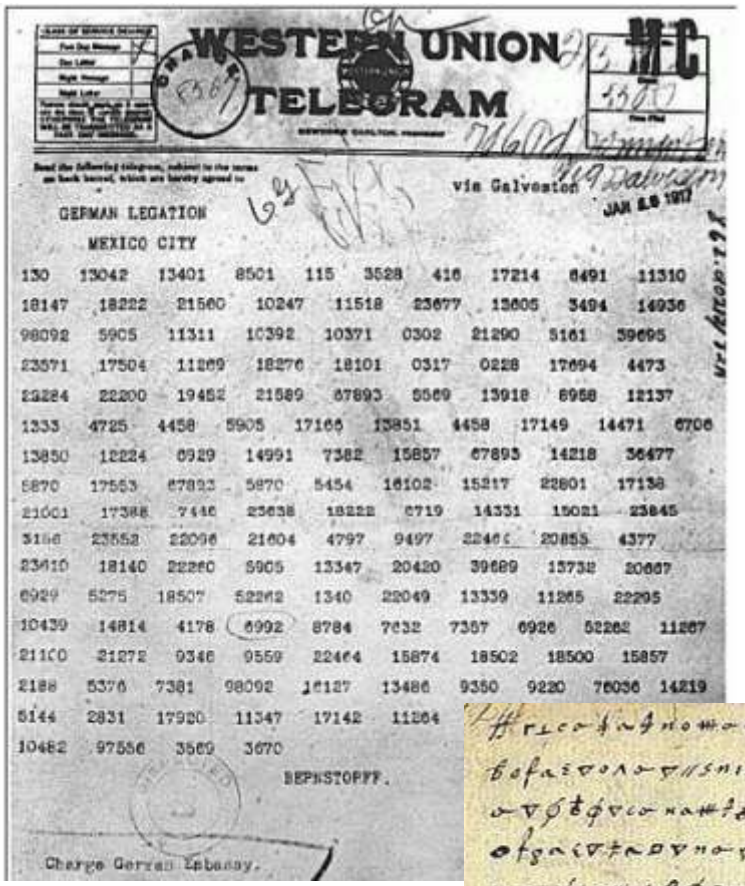
Historical Cryptography



WESTERN UNION TELEGRAM

via Galveston

JAN 16 1917

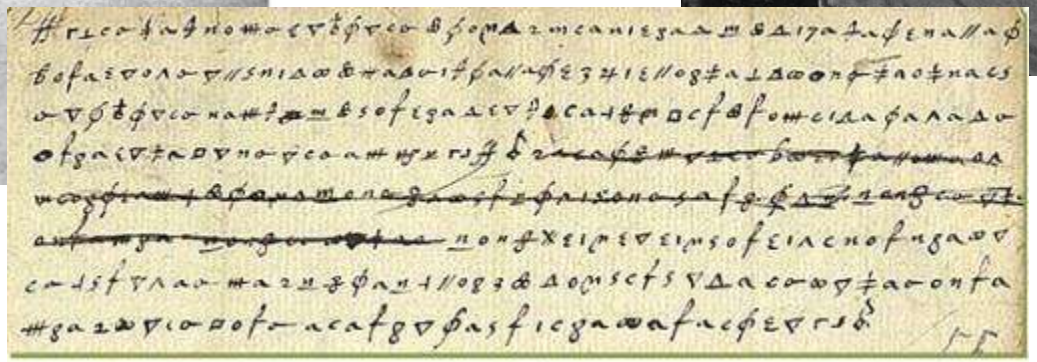
GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22224 22200 19452 21589 67893 5569 13918 6958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 0929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3184 23552 22098 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 15732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264
10482 97556 3569 3670

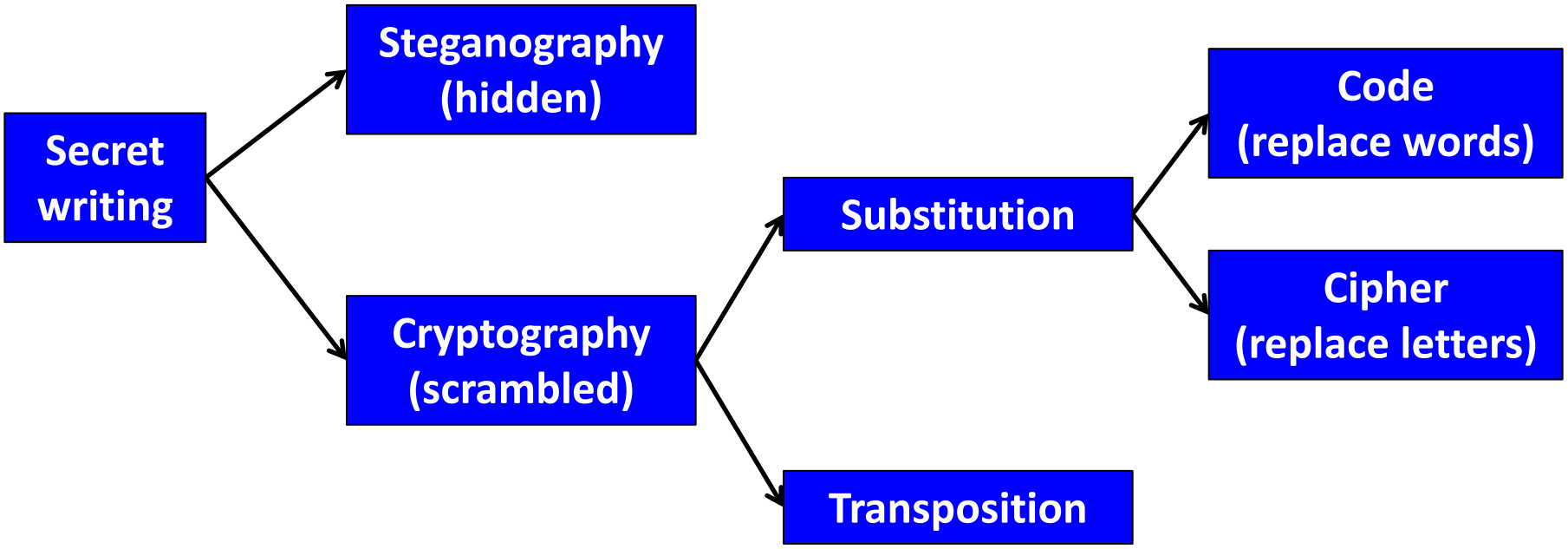
BERNSTORFF.

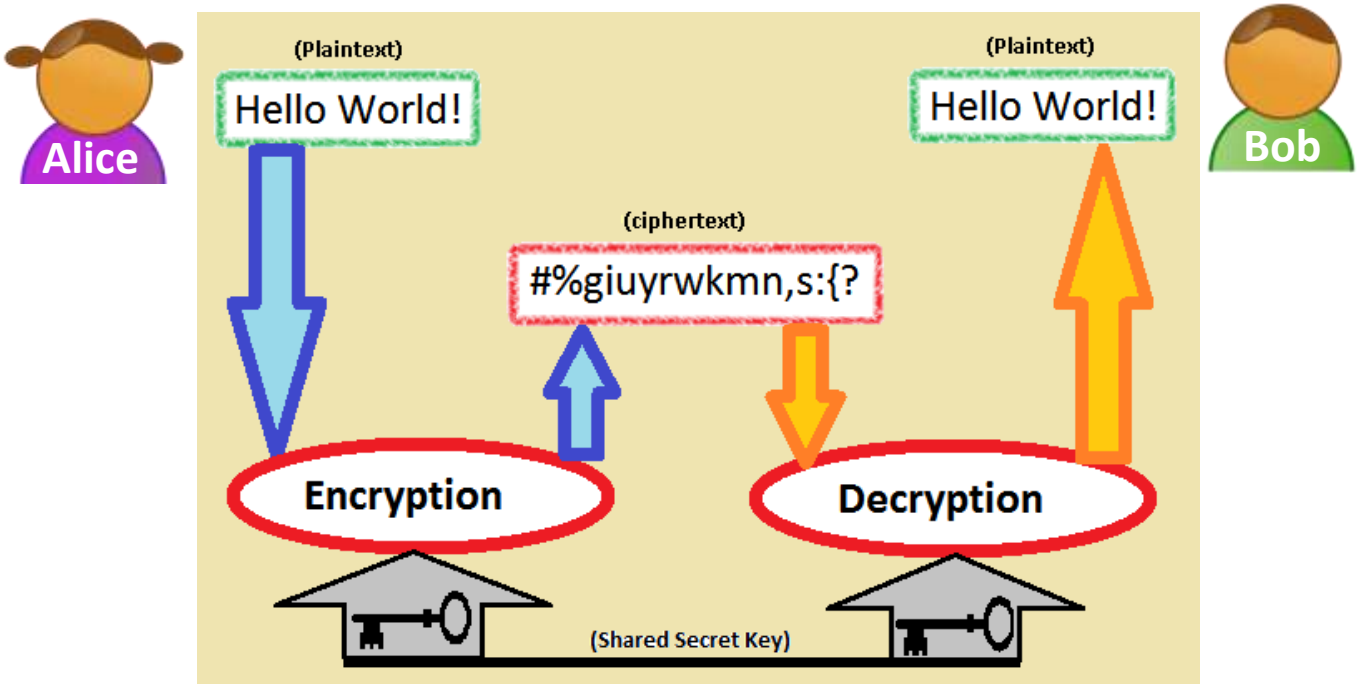
Charge German Embassy.



