

## Caesar Cipher Example

plaintext: Z O O

plaintext as numbers: 25 14 14

use key = 3     ↓ ↓ ↓

ciphertext as numbers: 28 17 17

ciphertext: C R R

## Groupwork

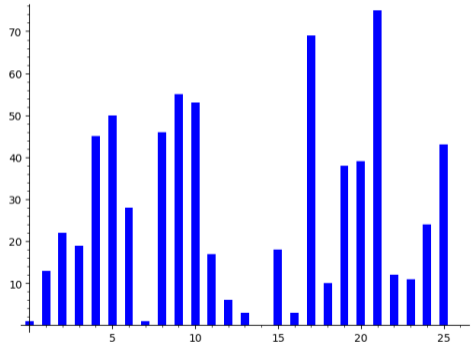
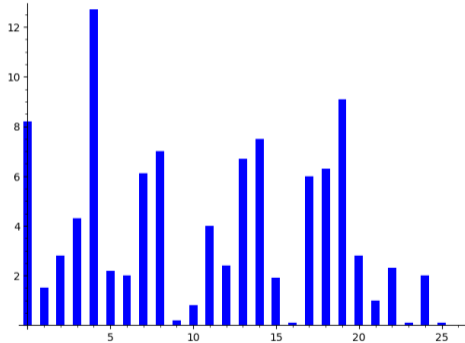
1. Log into our discord server.
2. Leave yourself muted on the main zoom call; I will also mute unless I have an announcement. But leave the zoom channel sound on, so if I make an announcement, it interrupts you.
3. Let  $n$  be your birthday of the month (1 through 31), or a madeup birthday. Take  $n$  modulo 7, with result that  $n$  is in the range 0 through 6.
4. In discord, under category "IN CLASS", enter the voice channel "Breakout  $n$ ".
5. Turn on voice and video in discord and say hello to your small group. Some people will be joining the discord server slowly, so wait a few minutes if you are alone.
6. I will announce when to start the activity via the main zoom channel and put the activity up on the video in the main zoom channel. Meanwhile, introduce yourselves, and when new people arrive, welcome them. (If you are still alone when I announce the main activity, pick a new birthday and join that room.)

## Groupwork

1. As a group, choose a cyclic ordering of the people. Alphabetical is convenient.
2. Everyone choose a secret key, a number between 1 and 25 inclusive.
3. Silently, decide on your answer to the question "What superpower do you want to have?" It should be one word or a few short words.
4. Encrypt your answer in Caesar cipher using the key you chose (by hand).
5. Give your key and ciphertext to the next person in the ordering by typing it into the corresponding voice channel "# group- $n$ " (everyone will see it, but indicate who it is for)
6. You will get a key and ciphertext from the previous person in the ordering. Decrypt it (by hand).
7. When everyone has decrypted, go around the ordering sharing what you decrypted and the encryptor can elaborate on the significance of their answer.
8. When you are done, type "group  $n$  done" into the coordination channel
9. Use the coordination channel to ask me questions or request I visit your group
10. Keep chatting until I call you all back to the main zoom call

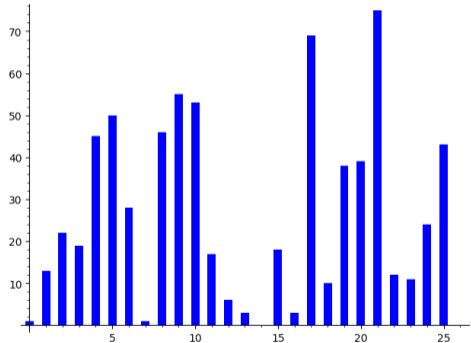
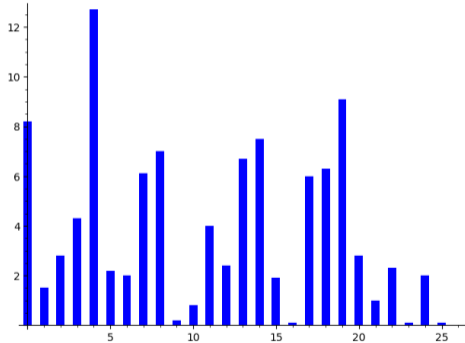
# Frequency Analysis

