Chapter 2: Crypto Basics（密码基础）

```
MXDXBVTZWVMXNSPBQXLIMSCCSGXSCJXBOVQXCJZMOJZCVC
TVWJCZAAXZBCSSCJXBQCJZCOJZCNSPOXBXSBTVWJC
JZDXGXXMOZQMSCSCJXBOVQXCJZMOJZCNSPJZHGXXMOSPLH
JZDXZAAXZBXHCSCJXTCSGXSCJXBOVQX
```

— ciphertext

课后习题第10题

Crypto

- □ **Cryptology（密码学）** — The art and science of making and breaking "secret codes"
- □ **Cryptography（密码编码）** — making "secret codes"
- □ **Cryptanalysis（密码分析）** — breaking "secret codes"
- □ **Crypto** — all of the above (and more)

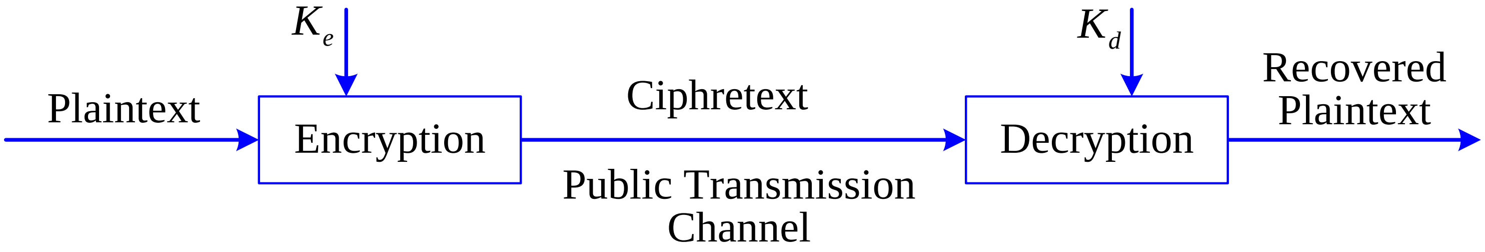
How to Speak Crypto

- A *cipher* or *cryptosystem* is used to *encrypt* the *plaintext*
- The result of encryption is *ciphertext*
- We *decrypt* ciphertext to recover plaintext
- A *key* is used to configure a cryptosystem
- A *symmetric key* cryptosystem uses the same key to encrypt as to decrypt
- A *public key* cryptosystem uses a *public key* to encrypt and a *private key* to decrypt

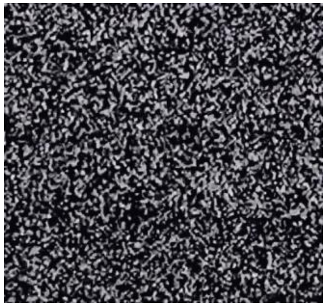
Crypto

- Basic assumptions
  - The system is completely known to the attacker
  - Only the key is secret
  - That is, crypto algorithms are not secret
- This is known as **Kerckhoffs' Principle**
- Why do we make such an assumption?
  - Experience has shown that secret algorithms tend to be weak when exposed
  - Secret algorithms never remain secret
  - Better to find weaknesses beforehand

密码的一般性模型



0100100101101
1100110011001
10



Cryptology:

Cryptography studies how to design good encryption algorithms

Cryptanalysis tries to find security weaknesses of proposed algorithms and studies whether they are vulnerable to some attacks

Kerckhoffs's Principle

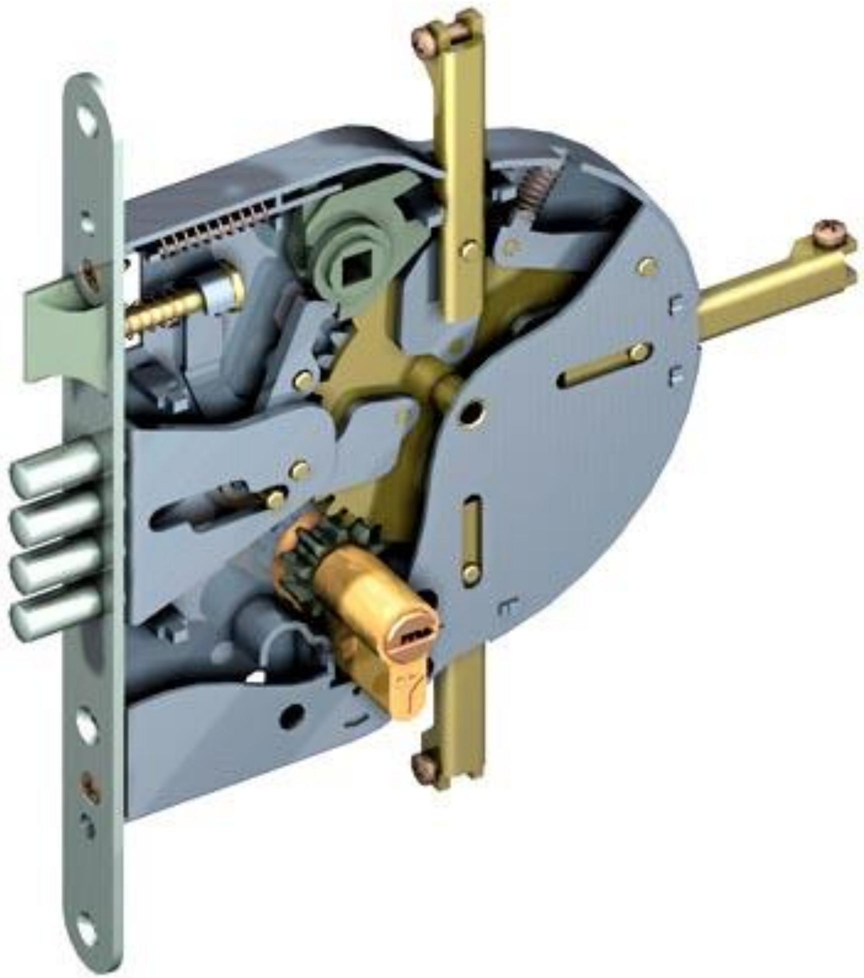
A cryptosystem should be secure even if everything about the system, except the **key**, is public knowledge.

1883 La Cryptographie Militaire ("Military Cryptography"),
le Journal des Sciences Militaires ("Journal of Military Science")

Dr. Jean Guillaume Auguste Victor François Hubert Kerckhoffs
(1835-1903), Dutch (Hollander)

https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle

Kerckhoffs's Principle (cont’d)



1. Key is reused
2. Structure is public

Claude Shannon's maxim

Claude Shannon's maxim:
"The enemy knows the system."