Overview

- Historical cryptography
  - Monoalphabetic substitution ciphers
    - Breaking them
    - Some improvements
    - The cipher of Mary Queen of Scots
  - Polyalphabetic substitution ciphers
  - Unbreakable encryption
  - WWI
    - Zimmerman telegram
  - WWII
    - Rise of the cipher machines
    - Engima


Secret writing
Steganography (hidden)
Cryptography (scrambled)
Substitution
Transposition
Code (replace words)
Cipher (replace letters)


Alice
(Plaintext)
Hello World!
(ciphertext)
#%giuyrwkmn,s:{?
(Plaintext)
Hello World!
Bob
Encryption
Decryption
(Shared Secret Key)

Monoalphabetic ciphers

- Monoalphabetic cipher
  - Use a fixed substitution over entire message
- Assigning the substitutions
  - Caesar shift cipher
  - Completely random
    - 26! ways to assign ≈ 400,000,000,000,000,000,000,000,000
    - But hard to remember
  - Based on key phrase
    - Shared secret: "ugly black swan"

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

Monoalphabetic ciphers

- Monoalphabetic cipher
  - Use a fixed substitution over entire message
- Assigning the substitutions
  - Caesar shift cipher
  - Completely random
    - 26! ways to assign ≈ 400,000,000,000,000,000,000,000,000
    - But hard to remember a completely random assignment
  - Based on key phrase
    - Shared secret: "ugly black swan"

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
U	G	L	Y	B	A	C	K	S	W	N															

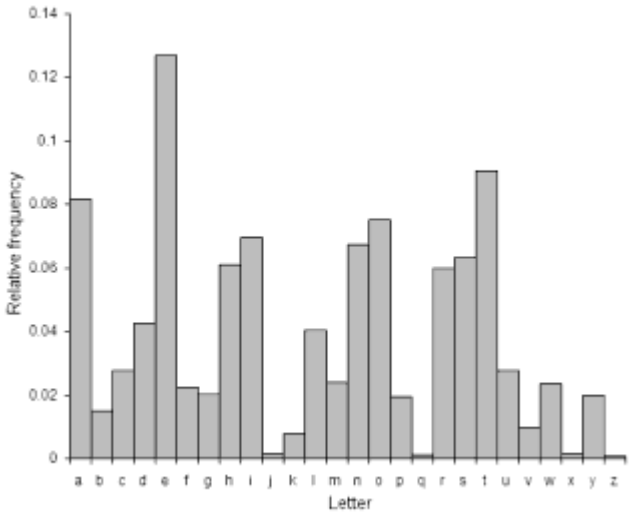
Monoalphabetic ciphers

- Monoalphabetic cipher
  - Use a fixed substitution over entire message
- Assigning the substitutions
  - Caesar shift cipher
  - Completely random
    - 26! ways to assign ≈ 400,000,000,000,000,000,000,000,000
    - But hard to remember a completely random assignment
  - Based on key phrase
    - Shared secret: "ugly black swan"

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

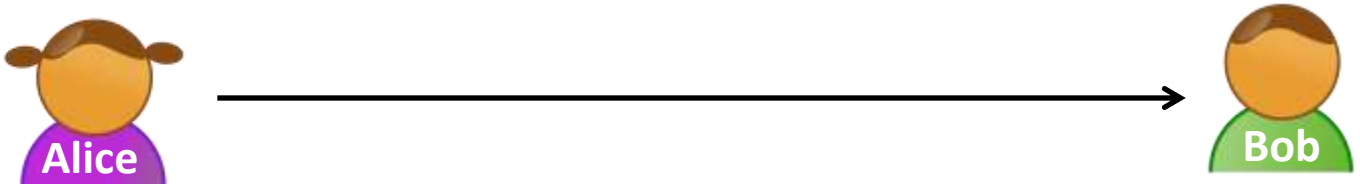
Monoalphabetic ciphers

- Dominated secret writing
  - Codemakers had a seemingly unbreakable code
    - No need for further innovation
  - At least for most of the first millennium AD
- Breaking monoalphabetic ciphers
  - Key idea: frequency analysis
  - Arabs ~800 AD



-Abu Yusuf Ya'qūb ibn Isḥāq al-Sabbah al-Kindī

Breaking a monoalphabetic cipher



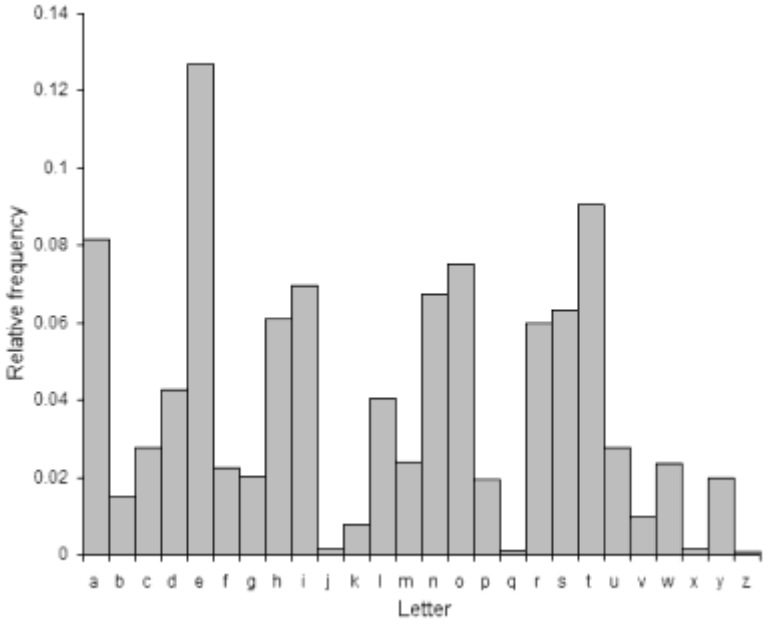

```
LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVSTYLXZIXLIKIIX
PIJVSZEYPERRGERIMWQLMGLMXQERIWGPSRIHMXQEREKIETXMJTPRGEVEKEITRE
WHEXXLEXXMZITWAWSQWXSWEXTVEPMRXRSJGSTVRIEYVIEXCVMUIMWERGMIWXMJ
MGCSMWXSJOMIQXLIVIQIVIXQSVSTWHKPEGARCSXRWIEVSWIIBXVIZMXFSJXLIK
EGAEWHEPSWYSWIWIEVXLISXLIVXLIRGEPIRQIVIIBGIIHMWYPFLEVHEWHYPSRR
FQMXLEPPXLIECCIEVEWGISJKTVWMRLIHYSPHXLIQIMYLXSJXLIMWRIGXQEROIV
FVIZEVAEKPIEWHXEAMWYEPPXLMWYRMWXSGSWRMHIVEXMSWMGSTPHLEVHPFKPEZ
INTCMXIVJSVLMRSCMWMSWVIRCIGXMWYMX
```