ciphertext = "JFEPJIVTVEKVLIFGVRETUIVCVRJVJWIFDRIKZJKJLTJRJTVCZEVUZFEJYRBZIRREUAVEEZWWICFGVQTFEKRZEJFEPURUT  
JTFGPGIFKVTKZFEDVKYFUDRIBVKVURJBVPRLUZFKYVJPJKVDEFIDRCCPGIVMVEKJLJVJWIFDIZGGZEXTUKIRTBKFDGWZC  
VJSPGCRTZEXRJDRCSSZKFWTFDGLKVIURKRFEKYVUZJTULIZEXKYVGIFTVJJFWDRBZEXKYVXCRJJDRJKVITUKYVEZEJKVRUF  
WIVTFXEZQZEXZEUMZULRCRLUZFKIRTBJRFTDGLKVIIVRUJKYVURKRKIRTBREUZXEFIVJKYVRLUZFKIRTBJGIVMVEKZEXGT  
GCRPSRTBFWKYVDLJZTFECPJKREURCFEVUVMZTVJJLTJRJYFDVJKVIVFJREUGFIKRSCVTUGCRPVIJTREIVTFXEZQVREUGCRP  
KYVRLUZFKIRTBJFEKYVUZJTJSPFSJTLIZEXKYVURKRKIRTBZNZKYRWVCKGVEDRIBFIRGZVTVFWFGRHLVRUYVJZMVGRGVIGIF  
KVTKVUUZJTJ CZBVUZFEJYRMVSVVEDRUVGCRPRSCVREUTFGPRSCVFEYFDVTFDGLKVIJSPIFEYRIIZJKYVRJJFTZRKVUGIVJJ  
WIZURPDRPKYZIKPWZIJKKNFKYFLJREUREUKNF"



# Frequency Analysis

ciphertext = "JFEPJIVTVEKVLIFGVRETUIVCVRJVJWIFDRIKZJKJLTJRJTVCZEVUZFEJYRBZIRREUAVEEZWWICFGVQTFEKRZEJFEPURUT  
JTFGPGIFKVTKZFEDVKYFUDRIBVKVURJBVPRLUZFKYVJPJKVDEFIDRCCPGIVMVEKJLJVJWIFDIZGGZEXTUKIRTBKFDGWZC  
VJSPGCR TZEXRJDRCSSZKFWTFDGLKVIURKRFEKYVUZJTULIZEXKYVGIFTVJJFWDRBZEXKYVXCRJJDRJKVITUKYVEZEJKVRUF  
WIVTFXEZQZEXZEUZMZULRCRLUZFKIRTBJR TFDGLKVIIVRUJKYVURKRKIRTBREUZXEFIVJKYVRLUZFKIRTBJGIVMVEKZEXGT  
GCRPSRTBFWKYVDLJZTFECPJKREURCFEVUVMZTVJJLTJRJYFDVJKVIVFJREUGFIKRSCVTUGCRPVIJTREIVTFXEZQVREUGCRP  
KYVRLUZFKIRTBJFEKYVUZJTJSPFSJTLIZEXKYVURKRKIRTBZNZKYRWVCKGVEDRIBFIRGZVTVFWFGRHLVRUYVJZMVGRGVIGIF  
KVTKVUUZJTJCZBVUZFEJYRMVSVVEDRUVGCRPRSCVREUTFGPRSCVFEYFDVTFDGLKVIJSPIFEYRIIZJKYVRJJFTZRKVUGIVJJ  
WIZURPDRPKYZIKPWZIJKKNFKYFLJREUREUKNF"



key = 17

# Vigenère Cipher Example

plaintext | L I V E L O N G A N D P R O S P E R

# Vigenère Cipher Example

plaintext		L	I	V	E	L	O	N	G	A	N	D	P	R	O	S	P	E	R
plain as #:		11	8	21	4	11	14	13	6	0	13	3	15	17	14	18	15	4	17

## Vigenère Cipher Example

plaintext	L	I	V	E	L	O	N	G	A	N	D	P	R	O	S	P	E	R
plain as #:	11	8	21	4	11	14	13	6	0	13	3	15	17	14	18	15	4	17
key (CRYPTO):	2	17	15	19	14	2	17	15	19	14	2	17	15	19	14	2	17	15

## Vigenère Cipher Example

plaintext	L	I	V	E	L	O	N	G	A	N	D	P	R	O	S	P	E	R
plain as #:	11	8	21	4	11	14	13	6	0	13	3	15	17	14	18	15	4	17
key (CRYPTO):	2	17	15	19	14	2	17	15	19	14	2	17	15	19	14	2	17	15
cipher as #:	13	25	36	23	25	16	30	21	19	27	5	32	32	33	32	17	21	32

