Sneaky & Snoopy

A BATTLE OF WITS

CODES

CODEBREAKERS

By Kinara Goyal

Sneaky and Snoopy

The Shenanigans Of Coders And Code-Breakers

By Kinara Goyal

Cover image created using pictures from pexels and openclipart.

Recipe For Secret Messages

Making A Code

Would you like to send secret messages? Suppose you have your own email account, but your mother checks in on it once in a while, and you need to send a private message to your friend, then how do you do it?

Here’s an idea. You and your friend decide that on code where the first letter key of a QWERTY keyboard from the top-left (Q) replaces the first letter of the alphabet (A) and

the second key from the top left(W) with the second letter from the alphabet(B) and so on as shown in the picture below.

On your keyboard, you can stick a sticker on each letter key replacing it the alphabet that goes in it place in an alphabetical order.

With this arrangement let’s see what happens to the word ‘CAT’. The sticker for the capital letter ‘C’ is on top of the key for the letter ‘E’ so even though you’re pressing the sticker ‘C’ on your computer screen you see ‘E’. Similarly, the sticker for the letter ‘A’ is on the key ‘Q’ and the sticker for the letter ‘T’ is on

the key ‘Z’. So the encoded word for ‘CAT’ is ‘EQZ’.

For a more sophisticated code, you can do this: stick stickers for the small letters in reverse alphabetical order as shown in the figure

below.

With this arrangement let’s see what happens to the word ‘cat’. The sticker for the small letter ‘c’ is on top of the key for the letter ‘b’ so even though you’re pressing the sticker ‘c’ on your computer screen you see ‘b’. Similarly, the sticker for the letter ‘a’ is on the key ‘m’ and the sticker for the letter ‘t’ is on the key ‘u’. So the encoded word for ‘cat’ is ‘bmu’.

This way you enhance your code making it harder for an outsider to crack.

Now you can send secret messages to each other without an outsider knowing the content.

While encoding you make a one-to-one map. For example, in this case, you map capital ‘A’ to ‘Q’ but you don’t map anything else to ‘Q’.

So it’s one letter mapped to one other letter, thus it’s called a one-to-one map.

Breaking A Code

One day when checking your email, your mom notices an exchange of incomprehensible messages between you and your friend. She realizes that these must be coded messages and decides to break your code.

How will your mom break the code? Here are some simple logical steps that she might use. In the english language there are only two one letter words I and a. In the middle of a

sentence, I is always written in capital and a in small. She'll look for a one letter word written in small and figure out that it's 'a'. Then once she finds another one letter word in the middle of a sentence she'll know it's 'I'. Since as a one letter word 'I' is always written capital then if she finds yet another one letter word at the start of a sentence, then the only thing it could be is 'A'.

Once she knows what 'I' and 'a' is replaced by then if you write 'I am' in your encoded message, she might figure out that f replaces m in your code.

If you write ‘I am at’ in your encoded format she might figure out that O mf mu can either be I am at, I am as or I am an. Since this is a secret message the most likely phrase would be I am at, because that would give a location.

Using A Code In A Secure Way

From the previous section we learn to avoid using one letter words. Instead of saying ‘I am at place A. Meet me there as soon as you can.’ say ‘meet me at place A as soon as possible’ making it shorter and harder to break the code. The person who receives this message will still know that they need to meet you at place A as

soon as he or she can. Especially since this is a secret message, you don't have to bother using full sentences, and proper grammar unless it is necessary to make the sentence/phrase readable.

Now suppose you say this 'I need apples, oranges, bananas, grapes, melons, and papayas. - KG' Your mom can then guess that the word after the last comma is 'and' especially if she has already figured out 'a'. That way she also figures out 'n' and 'd'. Now she knows a, m, t, n, d, I and A. Again since this is a secret message so don't use punctuations much because they give away a lot.

In the sentence you wrote you just need to covey your fruit needs so you don't need to put an 'and'. Your sentence should be more like this: 'Need apples oranges bananas grapes melons papayas – KG'. Shortening these sentences not only makes it harder for an outsider to crack, but it also makes it easier for an insider to decode quickly.

Actual intelligence agents use much more sophisticated techniques to make and break codes than this, but I used this to illustrate some key ideas in cryptography.

Writing A Program For Encoding And Decoding

If you want to automate this process and make it easier for your friend to decode the message then you can write a program to do the job instead. Then it'll take your friend very little time to decode the message. In the program we will write a different code. This program encodes letters and numbers, unlike our keyboard cipher which only encodes letters.

```
text = input("Give me the text
you want to encode.   ")


all_chars =
'abcdefghijklmnopqrstuvwxyzABCD
EFGHIKLMNOPQRSTUVWXYZ0123456789
'


def rotate(ch):
    if ch not in all_chars:
        return ch
    idx = all_chars.index(ch)
    return all_chars[(idx + 1)
```

```
% len(all_chars)]


print(''.join(map(rotate,
text)))
```

The first thing this program does is ask the user for the text they want to encode. The program has a list of letters and number written in this exact order

