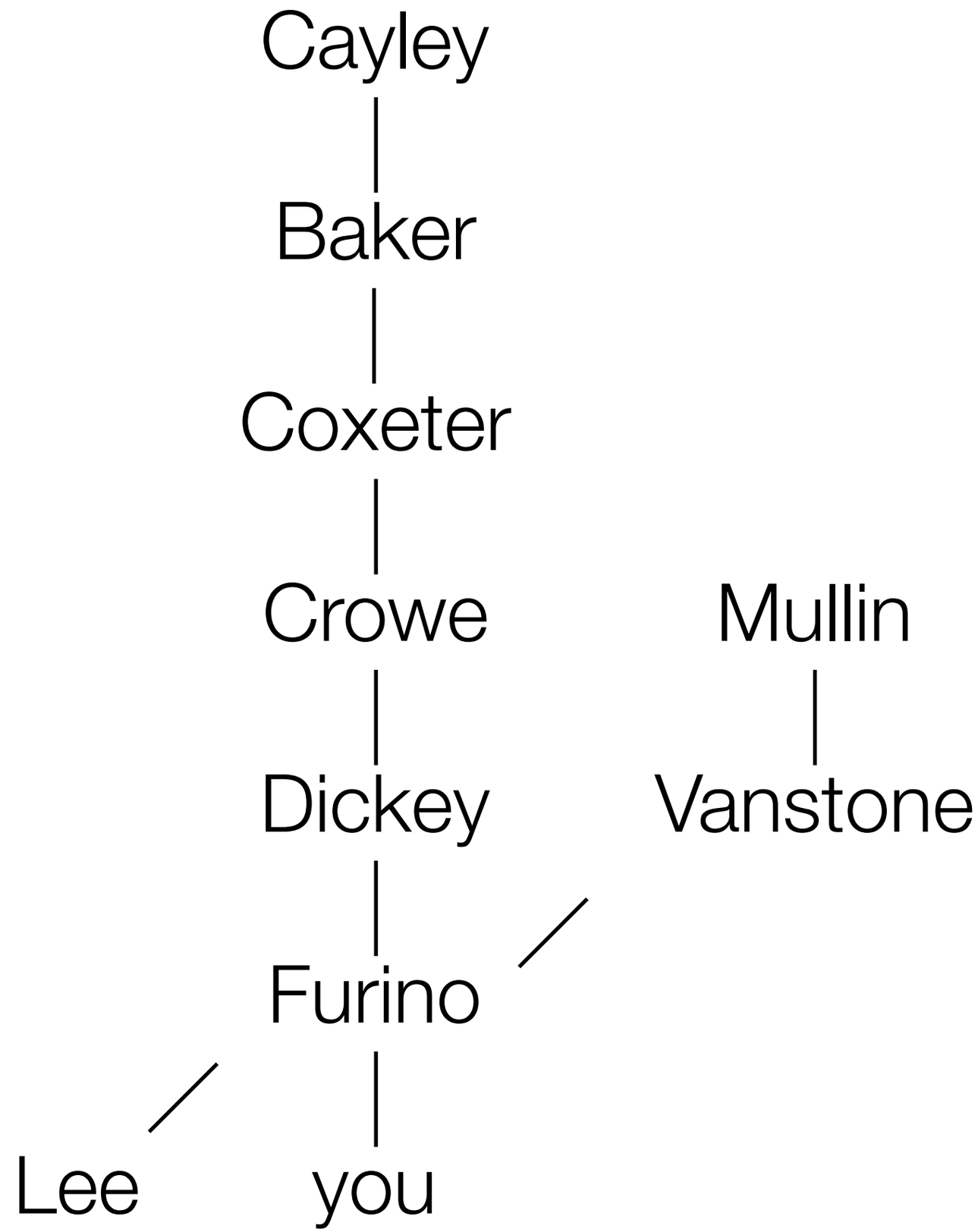
Dickey

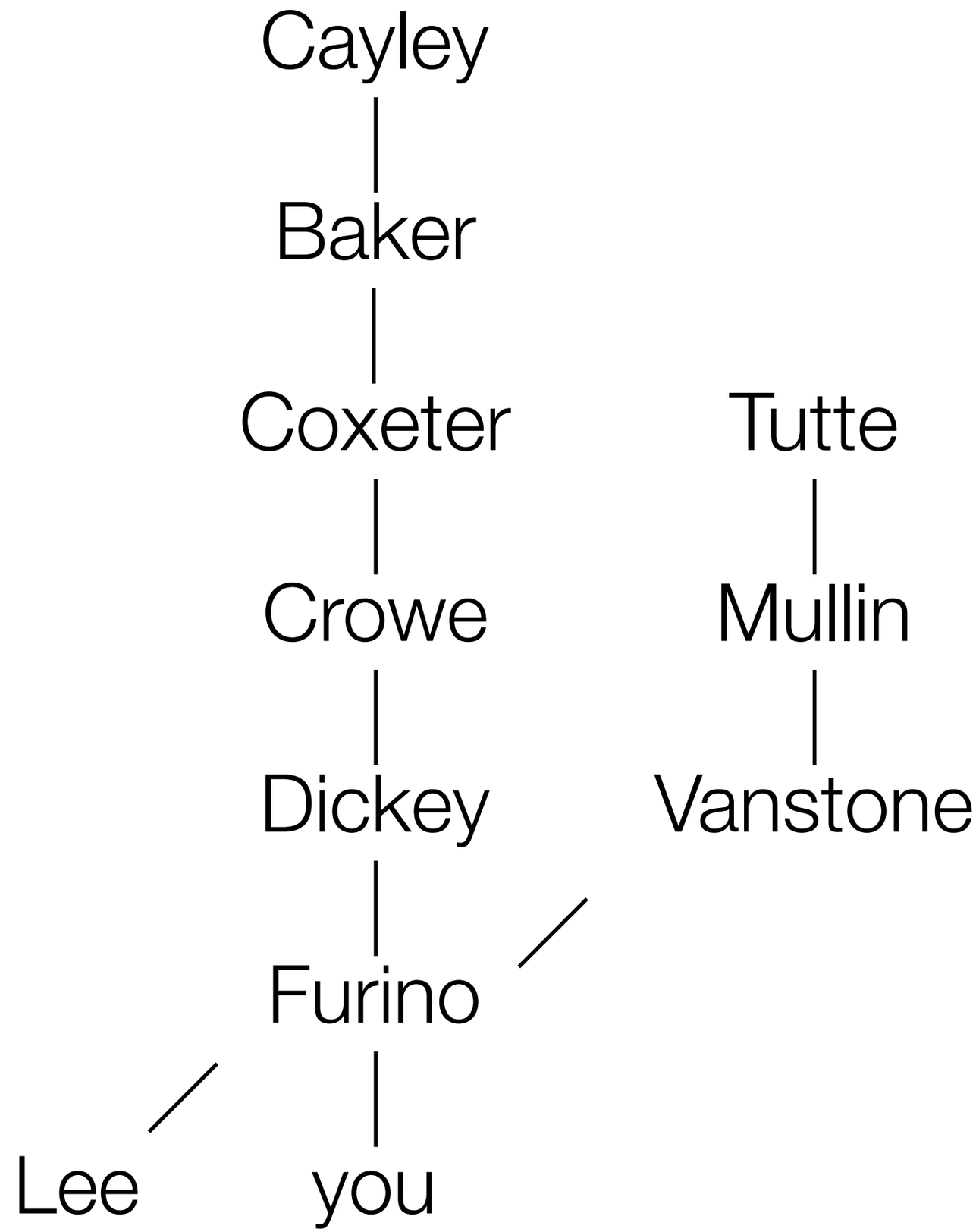
Furino

you


Cayley
Baker
Coxeter
Crowe
Dickey
Furino
Lee
you


Cayley
Baker
Coxeter
Crowe
Dickey
Vanstone
Furino
Lee
you


Cayley
Baker
Coxeter
Crowe
Mullin
Dickey
Vanstone
Furino
Lee
you


Cayley
Baker
Coxeter
Tutte
Crowe
Mullin
Dickey
Vanstone
Furino
Lee
you

William T Tutte
(1917 – 2002)

- “Foreign Office, Statistical” during WW II
- came to Canada in 1948
- came to Waterloo in 1962
- FRSC, FRS, OC 2001
- “the leading mathematician in combinatorics for three decades”

Your Lineage

- The Mathematics Genealogy Project
- http://genealogy.math.ndsu.nodak.edu

1

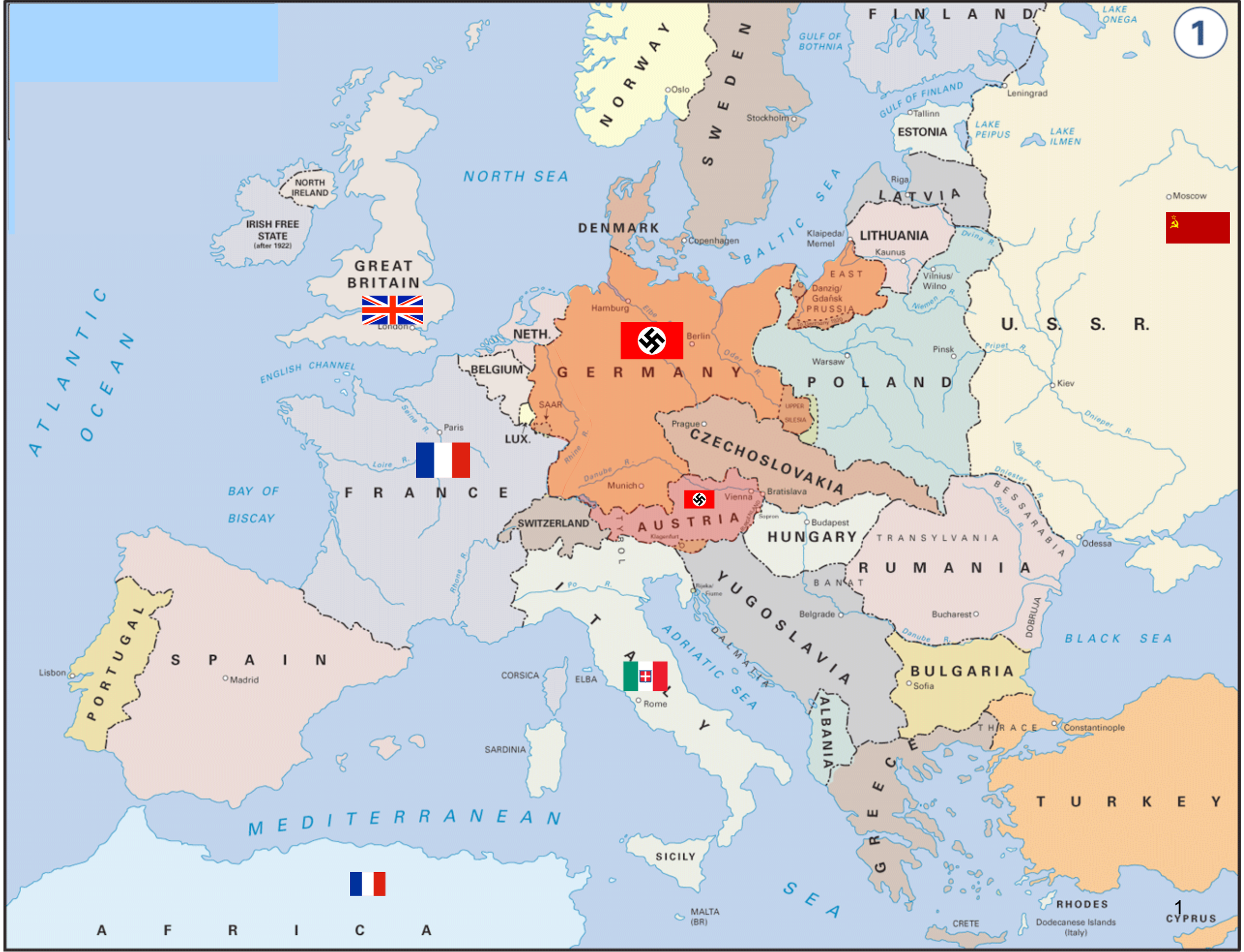
ATLANTIC OCEAN
NORTH SEA
NORWAY
SWEDEN
FINLAND
GULF OF BOTHNIA
LAKE ONEGA
Oslo
Stockholm
Leningrad
GULF OF FINLAND
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
Riga
LATVIA
BALTIC SEA
Moscow
NORTH IRELAND
IRISH FREE STATE
(after 1922)
GREAT BRITAIN
London
DENMARK
Copenhagen
Klaipeda/
Memel
LITHUANIA
Kaunus
Dvina R.
EAST
PRUSSIA
Danzig/
Gdańsk
Vilnius/
Wilno
Niemen R.
Hamburg
Elbe R.
NETH.
Berlin
U. S. S. R.
BELGIUM
GERMANY
Oder R.
Warsaw
Pinsk
Pripet R.
POLAND
ENGLISH CHANNEL
Kiev
SAAR
UPPER SILESIA
Seine R.
Paris
LUX.
Prague
Rhine R.
CZECHOSLOVAKIA
Dnieper R.
Loire R.
Danube R.
Munich
Vienna
Bratislava
Bug R.
Dniester R.
BAY OF BISCAY
FRANCE
SWITZERLAND
AUSTRIA
Sopron
Budapest
HUNGARY
TRANSYLVANIA
BESSARABIA
Pruth R.
Odessa
Rhone R.
TYROL
Klagenfurt
RUMANIA
BANAT
Rijeka/
Fiume
Po R.
YUGOSLAVIA
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ITALY
Rome
ADRIATIC SEA
DALMATIA
ALBANIA
BULGARIA
Sofia
THRACE
Constantinople
GREECE
TURKEY
SARDINIA
MEDITERRANEAN
SICILY
SEA
MALTA
(BR)
CRETE
RHODES
Dodecanese Islands
(Italy)
CYPRUS
AFRICA