Claude Elwood Shannon (1916-2001), father of information theory and cryptography

Shannon Claude
Communication Theory of Secrecy Systems
Bell System Technical Journal, vol. 28 no. 4, pp. 656-715, 1949
Cited **13071** times in Scholar.Google

www.bilibili.com/video/BV1YV411z7qo/?spm_id_from=333.337.search-card.all.click%20%0Bhttps://**thebitplayer**.com

Who meets Shannon or Shannon meets whom

Simple Substitution(简单替换)

- Plaintext: fourscoreandsevenyearsago
- Key:

Plaintext	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	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

- Ciphertext:

  IRXUVFRUHDQGVHYHQBHDUVDJR

- Shift by 3 is "Caesar's cipher"

Caesar's Cipher Decryption

- Suppose we know a Caesar's cipher is being used:

Plaintext	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	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

- Given ciphertext:
  VSRQJHEREVTXDUHSDQWV
- Plaintext: spongebobsquarepants

Caesar's Cipher

- Shift by n for some $n \in \{0,1,2,\ldots,25\}$
- Then key is n
- Example: key $n = 7$

Plaintext	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	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

Cryptanalysis I: Try Them All

- We know Caesar's cipher and shift by n used
  - But the specific key is unknown
- Given ciphertext: CSYEVIXIVQMREXIH
- How to determine the key?
- Only 26 possible keys — try them all!
- **Exhaustive key search(穷举搜索密钥)**
- Solution: key is $n = 4$

Simple Substitution: General Case

- In general, simple substitution key can be any **permutation** of letters**(字母的任意置换)**
  - Not necessarily a Caeser's cipher (shift)
- For example

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

- In general, $26! > 2^{88}$ possible keys

意味着Trudy用普通的穷举式密钥检索以每秒执行2^{40}次（千亿次级别）密钥计算的超级计算机，约需花费890万年才能尝试完所有可能的密钥，平均工作量也是445万年。

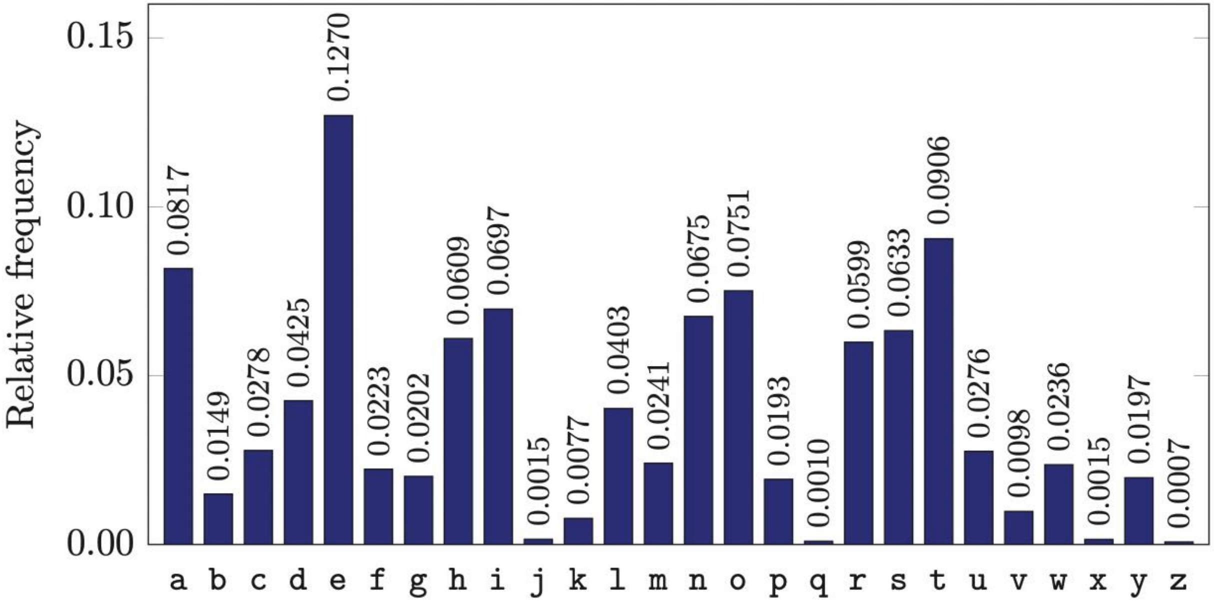
Cryptanalysis II: Be Clever

- We know that a simple substitution used
- But ***not*** necessarily a Ceasar's cipher (shift)
- Find the key given the ciphertext:

PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOX
BTFXQWAXBVCXQWAXFQJVWLEQNTOZQGGQLFXQWAKVWLXQ
WAEBIPBFXFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVWLXGD
PEQVPQGVPPBFTIXPFHXZHVFAGFOTHFEFBQUFTDHZBQPOTHXTY
FTODXQHFTDPTOGHFQPBQWAQJJTODXQHFOQPWTBDHHIXQV
APBFZQHCFWPFHPBFIPBQWKFABVYYDZBOTHPBQPQJTQOTOGHF
QAPBFEQJHDXXQVAVXEBQPEFZBVFOJIWFFACFCCFHQWAUVWF
LQHGFXVAFXQHFUFHILTTAVWAFFAWTEVOITDHFHFQAITIXPFH
XAFQHEFZQWGFLVWPTOFFA

Cryptanalysis II

- Cannot try all 2^{88} simple substitution keys
- Can we be more clever?
- English letter frequency counts… (英语字母的使用频率统计)



Cryptanalysis II

- Ciphertext:

```
PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQ
WAXBVCXQWAXFQJVWLEQNTOZQGGQLFXQWAKVWLXQWAEBIPBFXFQ
VXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVWLXGDPEQVPQGVPPBFTIXPFH
XZHVFAGFOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQPBQW
AQJJTODXQHFOQPWTBDHHIXQVAPBFZQHCFWPFHPBFIPBQWKFABVYY
DZBOTHPBQPQJTQOTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJIWFF
ACFCCFHQWAUVWFLQHGFXVAFXQHFUFHILTTAVWAFFAWTEVOITDHFH
FQAITIXPFHXAFQHEFZQWGFLVWPTOFFA
```

- Analyze this message using statistics below

Ciphertext frequency counts:

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
21	26	6	10	12	51	10	25	10	9	3	10	0	1	15	28	42	0	0	27	4	24	22	28	6	8

Cryptanalysis II

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
21	26	6	10	12	51	10	25	10	9	3	10	0	1	15	28	42	0	0	27	4	24	22	28	6	8

F→ e，Q或P或X→t

密文头几个字母PBFP…

1. 把F替换成e之后，PBeP….
2. 猜测P很可能是t
3. P替换成t之后，tBet….
4. 可以猜测B为h，因为the为一个常见的单词
5. 把密文中所有出现P，B，F的地方全部替换成明文再继续用类似的方法分析…..