## Vigenère Cipher Example

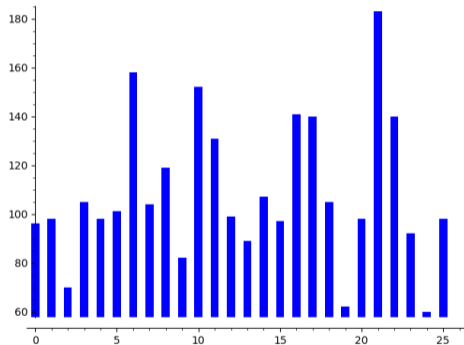
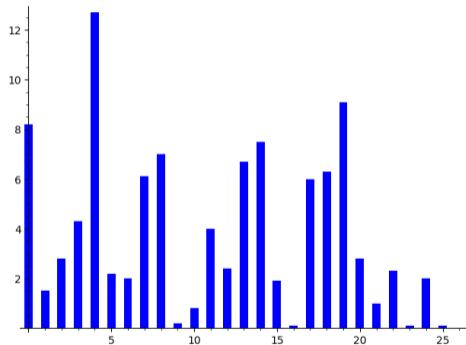
plaintext	L	I	V	E	L	O	N	G	A	N	D	P	R	O	S	P	E	R
plain as #:	11	8	21	4	11	14	13	6	0	13	3	15	17	14	18	15	4	17
key (CRYPTO):	2	17	15	19	14	2	17	15	19	14	2	17	15	19	14	2	17	15
cipher as #:	13	25	36	23	25	16	30	21	19	27	5	32	32	33	32	17	21	32
cipher as #:	13	25	10	23	25	16	4	21	19	1	5	6	6	7	6	17	21	6

## Vigenère Cipher Example

plaintext	L	I	V	E	L	O	N	G	A	N	D	P	R	O	S	P	E	R
plain as #:	11	8	21	4	11	14	13	6	0	13	3	15	17	14	18	15	4	17
key (CRYPTO):	2	17	15	19	14	2	17	15	19	14	2	17	15	19	14	2	17	15
cipher as #:	13	25	36	23	25	16	30	21	19	27	5	32	32	33	32	17	21	32
cipher as #:	13	25	10	23	25	16	4	21	19	1	5	6	6	7	6	17	21	6
ciphertext:	N	Z	K	X	Z	Q	E	V	T	B	F	G	G	H	G	R	V	G

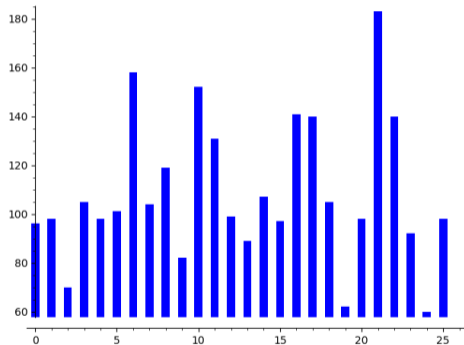
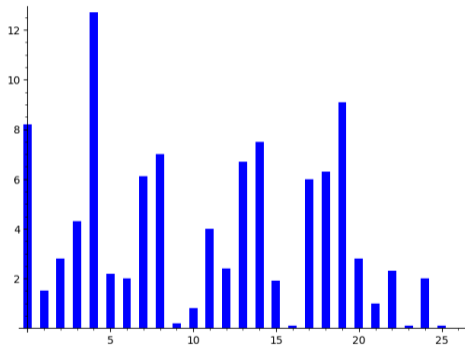
# Frequency Analysis on Vigenère

ciphertext = "PGHKXUWUAHKQVDBVCWIOVLVIZMEJLXCXHZQFPTSWGADVPKQRHKQNST'ZQLVHKRGLRVIEIPGXTFWE  
XWRNDYXUFUGCRBLKQPQPFJMTYVZGUMGHTYAFQVDLNFSQLRCSVUDTNOHZQVMNPTVHDFVMEZWVWDOGNDOM  
FZMCAJQXOTVJUQRKWZQIIVRIEKIIOPLFDUGYRGZHIWDLBJLBAYJUAVBQWFFLRVGKRQEBAKCXRJPZUTSR  
YDZIOVLOKWKVEAHLVRIODDKMCQVLKIUSRRNHZUKAZQIIVRIEGUUAWSGZHZCXHAWYMTCEJSQGNSORFHAU  
YJRAWPGBSSLKMOPSELMKMBHNQVEGBIYGQODOJBHBJOHNQVWHZLBLROTKTUKPGHSVFLIIPMMRKUMIKVQA..."