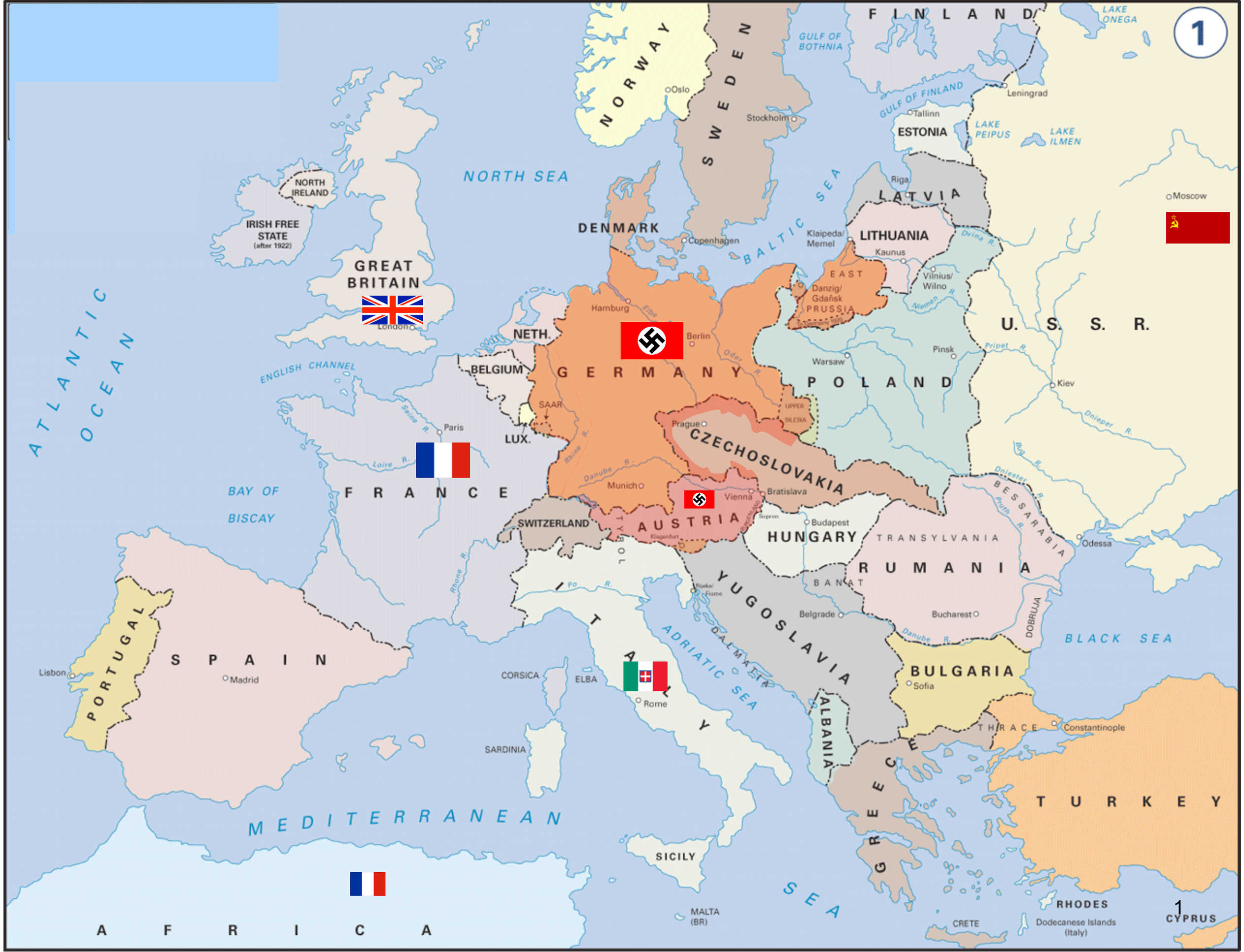
1

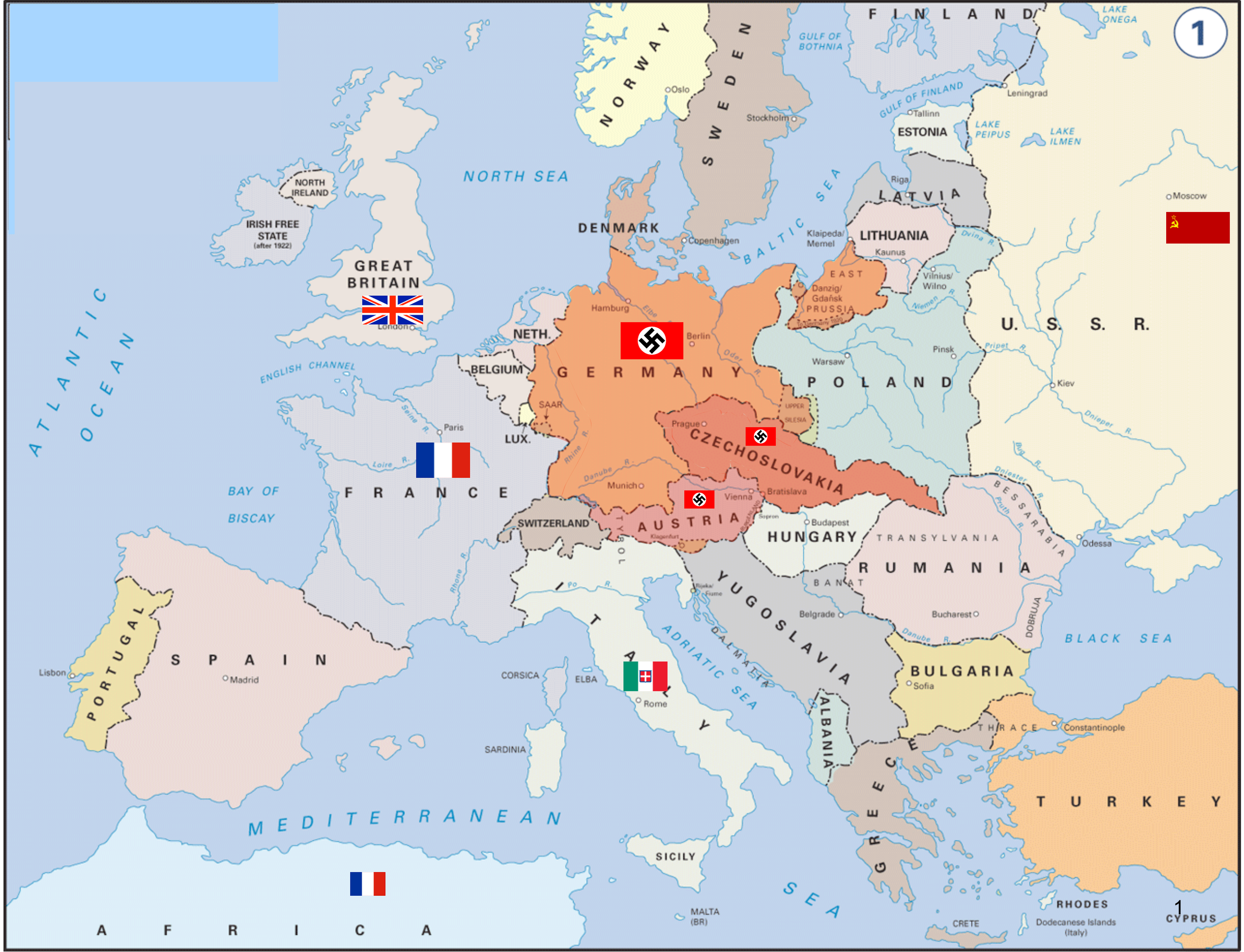
FINLAND
LAKE ONEGA
GULF OF BOTHNIA
NORWAY
SWEDEN
Oslo
Stockholm
GULF OF FINLAND
Leningrad
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
NORTH SEA
Riga
LATVIA
BALTIC SEA
Moscow
NORTH IRELAND
IRISH FREE STATE
(after 1922)
DENMARK
Copenhagen
Klaipeda/
Memel
LITHUANIA
Kaunus
Dvina R.
GREAT BRITAIN
London
EAST PRUSSIA
Danzig/
Gdańsk
Vilnius/
Wilno
Niemen R.
Hamburg
Elbe
NETH.
Berlin
U. S. S. R.
ATLANTIC OCEAN
ENGLISH CHANNEL
BELGIUM
GERMANY
Oder R.
Warsaw
Pinsk
Pripet R.
POLAND
SAAR
Seine R.
Paris
LUX.
Rhine R.
Prague
UPPER SILESIA
Kiev
Dnieper R.
CZECHOSLOVAKIA
Loire R.
Danube R.
Munich
Vienna
Bratislava
Bug R.
Dniester R.
BESSARABIA
Pruth R.
BAY OF BISCAY
FRANCE
SWITZERLAND
AUSTRIA
Innsbruck
TYROL
Klagenfurt
Sopron
Budapest
HUNGARY
TRANSYLVANIA
Odessa
Rhone R.
Po R.
Rijeka/
Fiume
YUGOSLAVIA
RUMANIA
BANAT
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ITALY
Rome
ADRIATIC SEA
DALMATIA
BULGARIA
Sofia
ALBANIA
THRACE
Constantinople
GREECE
TURKEY
SARDINIA
MEDITERRANEAN
SICILY
SEA
RHODES
Dodecanese Islands
(Italy)
CRETE
CYPRUS
MALTA
(BR)
AFRICA

1

FINLAND
LAKE ONEGA
GULF OF BOTHNIA
NORWAY
SWEDEN
Oslo
Stockholm
GULF OF FINLAND
Leningrad
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
NORTH SEA
Riga
LATVIA
Moscow
NORTH IRELAND
IRISH FREE STATE
(after 1922)
DENMARK
Copenhagen
BALTIC SEA
Klaipeda/
Memel
LITHUANIA
Kaunus
Dvina R.
GREAT BRITAIN
London
EAST PRUSSIA
Danzig/
Gdańsk
Vilnius/
Wilno
Niemen R.
Hamburg
Elbe
NETH.
Berlin
U. S. S. R.
ATLANTIC OCEAN
ENGLISH CHANNEL
BELGIUM
GERMANY
Oder R.
Warsaw
Pinsk
Pripet R.
POLAND
Kiev
SAAR
Seine R.
Paris
LUX.
Rhine R.
Prague
UPPER SILESIA
Dnieper R.
CZECHOSLOVAKIA
Loire R.
Danube R.
Munich
Vienna
Bratislava
Bug R.
Dniester R.
BESSARABIA
Pruth R.
BAY OF BISCAY
FRANCE
SWITZERLAND
AUSTRIA
Innsbruck
Klagenfurt
Sopron
Budapest
HUNGARY
TRANSYLVANIA
Odessa
TYROL
Rhone R.
Po R.
Rijeka/
Fiume
YUGOSLAVIA
RUMANIA
BANAT
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ITALY
Rome
ADRIATIC SEA
DALMATIA
ALBANIA
BULGARIA
Sofia
THRACE
Constantinople
GREECE
TURKEY
SARDINIA
MEDITERRANEAN
SICILY
SEA
MALTA
(BR)
CRETE
RHODES
Dodecanese Islands
(Italy)
CYPRUS
AFRICA


1
FINLAND
LAKE ONEGA
NORWAY
SWEDEN
Oslo
Stockholm
GULF OF BOTHNIA
GULF OF FINLAND
Leningrad
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
Riga
LATVIA
Moscow
NORTH SEA
NORTH IRELAND
IRISH FREE STATE
(after 1922)
GREAT BRITAIN
London
DENMARK
Copenhagen
BALTIC SEA
Klaipeda/
Memel
LITHUANIA
Kaunus
Dvina R.
Vilnius/
Wilno
Niemen R.
EAST
PRUSSIA
Danzig/
Gdańsk
ATLANTIC OCEAN
Hamburg
Elbe
NETH.
Berlin
Oder R.
BELGIUM
GERMANY
Warsaw
POLAND
Pinsk
Pripet R.
U. S. S. R.
Kiev
ENGLISH CHANNEL
Seine R.
Paris
SAAR
LUX.
Rhine R.
Prague
UPPER SILESIA
CZECHOSLOVAKIA
Dnieper R.
Loire R.
Danube R.
Munich
Vienna
Bratislava
Bug R.
Dniester R.
BESSARABIA
Pruth R.
BAY OF BISCAY
FRANCE
SWITZERLAND
AUSTRIA
TYROL
Innsbruck
Klagenfurt
Sopron
Budapest
HUNGARY
TRANSYLVANIA
RUMANIA
Odessa
Rhone R.
Po R.
BANAT
Rijeka/
Fiume
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
YUGOSLAVIA
DALMATIA
ADRIATIC SEA
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ITALY
Rome
ALBANIA
BULGARIA
Sofia
THRACE
Constantinople
GREECE
TURKEY
SARDINIA
MEDITERRANEAN
SICILY
SEA
MALTA
(BR)
CRETE
RHODES
Dodecanese Islands
(Italy)
CYPRUS
AFRICA
1


1
FINLAND
LAKE ONEGA
NORWAY
SWEDEN
Oslo
Stockholm
GULF OF BOTHNIA
GULF OF FINLAND
Leningrad
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
NORTH SEA
NORTH IRELAND
IRISH FREE STATE
(after 1922)
GREAT BRITAIN
London
ATLANTIC OCEAN
DENMARK
Copenhagen
BALTIC SEA
Riga
LATVIA
Moscow
Klaipeda/
Memel
LITHUANIA
Kaunus
Dvina R.
EAST
PRUSSIA
Danzig/
Gdańsk
Vilnius/
Wilno
Niemen R.
Hamburg
Elbe R.
NETH.
Berlin
U. S. S. R.
Oder R.
Pinsk
Pripet R.
BELGIUM
GERMANY
Warsaw
POLAND
ENGLISH CHANNEL
Kiev
SAAR
UPPER SILESIA
Seine R.
Paris
Prague
LUX.
Rhine R.
CZECHOSLOVAKIA
Dnieper R.
Loire R.
Danube R.
Munich
Vienna
Bratislava
Bug R.
Dniester R.
BAY OF BISCAY
FRANCE
SWITZERLAND
AUSTRIA
Budapest
HUNGARY
TRANSYLVANIA
BESSARABIA
Pruth R.
Odessa
Rhone R.
Po R.
RUMANIA
BANAT
Rijeka/
Fiume
YUGOSLAVIA
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ITALY
ADRIATIC SEA
DALMATIA
Rome
BULGARIA
Sofia
ALBANIA
THRACE
Constantinople
SARDINIA
GREECE
TURKEY
MEDITERRANEAN
SICILY
SEA
RHODES
Dodecanese Islands
(Italy)
CRETE
MALTA
(BR)
CYPRUS
AFRICA
1


1
FINLAND
LAKE ONEGA
NORWAY
SWEDEN
Oslo
Stockholm
GULF OF BOTHNIA
GULF OF FINLAND
Leningrad
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
NORTH SEA
NORTH IRELAND
IRISH FREE STATE
(after 1922)
GREAT BRITAIN
London
ATLANTIC OCEAN
DENMARK
Copenhagen
BALTIC SEA
Riga
LATVIA
Moscow
Klaipeda/
Memel
LITHUANIA
Kaunus
Dvina R.
EAST
PRUSSIA
Danzig/
Gdańsk
Vilnius/
Wilno
Niemen R.
Hamburg
Elbe R.
NETH.
Berlin
U. S. S. R.
Oder R.
Pinsk
Pripet R.
BELGIUM
GERMANY
Warsaw
POLAND
ENGLISH CHANNEL
Kiev
SAAR
UPPER SILESIA
Seine R.
Paris
Prague
Dnieper R.
LUX.
Rhine R.
CZECHOSLOVAKIA
Loire R.
Danube R.
Munich
Bug R.
Dniester R.
BAY OF BISCAY
FRANCE
Vienna
Bratislava
BESSARABIA
Pruth R.
SWITZERLAND
AUSTRIA
Sopron
Budapest
Odessa
HUNGARY
TRANSYLVANIA
Rhone R.
TYROL
RUMANIA
BANAT
Po R.
Rijeka/
Fiume
YUGOSLAVIA
Belgrade
Bucharest
DOBRUJA
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ADRIATIC SEA
DALMATIA
BULGARIA
Sofia
BLACK SEA
ITALY
Rome
ALBANIA
THRACE
Constantinople
GREECE
SARDINIA
TURKEY
MEDITERRANEAN
SICILY
RHODES
Dodecanese Islands
(Italy)
CRETE
CYPRUS
MALTA
(BR)
AFRICA
1

1

NORTH SEA

NORWAY

SWEDEN

FINLAND

GULF OF BOTHNIA

GULF OF FINLAND

LAKE ONEGA

Oslo

Stockholm

Leningrad

Tallinn

ESTONIA

LAKE PEIPUS

LAKE ILMEN

Riga

LATVIA

BALTIC SEA

Moscow

NORTH IRELAND

IRISH FREE STATE (after 1922)

GREAT BRITAIN

London

DENMARK

Copenhagen

Klaipeda/ Memel

LITHUANIA

Kaunus

Dvina R.

EAST PRUSSIA

Danzig/ Gdańsk

Vilnius/ Wilno

Niemen R.

ATLANTIC OCEAN

Hamburg

Elbe

NETH.

Berlin

U. S. S. R.

Oder R.

Pripet R.

Pinsk

Warsaw

ENGLISH CHANNEL

BELGIUM

GERMANY

POLAND

Kiev

SAAR

UPPER SILESIA

Seine R.

Paris

Prague

LUX.

Rhine R.

CZECHOSLOVAKIA

Dnieper R.

Loire R.

Danube R.

Munich

Bug R.

Dniester R.

BAY OF BISCAY

FRANCE

Vienna

Bratislava

BESSARABIA

Pruth R.

SWITZERLAND

AUSTRIA

Budapest

Odessa

HUNGARY

TRANSYLVANIA

RUMANIA

Rhone R.

BANAT

Belgrade

Bucharest

DOBRUJA

Danube R.

BLACK SEA

YUGOSLAVIA

ADRIATIC SEA

DALMATIA

PORTUGAL

SPAIN

Lisbon

Madrid

BULGARIA

Sofia

CORSICA

ELBA

ITALY

Rome

ALBANIA

THRACE

Constantinople

SARDINIA

GREECE

TURKEY

MEDITERRANEAN

SICILY

SEA

RHODES

Dodecanese Islands (Italy)

CRETE

CYPRUS

MALTA (BR)

AFRICA

1

NORWAY
SWEDEN
FINLAND
Oslo
Stockholm
Leningrad
Tallinn
ESTONIA
LAKE ONEGA
LAKE PEIPUS
LAKE ILMEN
GULF OF BOTHNIA
GULF OF FINLAND
NORTH SEA
BALTIC SEA
Riga
LATVIA
Moscow
NORTH IRELAND
IRISH FREE STATE
(after 1922)
GREAT BRITAIN
London
DENMARK
Copenhagen
Klaipeda/
Memel
LITHUANIA
Kaunus
EAST
PRUSSIA
Danzig/
Gdańsk
Hamburg
Elbe
Berlin
NETH.
BELGIUM
GERMANY
Oder R.
Warsaw
POLAND
Vistula R.
Vilnius/
Wilno
Niemen R.
Pinsk
Pripet R.
U. S. S. R.
Kiev
Dnieper R.
ATLANTIC OCEAN
ENGLISH CHANNEL
Seine R.
Paris
SAAR
LUX.
Rhine R.
Danube R.
Loire R.
Prague
UPPER SILESIA
CZECHOSLOVAKIA
Munich
Vienna
Bratislava
BAY OF BISCAY
FRANCE
SWITZERLAND
AUSTRIA
TYROL
Klagenfurt
Sopron
Budapest
HUNGARY
TRANSYLVANIA
RUMANIA
BANAT
Bug R.
Dniester R.
Pruth R.
BESSARABIA
Odessa
Rhone R.
Po R.
Rijeka/
Fiume
YUGOSLAVIA
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
ADRIATIC SEA
DALMATIA
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ITALY
Rome
BULGARIA
Sofia
ALBANIA
THRACE
Constantinople
GREECE
TURKEY
SARDINIA
MEDITERRANEAN
SICILY
MALTA
(BR)
SEA
CRETE
RHODES
Dodecanese Islands
(Italy)
CYPRUS
AFRICA

1

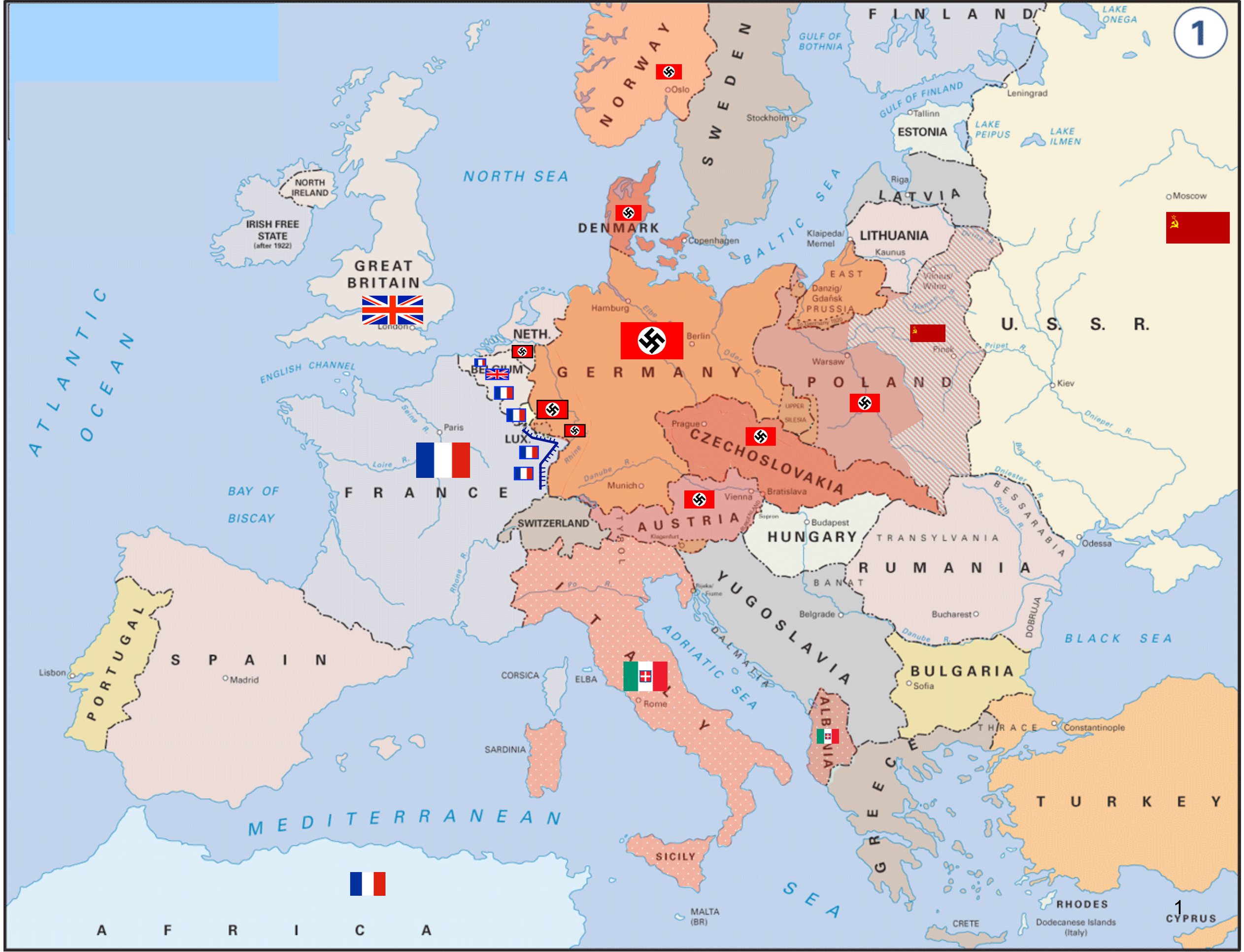
FINLAND
LAKE ONEGA
NORWAY
Oslo
SWEDEN
GULF OF BOTHNIA
Stockholm
GULF OF FINLAND
Leningrad
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
NORTH SEA
NORTH IRELAND
IRISH FREE STATE (after 1922)
GREAT BRITAIN
London
DENMARK
Copenhagen
BALTIC SEA
Riga
LATVIA
Moscow
Klaipeda/ Memel
LITHUANIA
Kaunus
EAST PRUSSIA
Danzig/ Gdańsk
Hamburg
Elbe
NETH.
Berlin
Oder R.
Vistula R.
Vilnius/ Wilno
Niemen R.
U. S. S. R.
Pripet R.
Pinsk
Warsaw
BELGIUM
GERMANY
POLAND
ENGLISH CHANNEL
Seine R.
Paris
LUX.
Rhine
Prague
UPPER SILESIA
CZECHOSLOVAKIA
Kiev
Dnieper R.
Loire R.
Danube R.
Munich
Vienna
Bratislava
Bug R.
Dniester R.
BESSARABIA
Pruth R.
BAY OF BISCAY
FRANCE
SWITZERLAND
AUSTRIA
TYROL
Sopron
Budapest
HUNGARY
TRANSYLVANIA
Odessa
Rhone R.
Po R.
Rijeka/ Fiume
YUGOSLAVIA
RUMANIA
BANAT
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ADRIATIC SEA
DALMATIA
ITALY
Rome
BULGARIA
Sofia
ALBANIA
THRACE
Constantinople
SARDINIA
GREECE
TURKEY
MEDITERRANEAN
SICILY
SEA
MALTA (BR)
CRETE
RHODES
Dodecanese Islands (Italy)
CYPRUS
AFRICA

