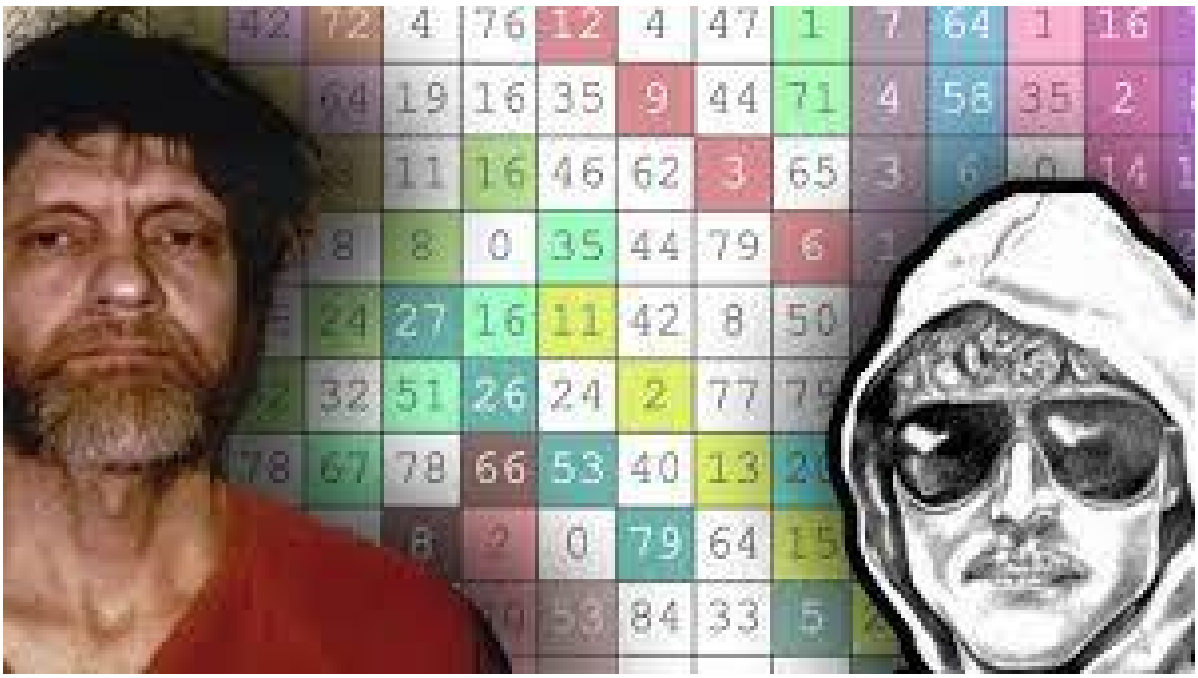
The Unabomber's Codes

David Oranchak



Feb 3, 2023

Contents

» Watch Here «

Introduction

In 1978, former math professor Theodore Kaczynski began a 17 year campaign of mailing letter bombs to people he believed were promoting modern technology and destroying the environment. His homemade bombs sent in the mail killed three people and injured 23 others before he was identified, the media started calling him the Unabomber.

He wasn't captured until 1996. FBI agents raided his remote primitive cabin in Montana, where they found many bomb making materials and 40,000 hand-written journal pages full of incriminating details of his crimes. And many pages were encrypted by some sort of code that he developed.

Zodiac comparisons

Theories quickly emerged that Kaczynski might be the Zodiac Killer. He lived in the San Francisco area during the Zodiac crimes. Like Zodiac, he was interested in bombs and codes. And they both threatened to commit more violence if newspapers didn't publish their works.

> [Ted K:] We promise to desist permanently from terrorism, AFTER our manuscript has been published.[1]

> [Journalist:] The Unabomber has suggested he may build one more bomb unless either the New York Times or Washington Post agrees to publish a 50-page manifesto outlining his anti-technology viewpoints.[2]

There are some similarities in their handwriting, too.

I'm not convinced Kaczynski was Zodiac. But I was very curious about how his ciphers worked. Maybe understanding how Kaczynski used cryptography can help us with other cases that involve codes and ciphers.

Luckily, the FBI found everything they needed to know about how to unlock Kaczynski's secret messages.

In 2015 FBI cryptanalyst Jeanne Anderson published a paper detailing what the FBI learned about the Unabomber's cryptographic methods.[3]

So let's see how the notorious domestic terrorist used his homemade cryptography to hide his darkest secrets.

[1] Unabomber: Publish me and I retire.

[2] Unabomber Sends New Warnings. Los Angeles Times.