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789

The program accesses the list, finds the character’s position in the list and replaces it

with the next character in the list. But then, what does the program replace 9 with? The program replaces 9 with ‘a’ as nothing else is to replaced by ‘a’ because even ‘a’ becomes ‘b’. Here is an example of an encoded message:

```
tipu prog % python codes1.py
Give me the text you want to encode.   Harry meet
 me in the canteen. Table opposite the window at
9 AM  - KG
Ibssz nffu nf jo uif dbouffo. Ubcmf pqqptjuf uif
xjoepx bu a BN  - LH
```

To decode this message, Harry will put this message into the decoder.

```
text = input("Give me the
encoded text.   ")


all_chars =
'abcdefghijklmnopqrstuvwxyzABCD
EFGHIJKLMNOPQRSTUVWXYZ012345678
9'


def rotate (ch):
    if ch not in all_chars:
        return ch
    idx = all_chars.index(ch)
    return all_chars [(idx - 1)
```

```
% len(all_chars)]


print(''.join(map(rotate,
text)))
```

The decoder goes back one character for every character except for a which it makes 9 as it has the exact same list as the encoder.

Now let’s learn a bit more about code making and breaking techniques that are used in modern times.

What is Cryptography?

Cryptography is the study of securely encoding or encrypting a bunch of characters. It could be a letter, a password, a secret message, a confidential report, etc.

There are many ways to encrypt these characters. For example, when purchasing goods online, your credit card number is scrambled using a method called RSA. This prevents any person who hacks into the system from knowing you real credit card number.

Another way to encrypt, is to add random binary numbers to the number code representing the characters, thus changing the characters, and making it very difficult to decrypt. But decoding is simple for someone who knows what the random binary number is. During the Cold War, the Soviets used a technique similar to this one.

The Fialka

The Soviet Union needed a method of encrypting messages that no one would be able to crack. Additionally, these codes needed to translate from one language to up to two others. These languages had many words that didn’t overlap and so it was going to be hard to invent a sort of encrypter-translator machine. That would take a miracle.

The Soviets invented the Fialka, a machine that could encrypt and decrypt messages in various languages. These machines mostly belonged to the armed forces the Soviet Union, and it was

rarely used by government officials.

So, how would the Fialka encrypt these messages? It did this by randomly switching each character with another one, and storing the information of how each character was switched. (It did this by changing the number code of the character, making it the number code of a different character, thus switching the character printed.)

The Fialka encoded the message in such a way, so that only a person who was particularly good at a type of math called non-carrying addition and subtraction or another machine of

it’s kind could break the code.

Although, this was a truly brilliant invention, it was done all by a simple wheel that rotates to add and subtract numbers to the number codes of each letter.

The Fialka was kept secret as the Soviets did not want America to be able to use or hack its secret power. Even today, no one but the Soviets really know exactly how it worked. And there are only one or two models that you can see in museums.

But, if these codes were really unbreakable,

then how were some of those Soviet spies caught? After all, who knew which of those trillions of codes they were using at that time? Who knew that there were trillions of codes? Did someone figure out the methods used in the Fialka?

The Code-Breakers

Angeline Nanni died at the age of 101 last year.

As a child, she enjoyed playing with numbers during her free time. Her farther worked in a grocery store. She used to read math books from the public library. Angeline was only 12 during the great depression. She lived in a village in Pennsylvania. At school, she opted for accounting classes.

Once Nanni graduated, she went to beauty school with her sisters. Nanni focused on the

business aspect of their endeavour, while her sisters preferred styling hair, etc.

After World War 2 was over, Mimi and Virginia, Angeline's sisters, wanted to move closer their beauty parlour in Blairsville, Pennsylvania. Angeline, who wanted to stay in the village with her farther, discontinued her work at the beauty parlour.

Looking for a job that would suit her skills with numbers, Angeline found a confidential code-breaking job that required her to pass a test. The test was to be held in a secret facility.

Angeline was very nervous. She had not been to collage like most of the other women taking the test. The test would determine weather or not she could stay in Pennsylvania.

To get the job, Angeline needed to break a code generated at the government facility. Determined to get the job, Angeline looked at the numbers, trying to find a pattern.

She heard the supervisor talk about non-carrying numbers, but she did not know what they were. But when she looked at the numbers on the paper she figured out what non-carrying numbers were, or at least what they seemed to

be. She solved the code faster than any of the other women and submitted her solution to the supervisor.

Once the supervisor checked her work, she announced that Angeline had successfully broken the code and got the job.

Angeline’s comfort with non carrying numbers changed her life. Instead of running a beauty parlour, she alongside the other women who passed the test, helped unmask Soviet spies everywhere.

This code-breaking effort was called Venona

and Angeline worked at breaking Soviet codes for 40 years of her life.

After the years of Angeline's work, the project was finally shut down. But even then, the linguist, who was a man, became the face of the project. All the maths done by the women in the facility was not revealed for a long, long time. Only a three or four years ago did the full story see the light of day.

Since we were talking so much about these number codes, now let's see, the number code of each character used today.

ASCII Codes

What is ASCII and How Does One Read An ASCII Table?