Eve counts up frequency of single letters, letter pairs (bigrams), letter triples (trigrams)

Breaking a monoalphabetic cipher

```
LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVSTYLXZIXLIKIIX
PIJVSZEYPERRGERIMWQLMGLMXQERIWGPSRIHMXQEREKIETXMJTPRGEVEKEITRE
WHEXXLEXXMZITWAWSQWXSWEXTVEPMRXRSJGSTVRIEYVIEXCVMUIMWERGMIWXMJ
MGCSMWXSJOMIQXLIVIQIVIXQSVSTWHKPEGARCSXRWIEVSWIIBXVIZMXFSJXLIK
EGAEWHEPSWYSWIWIEVXLISXLIVXLIRGEPIRQIVIIBGIIHMWYPFLEVHEWHYPSRR
FQMXLEPPXLIECCIEVEWGISJKTVWMRLIHYSPHXLIQIMYLXSJXLIMWRIGXQEROIV
FVIZEVAEKPIEWHXEAMWYEPPXLMWYRMWXSGSWRMHIVEXMSWMGSTPHLEVHPFKPEZ
INTCMXIVJSVLMRSCMWMSWVIRCIGXMWYMX
```

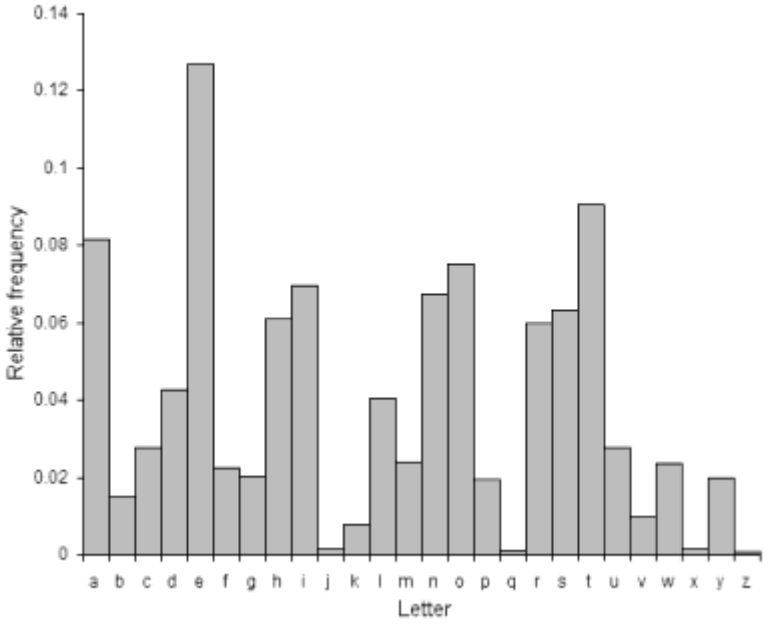
ciphertext	plaintext	
I		most common letter
XL		most common bigram
XLI		most common trigram
E		second most common letter



Breaking a monoalphabetic cipher

```
heVeTCSWPeYVaWHaVSReQMthaYVaOeaWHRtatePFaMVaWHKVSTYhtZetheKeet
PeJVSZaYPaRRGaReMWQhMGhMtQaReWGPSReHMtQaRaKeaTtMJTPRGaVaKaeTRa
WHatthattMZeTWAWSQWtSWatTVaPMRtRSJGSTVReaYVeatCVMUeMWaRGMeWtMJ
MGCSMWtSJOMeQtheVeQeVetQSVSTWHKPaGARCStRWeaVSWeeBtVeZMtFSJtheK
aGAaWHaPSWYSWeWeaVtheStheVtheRGaPeRQeVeeBGeeHMWYPFhaVHaWHYPSRR
FQMthaPPtheaCCeaVaWGeSJKTVWMRheHYSPHtheQeMYhtSJtheMWReGtQaROeV
FVeZaVAaKPeaWHtaAMWYaPPthMWYRMWtSGSWRMHeVatMSWMGSTPHhaVHPFKPaZ
eNTCMteVJSVhMRSCMWMSWVeRCeGtMWYMt
```

ciphertext	plaintext	
I	**e**	most common letter
XL	**th**	most common bigram
XLI	**the**	most common trigram
E	**a**	second most common letter



Breaking a monoalphabetic cipher

heVeTCSWPeYVaWHaVSReQMthaYVaOeaWH**Rtate**PFaMVaWHKVSTYhtZetheKeet
PeJVSZaYPaRRGaReMWQhMGhMtQaReWGPSReHMtQaRaKeaTtMJTPRGaVaKaeTRa
WH**atthattMZe**TWAWSQWtSWatTVaPMRtRSJGSTVReaYVeatCVMUeMWaRGMeWtMJ
MGCSMWtSJOMeQtheVeQeVetQSVSTWHKPaGARCStRWeaVSWeeBtVeZMtFSJtheK
aGAaWHaPSWYSWeWeaVtheStheVtheRGaPeRQeVeeBGeeHMWYPFhaVHaWHYPSRR
FQMthaPPtheaCCeaVaWGeSJKTVWMRheHYSPHtheQeMYhtSJtheMWReGtQaROeV
FVeZaVAaKPeaWHtaAMWYaPPthMWYRMWtSGSWRMHeVatMSWMGSTPHhaVHPFKPaZ
eNTCMteVJSVhMRSCMWMSWVeRCeGtMWYMt

Breaking a monoalphabetic cipher

```
heVeTCSWPeYVaWHaVSReQMthaYVaOeaWHRtatePFaMVaWHKVSTYhtZetheKeet
PeJVSZaYPaRRGaReMWQhMGhMtQaReWGPSReHMtQaRaKeaTtMJTPRGaVaKaeTRa
WHatthattMZeTWAWSQWtSWatTVaPMRtRSJGSTVReaYVeatCVMUeMWaRGMeWtMJ
MGCSMWtSJOMeQtheVeQeVetQSVSTWHKPaGARCStRWeaVSWeeBtVeZMtFSJtheK
aGAaWHaPSWYSWeWeaVtheStheVtheRGaPeRQeVeeBGeeHMWYPFhaVHaWHYPSRR
FQMthaPPtheaCCeaVaWGeSJKTVWMRheHYSPHtheQeMYhtSJtheMWReGtQaROeV
FVeZaVAaKPeaWHtaAMWYaPPthMWYRMWtSGSWRMHeVatMSWMGSTPHhaVHPFKPaZ
eNTCMteVJSVhMRSCMWMSWVeRCeGtMWYMt
```

ciphertext	plaintext	
V	r	heVe probably here
R	s	Rtate probably state
M	i	atthattMZe probably atthattime
Z	m	atthattMZe probably atthattime

Breaking a monoalphabetic cipher

```
hereTCSWPeYraWHarSseQithaYraOeaWHstatePFairaWHKrSTYhtmetheKeet
PeJrSmaYPassGaseiWQhiGhitQaseWGPSseHitQasaKeaTtiJTPsGaraKaeTsa
WHatthattimeTWAWSQWtSWatTraPistsSJGSTrseaYreatCriUeiWasGieWtiJ
iGCSiWtSJOieQthereQeretQSrSTWHKPaGAsCStsWearSWeeBtremitFSJtheK
aGAaWHaPSWYSWeWeartheStherthesGaPesQereeBGeeHiWYPFharHaWHYPSss
FQithaPPtheaCCearaWGeSJKTrWisheHYSPHtheQeiYhtSJtheiWseGtQasOer
FremarAaKPeaWHtaAiWYaPPthiWYsiWtSGSWsiHeratiSWiGSTPHharHPFKPam
eNTCiterJSrhisSCiWiSWresCeGtiWYit
```

and so on…

Breaking a monoalphabetic cipher

```
hereuponlegrandarosewithagraveandstatelyairandbroughtmethebeet
lefromaglasscaseinwhichitwasencloseditwasabeautifulscarabaeusa
ndatthattimeunknowntonaturalistsofcourseagreatprizeinascientif
icpointofviewthereweretworoundblackspotsnearoneextremityoftheb
ackandalongonenearthеotherthescaleswereexceedinglyhardandgloss
ywithalltheappearanceofburnishedgoldtheweightoftheinsectwasver
yremarkableandtakingallthingsintoconsiderationicouldhardlyblam
ejupiterforhisopinionrespectingit
```