[3] Kaczynski's Ciphers

Cabin raid

After the raid of Kaczynski's cabin in 1996, the FBI began processing piles of evidence, including the enciphered journal pages they found.

As Kaczynski's criminal trial developed, FBI codebreaker Michael Birch painstakingly deciphered Kaczynski's encrypted journals, and supplied the results as evidence.[1]

In his journals, Kaczynski gave detailed descriptions of his 16 attacks that resulted in the deaths of 3 victims and injuries to 23 others.

Some of the decipherments gave glimpses into his state of mind:

> Since committing the crimes reported elsewhere in my notes I feel better. I am still plenty angry...but the difference is that I am now able to strike back, to a degree . . . I am definitely glad I have done what I have.[2]

> Who says crime doesn't pay? I feel very good about this.[3]

And referring to one of his bomb attacks:

> Excellent. Humane way to eliminate somebody. He probably never felt a thing. 25000 dollar reward offered. Rather flattering.[4]

[1] Government cryptographer examines Kaczynski's journal. Kenosha News. Dec. 27, 1997.
[2] Ted Kaczynski's Journal in 1980-81
[3] Fully Coded Notebooks of Crimes
[4] Fully Coded Notebooks of Crimes

Decryption instructions

Jeanne's paper goes into detail about how Kaczynski's encryption system works. Luckily, Kaczynski's instructions about how to decipher his codes were found during the raid.

He developed two systems, called Code #I and Code #II.

In both systems, the ciphertext is just a series of mysterious numbers.

Kaczynski helpfully included instructions and an example for how to decipher Code #I.

Code I decryption

You need a few things to break his cipher:

- First you need the cipher text, a sequence of numbers that sometimes has punctuation in it.
- Then you need this huge grid that he filled with 2,268 over two thousand numbers.
- Finally, you need his so-called List of Meanings. This is basically just a dictionary of how numbers translate to different letters, groups of letters, words, spaces, and punctuation.

To decipher an encrypted message:

First you have to get the right numbers from the grid. Then do some simple arithmetic with them and the cipher numbers. Then finally, replace the numbers with their translations from the list of meanings.

Let's look at how Kaczynski uses his grid of numbers.

He describes a special way of reading off the numbers from the grid.

First, his cipher text will tell where to start in the grid. For example, his cipher might start with a circled 5. So, we begin on row 5 of the grid.

Then, we start the First Phase, where we simply read the numbers normally, from left to right, and write the numbers under our cipher text.

When we get to the end of the grid, we move into the Second Phase, and read the numbers vertically starting at the top right corner.

If we reach the end again we move into the Third Phase, where we start at the upper left corner, and read out the numbers diagonally.

Then we reach the Fourth Phase, again reading out numbers diagonally, but starting in the top right corner.

When we finish all of these, we start back over with the first phase, starting at the top of the grid.

O.K...? what was the point of all that?

Well, it produces a very long key that is combined with the message to make a pretty secure cipher.

The grid is huge: it has 2,268 numbers in it, but since it has 4 phases which goes through all the numbers 4 times in different orders, the key can get up to 9,072 numbers long before it repeats. That means it's virtually impossible to detect any useful patterns in the cipher text to crack it without the key.

This technique is basically a type of one time pad, which is a kind of cipher that is impossible to crack, if it's used properly, and the key (known as the pad) is kept secret.

Here's an example of a one-time pad used by Communist spy in Japan in 1961. It looks similar to Kaczynski's system.[1]

Let's look at his decipherment instructions.

He includes a sample cipher text, a series of numbers. His ciphers contain some random punctuation, like this question mark, that are misdirections. They don't translate to anything - they're just thrown in to confuse codebreakers.

To start decoding this cipher, we need to figure out where to start in the grid. In his example, he's starting at this position in the grid, and is in the first phase. So we read the numbers out horizontally and write them under the ciphertext numbers. Now, we do something called, modulo 90 addition. That sounds fancy, but it's simple. It's like regular addition, but you just subtract 90 from the sum until it's less than 90.

Let's do that with this first number from the cipher, 72. The number from the grid was 47. Add them together, and you get 119. That's bigger than 90, so let's subtract 90. That gives us 29, which we keep since it's less than 90. The next cipher number is 24. The number from the grid was 74. When we add these two numbers, we get 98. 98 is bigger than 90, so we subtract 90 and get... 8.

Let's keep doing this same modulo 90 addition for the rest of the cipher numbers. [stops at "?] At this point, a question mark appears in the middle of the cipher numbers. What do we do with this? Nothing! Kaczynski sticks random punctuation in his cipher text as a distraction, to make codebreakers go down the wrong path. So we'll just skip it. Let's finish the adding step for the rest of the numbers.

