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

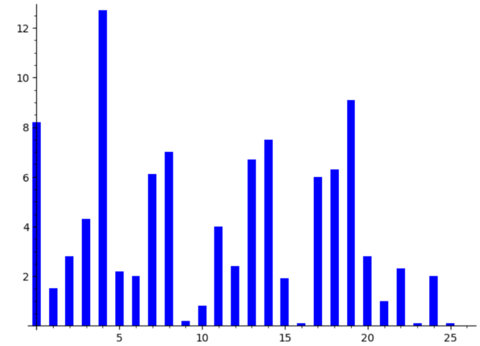
1. Log into our discord server.
2. Leave yourself muted on the main zoom call; I will also mute unless I have an announcement. But leave the zoom channel sound on, so if I make an announcement, it interrupts you.
3. Let n be your birthday of the month (1 through 31), or a madeup birthday. Take n modulo 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. Meawhile, 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.)

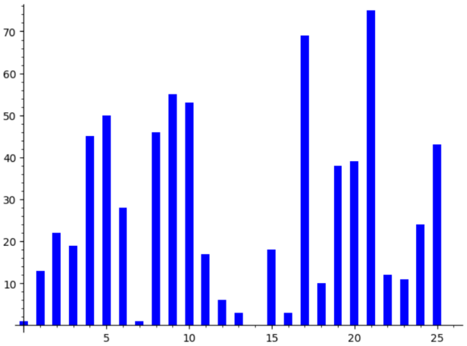
Groupwork

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

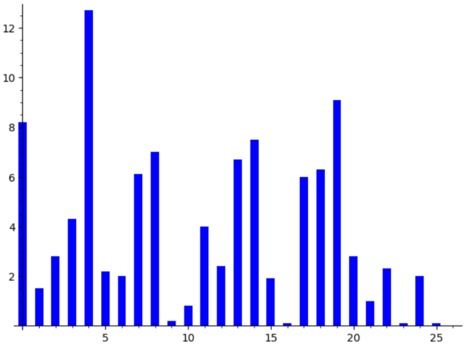
```
ciphertext = "JFEPJIVTVEKVLIFGVRETUIVCVRJVJWIFDRIKZJKJJLTYRJTVCZEVUZFEJYRBZIRREUAVEEZWVICFGVQTFEKRZEJFEPURUT
JTFGPGIFKVTKZFEDVKYFUDRIBVKVURJBVPRLUZFKYVJPJKVDEFIDRCCPGIVMVEKJLJVIJWIFDIZGGZEXTUKIRTBJKFDGWZC
VJSPGCRTZEXRJDRCCSZKFWTFDGLKVIURKRFEKYVUZJTULIZEXKYVGIFTVJJFWDRBZEXKYVXCRJJDRJKVITUKYVEZEJKVRUF
WIVTFXEZQZEXZEUZMZULRCRLUZFKIRTBJRTFDGLKVIIVRUJKYVURKRKIRTBREUZXEFIVJKYVRLUZFKIRTBJGIVMVEKZEXGT
GCRPSRTBFWKYVDLJZTFECPJKREURCFEVUVMZTVJJLTYRJYFDVJKVIVFJREUGFIKRSCVTUGCRPVIJTREIVTFXEZQVREUGCRP
KYVRLUZFKIRTBJFEKYVUZJTJSPFSJTLIZEXKYVURKRKIRTBNZKYRWVCKGVEDRIBFIRGZVTVFWFGRHLVRUYVJZMVGRGVIGIF
KVTKVUUZJTJCZBVUZFEJYRMVSVVEDRUVGCRPRSCVREUTFGPRSCVFEYFDVTFDGLKVIJSPIFEYRIIZJKYVRJJFTZRKVUGIVJJ
WIZURPDRPKYZIKPWZIJKKNFKYFLJREUREUKNF"
```

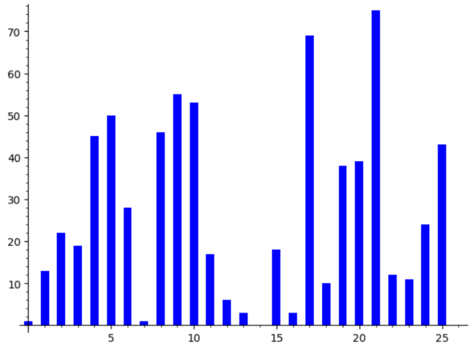




Frequency Analysis

ciphertext = "JFEPJIVTVEKVLIFGVRETUIVCVRJVJWIFDRIKZJKJJLTYRJTVCZEVUZFEJYRBZIRREUAVEEZWVICFGVQTFEKRZEJFEPURUT
JTFGPGIFKVTKZFEDVKYFUDRIBVKVURJBVPRLUZFKYVJPJKVDEFIDRCCPGIVMVEKJLJVIJWIFDIZGGZEXTUKIRTBJKFDGWZC
VJSPGCRTZEXRJDRCCSZKFWTFDGLKVIURKRFEKYVUZJTULIZEXKYVGIFTVJJFWDRBZEXKYVXCRJJDRJKVITUKYVEZEJKVRUF
WIVTFXEZQZEXZEUZMZULRCRLUZFKIRTBJRTFDGLKVIIVRUJKYVURKRKIRTBREUZXEFIVJKYVRLUZFKIRTBJGIVMVEKZEXGT
GCRPSRTBFWKYVDLJZTFECPJKREURCFEVUVMZTVJJLTYRJYFDVJKVIVFJREUGFIKRSCVTUGCRPVIJTREIVTFXEZQVREUGCRP
KYVRLUZFKIRTBJFEKYVUZJTJSPFSJTLIZEXKYVURKRKIRTBNZKYRWVCKGVEDRIBFIRGZVTVFWFGRHLVRUYVJZMVGRGVIGIF
KVTKVUUZJTJCZBVUZFEJYRMVSVVEDRUVGCRPRSCVREUTFGPRSCVFEYFDVTFDGLKVIJSPIFEYRIIZJKYVRJJFTZRKVUGIVJJ
WIZURPDRPKYZIKPWZIJKKNFKYFLJREUREUKNF"





key = 17

Vigenere Cipher Example

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

Vigenere 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

Vigenere 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

Vigenere 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

Vigenere 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

Vigenere 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
ciphetext:	N	Z	K	X	Z	Q	E	V	T	B	F	G	G	H	G	R	V	G