（课后习题的第9题）

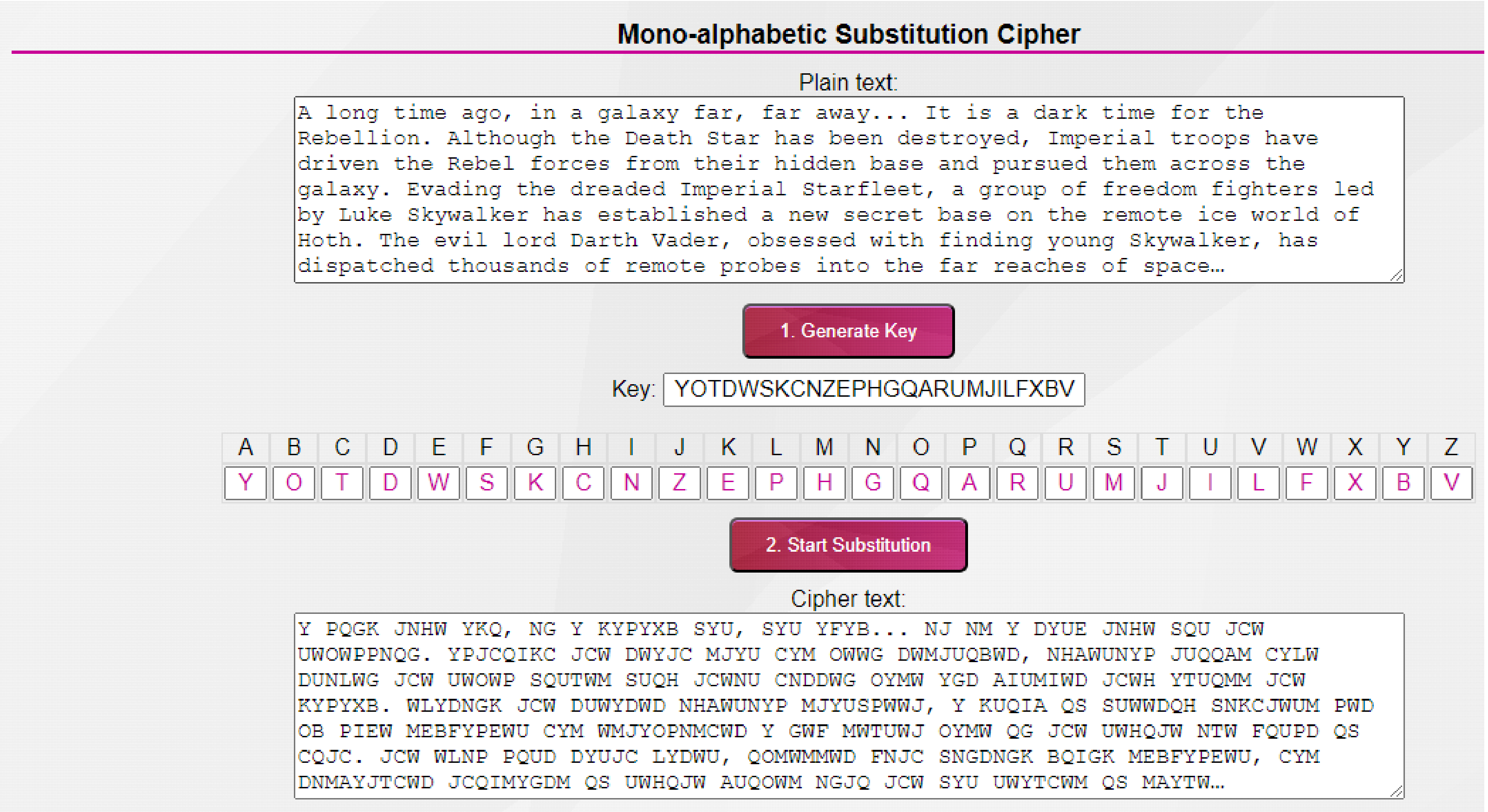
Cryptanalysis: Terminology

- Cryptosystem is **secure** if best know attack is to try all keys
  - Exhaustive key search, that is
- Cryptosystem is **insecure** if ***any*** shortcut attack is known
- But then insecure cipher might be harder to break than a secure cipher!
  - What the … ?

Mono-Alphabetic Substitution Cipher

A mono-alphabetic cipher (simple substitution cipher) is a substitution cipher where each letter of the plain text is replaced with another letter of the alphabet. It uses a fixed key which consist of the 26 letters of a “shuffled alphabet”.

You can generate your own encryption keys and encrypt your own messages using our online mono-alphabetic substitution engine:



Mono-alphabetic Substitution Cipher

Plain text:

```
A long time ago, in a galaxy far, far away... It is a dark time for the
Rebellion. Although the Death Star has been destroyed, Imperial troops have
driven the Rebel forces from their hidden base and pursued them across the
galaxy. Evading the dreaded Imperial Starfleet, a group of freedom fighters led
by Luke Skywalker has established a new secret base on the remote ice world of
Hoth. The evil lord Darth Vader, obsessed with finding young Skywalker, has
dispatched thousands of remote probes into the far reaches of space…
```

Key: YOTDWSKCNZEPHGQARUMJILFXBV

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

Cipher text:

```
Y PQGK JNHW YKQ, NG Y KYPYXB SYU, SYU YFYB... NJ NM Y DYUE JNHW SQU JCW
UWOWPPNQG. YPJCQIKC JCW DWYJC MJYU CYM OWWG DWMJUQBWD, NHAWUNYP JUQQAM CYLW
DUNLWG JCW UWOWP SQUTWM SUQH JCWNU CNDDWG OYMW YGD AIUMIWD JCWH YTUQMM JCW
KYPYXB. WLYDNGK JCW DUWYDWD NHAWUNYP MJYUSPWWJ, Y KUQIA QS SUWWDQH SNKCJWUM PWD
OB PIEW MEBFYPEWU CYM WMJYOPNMCWD Y GWF MWTUWJ OYMW QG JCW UWHQJW NTW FQUPD QS
CQJC. JCW WLNP PQUD DYUJC LYDWU, QOMWMMWD FNJC SNGDNGK BQIGK MEBFYPEWU, CYM
DNMAYJTCWD JCQIMYGDM QS UWHQJW AUQOWM NGJQ JCW SYU UWYTCWM QS MAYTW…
```

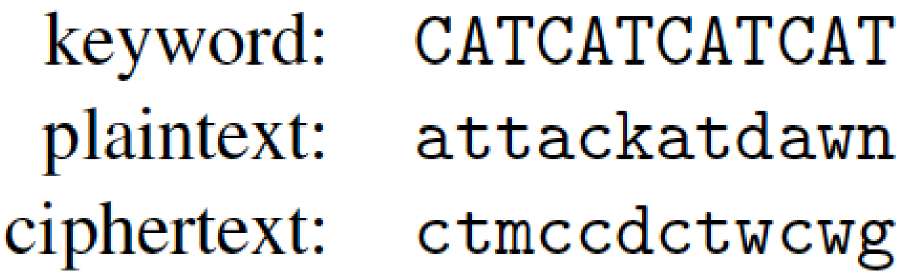
www.101computing.net/mono-alphabetic-substitution-cipher

Vigenere Cipher

- Simple substitution is ***monoalphabetic***(单字母替换)
- Vigenere cipher is simple example of a ***polyalphabetic*** substitution (多字母替换)
  - Caesars ciphers, based on a keyword D (shift by 3)
- For example, keyword CAT indicates shift by 2, shift by 0, shift by 19
  - Then repeat as needed

Vigenere Example

- Suppose that we want to encrypt attackatdawn
- Encryption:



keyword:	CATCATCATCAT
plaintext:	attackatdawn
ciphertext:	ctmccdctwcwg

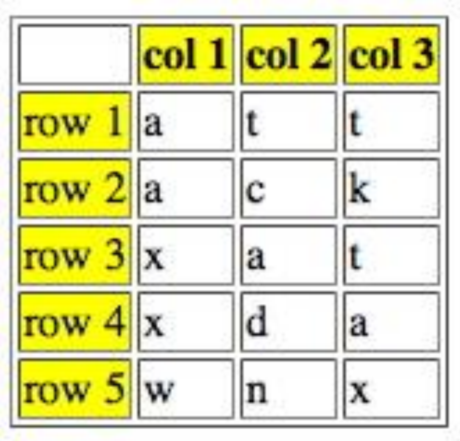
- Ciphertext is ctmccdctwcwg
- How to decrypt? How to attack?

To attack a Vigenere ciphertext, we first need to determine keyword length.