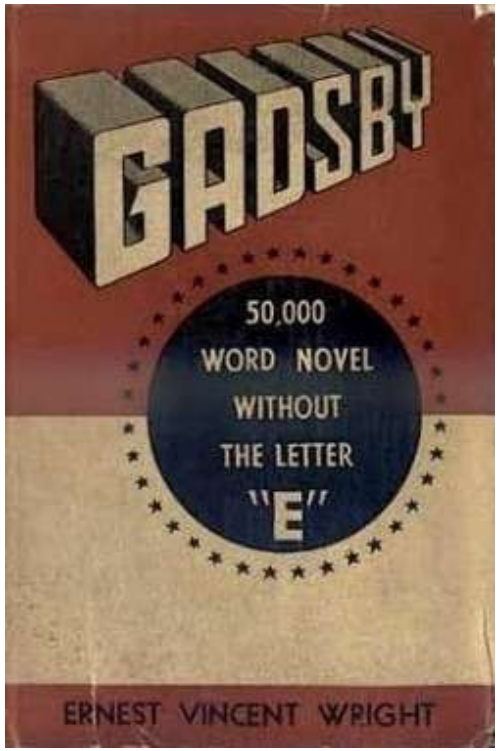
Hereupon Legrand arose, with a grave and stately air, and brought me the beetle from a glass case in which it was enclosed. It was a beautiful scarabaeus, and, at that time, unknown to naturalists—of course a great prize in a scientific point of view. There were two round black spots near one extremity of the back, and a long one near the other. The scales were exceedingly hard and glossy, with all the appearance of burnished gold. The weight of the insect was very remarkable, and, taking all things into consideration, I could hardly blame Jupiter for his opinion respecting it.

Or some code from the Internet...

```
c:\Dropbox\mtech\websci\resources>simpsub2.exe
Name of sample ("learning") file: moby.txt
Name of cipher file: mono2.txt
Is the cipher formatted with spaces? (y/n): n
Reading sample file...
Analyzing sample file...
Reading cipher file...
Analyzing cipher file...
Initial closeness is 1.487429, PLEASE WAIT...
DONE! Func value=0.866612
Key is: abcdefghijklmnopqrstuvwxyz
        ekghijylmdapzwscnvrxtoqbfu
hereuponlegrandarosewithagraveandstatelyairandbroughtmetheb
eetlefromaglasscaseinwhichitwasencloseditwasabeautifulscara
baeusandatthattimeunknowntonaturalistsofcourseagreatprizein
ascientificpointofviewthereweretworoundblackspotsnearoneext
remityofthebackandalongoneneartheotherthescaleswereexceedin
glyhardandglossywithalltheappearanceofburnishedgoldtheweigh
toftheinsectwasveryremarkableandtakingallthingsintoconsider
ationicouldhardlyblamequpiterforhisopinionrespectingit
```

Shoring up monoalphabetic ciphers

- Improved resistance to frequency analysis:
  - Insert nulls, symbols that represent nothing
    - e.g. cipher alphabet 1-99, 73 numbers represent nulls
  - Mespall thangs on pirpus
    - Screws up frequency, humans can correct
  - Use code words
    - Need to exchange large dictionary of codes
    - Capture of codebook destroys security
  - Homophonic substitution
    - Multiple cipher symbols per plaintext symbol
  - Nomenclature
    - Small list of words/syllables
    - Cipher alphabet with homophones



Homophonic substitution

- Improved resistance to frequency analysis:
  - Homophonic substitution
    - Plaintext symbol, set of cipher symbols
    - Set size proportional to frequency in the language

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
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

Mary Queen of Scots

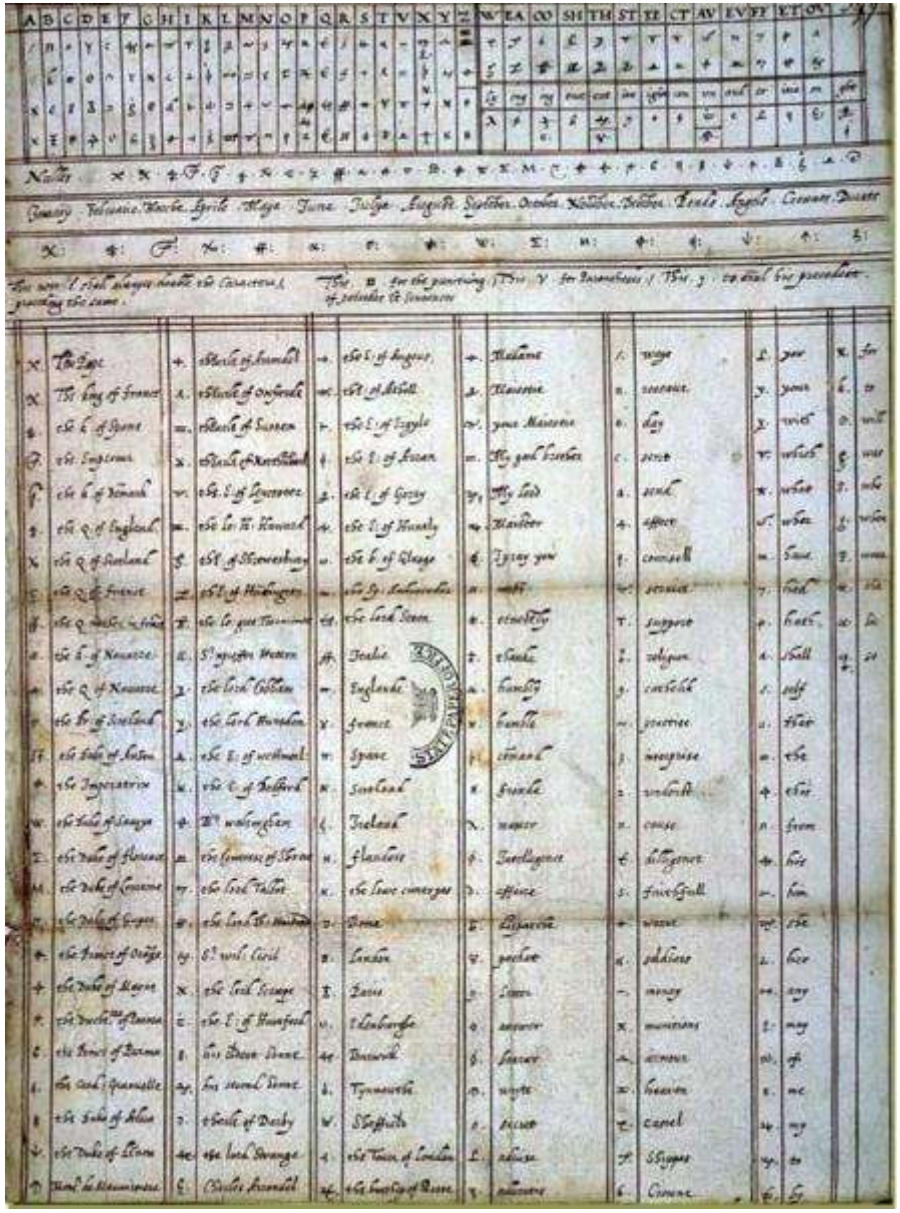
- Babington Plot
  - Mary imprisoned for 18 years
  - Gilbert Gifford double agent "recruited" to communicate with Mary
  - Detoured letters via Walsingham
  - Anthony Babington and company
    - Rescue Mary
    - Assassinate Elizabeth
    - Wanted blessing of Mary

Mary Queen of Scots

Elizabeth I

Francis Walsingham

Mary's nomenclature



Character	Meaning	Character	Meaning	Character	Meaning
O	A	7	X	ff. ⌐ . ⌙ . d .	Nulles
‡	B	8	Y	ơ	Dowbleth
\	C	9	Z	₂	And
⫴	D	3	For	d	Wyrt
ɑ	E	4	With	ſ	Send
□	F	4	That	ſ	Ire
θ	G	4	If	‡	Receave
∞	H	3	But	⊤	Bearer
I	I	♈	Where	⊥	I
♉	K	♑	As	⊢	Pray
♌	L	♍	Of	⊣	You
//	M	♊	The	♓	Mte
♐	N	♌	From	♆	Your Name
♈	O	♋	By	♋♋	Myne
♏	P	♐	So	♏	What
♍	Q	X	Not	♑	Is
♑	R	##	When	♎	Say
△	S	♊	There	♍	Me
ℰ	T	♑	This	♍	My
⊂	U	x	In	♑	Which