1

FINLAND
LAKE ONEGA
NORWAY
Oslo
SWEDEN
GULF OF BOTHNIA
Stockholm
GULF OF FINLAND
Leningrad
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
NORTH SEA
NORTH IRELAND
IRISH FREE STATE (after 1922)
GREAT BRITAIN
London
DENMARK
Copenhagen
BALTIC SEA
Riga
LATVIA
Moscow
Klaipeda/ Memel
LITHUANIA
Kaunus
EAST PRUSSIA
Danzig/ Gdańsk
Hamburg
Elbe
NETH.
Berlin
Oder R.
GERMANY
Warsaw
POLAND
U. S. S. R.
Pinsk
Pripet R.
Vilnius/ Wilno
Niemen R.
Dniester R.
ATLANTIC OCEAN
ENGLISH CHANNEL
BELGIUM
Seine R.
Paris
LUX.
Rhine
Loire R.
Prague
UPPER SILESIA
CZECHOSLOVAKIA
Kiev
Dnieper R.
Bug R.
Danube R.
Munich
Vienna
Bratislava
BAY OF BISCAY
FRANCE
SWITZERLAND
AUSTRIA
Sopron
Budapest
HUNGARY
TRANSYLVANIA
RUMANIA
BESSARABIA
Odessa
Pruth R.
Rhone R.
TYROL
Po R.
Rijeka/ Fiume
YUGOSLAVIA
BANAT
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ITALY
Rome
ADRIATIC SEA
DALMATIA
BULGARIA
Sofia
SARDINIA
ALBANIA
THRACE
Constantinople
GREECE
TURKEY
MEDITERRANEAN
SICILY
SEA
RHODES
Dodecanese Islands (Italy)
CRETE
CYPRUS
MALTA (BR)
AFRICA

1

ATLANTIC OCEAN
NORTH SEA
NORWAY
Oslo
SWEDEN
Stockholm
GULF OF BOTHNIA
FINLAND
LAKE ONEGA
Leningrad
GULF OF FINLAND
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
Riga
LATVIA
BALTIC SEA
Moscow
NORTH IRELAND
IRISH FREE STATE
(after 1922)
GREAT BRITAIN
London
DENMARK
Copenhagen
Klaipeda/
Memel
LITHUANIA
Kaunus
EAST
PRUSSIA
Danzig/
Gdańsk
Hamburg
Elbe
NETH.
Berlin
Oder R.
GERMANY
Warsaw
POLAND
Vistula R.
Vilnius/
Wilno
Pripet R.
Pinsk
U. S. S. R.
ENGLISH CHANNEL
BELGIUM
Seine R.
Paris
LUX.
Rhine
Prague
UPPER SILESIA
CZECHOSLOVAKIA
Kiev
Dnieper R.
Loire R.
Danube R.
Munich
Vienna
Bratislava
Bug R.
Dniester R.
BESSARABIA
Pruth R.
BAY OF BISCAY
FRANCE
SWITZERLAND
AUSTRIA
Klagenfurt
TYROL
Sopron
Budapest
HUNGARY
TRANSYLVANIA
RUMANIA
Odessa
Rhone R.
Po R.
Rijeka/
Fiume
YUGOSLAVIA
BANAT
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ITALY
Rome
ADRIATIC SEA
DALMATIA
BULGARIA
Sofia
ALBANIA
THRACE
Constantinople
GREECE
TURKEY
SARDINIA
MEDITERRANEAN
SICILY
SEA
MALTA
(BR)
CRETE
RHODES
Dodecanese Islands
(Italy)
CYPRUS
AFRICA


1
FINLAND
LAKE ONEGA
GULF OF BOTHNIA
NORWAY
Oslo
SWEDEN
Stockholm
GULF OF FINLAND
Leningrad
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
NORTH SEA
NORTH IRELAND
IRISH FREE STATE (after 1922)
GREAT BRITAIN
London
DENMARK
Copenhagen
BALTIC SEA
Riga
LATVIA
Moscow
Klaipeda/ Memel
LITHUANIA
Kaunus
EAST PRUSSIA
Danzig/ Gdańsk
Hamburg
Elbe
Berlin
NETH.
BELGIUM
ENGLISH CHANNEL
GERMANY
Oder R.
Warsaw
POLAND
U. S. S. R.
Pripet R.
Pinsk
Kiev
Dnieper R.
Seine R.
Paris
LUX.
Rhine
Prague
UPPER SILESIA
CZECHOSLOVAKIA
Loire R.
Danube R.
Munich
Vienna
Bratislava
BAY OF BISCAY
FRANCE
SWITZERLAND
AUSTRIA
Sopron
Budapest
HUNGARY
TRANSYLVANIA
RUMANIA
BESSARABIA
Odessa
Rhone R.
TYROL
Po R.
Rijeka/ Fiume
YUGOSLAVIA
BANAT
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ITALY
Rome
ADRIATIC SEA
DALMATIA
BULGARIA
Sofia
ALBANIA
THRACE
Constantinople
SARDINIA
GREECE
TURKEY
MEDITERRANEAN
SICILY
SEA
MALTA (BR)
CRETE
RHODES
Dodecanese Islands (Italy)
CYPRUS
AFRICA
ATLANTIC OCEAN

1

NORWAY
Oslo
SWEDEN
Stockholm
FINLAND
LAKE ONEGA
GULF OF BOTHNIA
GULF OF FINLAND
Leningrad
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
Riga
LATVIA
Moscow
NORTH SEA
NORTH IRELAND
IRISH FREE STATE (after 1922)
GREAT BRITAIN
London
DENMARK
Copenhagen
BALTIC SEA
Klaipeda/ Memel
LITHUANIA
Kaunus
EAST PRUSSIA
Danzig/ Gdańsk
Hamburg
Elbe
NETH.
BELGIUM
Berlin
GERMANY
Oder R.
Warsaw
POLAND
Pinsk
Pripet R.
U. S. S. R.
Kiev
Dnieper R.
ENGLISH CHANNEL
Seine R.
Paris
LUX.
Rhine
Loire R.
Prague
UPPER SILESIA
CZECHOSLOVAKIA
Danube R.
Munich
Vienna
Bratislava
AUSTRIA
SWITZERLAND
Budapest
HUNGARY
TRANSYLVANIA
RUMANIA
BANAT
Bug R.
Dniester R.
BESSARABIA
Odessa
Pruth R.
Rhone R.
Po R.
Rijeka/ Fiume
YUGOSLAVIA
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
ATLANTIC OCEAN
BAY OF BISCAY
FRANCE
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ITALY
Rome
ADRIATIC SEA
DALMATIA
BULGARIA
Sofia
THRACE
Constantinople
ALBANIA
GREECE
TURKEY
SARDINIA
MEDITERRANEAN
SICILY
MALTA (BR)
SEA
CRETE
RHODES
Dodecanese Islands (Italy)
CYPRUS
AFRICA

1

NORWAY
Oslo
SWEDEN
Stockholm
GULF OF BOTHNIA
FINLAND
LAKE ONEGA
Leningrad
GULF OF FINLAND
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
Riga
LATVIA
Moscow
NORTH SEA
NORTH IRELAND
IRISH FREE STATE (after 1922)
GREAT BRITAIN
London
DENMARK
Copenhagen
BALTIC SEA
Klaipeda/ Memel
LITHUANIA
Kaunus
EAST PRUSSIA
Danzig/ Gdańsk
Hamburg
Elbe
NETH.
Berlin
GERMANY
Oder R.
Warsaw
POLAND
Pinsk
Pripet R.
U. S. S. R.
Kiev
Dnieper R.
ATLANTIC OCEAN
ENGLISH CHANNEL
BELGIUM
SAAR
LUX.
Seine R.
Paris
Loire R.
Rhine R.
Prague
UPPER SILESIA
CZECHOSLOVAKIA
Danube R.
Munich
Vienna
Bratislava
AUSTRIA
SWITZERLAND
Budapest
HUNGARY
TRANSYLVANIA
RUMANIA
BESSARABIA
Pruth R.
Odessa
Dniester R.
Bug R.
BAY OF BISCAY
FRANCE
TYROL
Po R.
Rijeka/ Fiume
YUGOSLAVIA
BANAT
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ITALY
Rome
ADRIATIC SEA
DALMATIA
BULGARIA
Sofia
ALBANIA
THRACE
Constantinople
GREECE
TURKEY
SARDINIA
MEDITERRANEAN
SICILY
MALTA (BR)
SEA
CRETE
RHODES
Dodecanese Islands (Italy)
CYPRUS
AFRICA

1

NORWAY
Oslo
SWEDEN
Stockholm
GULF OF BOTHNIA
FINLAND
LAKE ONEGA
Leningrad
GULF OF FINLAND
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
Riga
LATVIA
Moscow
NORTH SEA
NORTH IRELAND
IRISH FREE STATE
(after 1922)
GREAT BRITAIN
London
DENMARK
Copenhagen
BALTIC SEA
Klaipeda/
Memel
LITHUANIA
Kaunus
EAST
PRUSSIA
Danzig/
Gdańsk
Hamburg
Elbe
Berlin
NETH.
BELGIUM
GERMANY
Oder R.
Warsaw
POLAND
U. S. S. R.
Pripet R.
Pinsk
Kiev
Dnieper R.
ENGLISH CHANNEL
Seine R.
Paris
SAAR
LUX.
Rhine R.
Prague
UPPER SILESIA
CZECHOSLOVAKIA
Danube R.
Munich
Vienna
Bratislava
Loire R.
FRANCE
BAY OF BISCAY
SWITZERLAND
AUSTRIA
TYROL
Sopron
Budapest
HUNGARY
TRANSYLVANIA
BESSARABIA
Dniester R.
Odessa
RUMANIA
BANAT
Po R.
Rijeka/
Fiume
YUGOSLAVIA
Belgrade
Bucharest
DOBRUJA
Danube R.
BLACK SEA
ADRIATIC SEA
DALMATIA
BULGARIA
Sofia
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
Rome
ITALY
ALBANIA
THRACE
Constantinople
GREECE
TURKEY
SARDINIA
MEDITERRANEAN
SICILY
SEA
MALTA
(BR)
CRETE
RHODES
Dodecanese Islands
(Italy)
CYPRUS
AFRICA

1

NORWAY
Oslo
SWEDEN
Stockholm
GULF OF BOTHNIA
FINLAND
LAKE ONEGA
Leningrad
GULF OF FINLAND
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
Riga
LATVIA
Moscow
NORTH SEA
NORTH IRELAND
IRISH FREE STATE
(after 1922)
GREAT BRITAIN
DENMARK
Copenhagen
BALTIC SEA
Klaipeda/
Memel
LITHUANIA
Kaunus
EAST
PRUSSIA
Danzig/
Gdańsk
Hamburg
Elbe
Berlin
NETH.
BELGIUM
GERMANY
Oder R.
Warsaw
POLAND
U. S. S. R.
Pinsk
Pripet R.
Kiev
Dnieper R.
ENGLISH CHANNEL
SAAR
LUX.
Seine R.
Paris
Loire R.
Rhine R.
Prague
UPPER SILESIA
CZECHOSLOVAKIA
Danube R.
Munich
Vienna
Bratislava
AUSTRIA
SWITZERLAND
TYROL
Sopron
Budapest
HUNGARY
TRANSYLVANIA
BESSARABIA
Dniester R.
Odessa
BAY OF BISCAY
FRANCE
Po R.
Rijeka/
Fiume
YUGOSLAVIA
BANAT
Belgrade
RUMANIA
Bucharest
DOBRUJA
BLACK SEA
ATLANTIC OCEAN
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ITALY
Rome
ADRIATIC SEA
DALMATIA
BULGARIA
Sofia
ALBANIA
THRACE
Constantinople
GREECE
TURKEY
SARDINIA
MEDITERRANEAN
SICILY
MALTA
(BR)
SEA
CRETE
RHODES
Dodecanese Islands
(Italy)
CYPRUS
AFRICA

1

NORWAY
Oslo
SWEDEN
Stockholm
GULF OF BOTHNIA
FINLAND
LAKE ONEGA
Leningrad
GULF OF FINLAND
Tallinn
ESTONIA
LAKE PEIPUS
LAKE ILMEN
Riga
LATVIA
Moscow
NORTH SEA
NORTH IRELAND
IRISH FREE STATE
(after 1922)
DENMARK
Copenhagen
BALTIC SEA
Klaipeda/
Memel
LITHUANIA
Kaunus
GREAT BRITAIN
EAST
PRUSSIA
Danzig/
Gdańsk
Hamburg
Elbe
NETH.
Berlin
U. S. S. R.
Vilnius/
Wilno
Pinsk
Pripet R.
ENGLISH CHANNEL
BELGIUM
GERMANY
Oder R.
Warsaw
POLAND
Kiev
SAAR
UPPER
SILESIA
Seine R.
Paris
LUX.
Prague
Dnieper R.
Rhine R.
CZECHOSLOVAKIA
Loire R.
Danube R.
Bug R.
Dniester R.
Munich
Vienna
Bratislava
BESSARABIA
Pruth R.
BAY OF
BISCAY
FRANCE
SWITZERLAND
AUSTRIA
TYROL
Sopron
Budapest
HUNGARY
TRANSYLVANIA
Odessa
Klagenfurt
Po R.
Rijeka/
Fiume
YUGOSLAVIA
BANAT
RUMANIA
Belgrade
Bucharest
DOBRUJA
Danube R.
PORTUGAL
SPAIN
Lisbon
Madrid
CORSICA
ELBA
ADRIATIC SEA
DALMATIA
BULGARIA
Sofia
BLACK SEA
Rome
ITALY
ALBANIA
THRACE
Constantinople
GREECE
TURKEY
SARDINIA
MEDITERRANEAN
SICILY
SEA
MALTA
(BR)
CRETE
RHODES
Dodecanese Islands
(Italy)
CYPRUS
AFRICA

Battle of the North Atlantic

Winston Churchill

Winston Churchill, June 1940

151

22.

~~The~~ battle of France is over

What General Weygand calls 'the battle of France' is over. The battle of Britain is about to begin. Upon this battle depends the survival of Christian civilisation. Upon it depends our own British life and the long continuity of our institutions, and our Empire. The whole fury and might of the enemy must very soon be turned on us. Hitler knows that ~~if~~ he will have to break us in this Island, or lose the war. If we can stand up to him, all Europe may be ~~liberated~~ freed, and the life of the world may move forward into broad and sunlit uplands. But if we fail, then the whole world, including the United States, and all that we have known and cared for, will sink into the abyss of a new Dark Age made more sinister & perhaps more protracted by the lights of perverted Science. Let us therefore brace ourselves to our duty, and so bear ourselves that if the British Empire and Commonwealth lasts for a thousand years, men will still say, 'This was their ~~my~~ finest hour.'

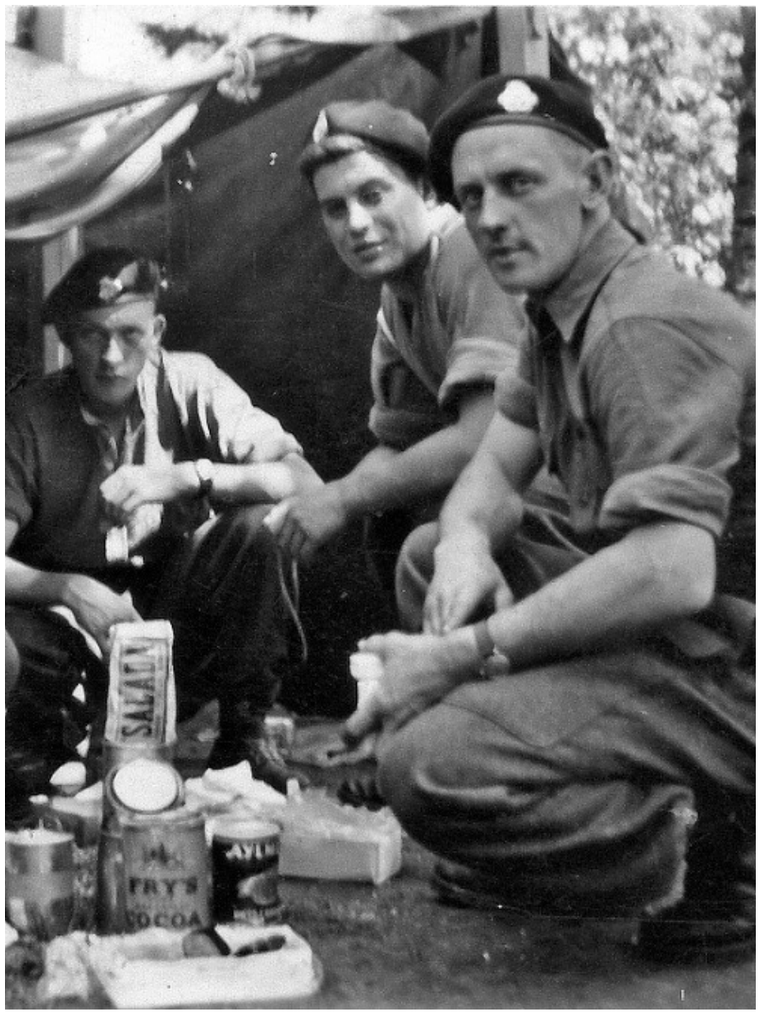
Winston Churchill, June 1940

151

22.