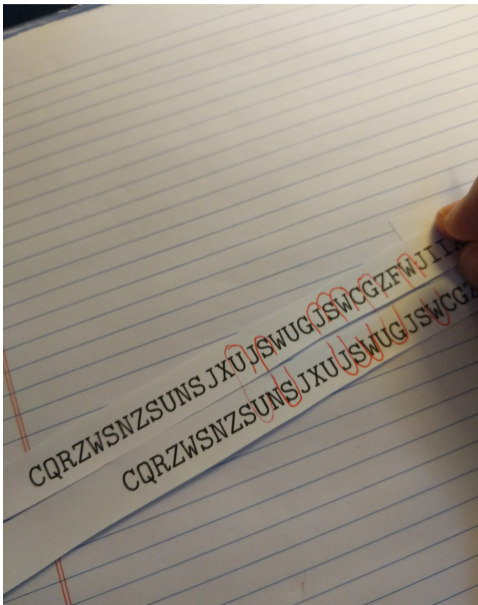
# Frequency Analysis on Vigenère

ciphertext = "PGHKXUWUAHKQVDBVCWIOVLVIZMEJLXCXHZQFPTSWGADVPKQRHKQNST'ZQLVHKRGLRVIEIPGXTFWE  
XWRNDYXUFDUGCRBLKQPQBPBJMTYVZGUMGH TYAFQVDLNFSQLRCSVUDTNOHZQVMNPTVHDVFMEZWVWDOGNDOM  
FZMCAJQXOTVJUQRKWZQIIVRIEKIIOSPLFDUGYRGZHIWDLBJLBAYJUAVBQWFFLRVGKRQEBAKCXRJPZUTSR  
YDZIOVLKWKVEAHLVRIODDKMCQVLKIUSRRNHZUKAZQIIVRIEGUUAWSGZH ZCXHAWYMTCEJSQGNSORFHAU  
YJRAWPGBSSLKMOPSELKMKBNQVEGBIYGQODOJBHBJOHNQVWHZLBLROTKTUKPGHSVFLIIPMMRKUMIKVQA..."

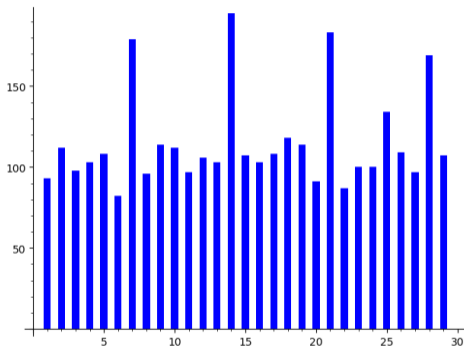


key = ?

## Vigenère cryptanalysis: determining key length

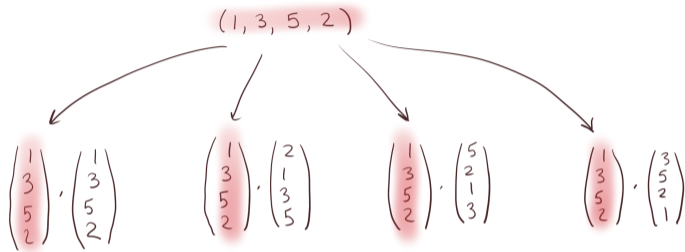


# Vigenère cryptanalysis: determining key length



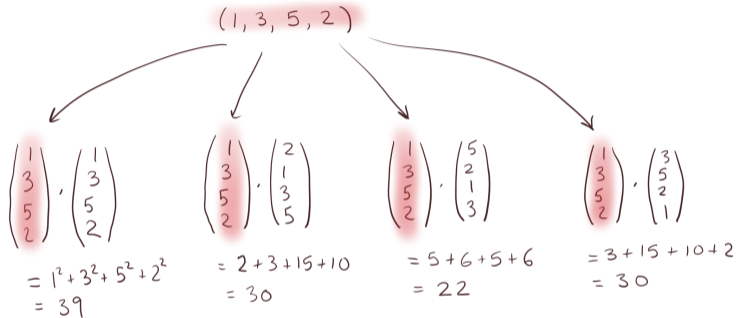
Number of coincidences as a function of offset