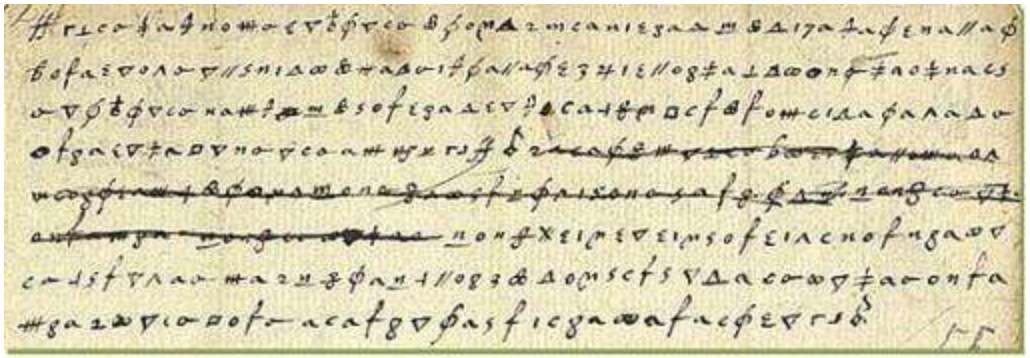
http://www.purplehell.com/riddletools/maryqos.htm

The plot

- Babington plot
  - Gifford delivers message from Mary to Babington
  - Babington replies with outline of plot

> "Myself with ten gentlemen and a hundred of our followers will undertake the delivery of your royal person from the hands of your enemies. For the dispatch of the usurper, from the obedience of whom we are by the excommunication of her made free, there be six noble gentlemen, all my private friends, who for the zeal they bear to the Catholic cause and your Majesty's service will undertake that tragical execution"

  - Mary replies endorsing plan
  - Walsingham forges postscript to Mary's letter asking Babington to name names




Den viii february werde onthalst Maria

Polyalphabetic cipher

- Monoalphabetic cipher
  - Single set of substitutions for all letters

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

- Polyalphabetic cipher
  - Multiple sets of substitutions
  - Switch between them during encryption
  - 1460s, Leon Alberti hits on idea of using two or more sets

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

Polyalphabetic cipher

- 1586, Vigenère cipher, "Le Chiffre Indéchiffrable"
  - Each letter Caesar shifted, but change based on keyword

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

Blaise de Vigenère

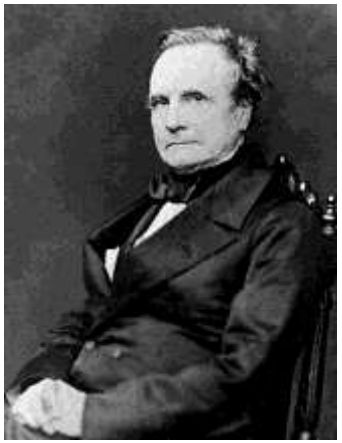
Plaintext	**attackatdawn**
Key	**LEMONLEMONLE**
Ciphertext	**LXFOPVEFRNHR**

Breaking the Vigenère Cipher

- Vigenère cipher
  - Much better at hiding letter frequency information
  - But key repeats:
    - If you know key length, just an interwoven set of Caeser ciphers

Key:	ABCDABCDABCDABCDABCDABCDABCD
Plaintext:	**CRYPTO**ISSHORTFOR**CRYPTO**GRAPHY
Ciphertext:	**CSASTP**KVSIQUTGQU**CSASTP**IUAQJB

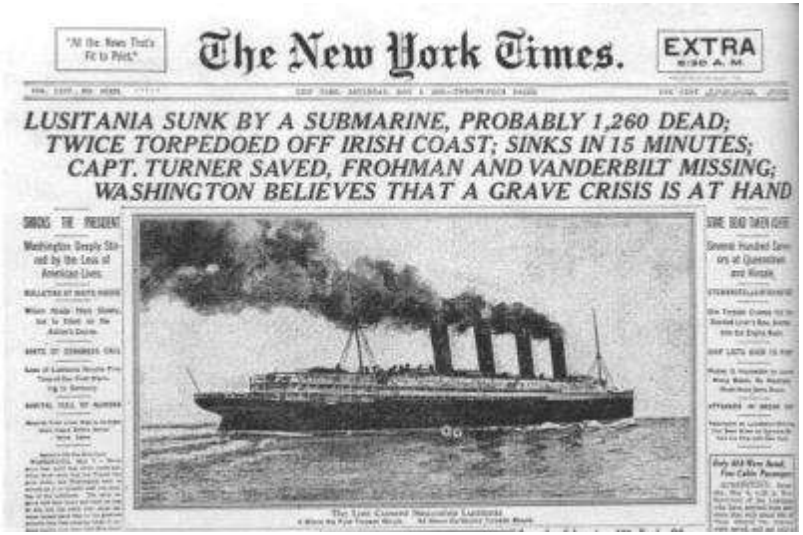
- Distance between repeats = 16
- Suggests key length if 16, 8, 4, 2, or 1
- Find additional repeats to narrow down lengths
- Frequency analyze each interwoven set



Charles Babbage

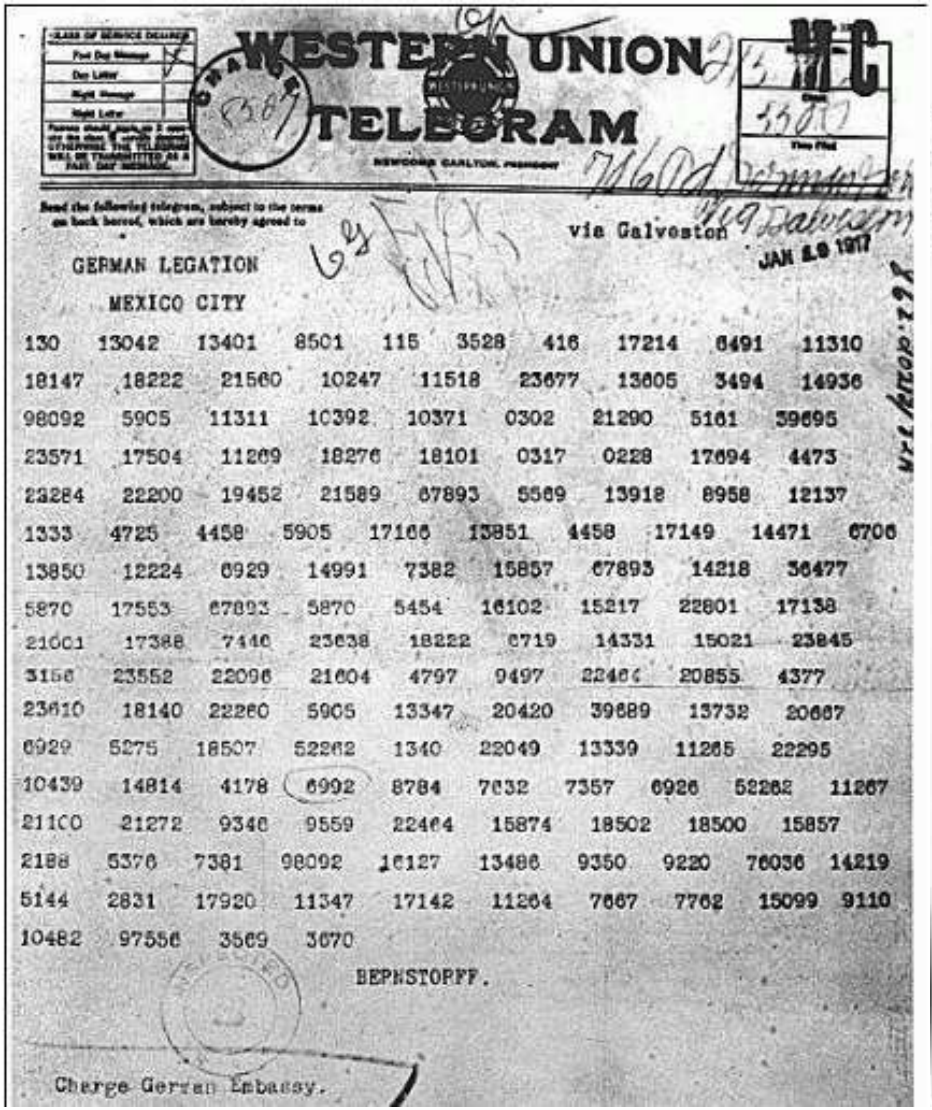
WWI: Zimmermann Telegram

- 1915, U-boat sinks Lusitania
  - 128 US Civilians
  - Promises to surface first
- 1916, new Foreign Minister
  - Arthur Zimmermann
- 1917, unrestricted submarine warfare
  - Zimmermann hatches plan
    - Keep American busy at home
    - Persuade Mexico to invade US
    - Get Mexico to persuade Japan to attack US