~~The~~ battle of France is over

What General Weygand calls 'the battle of France' is over. The battle of Britain is about to begin. Upon this battle depends the survival of Christian civilisation. Upon it depends our own British life and the long continuity of our institutions, and our Empire. The whole fury and might of the enemy must very soon be turned on us. Hitler knows that ~~if~~ he will have to break us in this Island, or lose the war. If we can stand up to him, all Europe may be ~~liberated~~ freed, and the life of the world may move forward into broad and sunlit uplands. But if we fail, then the whole world, including the United States, and all that we have known and cared for, will sink into the abyss of a new Dark Age made more sinister & perhaps more protracted by the lights of perverted Science. Let us therefore brace ourselves to our duty, and so bear ourselves that if the British Empire and Commonwealth lasts for a thousand years, men will still say, 'This was their ~~my~~ finest hour.'



Evo Furino (8th Canadian (NB) Hussars), Gerald Merchant (HMCS St Croix), Frank Merchant (pilot, RCAF)

Ottawa Lists 146 as Lost In Sinking of Destroyer

Ottawa, Oct. 1.—(CP)—Following is the Royal Canadian Navy's official casualty list in the sinking of the destroyer St. Croix, containing the names of 146 of those missing:

MISSING

Missing on war service, due to enemy action, while serving on convoy duty in the Atlantic:

Officers

DeFreitas, Percival Francis Mayow, Lt.-Cmdr., Oak Bay, Victoria.

Dobson, Andrew Hedley, D.S.C., Lt.-Cmdr., Halifax.

Gallagher, John Fraser, Lieut., St. John's, Nfld.

King, William Lyon Mackenzie, Surgeon Lt., Bedford, N.S.

Major Paul Simon, Lt.-Cmdr., Mount Royal, Que.

Page, William Leonard, Sub-Lt., Regina.

Porter, Robert Noel Timothy, Lieut., Vancouver.

Ridge, Derrick, Lieut. (engineer), Hampstead, Montreal.

Ross, Charles Alexander, Lieut., Halifax.

Wright, George Bucknam, Lieut., Winnipeg.

Ratings

Adamson, Selwyn Arthur, Leading Coder, Port Credit, Ont.

Armstrong, Hugh, Leading Stoker, Glengrove P.O., Ont.

Armstrong, William Morrison, Mechanician, Kamloops, B.C.

Bailey, Morris Benjamin, O.S., Claresholm, Alta.

Badour, William Rufus, A.B., Kingston, Ont.

Barnhart, Gordon Franklin, Stoker, Fort Erie, Ont.

Barriault, Joseph Ernest, A.B., Wellington, P.E.I.

Barwis, William Donald, A.B., Nelson, B.C.

Bass, George Othoe, Leading Stoker, Cardinal, Ont.

Bedford, Andrew Lawrence, A.B., South Porcupine, Ont.

Bell, Joseph Griffiths, Coder, Sarnia, Ont.

Berrisford, Gordon Harold, O.S., Selkirk, Man.

Booth, Robert Gordon, O.S., Saskatoon.

Botham, Robert John, A.B., Plato, Sask.

Bottomley, Stanley Rhodes, A.B., Edmonton.

Bowser, Fred Douglas, Supply P.O., Saint John, N.B.

Boyle, Thomas, Sigmn., Toronto.

Brennan, James Edward Stewart, Engine Room Artificer, Kingston, N.S.

Brett, Walter Bretwalda, Engine Room Artificer, Regina.

Brockman, Stanley Bertram, O.S., Burnaby, B.C.

Bruce, William, L.S., Dundee, Scotland.

Burgess, Ira Urban, A.B., Southwest Port Mouton, N.S.

Butterfield, Thomas William James, E.R.A., Vancouver.

Bydwell, Leslie Wellington, E.R.A., Saint John, N.B.

Carignan, Joseph Jean Baptiste, Stoker, St. Angele De Laval, Que.

Craig, Frederick Thomas, Leading Stoker, Halifax.

Dean, Alfred Costello, Leading Stoker, Morton, Ont.

Deeks, William Richard, O.S., Vernon, B.C.

DeGeer, Carl Gerhard Ludvig, A.B., Saint John, N.B.

Demers, Honore Wilfrid Joseph, Electrical Artificer, Melrose Highlands, Mass.

Denneny, James Gordon, Telegraphist, Montreal.

Des Brisay, Gordon Montgomery, Ordinary Signalman, Vancouver.

Deschamp, Winslow Alfonzo, A.B., Shelburne, N.S.

Dinner, Lorne, Supply Assistant, Montreal.

Dowell, Charles Brannagan, O.S., Windsor, Ont.

Edmonds, John Celestine, Stoker P.O., St. John's, Nfld.

Evans, Llewellyn, A.B., Peterboro', Ont.

Evans, William Leo, Stoker, Point St. Charles, Que.

Forbes, Garry Ferguson, A.B., Port Arthur.

Fulton, Henry, Stoker, St. John's, Nfld.

Good, James Hamilton, Ordinary Telegraphist, Raith, Ont.

Gordon, Cyril James Albert, leading sick berth attendant, Regina.

Goreham, Leslie Mackenzie, A.B., Ottawa.

Goulet, Joseph Philippe Lionel, Steward, St. Evariste, Que.

Grandy, Charles Reginald, L.S., Grand Bank, Nfld.

Grant, Ronald Earl, A.B., Toronto.

Greggio, William Alexander, Ordinary Telegraphist, Humberstone, Ont.

Grenon, Albert Joseph, A.B., Somerset, Man.

Guay, Vincent Elwood, A.B., Corbyville, Ont.

Hann, Peter Martin Joseph, P.O., Steward, Halifax.

Hillier, George Abraham, A.B., Lamalin, Nfld.

Hodgson, Albert John, Stoker P.O., Blue Ridge, Alta.

Hutton, Jack, Leading Sigmn., Vancouver.

Kidson, Weldon Alexander, Leading Stoker, Victoria.

Lanrigan, Frederick, Stoker (1st class), Toronto.

Lane, Arthur Douglas, A.B., Windsor, Ont.

Lanktree, William, Leading Stoker, Port Arthur.

Lillyman, Raymond Frederick, Ordinary Telegraphist, Winnipeg.

Locke, Oscar James, Stoker, Ansonville, Ont.

Long, Ronald James, A.B., Windsor, Ont.

Lopuck, Antoni, Leading Stoker, East Transcona, Man.

Luchan, Edmund Victor, Stoker, Schumacher, Ont.

Marmon, Thomas, L.S., Verdun, Que.

Melnitsky, Theodore, Cook (seamen's), St. Lambert, Que.

Meloche, Joseph Orphee, Telegraphist, Montreal.

Mercham, Joseph Gerald, Electrical Artificer, Sturgeon Falls, Ont.

McKeown, John Edward, Leading Stoker, Toronto.

McKinney, Lawrence Albert, A.B., Montreal.

McKinnon, Alexander, Chief Stoker, Rosemount, Montreal.

McMaster, Alexander Peter, L.S., Toronto.

McNeney, James Robert, Yeoman of Signals, New Westminster, B.C.

McPherson, Clifford Albert, A.B., Tilbury, Ont.

Newhouse, John Stanley, Leading Telegraphist, Calgary.

Newstead, Kenneth Edwin, Cook (seamen's), Toronto.

O'Connor, Thomas Patrick, Stoker, P.O., Montreal.

Osborne, Robert James, Leading Stoker, Montreal.

Parker, Robert Borden, Stoker, P.O., Halifax.

Parnell, George Frederick, E.R.A. (4th class), Hoey, Sask.

Pasquantonio, Ralph Joseph, Leading Stoker, A1228, R.C.N.R., Mrs. Elisa Currcio (sister), Port Colborne, Ont.

Pastorek, John O.S., Hammond, B.C.

Payne, Sydney Rudolph, Stoker (1st class), Fort William.

Pidlaski, Nicholas, O.S., Winnipeg.

Pook, William Frederick, Assistant Cook (seamen's), Seattle, Wash.

Priske, Sydney Robert, P.O., Port Arthur.

Prosch, Joseph, Leading Stoker, West Hartlepool, Eng.

Pudney, William Sydney David, Sigmn., Toronto.

Reid, Edward Roddick, A.B., Brandon.

Richardson, Jasper James, Ordinary Coder, Brandon, Man.

Riecke, Harry Carl, P.O., Montreal.

Rigby, Robert Charles, Ordinary Telegrapher, Sarnia, Ont.

Rising, Jack Humphrey, Ordnance Artificer, Moncton, N.B.

Robertson, Theodore Maxwell, Stoker P.O., Halifax.

Roder, William Norman, Stoker (2nd class), Arkona, Ont.

Rowell, David Bayford, A.B., V8359, R.C.N.V.A., Miss Sulta Rowell (sister), 208 Maple avenue, Hamilton.

Russ, Frank Abseth, P.O., Telegraphist, Toronto.

Rosso, Anthony Francis, L.S., Montreal.

Savage, Francis Herbert, A.B., Ashton, Ont.

Scudamore, Frederick Herbert, Leading Stoker, Mimico, Ont.

Simard, Joseph Hidola Michel, A.B., Quebec.

Sims, Hartman William, L.S., London, Ont.

Smith, Joseph Walter, Leading Cook (seamen's), Emerald Junction, P.E.I.

Stephenson, Francis Woodrow, P.O., Montreal.

Stephenson, Carmen Ernest, L.S., Montreal.

Stevenson, William Lyle, O.S., Truro, N.S.

Strange, William Robert, Stoker (1st class), Edmonton.

Tagg, James, E.R.A., Scotland.

Terry, John Malcolm, A.B., Toronto.

Thicke, Charles Frederick, A.B., Wellington, B.C.

Tipe, Carl, Stoker (1st class), Toronto.

Turner, Alexander, A.B., Toronto.

Urquhart, Donald LeRoy, A.B., Taymouth, N.B.

VanSickle, Harold Allen, O.S., Swan River, Man.

Vey, John Wellington, A.B., Sainte John, N.B.

Walker, George Edward, A.B., Montreal.

Walsh, Patrick Douglas, Stoker, Jasmin, Sask.

Warner, Gordineer Wendell, Stoker (1st class), Phillipsville, Ont.

Watson, Horace William, C.P.O., Halifax.

Whitaker, Ronald, Steward, Attercliff, Sheffield, Yorkshire, Eng.

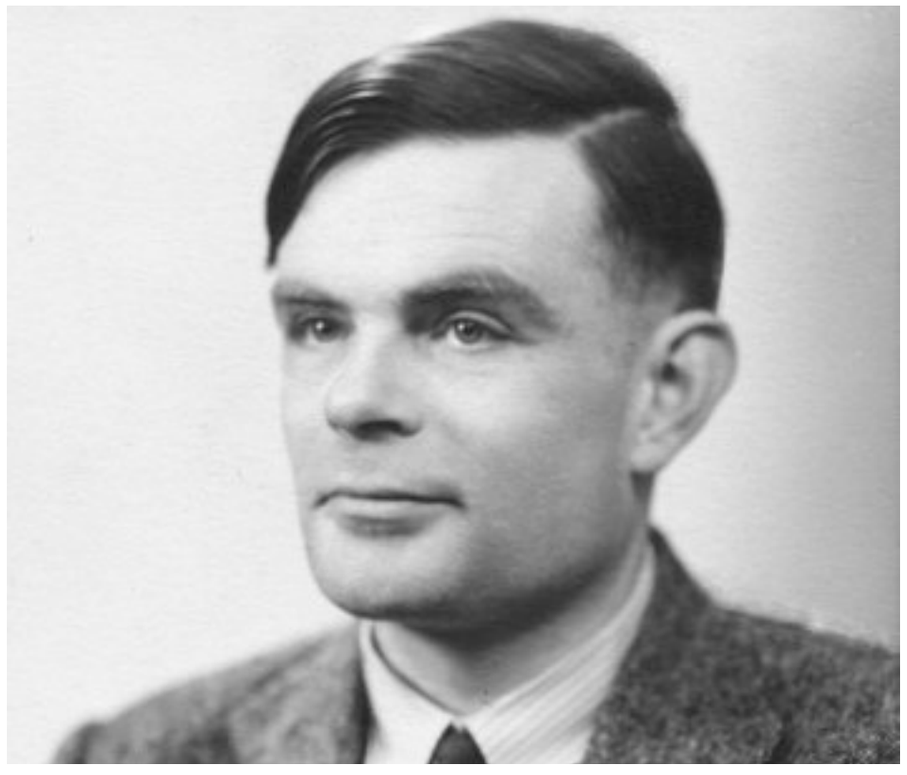
White, Robert Edwin, A.B., Calgary.

Winch, Wilmer James, Leading Stoker, Wiarton, Ont.

Wyckoff, Gordon Colquhoun, L.S., Calgary.

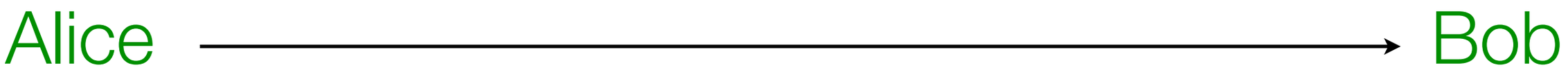
149
WAR
EUROPEAN
1939
CANADA
NAVY
DESTROYER
ST.
CROIX

Mercham, Joseph Gerald, Electrical Artificer, Sturgeon Falls, Ont.

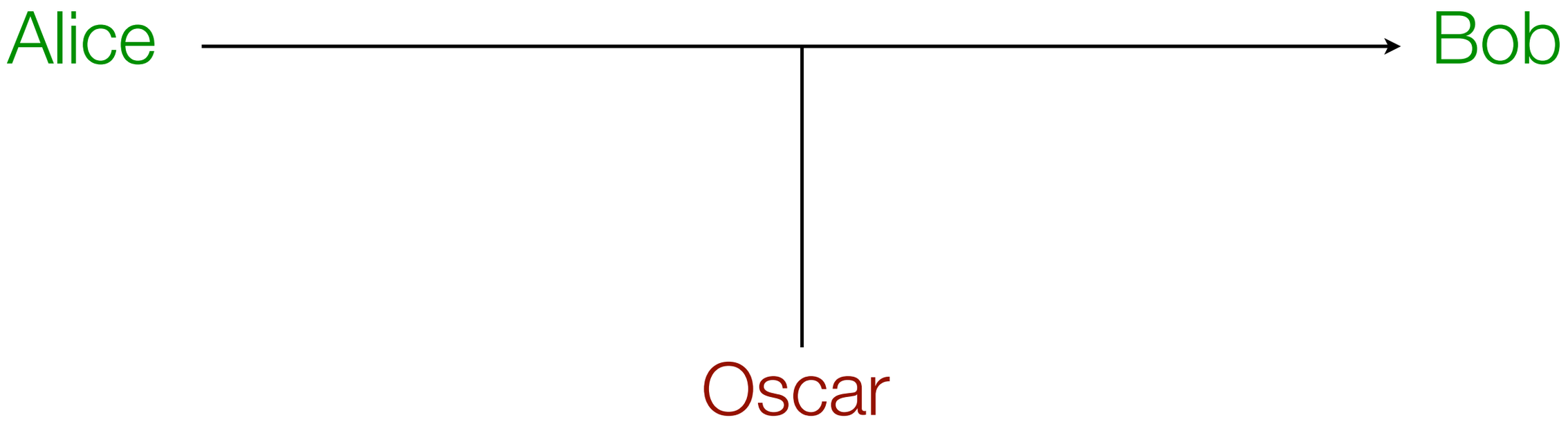


Enigma machine, Bletchley Park (centre for British decryption efforts in WW II), Alan Turing