Crack Vigenere Ciphertext using statistic method
https://github.com/DavidLee528/VigenereCracker

Double Transposition

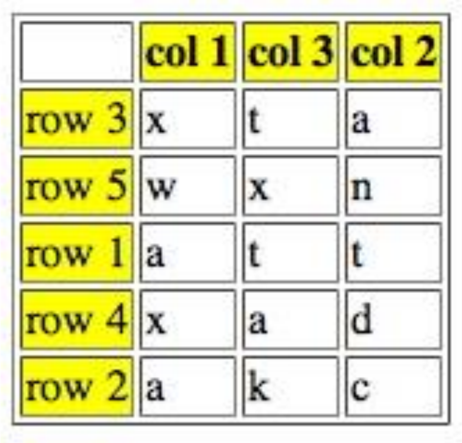
- Plaintext: attackxatxdawn



	col 1	col 2	col 3
row 1	a	t	t
row 2	a	c	k
row 3	x	a	t
row 4	x	d	a
row 5	w	n	x

Permute rows and columns

⇒



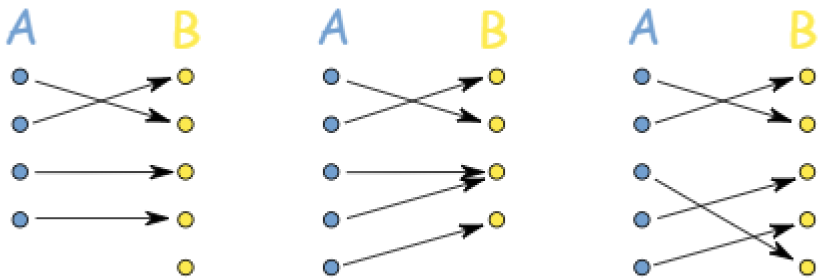
	col 1	col 3	col 2
row 3	x	t	a
row 5	w	x	n
row 1	a	t	t
row 4	x	a	d
row 2	a	k	c

- Ciphertext: xtawxnattxadakc
- Key is matrix size (3, 5) and permutations: (1,4,2) and (1,3,2)

Transposition Cipher（置换密码）

（置换）有限集X上的运算σ：X→X， σ是一个双射函数。

- σ既是单射又是满射，并且定义域和值域相同，那么称σ为一个置换。



单射
非满射

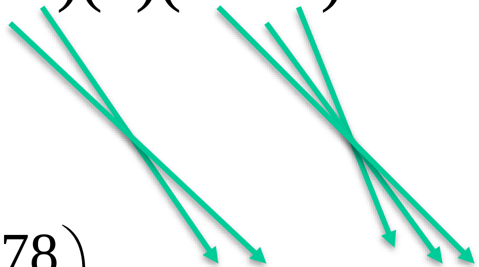
满射
(非单射)

双射
(单射及满射)

- 若σ是一个置换，∀*x*∈X，存在唯一的*x*使得σ(*x*)= *x* ' 。
- 同理可以定义逆置换σ^{-1} ：X→X，σ^{-1}也是双射函数，并且σ^{-1}的定义域和值域相同，即∀*x*′∈X,存在唯一的*x*∈X使得$\sigma^{-1}(x')=x$。
- $\sigma\sigma^{-1}$ =I（单位变换）

设有限集X={1,2,3,4,5,6,7,8}，σ为X上的一个置换，并且满足σ(1)=2, σ(2)=5, σ(3)=3, σ(4)=6, σ(5)=1, σ(6)=8, σ(7)=4, σ(8)=7.因为置换可以简单用对换表示，所以上述置换σ可以形式化表示为对换的乘积，即

$$\sigma = \begin{pmatrix} 12345678 \\ 25361847 \end{pmatrix} = (125)(3)(4687)$$



则其逆置换σ^{-1}可以表示为

$$\sigma^{-1} = \begin{pmatrix} 12345678 \\ 25361847 \end{pmatrix}^{-1} = \begin{pmatrix} 12345678 \\ 51372486 \end{pmatrix} = (152)(3)(4786)$$

C. Li, K.-T. Lo
Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks
https://doi.org/10.1016/j.sigpro.2010.09.014

One-Time Pad: Encryption

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Encryption: Plaintext ⊕ Key = Ciphertext

	h	e	i	l	h	i	t	l	e	r
Plaintext:	001	000	010	100	001	010	111	100	000	101
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	110	101	100	001	110	110	111	001	110	101
	s	r	l	h	s	s	t	h	s	r

One-Time Pad: Decryption

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Decryption: Ciphertext ⊕ Key = Plaintext

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
Key:	111	101	110	101	111	100	000	101	110	000
Plaintext:	001	000	010	100	001	010	111	100	000	101
	h	e	i	l	h	i	t	l	e	r

One-Time Pad

Double agent claims following "**key**" was used:

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
"**key**":	101	111	000	101	111	100	000	101	110	000
"Plaintext":	011	010	100	100	001	010	111	100	000	101
	k	i	l	l	h	i	t	l	e	r

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

One-Time Pad

Or, might claim the key is…

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
"key":	111	101	000	011	101	110	001	011	101	101
"Plaintext":	001	000	100	010	011	000	110	010	011	000
	h	e	l	i	k	e	s	i	k	e

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

One-Time Pad Summary

- Provably secure
  - Ciphertext gives no useful info about plaintext
  - All plaintexts are ***equally likely***
- BUT, only when be used correctly
  - Pad must be random, used only once
  - Pad is known only to sender and receiver
- Note: pad (key) is same size as message
- So, why not distribute message itself, instead of the pad?

Real-World One-Time Pad

- Project VENONA
  - Soviet spies encrypted messages from U.S. to Moscow in 30's, 40's, and 50's
  - Nuclear espionage, etc.
  - Thousands of messages
- Spy carried one-time pad into U.S.
- Spy used pad to encrypt secret messages
- Repeats within the "one-time" pads made cryptanalysis possible

Venona project

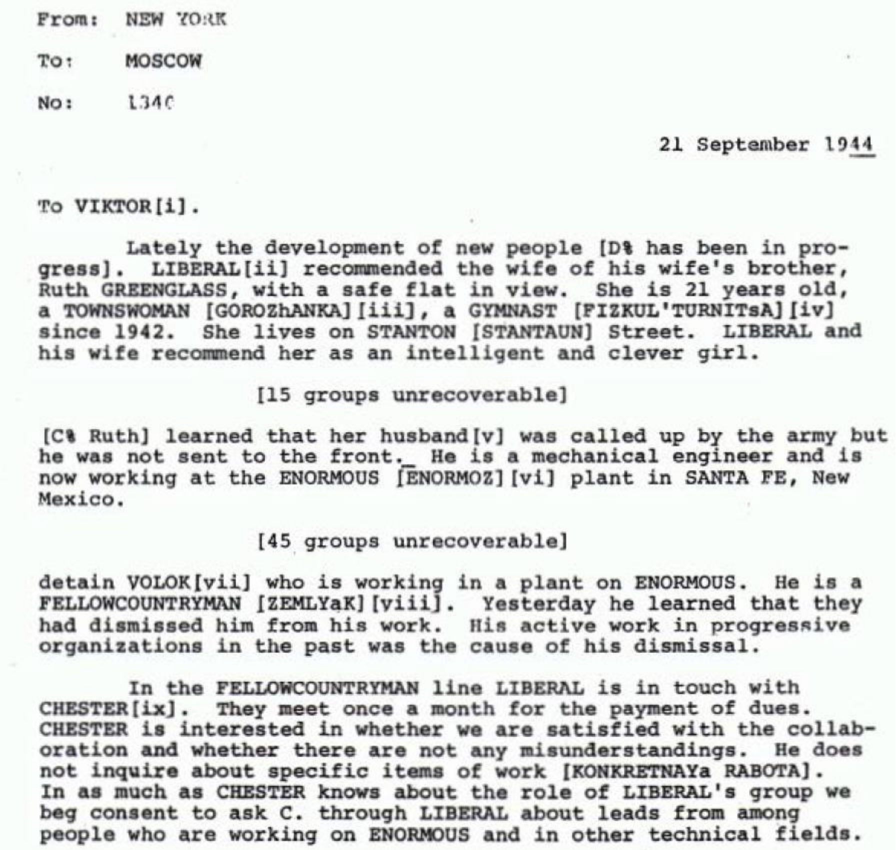
The Venona project was a United States counterintelligence program initiated during World War II by the United States Army's Signal Intelligence Service and later absorbed by the National Security Agency (NSA), that ran from February 1, 1943, until October 1, 1980. It was intended to decrypt messages transmitted by the intelligence agencies of the Soviet Union (e.g. the KGB).