The New York Times. EXTRA

LUSITANIA SUNK BY A SUBMARINE, PROBABLY 1,260 DEAD; TWICE TORPEDOED OFF IRISH COAST; SINKS IN 15 MINUTES; CAPT. TURNER SAVED, FROHMAN AND VANDERBILT MISSING; WASHINGTON BELIEVES THAT A GRAVE CRISIS IS AT HAND

Arthur Zimmermann



WESTERN UNION TELEGRAM

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 8.8 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Unbreakable encryption

- 1882, One-time pad
  - Use a key as long as the message
  - Choose the key (truly) randomly
  - Only use the key once and only once
  - Provably secure

```
      H       E       L       L       O   message
   7 (H)   4 (E)  11 (L)  11 (L)  14 (O)  message
+ 23 (X)  12 (M)   2 (C)  10 (K)  11 (L)  key
= 30      16      13      21      25      message + key
=  4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z)  message + key (mod 26)
      E       Q       N       V       Z   ciphertext
```

```
      E       Q       N       V       Z   ciphertext
   4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z)  ciphertext
-  23 (X)  12 (M)   2 (C)  10 (K)  11 (L)  key
= -19      4       11      11      14      ciphertext - key
=  7 (H)   4 (E)  11 (L)  11 (L)  14 (O)  ciphertext - key (mod 26)
      H       E       L       L       O   message
```

Breaking one-time pads?

- Try all possible keys
  - 26^length = big
  - Generates all possible sequences

```
       E        Q        N        V        Z   ciphertext
    4 (E)   16 (Q)   13 (N)   21 (V)   25 (Z)  ciphertext
-  23 (X)   12 (M)    2 (C)   10 (K)   11 (L)  key
= -19        4       11       11       14      ciphertext - key
=   7 (H)    4 (E)   11 (L)   11 (L)   14 (O)  ciphertext - key (mod 26)
       H        E        L        L        O   message
```

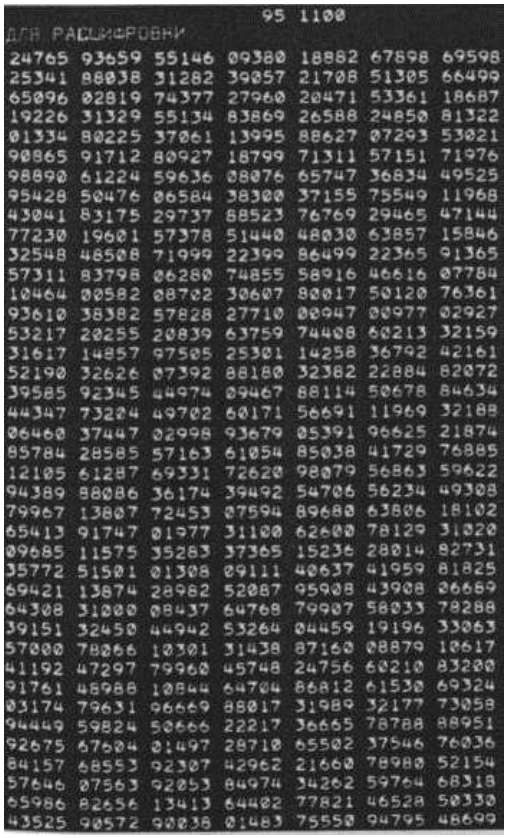
Correct key

```
       E        Q        N        V        Z   ciphertext
    4 (E)   16 (Q)   13 (N)   21 (V)   25 (Z)  ciphertext
-  19 (T)   16 (Q)   20 (U)   17 (R)    8 (I)  possible key
= -15        0       -7        4       17      ciphertext-key
=  11 (L)    0 (A)   19 (T)    4 (E)   17 (R)  ciphertext-key (mod 26)
       L        A        T        E        R   possible message
```

Some other key

Unbreakable encryption

- Problems with one-time pads:
  - Must distribute pads securely
  - Must use truly random numbers
    - Not pseudo-random
    - Not random typing on a keyboard
  - Must never reuse the same key



"As a practical person, I've observed that one-time pads are theoretically unbreakable, but practically very weak. By contrast, conventional ciphers are theoretically breakable, but practically strong." -Steve Bellovin

Mechanization of secret writing

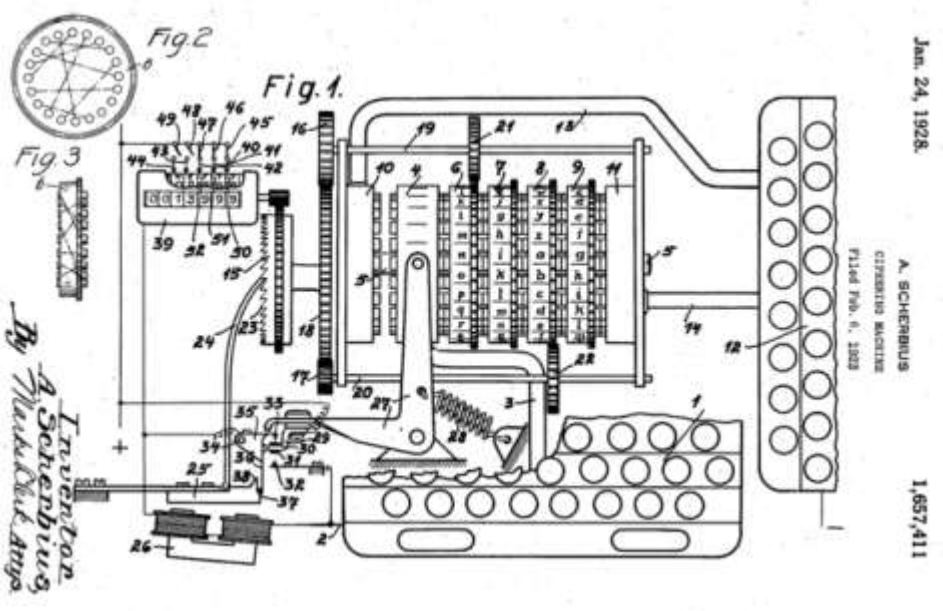
- Pencil and paper
  - Security limited by what humans can do quickly and accurately in the heat of battle
- Enter the machine