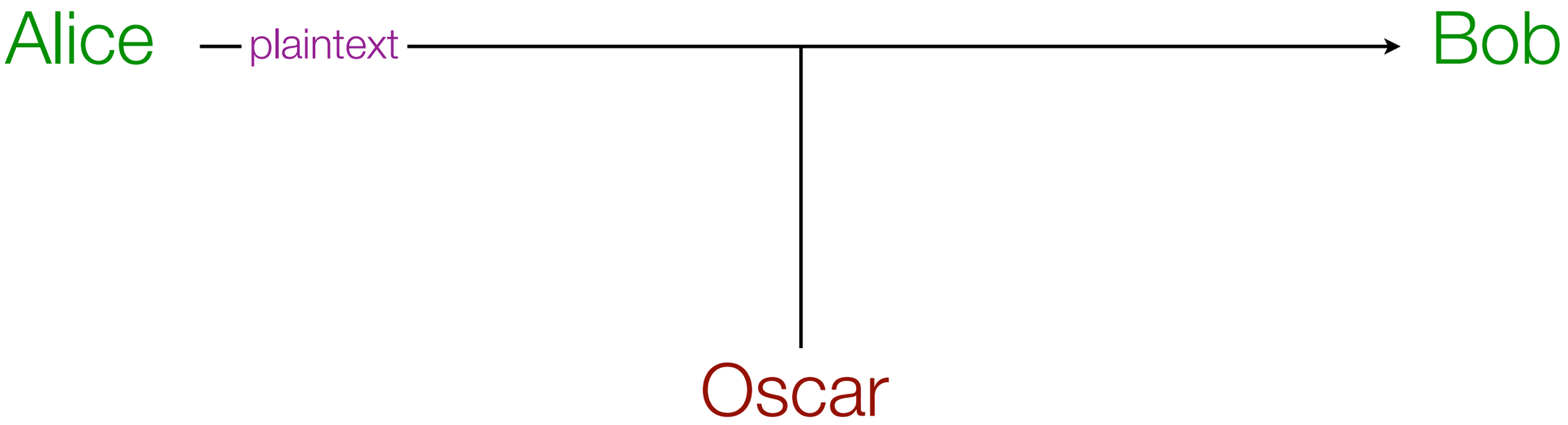
Cryptography



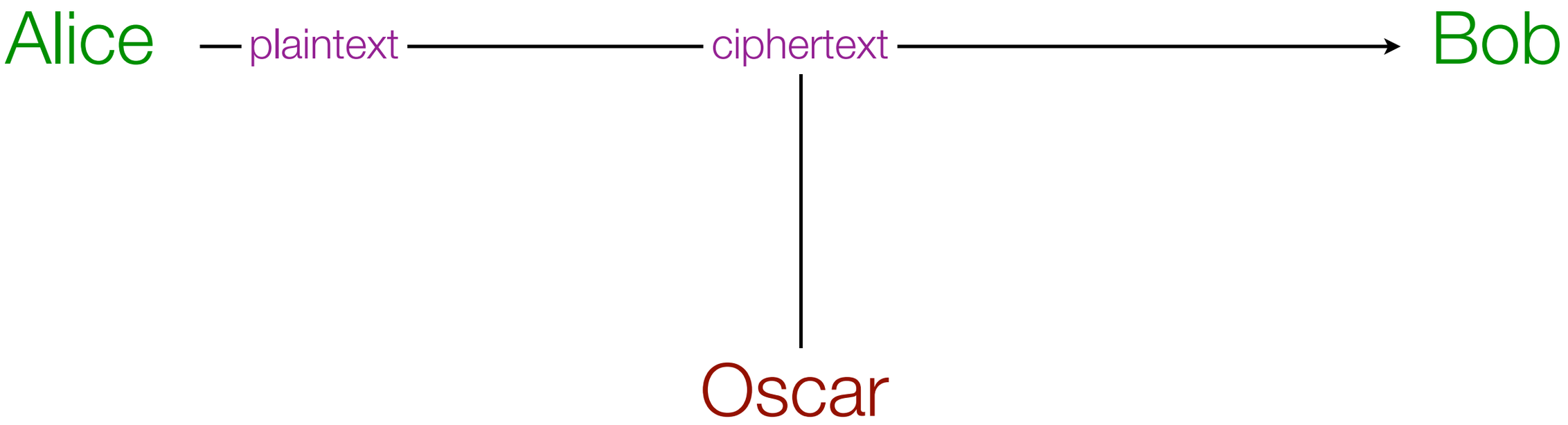
Cryptography



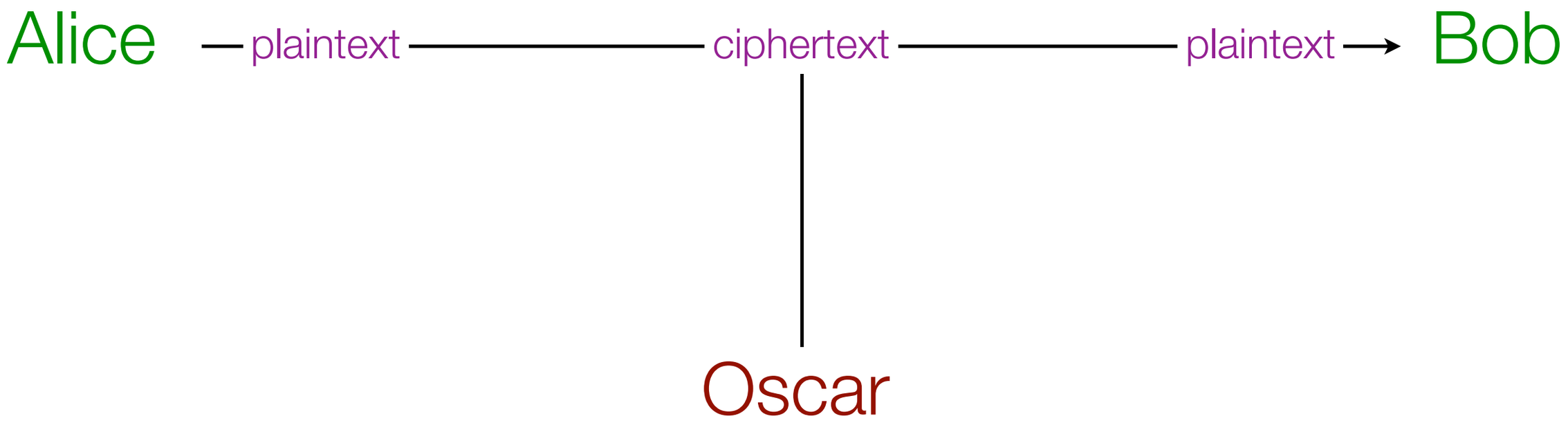
Cryptography



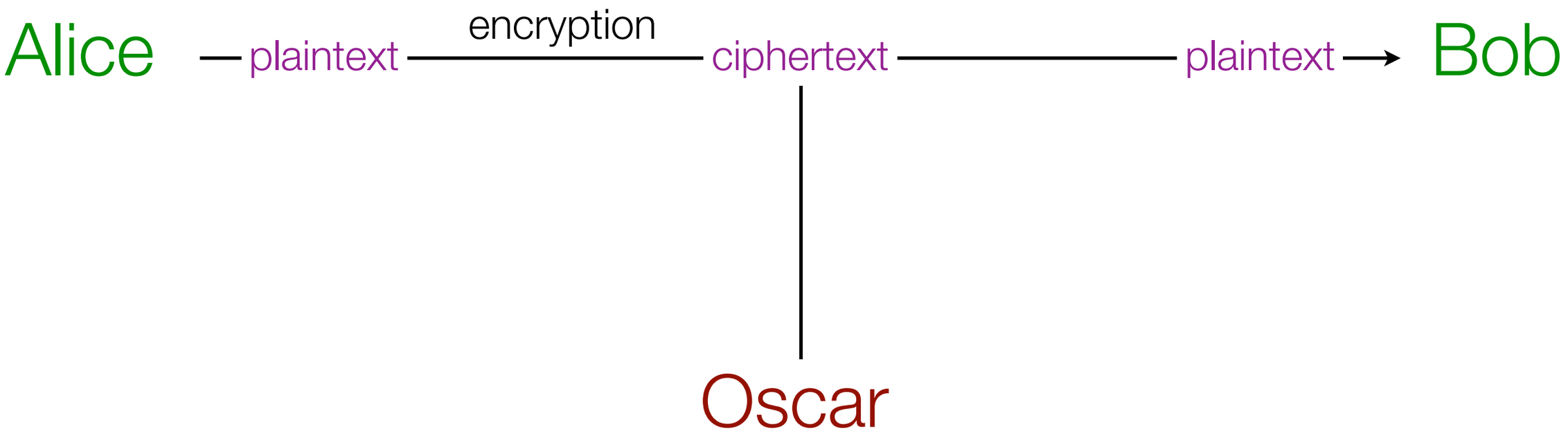
Cryptography



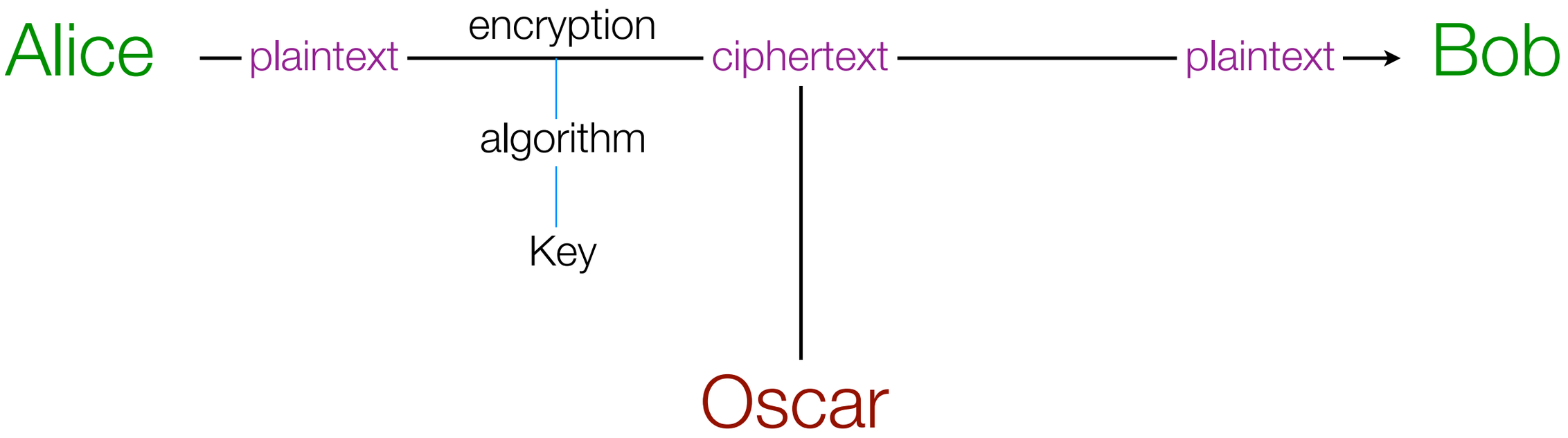
Cryptography



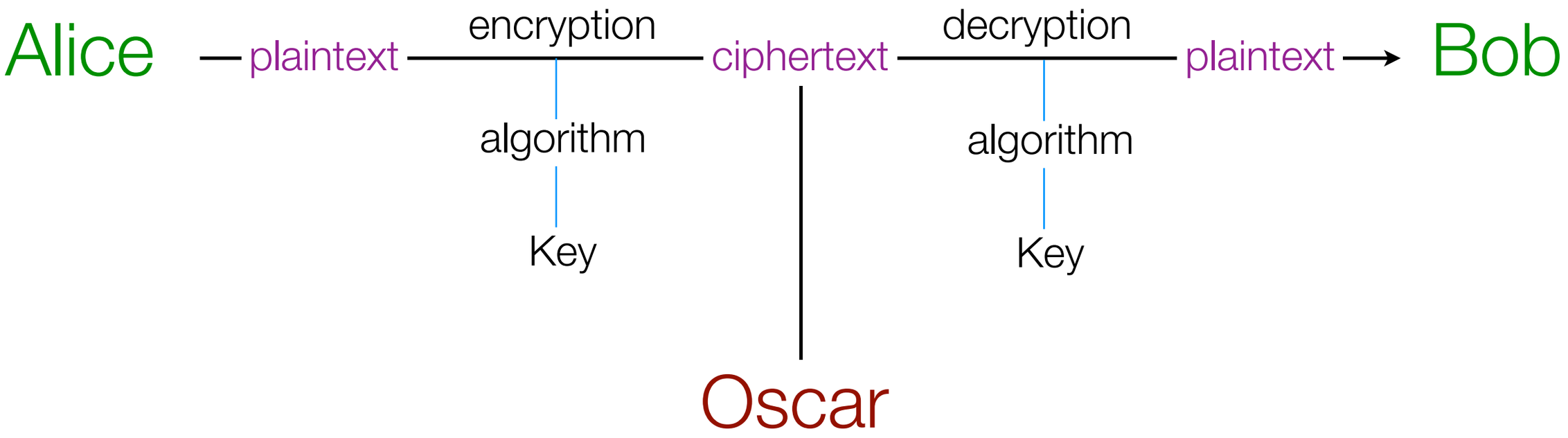
Cryptography



Cryptography



Cryptography



Substitution Cipher

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

Substitution Cipher

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

Plaintext

```
We shall fight on the beaches,
We shall fight on the landing grounds,
We shall fight in the fields and in the streets,
We shall fight in the hills;
We shall never surrender
```

Substitution Cipher

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

Plaintext

```
We shall fight on the beaches,
We shall fight on the landing grounds,
We shall fight in the fields and in the streets,
We shall fight in the hills;
We shall never surrender
```

Ciphertext

Substitution Cipher

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

Plaintext

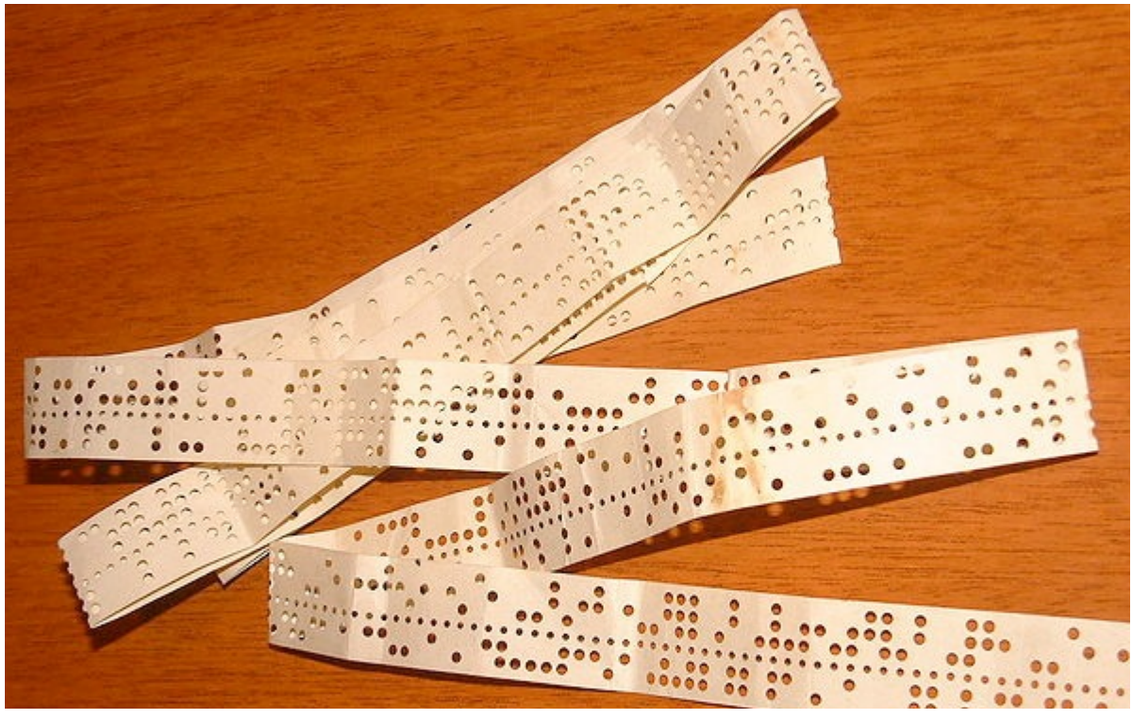
```
We shall fight on the beaches,
We shall fight on the landing grounds,
We shall fight in the fields and in the streets,
We shall fight in the hills;
We shall never surrender
```

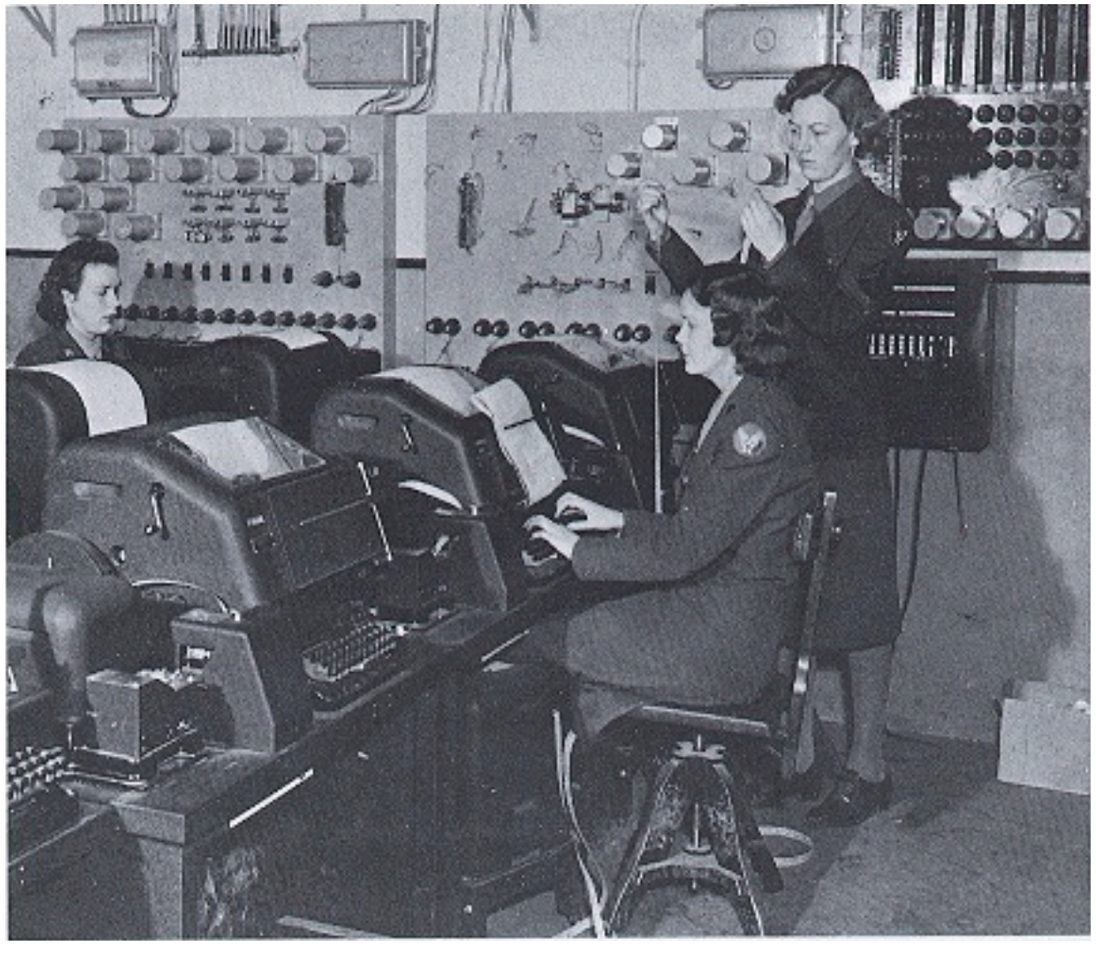
Ciphertext

```
SB PVQXX ETRVH IZ HVB MBQWVBP
SB PVQXX ETRVH IZ HVB XQZNTZR RKIAZNP
SB PVQXX ETRVH TZ HVB ETBXNP QZN TZ HVB PHKBBHP
SB PVQXX ETRVH TZ HVB VTXXP
SB PVQXX ZBGBK PAKKBZNBK
```

Fish

- a new cryptographic system, more sophisticated than Enigma
- teletype





Fish

Fish

- Allies did not possess the device or have any knowledge of the architecture of the machine

Fish

- Allies did not possess the device or have any knowledge of the architecture of the machine
- carried highest level of intelligence, encrypted communication between German High Command and Army Group headquarters in the field

Fish

- Allies did not possess the device or have any knowledge of the architecture of the machine
- carried highest level of intelligence, encrypted communication between German High Command and Army Group headquarters in the field
- Tutte was assigned to Fish in October 1941

Tutte has problems

Tutte has problems

- Inexperienced, 24 year old university student

Tutte has problems

- Inexperienced, 24 year old university student
- No information on what the machine looked like

Tutte has problems

- Inexperienced, 24 year old university student
- No information on what the machine looked like
- Doesn’t speak German

Tutte has problems

- Inexperienced, 24 year old university student
- No information on what the machine looked like
- Doesn’t speak German
- Doesn’t know what the contents are about

Tutte has problems

- Inexperienced, 24 year old university student
- No information on what the machine looked like
- Doesn’t speak German
- Doesn’t know what the contents are about
- Based on radio intercepts that may introduce errors

Tutte has problems

- Inexperienced, 24 year old university student
- No information on what the machine looked like
- Doesn’t speak German
- Doesn’t know what the contents are about
- Based on radio intercepts that may introduce errors
- No computing capabilities other than pencil and paper

Tutte has more problems

Tutte has more problems

- Axis has the advantage on the battlefield so pressure to break the code is intense. USSR invaded in 1941 and suffers huge losses.