OK, we're done with all the adding. Now we need to use the List of Meanings to translate these numbers into a message.

Let's start with 29. In his list, 29 is equal to one of these words: I, ME, MINE, or MY. So he's using that number any time he refers to himself. We'll have to pick the right word based on the context of the message. So let's just note them all for now.

[1] kahn one time pad

Next up is the number 8. In the list, he translates it to HAVE, but marks it as future tense. So, the way to say that with future tense, is WILL HAVE. The next number is 48, which stands for F. 60, stands for R. 66, stands for U. Then, just keep going like this, for the rest of the numbers.

10 has a special meaning. In his list, he says 10 tagged onto the end of any verb indicates the future tense of that verb. Let's make a note of that... and continue.

OK, we're done with the substitutions. Now we can fix up the message. We need to figure out which word to use for the number 29. It could be I, ME, MINE, or MY. Let's pick "I" because it makes the most sense when you read it with "WILL HAVE".

This word looks strange ("FRUHSTU CK"). Kaczynski liked to toss in Spanish and German words to further disguise his message. Turns out, this is a German word, Frühstück, and it means BREAKFAST.

Next we get to a word, spelled "E V R Y", but it seems clear that it's intended to be the word EVERY, misspelled on purpose to make our task more difficult.

Now, Kaczynski makes a note about this number 42 which decodes to C. He says, "with each letter underlined (with this squiggle symbol), the encoder has made an error in the first digit of the number." OK so that means the 4 in 42 is wrong. If we look at the list of meanings, 32 stands for word spacer, which makes sense in this spot, since it's followed by a complete word, ENJOY. So let's fix 42 with 32, and put the word spacer here.

Here's another 29, where we have to pick from one of these words again. "I" makes the most sense, since it makes this say "I ENJOY". So let's choose "I".

The number 10 has a special meaning. It means the previous word is in future tense. So we'll make a note that this should be WILL ENJOY.

31 can be any of these pronouns: HE, SHE, IT, HIM, HER, HIS, HERS, or ITS. IT makes the most sense since he's talking about breakfast.

This word looks like it says DIGESTION but the J is wrong. The decoded number is 52, and Kaczynski said errors might be with the first digit. Sure enough, the list of meanings has S for 62. So let's fix the misspelling...

And here's another word with a possible misspelling. Is this supposed to be FOOD? GOOD? WOOD? MOOD? The decoded number is 39. In the list of meanings, G is 49, and the other options like F, W, and M don't end in 9. So let's go with GOOD.

Let's go back here where there's another 29. We can pick the right word now, because the only way it reads right is: MY DIGESTION IS GOOD. Same thing here - it makes the most sense for this to say I DO.

And now we're done with his example. It reads: I WILL HAVE BREAKFAST EVERY MORNING, AND I WILL ENJOY IT. MY DIGESTION IS GOOD.

We only used a small part of his number grid. His real messages, though, were much longer, so we would eventually have needed to read out the numbers in different directions, according to his instructions.

Code I encryption

OK - Now what about the other way round? How do you use his system to encrypt a message? Let's start with the same message from his example:

I WILL HAVE BREAKFAST EVERY MORNING, AND I WILL ENJOY IT. MY DIGESTION IS GOOD.

So we just do the same steps in reverse. Let's throw in a German word. Replace breakfast with Fruhstuck:

I WILL HAVE FRUHSTUCK EVERY MORNING, AND I WILL ENJOY IT. MY DIGESTION IS GOOD.

He liked to throw in meaningless punctuation in the middle of his cipher numbers to throw people off. So let's mark this spot with a question mark for sticking in the cipher later:

I WILL HAVE FRUHSTU[?]CK EVERY MORNING, AND I WILL ENJOY IT. MY DIGESTION IS GOOD.

Let's throw in some errors on purpose, to throw off codebreakers. Delete an E in EVERY:

I WILL HAVE FRUHSTU[?]CK EVRY MORNING, AND I WILL ENJOY IT. MY DIGESTION IS GOOD.

Mess up the space between the words here. <maybe show this as the squiggle symbol:

I WILL HAVE FRUHSTU[?]CK EVRY MORNING, AND I[~]WILL ENJOY IT. MY DIGESTION IS GOOD.

Introduce an error in the word DIGESTION:

I WILL HAVE FRUHSTU[?]CK EVRY MORNING, AND I[~]WILL ENJOY IT. MY DIGE[~]TION IS GOOD.