During the 37-year duration of the Venona project, the Signal Intelligence Service decrypted and translated approximately 3,000 messages. The signals intelligence yield included discovery of the Cambridge Five espionage ring in the United Kingdom and Soviet espionage of the Manhattan Project in the US.

Some of the espionage was undertaken to support the Soviet atomic bomb project. The Venona project remained secret for more than 15 years after it concluded. Some of the decoded Soviet messages were not declassified and published by the United States until 1995.

https://en.wikipedia.org/wiki/Venona_project

VENONA Decrypt (1944)



From: NEW YORK

To: MOSCOW

No: 1340

21 September 1944

To VIKTOR[i].

Lately the development of new people [D% has been in progress]. LIBERAL[ii] recommended the wife of his wife's brother, Ruth GREENGLASS, with a safe flat in view. She is 21 years old, a TOWNSWOMAN [GOROZhANKA][iii], a GYMNAST [FIZKUL'TURNITsA][iv] since 1942. She lives on STANTON [STANTAUN] Street. LIBERAL and his wife recommend her as an intelligent and clever girl.

[15 groups unrecoverable]

[C% Ruth] learned that her husband[v] was called up by the army but he was not sent to the front. He is a mechanical engineer and is now working at the ENORMOUS [ENORMOZ][vi] plant in SANTA FE, New Mexico.

[45 groups unrecoverable]

detain VOLOK[vii] who is working in a plant on ENORMOUS. He is a FELLOWCOUNTRYMAN [ZEMLYaK][viii]. Yesterday he learned that they had dismissed him from his work. His active work in progressive organizations in the past was the cause of his dismissal.

In the FELLOWCOUNTRYMAN line LIBERAL is in touch with CHESTER[ix]. They meet once a month for the payment of dues. CHESTER is interested in whether we are satisfied with the collaboration and whether there are not any misunderstandings. He does not inquire about specific items of work [KONKRETNAYa RABOTA]. In as much as CHESTER knows about the role of LIBERAL's group we beg consent to ask C. through LIBERAL about leads from among people who are working on ENORMOUS and in other technical fields.

- "Ruth" == Ruth Greenglass
- "Liberal" == Julius Rosenberg
- "Enormous" == the atomic bomb

https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/venona/dated/1944/21sep_recruitment_by_rosenbergs.pdf

Codebook Cipher

- Literally, a book filled with "codewords"
- Zimmerman Telegram encrypted via codebook

Februar	13605
fest	13732
finanzielle	13850
folgender	13918
Frieden	17142
Friedenschluss	17149
:	:

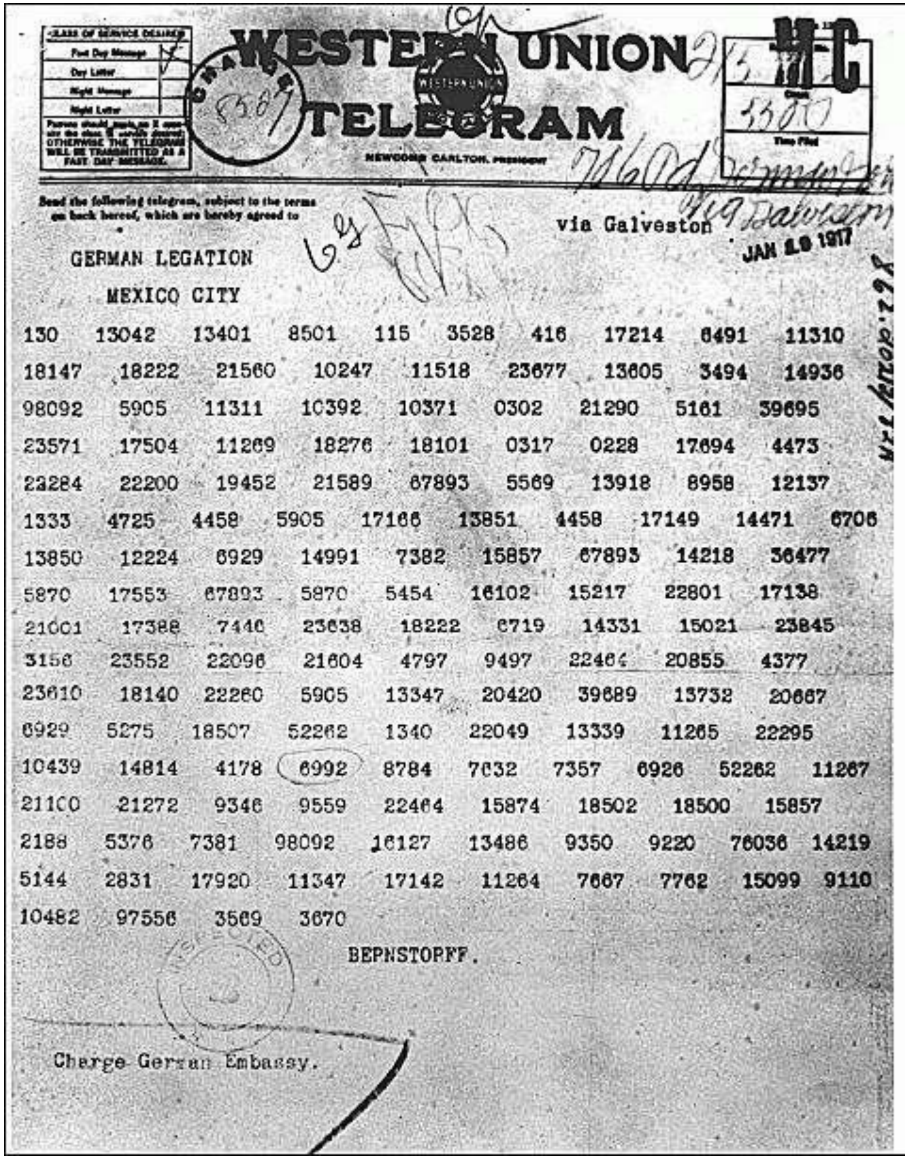
- Modern block ciphers are codebooks!
- More about this later…

Codebook Cipher: Additive

- Codebooks also (usually) use **additive**
- Additive — book of “random” numbers
  - Encrypt message with codebook
  - Then choose position in additive book
  - Add additive sequence to get ciphertext
  - Send ciphertext and additive position (MI)
  - Recipient subtracts additives before decrypting
- Why use an additive sequence?