Tutte has more problems

- Axis has the advantage on the battlefield so pressure to break the code is intense. USSR invaded in 1941 and suffers huge losses.
- Even if he can discover what the encryption device looks like, he must still decipher individual messages

Tutte has more problems

- Axis has the advantage on the battlefield so pressure to break the code is intense. USSR invaded in 1941 and suffers huge losses.
- Even if he can discover what the encryption device looks like, he must still decipher individual messages
- There is no wikipedia or electronic library

Tutte has more problems

- Axis has the advantage on the battlefield so pressure to break the code is intense. USSR invaded in 1941 and suffers huge losses.
- Even if he can discover what the encryption device looks like, he must still decipher individual messages
- There is no wikipedia or electronic library
- He cannot talk about the problem with others outside his group

Tutte's Success

Tutte's Success

- Because of a German operator error, Col John Tiltman of Bletchley Park was able to decipher a message of roughly 4000 characters

Tutte's Success

- Because of a German operator error, Col John Tiltman of Bletchley Park was able to decipher a message of roughly 4000 characters
- Three months later, no progress had been made in understanding the structure of Fish

Tutte’s Success

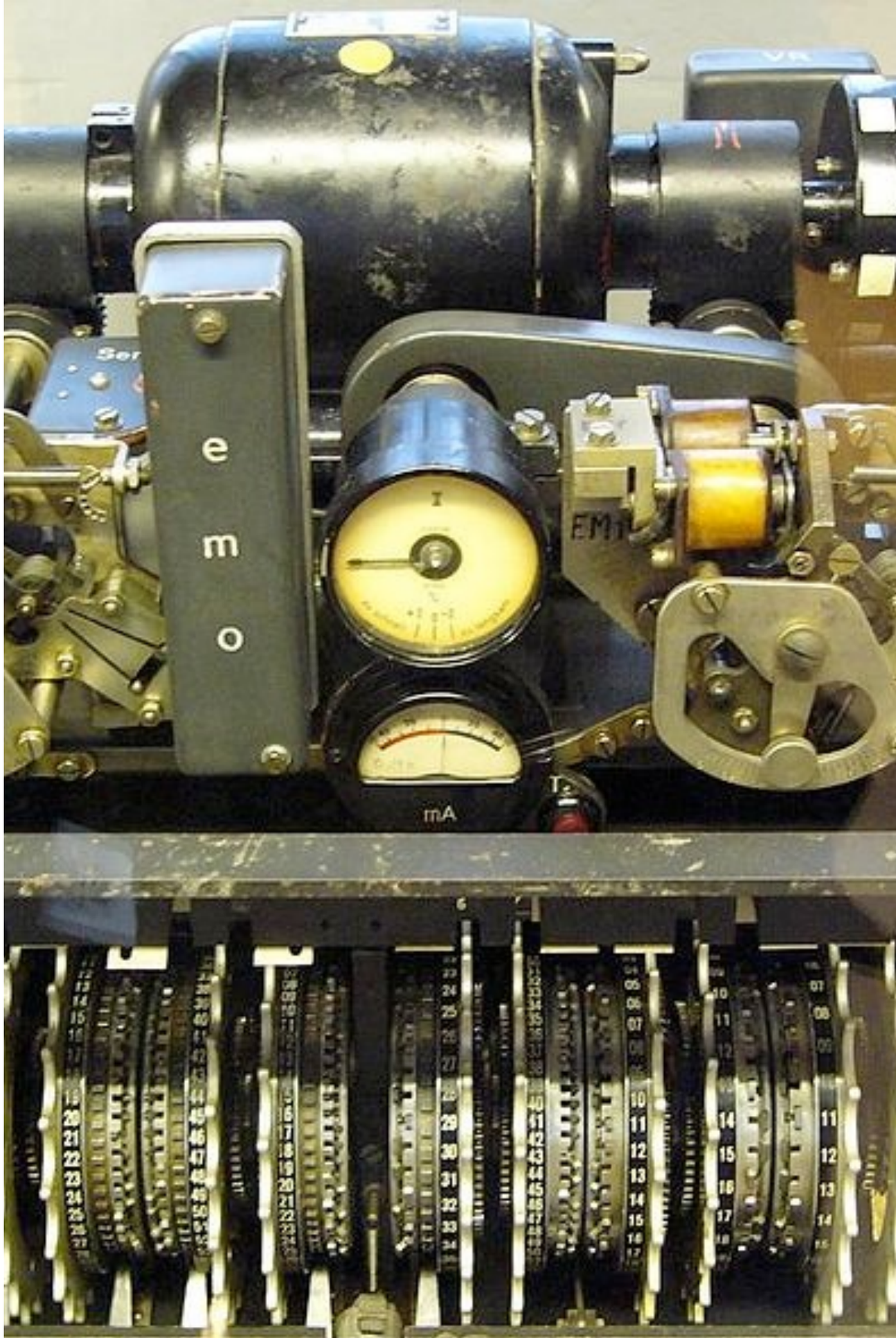
- Because of a German operator error, Col John Tiltman of Bletchley Park was able to decipher a message of roughly 4000 characters
- Three months later, no progress had been made in understanding the structure of Fish
- Head of the Research Section, Major Gerry Morgan, says to Tutte “See what you can do with this.”

Tutte's Success

- Because of a German operator error, Col John Tiltman of Bletchley Park was able to decipher a message of roughly 4000 characters
- Three months later, no progress had been made in understanding the structure of Fish
- Head of the Research Section, Major Gerry Morgan, says to Tutte "See what you can do with this."
- Using only this message and working by hand with the teletype codes (not the letters of the alphabet) Tutte was able to identify the internal structure and behaviour of the encryption machine

Lorenz Schlusselzusatz 40

- 12 wheels all with a different number of teeth
- some with irregular movements
- arranged in three groups
- using 5 bitstreams



How dramatic was this?

- “the greatest intellectual feat of the whole war”, Tony Sales quoted in “Colossal Adventures”, New Scientist, 10 May 1997
- “only six people outside the Lorenz codebreaking team ever understood the significance”, Tony Sales

Attacks on Current Traffic

Attacks on Current Traffic

- Lorenz Machine was understood but that still left an enormously difficult task in deciphering particular messages

Attacks on Current Traffic

- Lorenz Machine was understood but that still left an enormously difficult task in deciphering particular messages
- Some early successes but these stopped when the Germans improved their protocols

Attacks on Current Traffic

- Lorenz Machine was understood but that still left an enormously difficult task in deciphering particular messages
- Some early successes but these stopped when the Germans improved their protocols
- Tutte devised the “statistical method” that would work against Fish but...

Attacks on Current Traffic

- Lorenz Machine was understood but that still left an enormously difficult task in deciphering particular messages
- Some early successes but these stopped when the Germans improved their protocols
- Tutte devised the “statistical method” that would work against Fish but...
- What was needed was an analysis of each message that was thousands of times faster than computations by hand

Attacks on Current Traffic

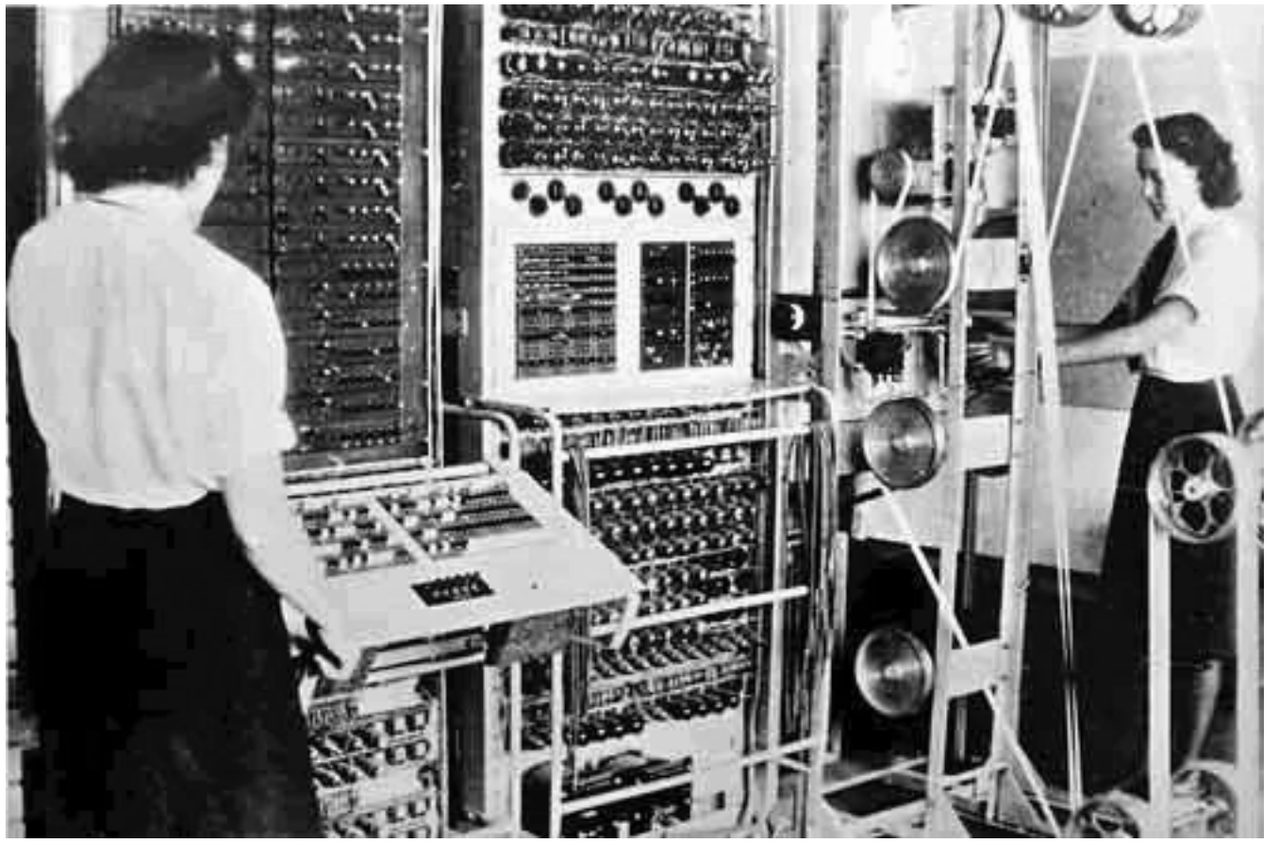
- Lorenz Machine was understood but that still left an enormously difficult task in deciphering particular messages
- Some early successes but these stopped when the Germans improved their protocols
- Tutte devised the “statistical method” that would work against Fish but...
- What was needed was an analysis of each message that was thousands of times faster than computations by hand
- Could a machine be invented to do this?

Attacks on Current Traffic

- Lorenz Machine was understood but that still left an enormously difficult task in deciphering particular messages
- Some early successes but these stopped when the Germans improved their protocols
- Tutte devised the “statistical method” that would work against Fish but...
- What was needed was an analysis of each message that was thousands of times faster than computations by hand
- Could a machine be invented to do this?
- Tutte explained his ideas to Gerry Morgan and Max Newman

Colossus

- Prototype finished in Dec 1943
- Designed by Tommy Flowers of the Post Office
- Used an unprecedented number of vacuum tubes
- Its existence was not publicly acknowledged until decades after the war



Battle of Kursk, USSR, Jul and Aug 1943

The Armies

	Germany	USSR
Soldiers	781,000	1,910,000
Tanks	3,000	5,000
Artillery	10,000	25,000
Aircraft	2,100	2,800
Casualties	170,000 (54,000 d)	863,000 (180,000 d)
Tanks Lost	720	2,600
Aircraft Lost	680	2,000

Fish Decrypt

To OKH/OP. ABT. and to OKH/Foreign Armies East, from Army Group South IA/01, No. 411/43, signed von Weichs, General Feldmarschall, dated 25/4:-

Comprehensive appreciation of the enemy for "Zitadelle"

In the event of "Zitadelle", there are at present approximately 90 enemy formations west of the line Belgorod--Kursk--Maloarkhangelsk. The attack of the Army Group will encounter stubborn enemy resistance in a deeply echeloned and well developed main defence zone, (with numerous dug in tanks, strong artillery and local reserves) the main effort of the defence being in the key sector Belgorod--Tamarovka.

If the enemy throws in all strategic reserves on the Army Group front into the Kursk battle, the following may appear on the battle field:- On day 1 and day 2, 2 armoured divisions and 1 cavalry corps. On day 3, 2 mech and 4 armoured corps. On day 4, 1 armoured and 1 cavalry corps. On day 5, 3 mech corps. On day 6, 3 cavalry corps. On day 6 and/or day 7, 2 cavalry corps.

About the Importance of Codebreaking

- “[the war] was shortened by not less that two years and probably by four years”, Sir Harry Hinsley, official historian, British intelligence efforts in WW II
- An exhibit in 2003 on “Secret War” at the Imperial War Museum, in London, quoted British Prime Minister Winston Churchill telling King George VI, “It was thanks to [codebreaking] that we won the war.”

Attacking a Substitution Cipher

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

Ciphertext (26! = 403,291,461,126,605,635,584,000,000 possible keys)

```
SB PVQXX ETRVH IZ HVB MBQWVBP
SB PVQXX ETRVH IZ HVB XQZNTZR RKIAZNP
SB PVQXX ETRVH TZ HVB ETBXNP QZN TZ HVB PHKBBHP
SB PVQXX ETRVH TZ HVB VTXXP
SB PVQXX ZBHBK PAKKBZNBK
```

Possible Plaintext

```
SB PVQXX ETRVH IZ HVB MBQWVBP
SB PVQXX ETRVH IZ HVB XQZNTZR RKIAZNP
SB PVQXX ETRVH TZ HVB ETBXNP QZN TZ HVB PHKBBHP
SB PVQXX ETRVH TZ HVB VTXXP
SB PVQXX ZBGBK PAKKBZNBK
```

Attacking a Substitution Cipher

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

Ciphertext

```
SB PVQXX ETRVH IZ HVB MBQWVBP
SB PVQXX ETRVH IZ HVB XQZNIZG GKIAZNP
SB PVQXX ETRVH TZ HVB ETBXNP QZN TZ HVB PHKBBHP
SB PVQXX ETRVH TZ HVB VTXXP
SB PVQXX ZBHBK PAKKBZNBK
```

Possible Plaintext

```
SE PHQXX ETRHT IZ THE MEQWHEP
SE PHQXX ETRHT IZ THE XQZNTZR RKIAZNP
SE PHQXX ETRHT TZ THE ETEXNP QZN TZ THE PTKEETP
SE PHQXX ETRHT TZ THE HTXXP
SE PHQXX ZEGEK PAKKEZNEK
```

Attacking a Substitution Cipher

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

Ciphertext

```
SB PVQXX ETRVH IZ HVB MBQWVBP
SB PVQXX ETRVH IZ HVB XQZNIZG GKIAZNP
SB PVQXX ETRVH TZ HVB ETBXNP QZN TZ HVB PHKBBHP
SB PVQXX ETRVH TZ HVB VTXXP
SB PVQXX ZBHBK PAKKBZNBK
```

Possible Plaintext

```
SE PHAXX ETRHT IN THE MEAWHEP
SE PHAXX ETRHT IN THE XANDTNR RKIANDP
SE PHAXX ETRHT TN THE ETEXDP AND TN THE PTKEETP
SE PHAXX ETRHT TN THE HTXXP
SE PHAXX NEGEK PAKKENDEK
```

A Better Substitution Cipher

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

Plaintext

```
We shall fight on the beaches,
We shall fight on the landing grounds,
We shall fight in the fields and in the streets,
We shall fight in the hills;
We shall never surrender
```