And in the word GOOD:

I WILL HAVE FRUHSTU[?]CK EVRY MORNING, AND I[~]WILL ENJOY IT. MY DIGE[~]TION IS [~]OOD.

OK - now we can start with the substitutions. The first word is "I" which has a special entry in his list of meanings, along with ME, MINE and MY. So replace it with 29. WILL HAVE matches the future tense version of HAVE in his list, which is the number 8.

Let's continue by replacing these letters with their numbers. Notice that some letters show up more than once in the list. For example, A could be 39 or 40. D could be 43 or 44. And he has two different numbers, 32 and 33, for the word spacer. So when we assign a number, we can pick any of the options. The multiple choices make the cipher a bit more secure.

This is similar to Zodiac's homophonic ciphers, where he picked from multiple choices for his letter substitutions.

OK, let's encode the letters in the German word. And keep the question mark as a diversion... Now let's mark the word spacer since we're between words. Make the substitutions for the letters in EV[E]RY... Then for MORNING...

Now, I-N-G shows up in a lot of words. So Kaczynski has a number just for ING. Substitute the comma... AND is a common word and has ITS own number... The word "I" has its special number... Now we want to put an error here. A word spacer WOULD have gone here, but we're going to pick a different substitution. Let's use the "first digit wrong" rule. We could have used 32 for the space. Let's change the first digit to 4, so now it's 42. That stands for the letter C so let's use that.

Now, the phrase WILL ENJOY uses the word ENJOY in future tense. Kaczynski has a special code to mark future tense. So we can take out WILL... Encode the letters in ENJOY... Then add the future tense code after it...

The word IT has a dedicated number, along with several other pronouns like HE, SHE, HIM, and so on. Here's the period... Another substitution for the word I... Now the letters in DIGESTION.

We want to insert another error here where the S should have been. If we pick this S, its number is 62. Let's change the first number to 5 to make it 52, which is J in the list. So let's use that.

And T-I-O-N has its own number in the list... Put in a space... IS has its own entry in the list. He has a number just for the word BE in its present tense forms such as AM, IS, and ARE. So we'll use the number 1 here.

Now we want to start the word GOOD, but put in an error for the G. G is 49 in the list. Change the first number 4 to a 3, and we get 39, which is A. So let's put that here.

Then finish off the word... And finally, the code for a period.

Now we're done with the substitution phase. Next, we have to get numbers from the big grid to further encode the cipher.

I'll start where Kaczynski started in his example, at this spot in the grid. We're in the first phase, so we're going to read the numbers out horizontally. And write them all out above the numbers from our substitutions.

Now we need to do the special modulo 90 arithmetic I showed earlier for the deciphering steps, but in reverse. It's pretty simple to do: First, look at the two numbers. If the bottom number is smaller than the top number, then add 90 to the bottom number.

So here, 29 is smaller than 47 so add 90 to it. And we get 119. Then, subtract the top number. So here we subtract 47 from 119, and we get 72.

So 72 is the first number that forms our final cipher message. Let's look at the second number, 8.

It's smaller than 74, so add 90 to get 98. Then, 98 minus 74, makes 24, our 2nd cipher number.

Let's keep going with these steps...

Here we reach an example where the first number is bigger than the second number. 63 is bigger than 5. So we don't need to add 90. Just take 63 minus 5, and you get 58. Let's finish applying these steps to the rest of the message.

And, we're done! We get this final cipher sequence. A list of mysterious numbers with a question mark thrown in.

That was a short example. But if that was part of much longer message, we would need more numbers from the grid. We would have kept reading from the grid in the first phase, horizontal direction, until using up all the numbers. Then we'd continue with the second phase, reading numbers vertically. And so on, until we get to the end of the cipher text.

So that's how his first code system works. In the end, it's not TOO complicated... Just pick the right numbers from the grid, in the right order. Do some simple arithmetic. Then look up the decodings from his little dictionary.

It's just, kind of tedious. This is a system that was great for Kaczynski, but would have been terrible for more than one person to use. They would have had to share the grid, the details of its use, the list of meanings, and all the little tricks like errors and other languages.

Code I security

But, how secure is this system?

The first step of this system is simple substitution of letters, fragments, and words. If Kaczynski had made that the only step, his ciphers could easily be decoded without the key, since his enciphered messages were very long. So frequency analysis would have made quick work of those.

But his second step, adding numbers from the large grid, almost guarantees that no one can unlock it without the key. His cipher acts like a one time pad, a 140-year old encryption technique that is impossible to crack, but only if these conditions are met:

1. The key (or pad) must be as long as the plaintext message
2. The key must be completely random and unpredictable.
3. The whole key, or even parts of the key, must never be reused.
4. And, the key must be kept a secret by whoever uses it.