## A useful vector idea.



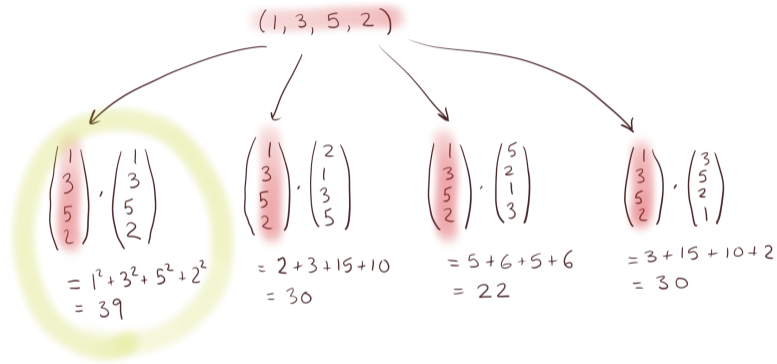
Dot one vector with all its cyclic permutations.

## A useful vector idea.



Dot one vector with all its cyclic permutations.

## A useful vector idea.



Dotted with itself, it is largest.

A useful vector idea.

$$\vec{V} \cdot \vec{W} = |\vec{V}| |\vec{W}| \cos \theta$$



Why? Dot product depends on cosine.

A useful vector idea.

$$\vec{V} \cdot \vec{W} = |\vec{V}| |\vec{W}| \cos \theta$$



always  
the  
same


Why? Dot product depends on cosine.

## A useful vector idea.

$$\vec{V} \cdot \vec{W} = |\vec{V}| |\vec{W}| \cos \theta$$

biggest when  $\theta = 0$   
(parallel)

always the same



Why? Dot product depends on cosine.

## A useful vector idea: applied to coincidences

$$\begin{aligned} \text{Prob}(\text{coincidence}) &= \left( \begin{smallmatrix} \text{prob}(a) \\ \text{top} \end{smallmatrix} \right) \left( \begin{smallmatrix} \text{prob}(a) \\ \text{bottom} \end{smallmatrix} \right) + \dots + \left( \begin{smallmatrix} \text{prob}(z) \\ \text{top} \end{smallmatrix} \right) \left( \begin{smallmatrix} \text{prob}(z) \\ \text{bottom} \end{smallmatrix} \right) \\ &= \left( \begin{smallmatrix} \text{prob}(a) \\ \text{top} \end{smallmatrix}, \begin{smallmatrix} \text{prob}(b) \\ \text{top} \end{smallmatrix}, \dots, \begin{smallmatrix} \text{prob}(z) \\ \text{top} \end{smallmatrix} \right) \cdot \left( \begin{smallmatrix} \text{prob}(a) \\ \text{bottom} \end{smallmatrix}, \dots, \begin{smallmatrix} \text{prob}(z) \\ \text{bottom} \end{smallmatrix} \right) \end{aligned}$$

vector of frequencies of top letter

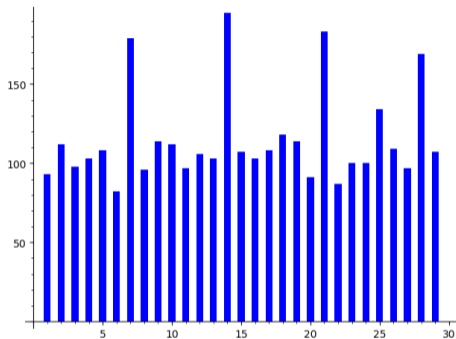
vector of frequencies of bottom letter

The probability of a coincidence between an alphabet with frequencies  $\mathbf{v}$  and one with frequencies  $\mathbf{w}$  is  $\mathbf{v} \cdot \mathbf{w}$ .

So we get more coincidences when we are using the same frequencies (same shift).

# Vigenère cryptanalysis: determining key length

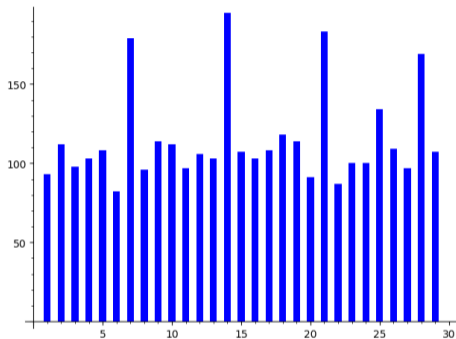
1. Compute the number of coincidences between ciphertext and ciphertext offset by  $n$ .
2. Graph this as a function of  $n$ .
3. Peaks should occur at multiples of the keylength.