Ciphertext

A Better Substitution Cipher

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

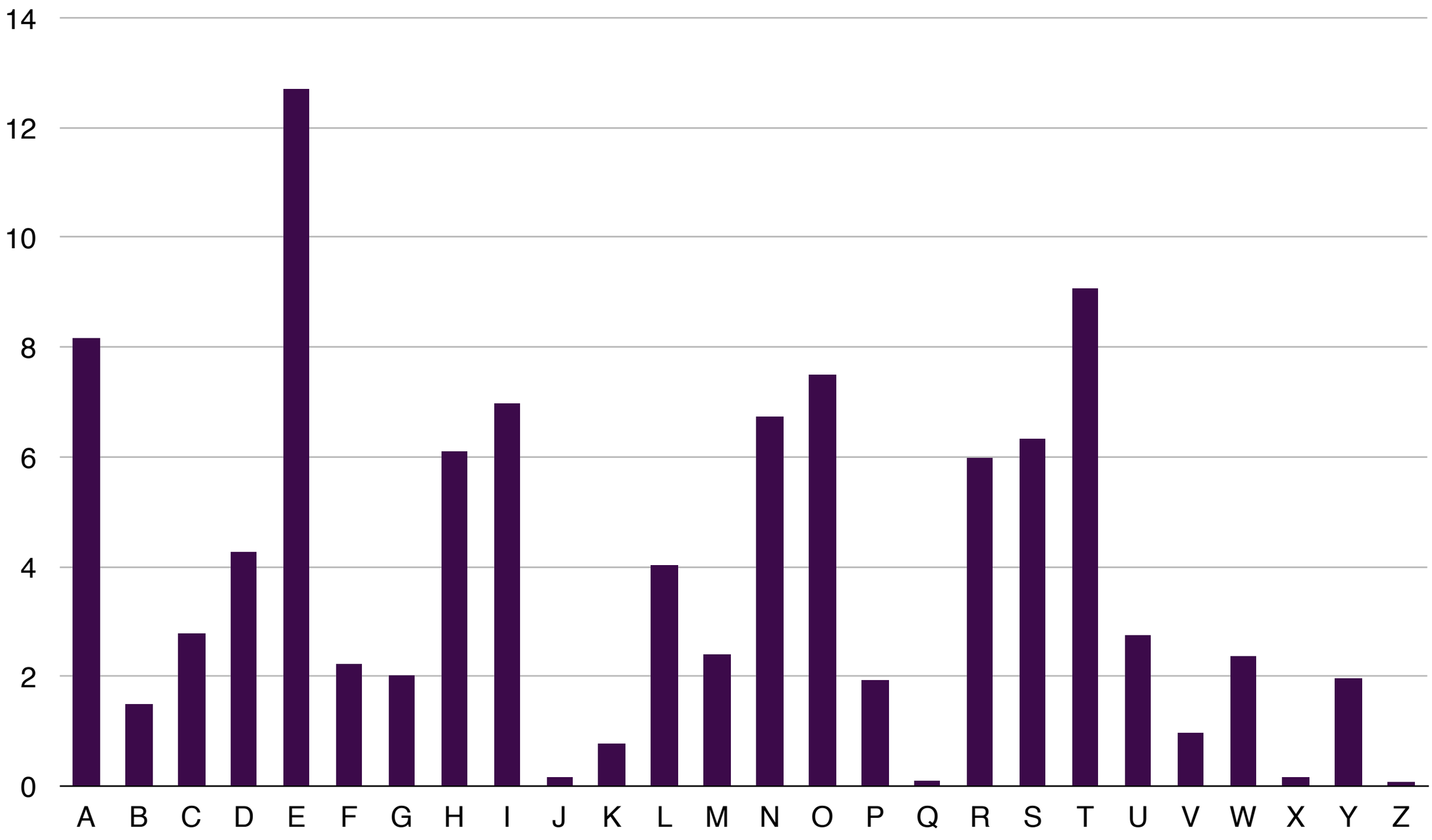
Plaintext

```
We shall fight on the beaches,
We shall fight on the landing grounds,
We shall fight in the fields and in the streets,
We shall fight in the hills;
We shall never surrender
```

Ciphertext

```
SBPVQ XXETR VHIZH VBMBQ WVBPS BPVQX XETRV HIZHV BXQZN TXRRK
IAZNP SBPVQ XXETR VHTZH VBETB XNPQZ NTZHV BPHKB BHPSB PVQXX
ETRVH TZHVB VTXXP SBPVQ XXZBL BKPAK KBZNB
```

Relatively Frequency of the English Alphabet



Letters Grouped by Relative Frequency

- E
- T, A, O, I, N, S, H, R
- D, L
- C, U, M, W, F, G, Y, P, B
- V, K, J, X, Q, Z
- Might also consider relative frequencies of letters that start or end words

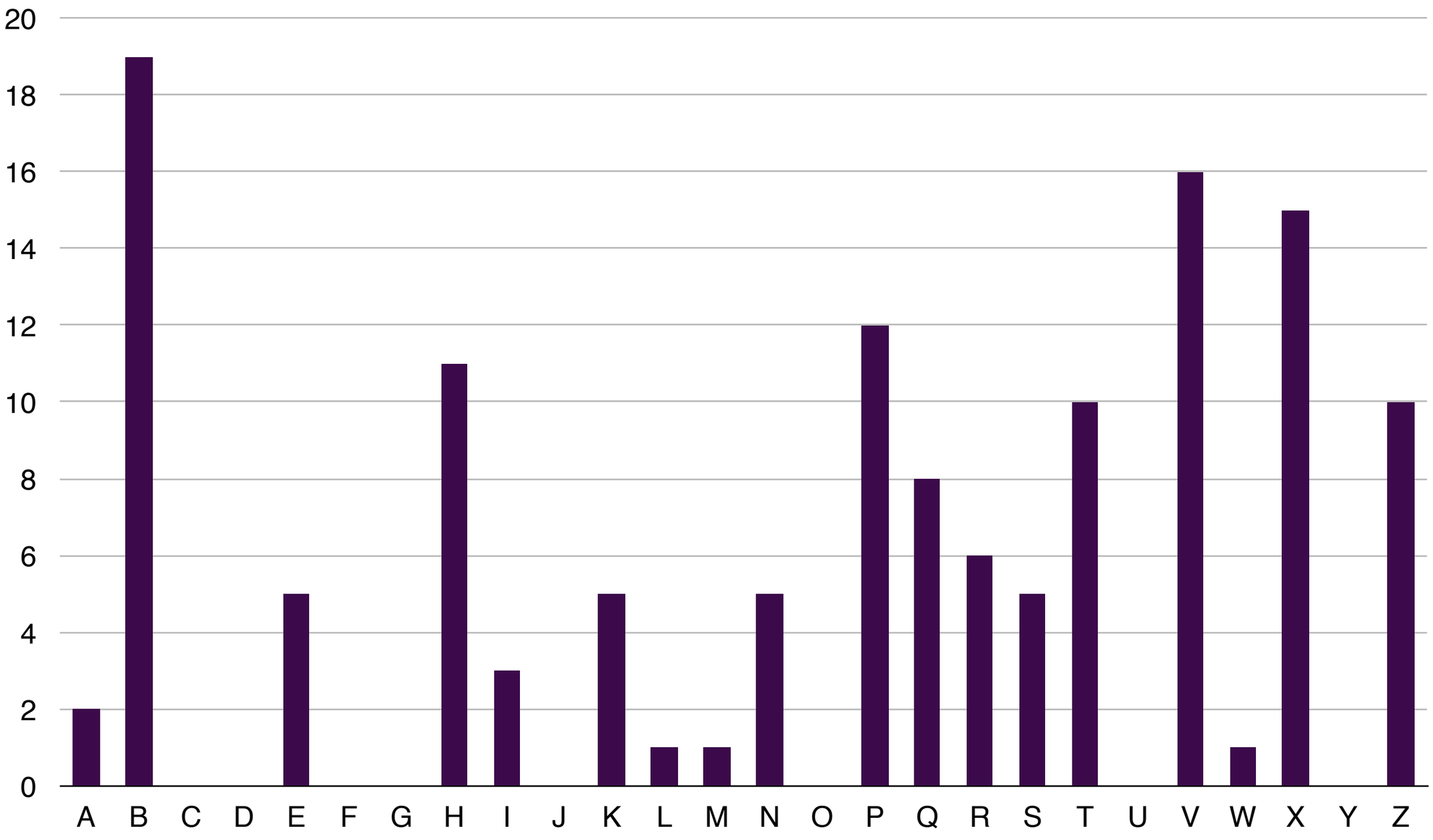
Common Pairs of Letters

- TH (3.015% of all pairs of letters)
- HE (3.004%)
- IN (1.872%)
- ER (1.860%)
- AN (1.419%)
- Might also consider pairs of identical letters: TT, LL, RR

Common Triples of Letters

- THE (2.032% of all triplets of letters)
- ING (0.747%)
- AND (0.667%)
- HER (0.547%)
- ERE (0.448%)

Relatively Frequency of the Ciphertext



Decrypting A Substitution Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	19	0	0	5	0	0	11	3	0	5	1	1	5	0	12	8	6	5	10	0	16	1	15	0	10

Ciphertext

```
SBPVQ XXETR VHIZH VBMBQ WVBPS BPVQX XETRV HIZHV BXQZN TXRRK
IAZNP SBPVQ XXETR VHTZH VBETB XNPQZ NTZHV BPHKB BHPSB PVQXX
ETRVH TZHVB VTXXP SBPVQ XXZBL BKPAK KBZNB
```

Plaintext

```
SBPVQ XXETR VHIZH VBMBQ WVBPS BPVQX XETRV HIZHV BXQZN TXRRK
IAZNP SBPVQ XXETR VHTZH VBETB XNPQZ NTZHV BPHKB BHPSB PVQXX
ETRVH TZHVB VTXXP SBPVQ XXZBL BKPAK KBZNB
```

Decrypting A Substitution Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	19	0	0	5	0	0	11	3	0	5	1	1	5	0	12	8	6	5	10	0	16	1	15	0	10
	E																								

Ciphertext

```
SBPVQ XXETR VHIZH VBMBQ WVBPS BPVQX XETRV HIZHV BXQZN TXRRK
IAZNP SBPVQ XXETR VHTZH VBETB XNPQZ NTZHV BPHKB BHPSB PVQXX
ETRVH TZHVB VTXXP SBPVQ XXZBL BKPAK KBZNB
```

Plaintext

```
SEPVQ XXETR VHIZH VEMEQ WVEPS EPVQX XETRV HIZHV EXQZN TXRRK
IAZNP SEPVQ XXETR VHTZH VEETB XNPQZ NTZHV EPHKE EHPSE PVQXX
ETRVH TZHVE VTXXP SEPVQ XXZEL EKPAK KEZNE
```

Decrypting A Substitution Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	19	0	0	5	0	0	11	3	0	5	1	1	5	0	12	8	6	5	10	0	16	1	15	0	10
	E																				T				

Ciphertext

```
SBPVQ XXETR VHIZH VBMBQ WVBPS BPVQX XETRV HIZHV BXQZN TXRRK
IAZNP SBPVQ XXETR VHTZH VBETB XNPQZ NTZHV BPHKB BHPSB PVQXX
ETRVH TZHVB VTXXP SBPVQ XXZBL BKPAK KBZNB
```

Plaintext

```
SEPTQ XXETR THIZH TEMEQ WTEPS EPTQX XETRT HIZHT EXQZN TXRRK
IAZNP SEPTQ XXETR THTZH TEETB XNPQZ NTZHT EPHKE EHPSE PTQXX
ETRTH TZHTE TTXXP SEPTQ XXZEL EKPAK KEZNE
```

“T” Didn’t Work, Look for “THE”

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	19	0	0	5	0	0	11	3	0	5	1	1	5	0	12	8	6	5	10	0	16	1	15	0	10
	E																								

Ciphertext

```
SBPVQ XXETR VHIZH VBMBQ WVBPS BPVQX XETRV HIZHV BXQZN TXRRK
IAZNP SBPVQ XXETR VHTZH VBETB XNPQZ NTZHV BPHKB BHPSB PVQXX
ETRVH TZHVB VTXXP SBPVQ XXZBL BKPAK KBZNB
```

Plaintext

```
SEPVQ XXETR VHIZH VEMEQ WVEPS EPVQX XETRV HIZHV EXQZN TXRRK
IAZNP SEPVQ XXETR VHTZH VEETB XNPQZ NTZHV EPHKE EHPSE PVQXX
ETRVH TZHVE VTXXP SEPVQ XXZEL EKPAK KEZNE
```

“T” Didn’t Work, Look for “THE”

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	19	0	0	5	0	0	11	3	0	5	1	1	5	0	12	8	6	5	10	0	16	1	15	0	10
	E						T														H				

Ciphertext

```
SBPVQ XXETR VHIZH VBMBQ WVBPS BPVQX XETRV HIZHV BXQZN TXRRK
IAZNP SBPVQ XXETR VHTZH VBETB XNPQZ NTZHV BPHKB BHPSB PVQXX
ETRVH TZHVB VTXXP SBPVQ XXZBL BKPAK KBZNB
```

Plaintext

```
SEPHQ XXETR HTIZT HEMEQ WHEPS EPHQX XETRH TIZTH EXQZN TXRRK
IAZNP SEPHQ XXETR HTTZT HEETB XNPQZ NTZTH EPTKE ETPSE PHQXX
ETRHT TZTHE HTXXP SEPHQ XXZEL EKPAK KEZNE
```

Realigning The Text

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	19	0	0	5	0	0	11	3	0	5	1	1	5	0	12	8	6	5	10	0	16	1	15	0	10
	E						T														H				

Plaintext

```
SBPVQ XXETR VHIZH VBMBQ WVBPS BPVQX XETRV HIZHV BXQZN TXRRK
IAZNP SBPVQ XXETR VHTZH VBETB XNPQZ NTZHV BPHKB BHPSB PVQXX
ETRVH TZHVB VTXXP SBPVQ XXZBL BKPAK KBZNB
```

Plaintext (Rearranged)

```
SEPHQXXETRHTIZ THE MEQWHEPSEPHQXXETRHTIZ THE XQZNTXRRKIAZNPSEPHQ
XXETRHTTZ THE ETBXNPQZNTZ THE PTKEETPSEPHQXXETRHTTZ THE
HTXXPSEPHQ XXZELEKPAKKEZNE
```

What About “XX”?

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	19	0	0	5	0	0	11	3	0	5	1	1	5	0	12	8	6	5	10	0	16	1	15	0	10
	E						T														H				

Plaintext

```
SBPVQ XXETR VHIZH VBMBQ WVBPS BPVQX XETRV HIZHV BXQZN TXRRK
IAZNP SBPVQ XXETR VHTZH VBETB XNPQZ NTZHV BPHKB BHPSB PVQXX
ETRVH TZHVB VTXXP SBPVQ XXZBL BKPAK KBZNB
```

Plaintext (Rearranged)

```
SEPHQXXETRHTIZ THE MEQWHEPSEPHQXXETRHTIZ THE XQZNTXRRKIAZNPSEPHQ
XXETRHTTZ THE ETBXNPQZNTZ THE PTKEETPSEPHQXXETRHTTZ THE
HTXXPSEPHQ XXZELEKPAKKEZNE
```

What About “XX”?

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	19	0	0	5	0	0	11	3	0	5	1	1	5	0	12	8	6	5	10	0	16	1	15	0	10
	E						T														H		L		

Plaintext

```
SBPVQ XXETR VHIZH VBMBQ WVBPS BPVQX XETRV HIZHV BXQZN TXRRK
IAZNP SBPVQ XXETR VHTZH VBETB XNPQZ NTZHV BPHKB BHPSB PVQXX
ETRVH TZHVB VTXXP SBPVQ XXZBL BKPAK KBZNB
```

Plaintext (Rearranged)

```
SEPHQLLETRHTIZ THE MEQWHEPSEPHQLLETRHTIZ THE LQZNTLRRKIAZNPSEPHQ
LLETRHTTZ THE ETBLNPQZNTZ THE PTKEETPSEPHQLLETRHTTZ THE
HTLLPSEPHQ LLZELEKPAKKEZNE
```

Vigenere Ciphers

Vigenere Ciphers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Vigenere Ciphers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

As Letters

Vigenere Ciphers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

As Letters

Plaintext	I	T		W	A	S		A		D	A	R	K		A	N	D		S	T	O
Key																					
Ciphertext																					

Vigenere Ciphers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

As Letters

Plaintext	I	T		W	A	S		A		D	A	R	K		A	N	D		S	T	O
Key																					
Ciphertext																					

As Numbers

Vigenere Ciphers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

As Letters

Plaintext	I	T		W	A	S		A		D	A	R	K		A	N	D		S	T	O
Key																					
Ciphertext																					

As Numbers

Plaintext	8	19		22	0	18		0		3	0	17	10		0	13	3		18	19	14
Key																					
Ciphertext																					

Vigenere Ciphers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

As Letters

Plaintext	I	T		W	A	S		A		D	A	R	K		A	N	D		S	T	O
Key	S	N		O	O	P		Y		S	N	O	O		P	Y	S		N	O	O
Ciphertext																					

As Numbers

Plaintext	8	19		22	0	18		0		3	0	17	10		0	13	3		18	19	14
Key	18	13		14	14	15		24		18	13	14	14		15	24	18		13	14	14
Ciphertext																					

Vigenere Ciphers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

As Letters

Plaintext	I	T		W	A	S		A		D	A	R	K		A	N	D		S	T	O
Key	S	N		O	O	P		Y		S	N	O	O		P	Y	S		N	O	O
Ciphertext	A	G		K	O	H		Y		V	N	F	Y		P	L	V		F	H	C

As Numbers

Plaintext	8	19		22	0	18		0		3	0	17	10		0	13	3		18	19	14
Key	18	13		14	14	15		24		18	13	14	14		15	24	18		13	14	14
Ciphertext	0	6		10	14	7		24		21	13	5	24		15	11	21		5	7	2

Vigenere Cipher

Plaintext

Key

Ciphertext

Vigenere Cipher

Plaintext

```
IT WAS A DARK AND STORMY NIGHT; THE RAIN FELL IN TORRENTS —
EXCEPT AT OCCASIONAL INTERVALS, WHEN IT WAS CHECKED BY A
VIOLENT GUST OF WIND WHICH SWEPT UP THE STREETS (FOR IT IS IN
LONDON THAT OUR SCENE LIES), RATTLING ALONG THE HOUSETOPS, AND
FIERCELY AGITATING THE SCANTY FLAME OF THE LAMPS THAT STRUGGLED
AGAINST THE DARKNESS.
```

Key

Ciphertext

Vigenere Cipher

Plaintext

```
IT WAS A DARK AND STORMY NIGHT; THE RAIN FELL IN TORRENTS —
EXCEPT AT OCCASIONAL INTERVALS, WHEN IT WAS CHECKED BY A
VIOLENT GUST OF WIND WHICH SWEPT UP THE STREETS (FOR IT IS IN
LONDON THAT OUR SCENE LIES), RATTLING ALONG THE HOUSETOPS, AND
FIERCELY AGITATING THE SCANTY FLAME OF THE LAMPS THAT STRUGGLED
AGAINST THE DARKNESS.
```