Zimmermann Telegram

- Perhaps most famous codebook ciphertext ever
- A major factor in U.S. entry into World War I



CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Check

Time Filed

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

via Galveston

JAN 19 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  7440   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
```

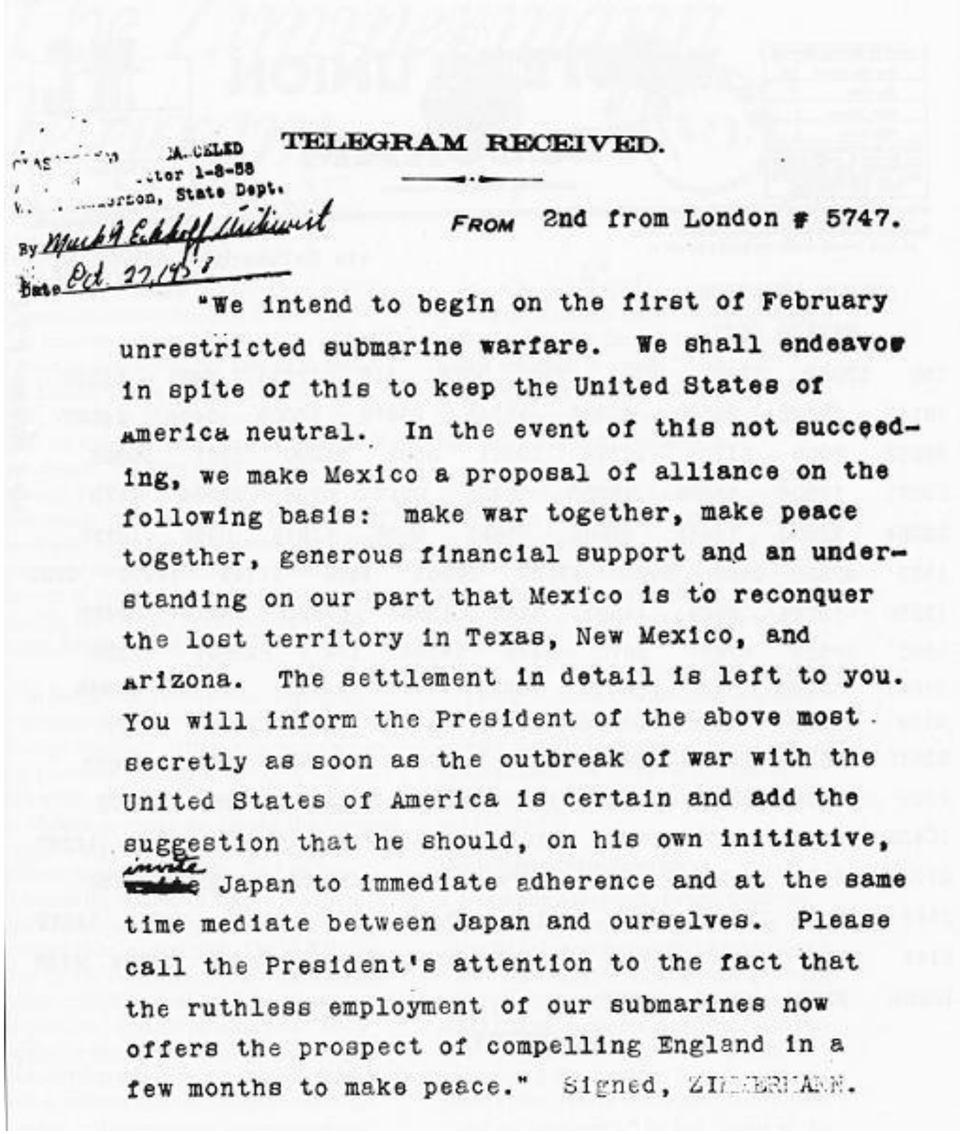
BEPNSTOPFF.

INSPECTED

Charge German Embassy.

Zimmermann Telegram Decrypted

- British had recovered partial codebook
- Then able to fill in missing parts



..CELED
..tor 1-8-58
..rton, State Dept.

By Mack A Eckhoff Archivist

Date Oct. 22,1957

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.

Random Historical Items（历史上密码事件）

- Crypto timeline
- Spartan Scytale — transposition cipher （大约公元前5世纪内，置换密码）
- Caesar's cipher （公元前1世纪内，替换密码）
- Edgar Allan Poe's short story: *The Gold Bug (1843)*（对字母的频率分析）
- Election of 1876 （置换与替替换的结合）

Election of 1876

- Rutherfraud Hayes vs SwindlingTilden
- Electoral college delegations for 4 states (including Florida) in dispute（选举团在4个州存在分歧）
- Commission gave all 4 states to Hayes
  - Vote on straight party lines
- Tilden accused Hayes of bribery
  - Was it true?（全部投给共和党被控告贿赂？）

Election of 1876

- Encrypted messages by Tilden supporters later emerged
- Cipher: Partial codebook, plus transposition
- Codebook substitution for important words

ciphertext	**plaintext**
Copenhagen	Greenbacks
Greece	Hayes
Rochester	votes
Russia	Tilden
Warsaw	**telegram**
:	:

Election of 1876

- Apply codebook to original message
- Pad message to multiple of 5 words (total length, 10,15,20,25 or 30 words)
- For each length, a fixed permutation applied to resulting message
- Permutations found by comparing several messages of same length