Number of coincidences as a function of offset

## Vigenère cryptanalysis: determining key length

1. Compute the number of coincidences between ciphertext and ciphertext offset by  $n$ .
2. Graph this as a function of  $n$ .
3. Peaks should occur at multiples of the keylength.



Number of coincidences as a function  
of offset  
Looks like key length is 7!

## Vigenère cryptanalysis: once you have key length

Suppose key length is  $n$ .

Break the ciphertext  $a_0a_1a_2\dots$  into subsets:

$$\{a_i : i \equiv 0 \pmod{n}\}, \quad \{a_i : i \equiv 1 \pmod{n}\}, \quad \dots \{a_i : i \equiv n-1 \pmod{n}\}.$$

For example, for  $n = 7$ , the second set is the letters

$$\{a_1, a_8, a_{15}, a_{22}, \dots\}$$

The letters from one set are all shifted by the same amount. So use frequency analysis to guess the amount.

The amounts, in order, form the key. (See Sage demo)

# The One-Time Pad

Suppose we use Vigenère, with a key length equal to the message length. This is what is called a *one-time pad*.

As vectors:

$$\text{ciphertext} = \text{plaintext} + \text{key}$$

# The One-Time Pad

Suppose we use Vigenère, with a key length equal to the message length. This is what is called a *one-time pad*.

As vectors:

$$\text{ciphertext} = \text{plaintext} + \text{key}$$

1. It is absolutely secure. For any plaintext, there is a key (namely ciphertext - plaintext) that would encrypt it to the given ciphertext.

# The One-Time Pad

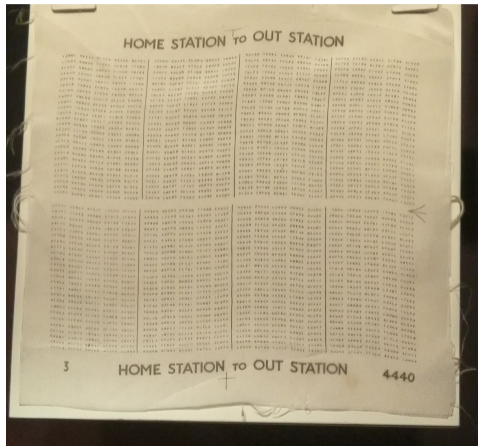
Suppose we use Vigenère, with a key length equal to the message length. This is what is called a *one-time pad*.

As vectors:

$$\text{ciphertext} = \text{plaintext} + \text{key}$$

1. It is absolutely secure. For any plaintext, there is a key (namely ciphertext - plaintext) that would encrypt it to the given ciphertext.
2. By contrast the reason Vigenère is insecure is that the key vector must be a repeating string; this removes so many possible plaintexts, there's likely only one in english.

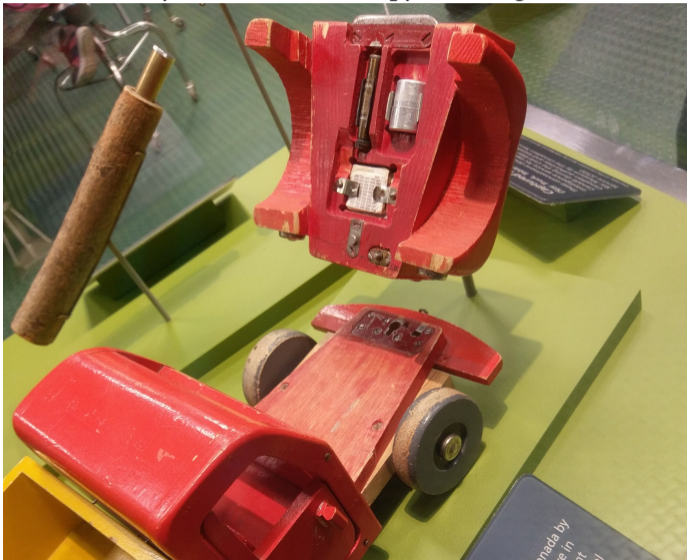
# One-Time Pad



Silk one-time pad circe 1940-45 (British, WWII). Used once and then destroyed.

# One-Time Pad

1960s toy truck for son of spy entering Canada.



# One-Time Pad

One-time pad, microdot reader and special lens.