One well known number code for keyboard characters is ASCII (American Standard Code For Information Interchange).

Every single English keyboard character has it's own ASCII code represented in binary format. In the binary number system, there are only two digits 0 and 1. So 0 in binary is 0 in decimal and 1 in binary is 1 in decimal. As there are only two symbols in binary, the decimal number 2 has to be represented as a

two digit number. So 2 in decimal is 10 in binary, and so on.

ASCII codes for each character, from the standard set of characters, are 7-bit long. For example, the ASCII code for *i* is 1101001.

But how do we know which ASCII code is for which character? The ASCII codes for each character is standardized and you can read an ASCII table to figure out the ASCII codes for each character. An ASCII table looks like this:

USASCII code chart

Bits b_7 b_6 b_5 →	0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
b_4 b_3 b_2 b_1 ↓ Row / Column →	0	1	2	3	4	5	6	7
0 0 0 0	0	NUL	DLE	SP	0	@	P	`	p
0 0 0 1	1	SOH	DC1	!	1	A	Q	a	q
0 0 1 0	2	STX	DC2	"	2	B	R	b	r
0 0 1 1	3	ETX	DC3	#	3	C	S	c	s
0 1 0 0	4	EOT	DC4	$	4	D	T	d	t
0 1 0 1	5	ENQ	NAK	%	5	E	U	e	u
0 1 1 0	6	ACK	SYN	&	6	F	V	f	v
0 1 1 1	7	BEL	ETB	'	7	G	W	g	w
1 0 0 0	8	BS	CAN	(	8	H	X	h	x
1 0 0 1	9	HT	EM	)	9	I	Y	i	y
1 0 1 0	10	LF	SUB	*	:	J	Z	j	z
1 0 1 1	11	VT	ESC	+	;	K	[	k	{
1 1 0 0	12	FF	FS	,	<	L	\	l	|
1 1 0 1	13	CR	GS	-	=	M	]	m	}
1 1 1 0	14	SO	RS	.	>	N	^	n	~
1 1 1 1	15	SI	US	/	?	O	_	o	DEL

The ASCII table as you can see is a grid. Each character is in a box which has a row number and a column number. The row number and the column number determine the ASCII code for the character in the box. The three digits in the

column number are given by the values of b7, b6 and b5. The 4 digits in the row number are given by the values of b4, b3, b2, and b1. The binary number code for a particular character places the digits to be in the order b7 b6 b5 b4 b3 b2 b1. For example, as you can see in the chart above, d = 1100100.

Positions On The ASCII Table

The idea of ASCII came out from telegraphy codes, so naturally there were control characters as well as punctuations, symbols,

numbers and letters. Let's study the ASCII table and see how it's arranged.

From 0_{dec} to 31_{dec}, or equivalently in binary ASCII representation, from 00000000_{bin} to 0011111_{bin} are control characters. And 1111111_{bin} or 127_{dec} is delete. Each control character has it's short form written on the table. The ASCII code for 0 is 0011000_{bin} = 48_{dec}. The ASCII code for 9 is 0111001 = 57_{dec}.

All the binary values between 0011111_{bin} and 0011000_{bin} are some basic punctuation marks. Then $58_{dec}(0111010_{bin})$ to $63_{dec}(0111111_{bin})$ are punctuation marks.

$64_{Dec}(1000000)$ to $90_{dec}(1011010)$ are capital letters. $91_{Dec}(1011011)$ to $96_{dec}(1100000)$ are more punctuation marks.

And $97_{dec}(1100001)$ to $122_{dec}(1111010)$ are small letters. Finally $123_{dec}(1111011)$ to $126_{dec}(1111101)$ are punctuation marks.

Codes In Movies and TV

You must have either read, watched some TV show, or played a video game about spies or intelligence officers. In TV especially, you must have seen all their fancy fingerprint scanners, GPS trackers, wall monitors, etc. Certain data shows that several TV shows highly exaggerate not only the premises of intelligence agencies but also the range and capability of the equipment supplied to intelligence officers.

In fact, if you have watched spy movies and TV shows, you may be really disappointed at

what an actually office for spies looks like.

It’s probably going to look a lot like a really shabby and disheveled post office. It’ll have striped bags full of confidential papers for burning everywhere because you can’t keep confidential documents in case they are stolen, or the information from them is leaked, etc.

According to the Atlantic, spy themed TV shows and movies especially *24* give people the wrong impression about how intelligence agencies work.

In America the CIA (Central intelligence

agency) only makes and breaks codes to help the NCTC (National Counter-terrorism center) catch terrorists. Only half of the American citizens who participated in a poll knew that.

Intelligence Agencies attempt to project an image that's totally out of a *James Bond* movie to exaggerate the urgency and destructiveness of terrorist threats to increase their funding, recruits and powers.

Secret messages, political intrigue, criminal organizations and spies are thrilling to read about and codes are fascinating puzzles to crack. It's no wonder that codes and ciphers

capture the imagination of people of all ages and kinds from young readers of Enid-Blyton mysteries and older James bond movie enthusiasts to genius mathematicians.