- Note that the **same key** is applied to all messages of a given length

Election of 1876

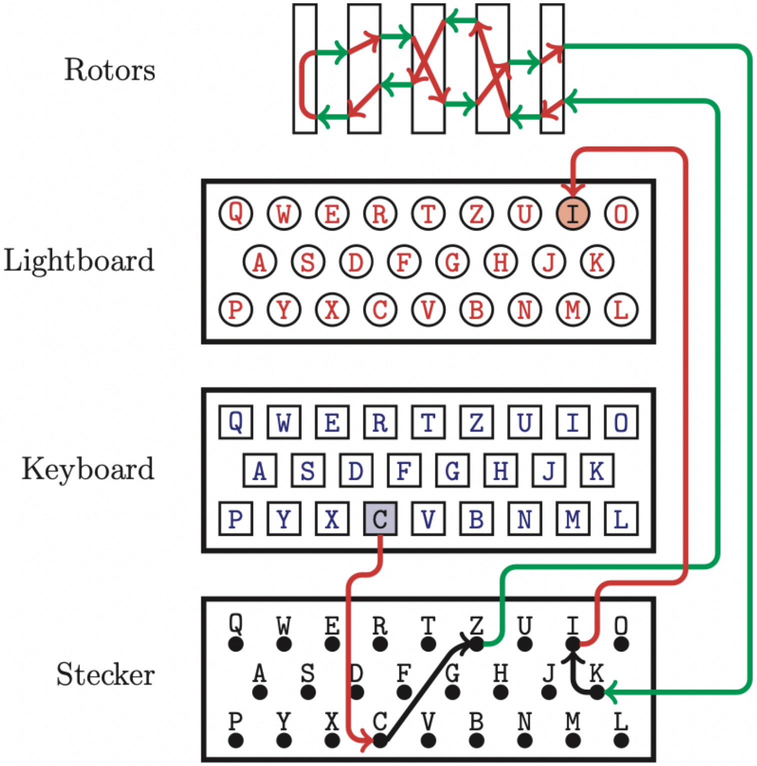
- Ciphertext: **Warsaw they read all unchanged last are idiots can't situation**
- Codebook: Warsaw == telegram
- Transposition: 9,3,6,1,10,5,2,7,4,8
- Plaintext: **Can't read last telegram. Situation unchanged. They are all idiots.**
- A weak cipher made worse by reuse of key
- Lesson? Don't overuse keys!

Early 20th Century

- WWI — Zimmermann Telegram
- "Gentlemen do not read each other's mail"
  - Henry L. Stimson, Secretary of State, 1929
- WWII — golden age of cryptanalysis
  - Midway/Coral Sea
  - Japanese **Purple** (codename **MAGIC**)
  - German **Enigma** (codename **ULTRA**)

Enigma Cipher Machine

- Most famous cipher of WWII
  - Electro-mechanical device
  - Very rugged, used in the field

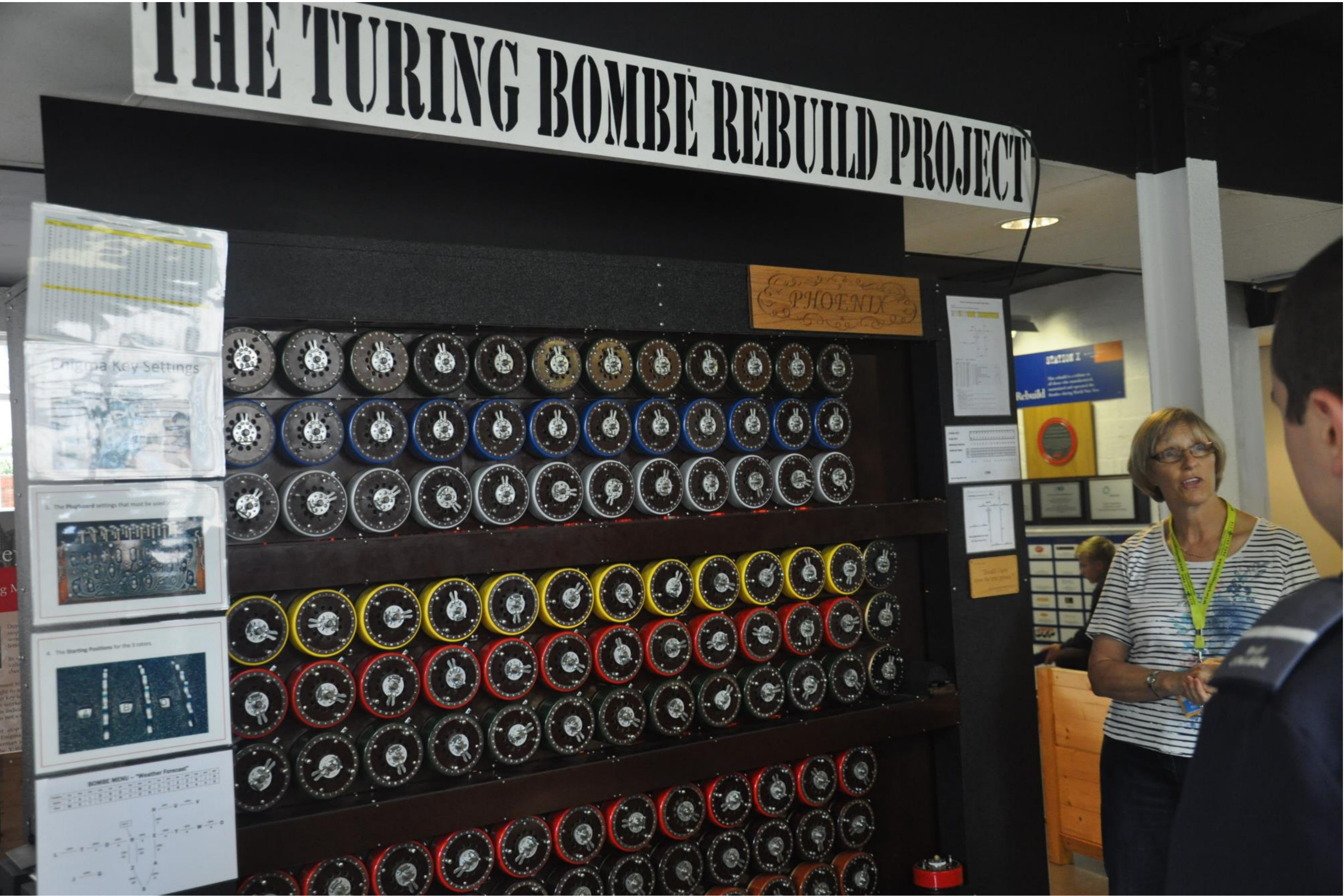


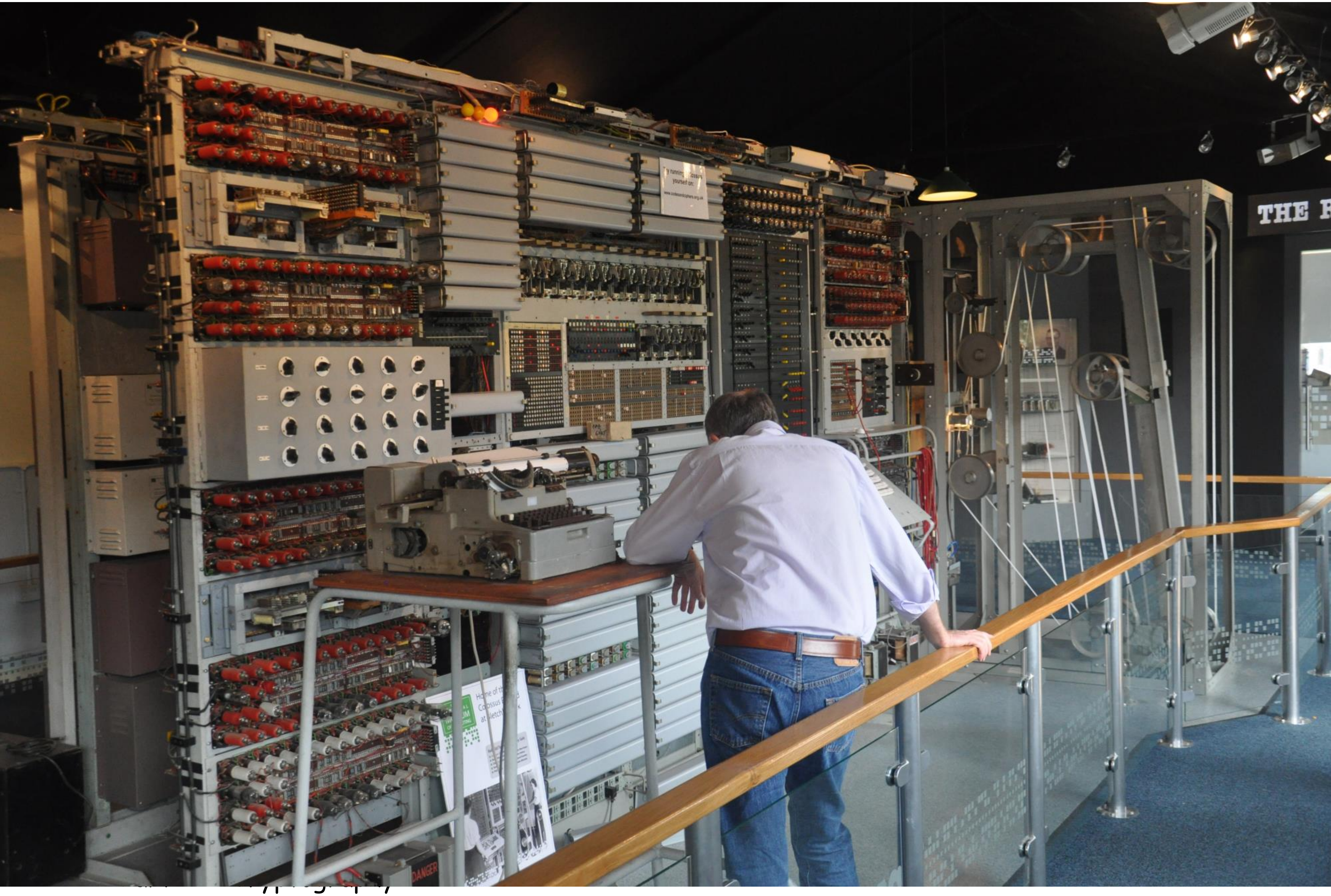
An Acoustic Side Channel Attack on Enigma
https://eprints.ncl.ac.uk/211469

Post-WWII History

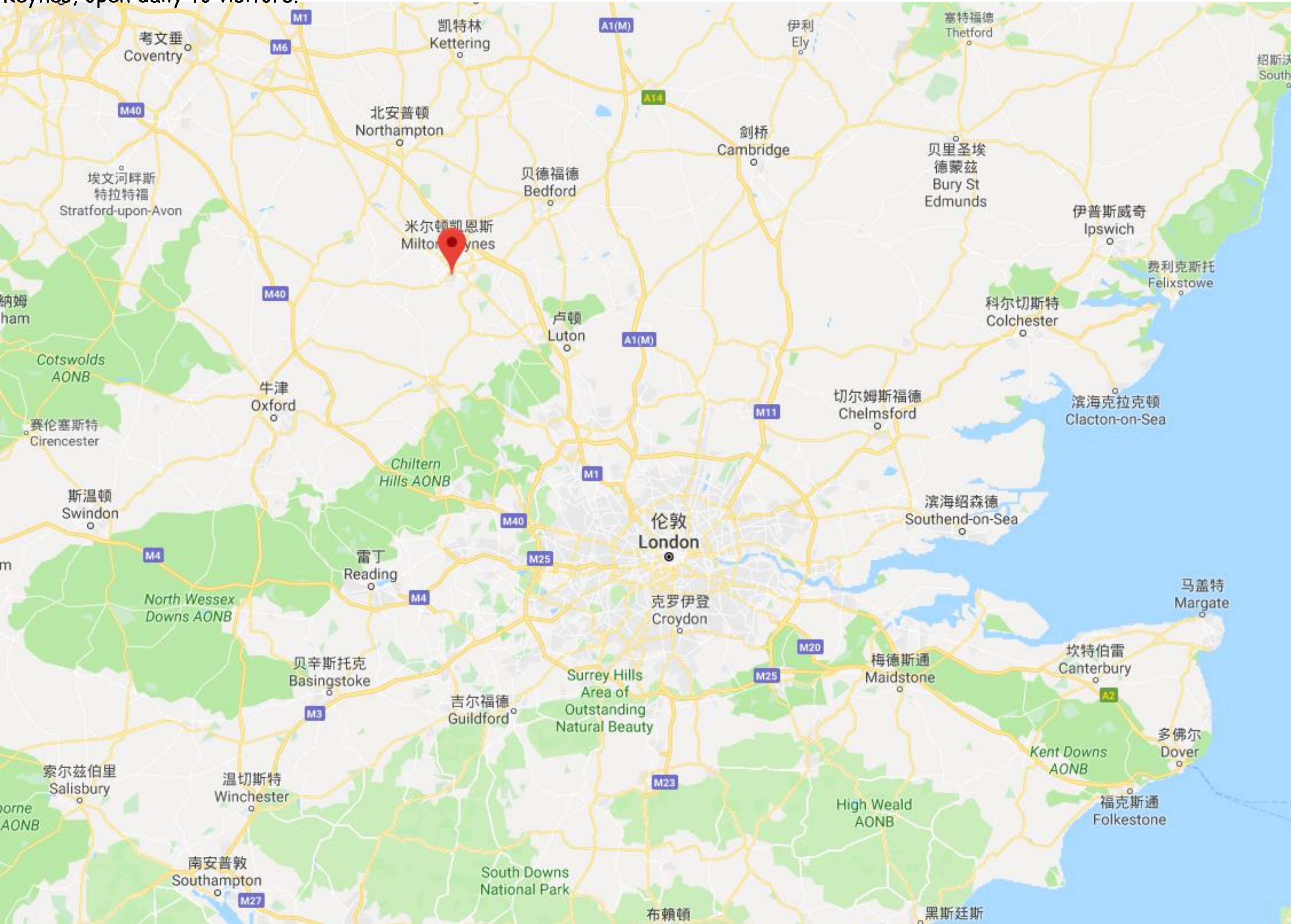
- Claude Shannon — father of the science of information theory
- Computer revolution — lots of data to protect
- Data Encryption Standard (DES), 70's
- Public Key cryptography, 70's
- CRYPTO conferences, 80's
- Advanced Encryption Standard (AES), 90's
- The crypto genie is out of the bottle…

The bombe was an electro-mechanical device used by British cryptologists to help decipher German Enigma-machine-encrypted secret messages during World War II.
https://en.wikipedia.org/wiki/Bombe


THE TURING BOMBE REBUILD PROJECT
PHOENIX
Enigma Key Settings
BOMBE MENU – "Weather Forecast"


Try running Colossus yourself on:
THE R
DANGER