Key `SNOOPY`

Ciphertext

Vigenere Cipher

Plaintext

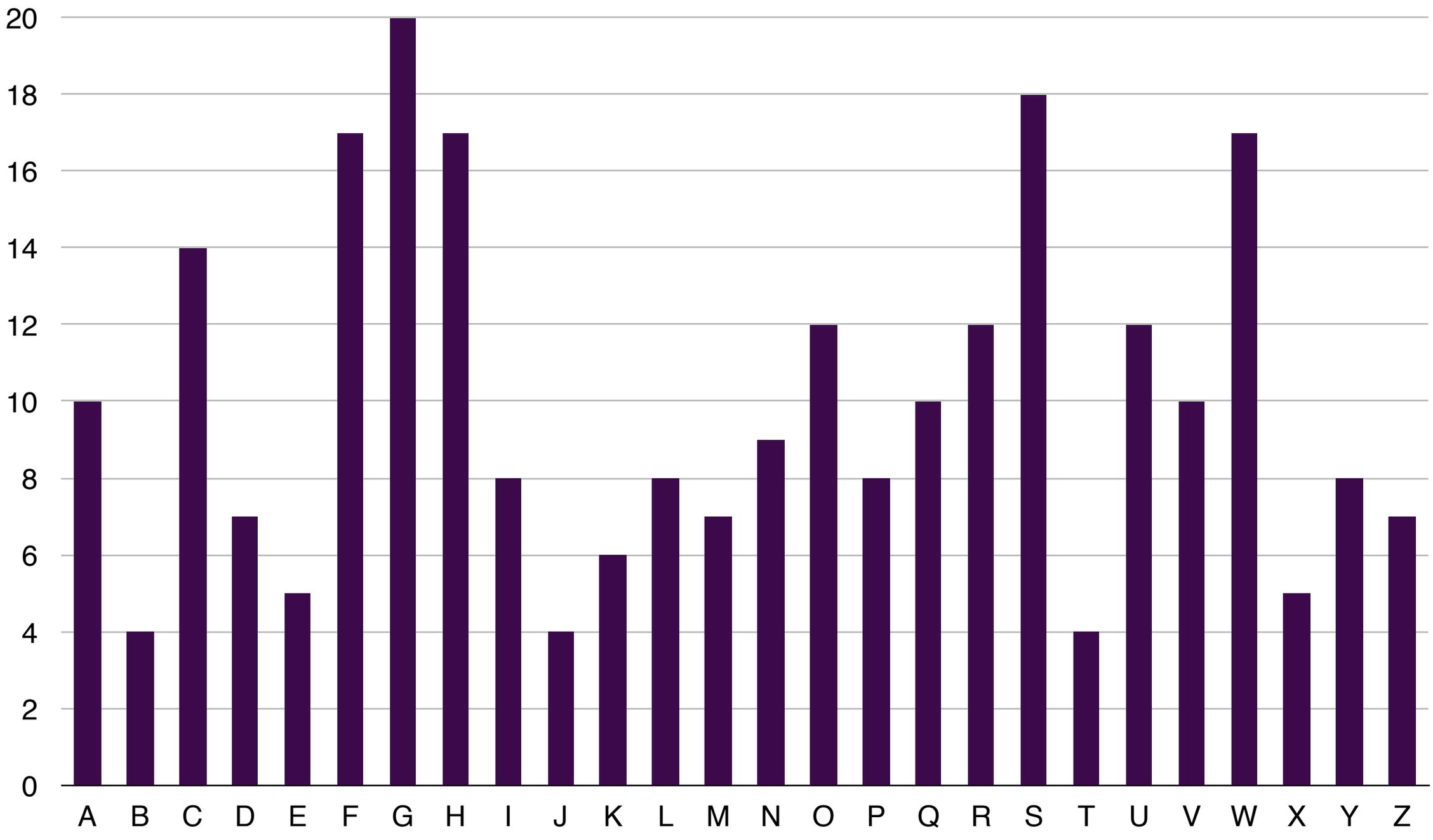
```
IT WAS A DARK AND STORMY NIGHT; THE RAIN FELL IN TORRENTS —
EXCEPT AT OCCASIONAL INTERVALS, WHEN IT WAS CHECKED BY A
VIOLENT GUST OF WIND WHICH SWEPT UP THE STREETS (FOR IT IS IN
LONDON THAT OUR SCENE LIES), RATTLING ALONG THE HOUSETOPS, AND
FIERCELY AGITATING THE SCANTY FLAME OF THE LAMPS THAT STRUGGLED
AGAINST THE DARKNESS.
```

Key `SNOOPY`

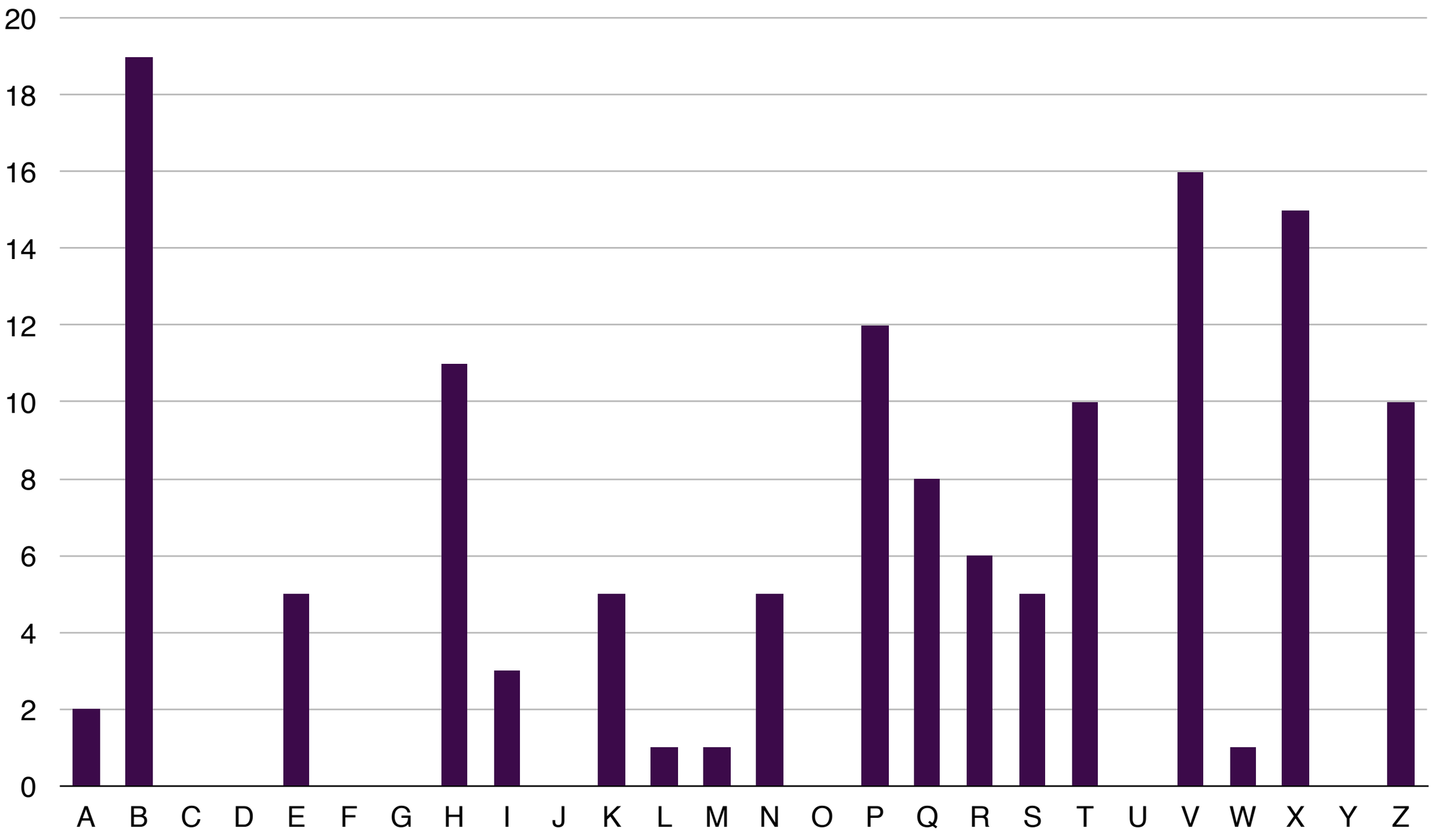
Ciphertext

```
AGKOH YVNFY PLVFH CGKQA WUWRL USFPG FSSZA GFGCF GCFGG SMAWC
HOIMU POGXM FNZWC RWEJO AQOUS BXRON GQWCU XSRQW SIWCA CFGUI
HRGSK WCBOU WQWQO RDHJN LUSGI PWRHG UMJVH WHGFY CBSMF GVOIM
MEGQT LWYWS HPSGH ZXLYN ZCCEL USVDS KRHCE QSART XCJPS ZNYYV
HOIGF THVTQ UNBHN DDNAS DDLUS ZPKHF HVPRK GFIVE DRROV YAAGH
IFWQO FZLWF G
```

Relatively Frequency of the Vigenere Ciphertext



Relatively Frequency of the Substitution Ciphertext



Need A Plan To Attack The Vigenere Cipher

Need A Plan To Attack The Vigenere Cipher

- If the key used in the Vigenere cipher is of length k, then the Vigenere cipher is simply k substitution (additive) ciphers.

Need A Plan To Attack The Vigenere Cipher

- If the key used in the Vigenere cipher is of length k, then the Vigenere cipher is simply k substitution (additive) ciphers.
- We know how to attack substitution ciphers. In fact, each of these k ciphers is the simplest kind of substitution cipher, just translate all of the letters the same amount.

Need A Plan To Attack The Vigenere Cipher

- If the key used in the Vigenere cipher is of length k, then the Vigenere cipher is simply k substitution (additive) ciphers.
- We know how to attack substitution ciphers. In fact, each of these k ciphers is the simplest kind of substitution cipher, just translate all of the letters the same amount.
- If we could determine the length of the key, k, then we could divide the ciphertext into k streams each of which could be examined. The letters in stream 1 would be all the letters whose position is 1 mod k, that is, the letters in position 1, k+1, 2k+1, and so on. The letters in stream i would be all the letters whose position is i mod k.

Dividing the Cipher Text

Key Length 6

Ciphertext

```
AGKOH YVNFY PLVFH CGKQA WUWRL USFPG FSSZA GFGCF GCFGG SMAWC
HOIMU POGXM FNZWC RWEJO AQOUS BXRON GQWCU XSRQW SIWCA CFGUI
HRGSK WCBOU WQWQO RDHJN LUSGI PWRHG UMJVH WHGFY CBSMF GVOIM
MEGQT LWYWS HPSGH ZXLYN ZCCEL USVDS KRHCE QSART XCJPS ZNYYV
HOIGF THVTQ UNBHN DDNAS DDLUS ZPKHF HVPRK GFIVE DRROV YAAGH
IFWQO FZLWF G
```

```
AVVQLF... translated by S
GNFAUS... translated by N
KFHWSS... translated by O
OYCUFZ... translated by O
HPGWPA... translated by P
YLKRGG... translated by Y
```

How Do We Find The Key Length k?

- Consider pairs of letters.
- Suppose we have a random sequence of letters from the English alphabet and we choose the i-th letter. Since there are 26 possibilities and they are all equally likely, the probability of the choice being any particular letter is 1/26.
- Now suppose that there are two random sequences of letters and we examine the ordered pair of characters from the i-th position in the sequence. Since the two sequences are independent, the probability of choosing any particular ordered pair is (1/26)^2. The probability of choosing an *identical* pair of letters is

$$26 \times \left(\frac{1}{26}\right)^2 = \frac{1}{26} \approx 0.038$$

Random Passages Instead of Random Sequences

- If we replace the two random sequence of letters by two randomly chosen passages of English text, the probabilities change. Instead of being uniformly 1/26 they are the probabilities that appear in the table of relative frequencies. If p_λ is the probability that the letter λ appears in a given position in a string, then the probability that λ appears in the same position in two strings is

$$\sum_{\lambda=A}^{Z} (p_\lambda)^2 \approx 0.065$$

Measuring “Flatness”

- If the histogram of relative frequencies for letters in a ciphertext was absolutely flat, then each letter would occur with probability 1/26 and there would be relatively little information statistical information available for the cryptanalyst. If the histogram is not flat, we need some way to measure how much it varies from the flat histogram to help us determine the relative frequency of the letters. As a first guess we could try

$$\sum_{\lambda=A}^{Z}\left(p_\lambda-\frac{1}{26}\right)$$

- But that fails since

$$\sum_{\lambda=A}^{Z}\left(p_\lambda-\frac{1}{26}\right)=\sum_{\lambda=A}^{Z}p_\lambda-\sum_{\lambda=A}^{Z}\frac{1}{26}=1-26\times\frac{1}{26}=0$$

Measuring “Flatness” - Usefully

- The problem with the previous guess is that positive differences cancel negative differences. We can accentuate the differences by squaring the terms.

$$\sum_{\lambda=A}^{Z} \left(p_\lambda - \frac{1}{26} \right)^2$$

$$
\begin{aligned}
\sum_{\lambda=A}^{Z}\left(p_\lambda-\frac{1}{26}\right)^2 &= \sum_{\lambda=A}^{Z}\left(p_\lambda\right)^2-2\sum_{\lambda=A}^{Z}\frac{1}{26}p_\lambda+\sum_{\lambda=A}^{Z}\left(\frac{1}{26}\right)^2 \\
&= \sum_{\lambda=A}^{Z}\left(p_\lambda\right)^2-\frac{2}{26}\sum_{\lambda=A}^{Z}p_\lambda+\left(\frac{1}{26}\right)^2\sum_{\lambda=A}^{Z}1 \\
&= \sum_{\lambda=A}^{Z}\left(p_\lambda\right)^2-\frac{2}{26}\times 1+26\times\left(\frac{1}{26}\right)^2 \\
&= \sum_{\lambda=A}^{Z}\left(p_\lambda\right)^2-\frac{1}{26} \\
&= \sum_{\lambda=A}^{Z}\left(p_\lambda\right)^2-0.038 \\
&\approx 0.065-0.038 \\
&= 0.027
\end{aligned}
$$

Another Way To Count

- Suppose we have just one ciphertext. As before, let p_λ be the probability that the letter λ appears in a given position in the ciphertext. If we choose a second position in the ciphertext independent of the first choice, the probability of λ appearing again is p^2_λ.

- Thus the probability that two positions, randomly selected, will contain the same letter λ is

$$\sum_{\lambda=A}^{Z} (p_\lambda)^2$$

Estimating $\sum_{\lambda=A}^{Z} (p_\lambda)^2$

- Let f_λ be the frequency, not the probability, that the letter λ occurs in a particular cipher text. The number of unordered pairs containing two λs is $\binom{f_\lambda}{2}$
- Thus, the total number of unordered pairs containing two λs is

$$\sum_{\lambda=A}^{Z} \binom{f_\lambda}{2}$$

Index of Coincidence

- If the ciphertext has n characters then the the total number of unordered pairs is n choose 2 and so the likelihood of two randomly chosen letters being the same is

$$I_C = \frac{\sum_{\lambda=A}^{Z} \binom{f_\lambda}{2}}{\binom{n}{2}} = \frac{\sum_{\lambda=A}^{Z} f_\lambda \left(f_\lambda - 1\right)}{n\left(n-1\right)}$$

- I_C is the **index of coincidence** and is an approximation of

$$\sum_{\lambda=A}^{Z} \left(p_\lambda\right)^2$$

Estimating Key Length

- Suppose we possess a ciphertext of length n created by a Vigenere cipher with a key of length k all of whose characters are different. Then we can write our ciphertext in k rows such that letters in the same row have been enciphered using the same additive cipher but any two letters from different rows come from different additive ciphers. We then have k rows with approximately n/k letters in each row.

- If we pick two positions in any one row then the probability of getting identical letters is 0.065 since they originate from the same substitution cipher.

- If we pick two positions in different rows, then the probability of getting identical letters is 0.038 since they are randomly correlated.

Count The Number of Unordered Pairs of Positions

- Let us count the number of unordered pairs of positions in the ciphertext in two ways.
- Since there are n positions in the ciphertext, there are n choose 2 unordered pairs of positions.
- Alternatively, choose any position. We can do this in n ways. How do we choose the second position? If the second position is in the same row as the first position, it can be chosen in any of the remaining n/k - 1 positions. Thus the number of unordered pairs from one row is

$$\frac{1}{2}n\left(\frac{n}{k}-1\right)$$

- If the second position is in a different row from the first position, it can be chosen in any of the remaining n - n/k positions. Thus the number of unordered pairs from other rows is

$$\frac{1}{2}n\left(n-\frac{n}{k}\right)$$

Count The Number of Identical Pairs

- Now we count the number of unordered pairs of identical letters in two ways.
- First, we take the product of all unordered positions and the probability that a given unordered position contains identical letters.

$$\frac{1}{2}n(n-1)I_C$$

- Second, we add the probability that pairs of positions in the same rows generate identical letters and pairs in different positions generate identical letters.

$$\frac{1}{2}n\left(\frac{n}{k}-1\right)\times 0.065+\frac{1}{2}n\left(n-\frac{n}{k}\right)\times 0.038$$

- The two are approximately, not exactly, equal so

$$\frac{1}{2}n(n-1)I_C \approx \frac{1}{2}n\left(\frac{n}{k}-1\right)\times 0.065+\frac{1}{2}n\left(n-\frac{n}{k}\right)\times 0.038$$

Estimating Key Length

- Rearranging gives

$$k \approx \frac{0.027n}{I_C(n-1) - 0.038n + 0.065}$$

Attacking a Vigenere Cipher

- Approximate the key length k.
- Divide the ciphertext into k separate additive ciphers where the character in position i of the cipher text belongs to the (i mod k)-th additive cipher.
- Use the previously discussed relative frequency method to attack each additive cipher.
- Repeat as necessary by modifying your estimate of k.

More about William T Tutte

- http://www.math.uwaterloo.ca/CandO_Dept/William_Tutte/Canmath.shtml, by Prof. Dan Younger
- http://de.uwaterloo.ca/demo/math680/modules/Module_01/ history, interviews and accessible examples of the types of problems that Tutte worked on

Sources

- image of Arthur Cayley, Wikimedia Commons
- image of W T Tutte, University of Waterloo
- animated map: Amazing Battle Map of WWII Europe, by Kaspars, StrangeCosmo
- Winston Churchill, “The Roaring Lion”, http://www.flickr.com/photos/cstm-mstc/3082707918/
- Winston Churchill, text of “Finest Hour speech”, Churchill Archives Centre, Archival Reference #9/172/152

- Battle of the North Atlantic: uboataces.com and public domain
- Winston Churchill, sound clip from “Finest Hour” speech, Library of Congress, Motion Picture, Broadcasting and Recorded Sound Division
- image of Evo Furino, Gerald Merchant, Frank Merchant courtesy of Michael Furino
- newspaper clipping, Hamilton Spectator
- brass name plates, Steven Furino

- Bletchley Park mansion, http://www.bletchleypark.org.uk/
- Enigma machine, Wikimedia Commons
- Alan Turing, Wikipedia
- Baudot tape, Wikimedia Commons
- WACS operating telettype machines, Wikimedia Commons
- Lorenz SZ 42, Wikimedia Commons

- Colossus, Wikimedia Commons
- Kursk map, Wikimedia Commons