Thomas Jefferson's wheel cipher

Captain Midnight's Code-o-Graph

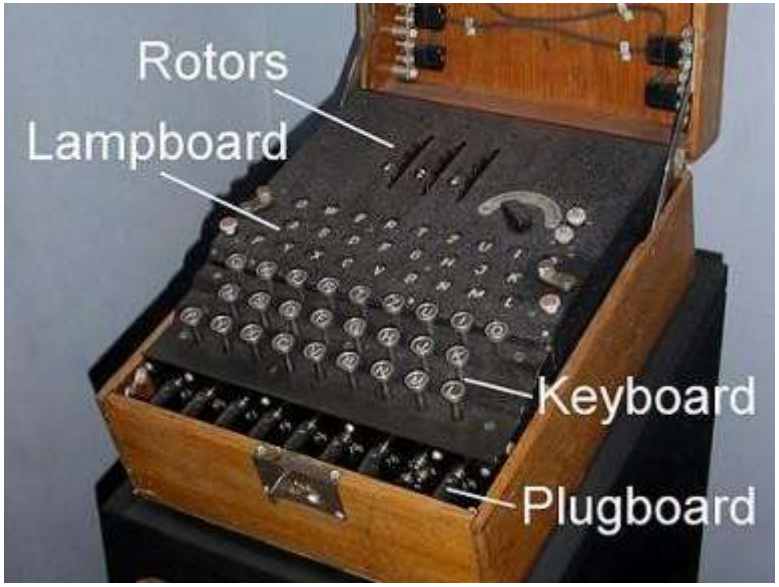
Enigma machine

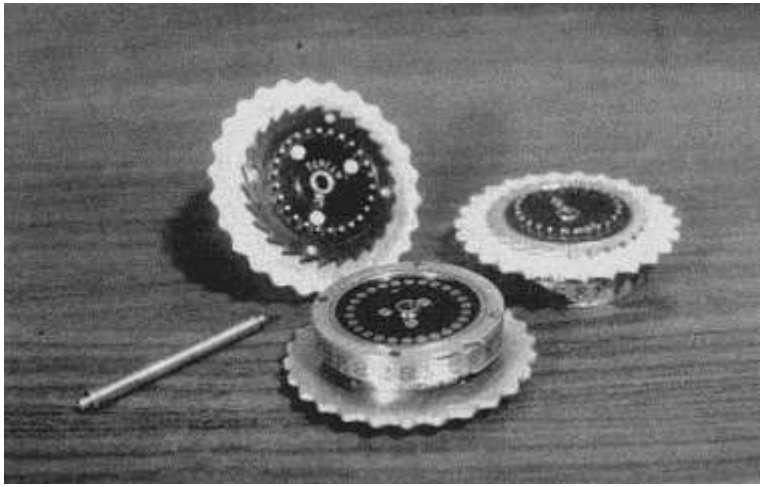
- Enigma cipher machine
  - 1918, patented by German engineer Arthur Scherbius

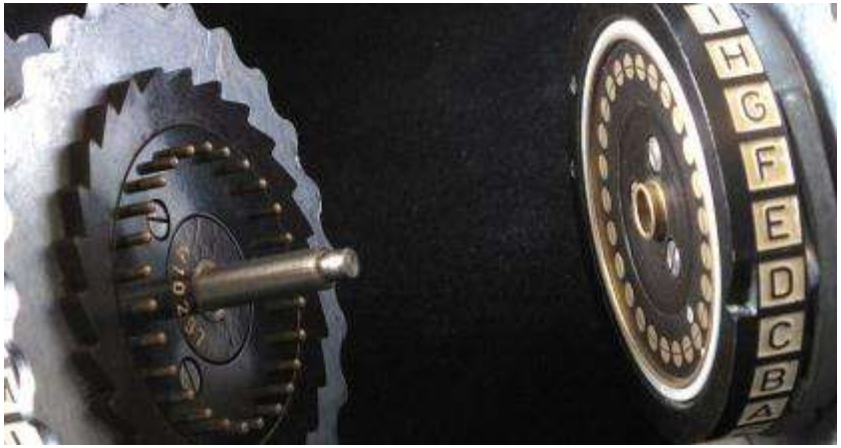


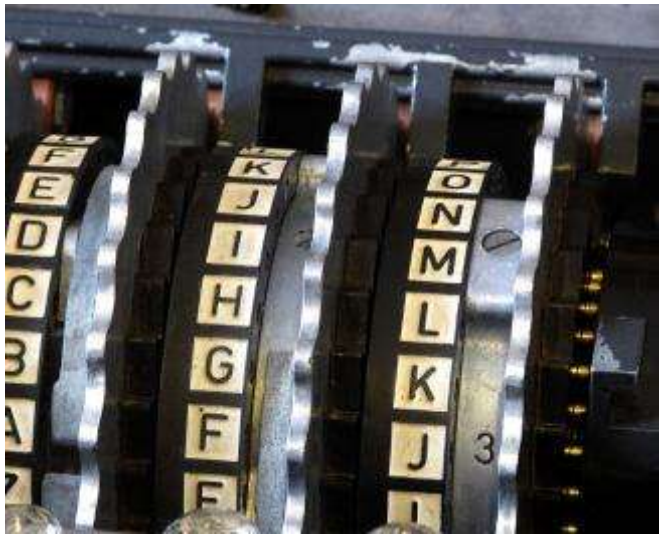
Arthur Scherbius

  - A electrical/mechanical implementation of a polyalphabetic substitution cipher


Rotors
Lampboard
Keyboard
Plugboard

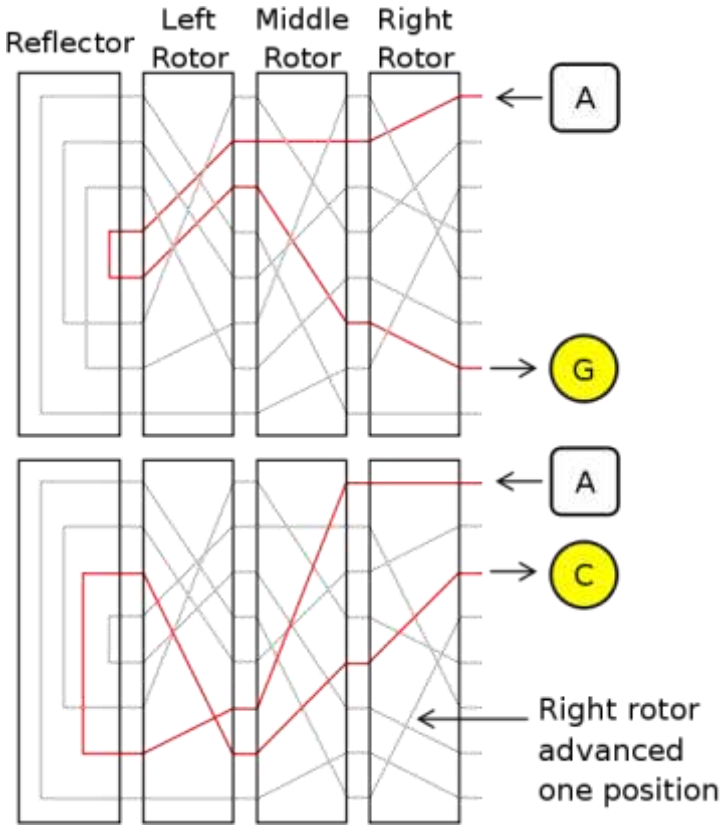



H
G
F
E
D
C
B
A


E
D
C
B
A
K
J
I
H
G
F
N
M
L
K
J
3

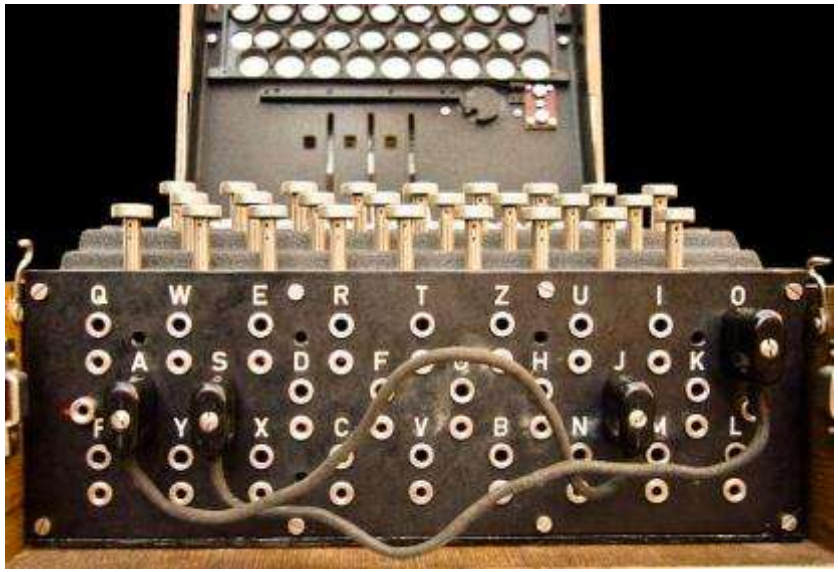
Enigma rotors

- Rotor (wheel, drum)
  - An monoalphabetic substitution cipher implemented via a complex wiring pattern
  - Set to one of 26 initial positions
  - Geared to rotate after each letter
- Rotor set
  - 3 rotors in 3!=6 possible orders
    - Eventually set increased to 3 out of 5
    - Navy used even more
  - Possible keys:
    - $3! * 26^3 = 6 * 17{,}576 = 105{,}456$