Bletchley Park, once the top-secret home of the World War Two Codebreakers, is now a vibrant heritage attraction in Milton Keynes, open daily to visitors.



Post-WWII History

- Claude Shannon — father of the science of information theory
- Computer revolution — lots of data to protect
- Data Encryption Standard (DES), 70's
- Public Key cryptography, 70's
- CRYPTO conferences, 80's
- Advanced Encryption Standard (AES), 90's
- The crypto genie is out of the bottle…

Claude Shannon

- Founded field of information theory
- His 1949 paper: *Communication Theory of Secrecy Systems*
- Fundamental concepts
  - **Confusion** — obscure relationship between plaintext and ciphertext
  - **Diffusion** — spread plaintext statistics through the ciphertext
- Proved one-time pad is secure
- One-time pad is confusion-only, while double transposition is diffusion-only

The Bit Player. 2018
www.bilibili.com/video/BV1EZ4y1377j?spm_id_from=333.337.search-card.all.click

Taxonomy of Cryptography

- **Symmetric Key**
  - Same key for encryption and decryption
  - Modern types: Stream ciphers, Block ciphers
- **Public Key** (or "asymmetric" crypto)
  - Two keys, one for encryption (public), and one for decryption (private)
  - And digital signatures — nothing comparable in symmetric key crypto
- **Hash algorithms**
  - Can be viewed as "one way" crypto

Taxonomy of Cryptanalysis（密码分析的分类）

- From perspective of info available to Trudy
  - Ciphertext only（ Trudy只知道密文）
  - Known plaintext（Trudy知道部分明文-密文对）
  - Chosen plaintext（Trudy可以选择部分明文来加密）
    - “Lunch time attack”（Alice吃午饭忘退出电脑，Trudy在她回来之前可以加密部分选定的消息）
    - Protocols might encrypt chosen data
  - Adaptively chosen plaintext（Trudy根据观测到的密文选择下一个明文）
  - Forward search (只适用于公钥密码，用公钥加密假定的明文去与截获的密文匹配)
  - And others…

作业题

- 第2章的29个题目，每人所做题目为学号的后两位%29！学号末尾为29的同学做第29题。