Enigma plugboard

- Plugboard
  - Operate inserts cables to swap letters
  - Initially 6 cables
    - Swaps 6 pairs of letters
    - Leaves 14 letters unswapped
  - Possible configurations:
    - 100,391,791,500



- Total keys:
  - 17,576 * 6 * 100,391,791,500 ≈ 10,000,000,000,000,000

Enigma

- Enigma machine
  - Sales initially slow
  - 1923, Germans find out about failures of communication security in WWI
  - 1925, Scherbius starts mass production
  - German military eventually buys 30,000 Enigma machines
  - 1929, Scherbius dies in carriage accident

Arthur Scherbius

Cracking the Enigma

- Step 1: Espionage
  - Disgruntled Schmidt meets with French secret agent
  - Sells Enigma user manuals
    - Allows replica to be constructed
    - Also codebook and daily key scheme
  - French just give intelligence to Poles

Hans-Thilo Schmidt

"It is assumed in judging the security of the cryptosystem that the enemy has at his disposition the machine."
-German memorandum

Cracking the Enigma

- Step 2: Poles identify weakness
  - German's had day code specifying:
    - Configuration of rotors
    - Settings of rotors
    - Settings of plugboard
  - Unique key per message:
    - Send 3 letters, encrypted with day key
    - Letters specify new setting of rotors
    - New rotors setting used for message payload
    - Repeat the 3 initial letters twice

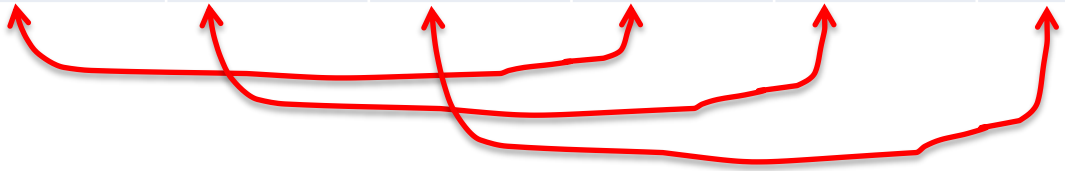
Marian Rejewski

Repetition is the enemy of security!

Cracking the Enigma

- Find patterns in first 6 letters
  - 1^{st}-4^{th}, 2^{rd}-5^{th}, and 3^{rd}-6^{th} are ciphers of same letter

Message	1st	2nd	3rd	4th	5th	6th
1	L	O	K	R	G	M
2	M	V	T	X	Z	E
3	J	K	T	M	P	E
4	D	V	Y	P	Z	X

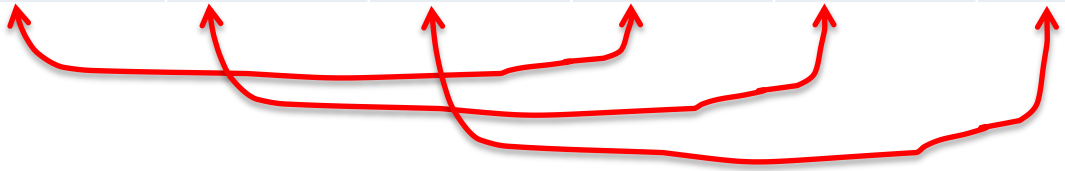


1st	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4th				P						M		R	X													

Cracking the Enigma

- Given enough messages:
  - Fill in full table of relations between 3 pairs

Message	1st	2nd	3rd	4th	5th	6th
1	L	O	K	R	G	M
2	M	V	T	X	Z	E
3	J	K	T	M	P	E
4	D	V	Y	P	Z	X



1st	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
4th	F	Q	H	P	L	W	O	G	B	M	V	R	X	U	Y	C	Z	I	T	N	J	E	A	S	D	K

Fingerprinting a day key

- Find chains
  - Found to change every day depending on day key

1st	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
4th	F	Q	H	P	L	W	O	G	B	M	V	R	X	U	Y	C	Z	I	T	N	J	E	A	S	D	K

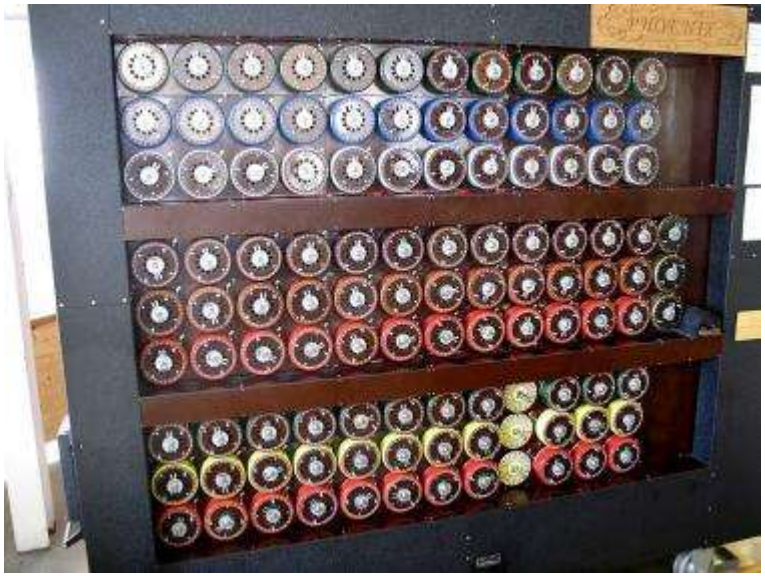
A → F → W → A	3 links
B → Q → Z → K → V → E → L → R → I → B	9 links
C → H → G → O → Y → D → P → C	7 links
J → M → X → S → T → N → U → J	7 links

  - Also for 2nd-5th and 3rd-6th letter pairs
  - Number of chains and length is independent of plugboard
  - Catalog each of 105,456 rotors settings using replica

WWII

- 1938, Germany increases Enigma security
  - Add two additional rotors, C(5, 3) = 60
  - 10 plugboard cables instead of 6
  - Poles couldn't build big enough "bombes" to break
  - Poles hand over research to British/French

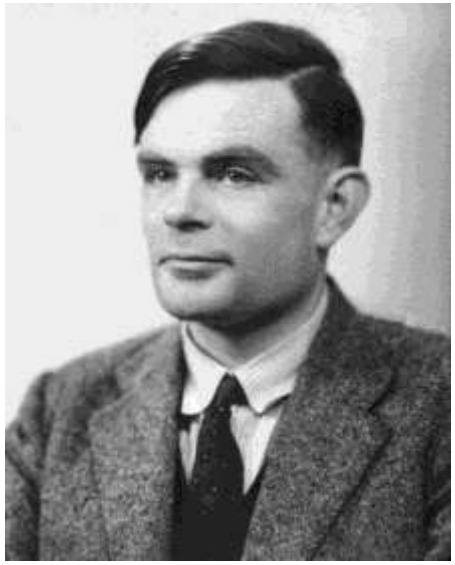
US Navy bombe



Bletchley Park bombe

Bletchley Park

- Government Code and Cypher School
  - Height of WWII, 9000 people
  - Battled against improvements to Enigma
  - May 1, 1940 Germans stop repetition of message key
    - Turing had already developed technique + machine to crack using "crib" instead of repetition of key



Alan Turing

Cribs

- Cribs
  - Some plaintext you think is in the ciphertext
    - Ideally also the location
  - e.g. Germans usually broadcast weather report at 6am
    - "wetter" somewhere at start of message
  - German Navy had strongest crypto
    - 3 rotors out of 8
    - Reflector with 26 orientations
    - Avoided stereotypical messages
  - Allies
    - Mine areas to generate messages with known grid reference
    - Stole code books

Type VII U-boot

Summary

- History of Cryptography
  - Substitution ciphers
    - Monoalphabetic
    - Polyalphabetic
  - One-time pads
    - Provably unbreakable (if used carefully)
  - Cryptography in WWI and WWII
    - Zimmerman telegraph
    - Enigma