The FBI was able to break Kaczynski's ciphers because they found his key and instructions when they raided his cabin. But I've always wondered: What if they hadn't found the key? Would the FBI codebreakers have been able to unlock his secret messages? I think it would have been nearly impossible. But, there are some caveats.

Here's the list of conditions again for what makes a one time pad secure. The thing that absolutely ruined the security of Kaczynski's cipher was leaving the key laying around for the FBI to find.

But let's assume they didn't find the key and this condition was met. OK - The first condition says the key must be as long as the message. His grid truly is pretty damn big. It's 42 columns by 54 rows, which contains 2,268 numbers.

But, there are 4 different phases, or reading directions, which means the key length is actually up to 9,072 numbers.

So he can make messages up to 9,072 characters long before repeating his key. Theoretically, if his coded messages were very much longer than that, then his method would be much less secure.

That's because a codebreaker could find patterns based on the repeating key. But still, a key that is 9,072 numbers long is an extremely difficult hill to climb for a codebreaker.

Code I patterns

The second condition says the key must be completely random and unpredictable. At first glance at his key, it looks like there's no rhyme or reason to the pile of numbers. But if you look long enough, you can find some patterns. Such as long sequences of one digit numbers that tend to hang out together.

In some places, you can find numbers that tend to be in order, like here, where you can see the numbers 0 through 9 close together...

And here's 0 through 7 clumped together...

Here you can see a sequence close together: the numbers in order, 67 through 76...

In this part it looks like he put 1 through 16 all together...

He made other patterns too. Here's a sequence where he added 3 each time...

And another...

And here he adds 4 each time...

Here's an interesting pattern. He adds 4 to each number in this sequence with gaps...

But then he fills in the gaps, where he also adds 4 to each number...

Sure enough, you can find places where he counts by 5s...

Here's another place where he mixes two sequences. First he counts by 5s, with gaps in between...

And then fills in the gaps with numbers made by adding 5 each time...

by 6:...

He counts by 10, too. Here he starts with 40:...

And here he starts with 5 and adds 10 each time...

On the same line, he starts with 9 and adds 10 each time...

So it's clear Kaczynski filled the grid using some simple number adding schemes. But there's another scheme he used that really stands out. This was discovered by Jelberg, a user on a Zodiac Killer forum. He investigated similarities between Kaczynski's number grid and Zodiac's 340 cipher. And discovered interesting patterns along the diagonals of Kaczynski's grid.[2]

Instead of adding the same value to each number in the sequence, Kaczynski added two previous numbers to produce a third number...

This is similar to the famous Fibonacci sequence. In this sequence, you start with 0 and 1. To get the next number, you add the previous two numbers. So we add 0 and 1 and get 1. What's the next number? Add the two previous numbers. 1 plus 1 is 2. Then the next number comes from: 1 plus 2 equals 3. Then 2 plus 3 is 5. 3 plus 5 is 8. 5 plus 8 is 13. 8 plus 13 is 21. And so on!

Turns out, Kaczynski was doing something like that all over his grid.

There are 4 of these Fibonacci sequences. The first one goes: 0 plus 1 is 1. 1 plus 1 is 2. 1 plus 2 is 3. 2 plus 3 is 5. 3 plus 5 is 8.

Then a new sequence starts. 8 plus 8 is 16. 8 plus 16 is 24. 16 plus 24 is 40. 24 plus 40 is 64.

And another sequence. 5 plus 2 is 7. 2 plus 7 is 9. And so on, and so on.

He did this in many places, especially in the bottom half of his grid, where it is jam packed with Fibonacci sequences. These kinds of patterns make his grid of numbers much less random.

We can also look at how many times he uses each number. Since he uses modulo 90 arithmetic, he only uses the numbers 0 through 89 on his grid.

Here's a plot of how many times he uses each number. The highest bars are for the numbers zero through 9. So, he clearly had a preference for one-digit numbers.

Here they are in the grid...

The number he uses the most is 1, which shows up 107 times on his grid.

He uses the rest of the numbers a fair amount, up until 84. 85, 87, and 88 do not appear in his grid at all. And he only uses 86 and 89 once.

So all these features, like the patterns and the uneven distribution of numbers, make the grid less random and slightly more predictable. And that weakens the 2nd condition of security for one time pads.

Is it enough to make Kaczynski's cipher vulnerable to attacks without the key? Maybe not - it's still a very large key, and we only knew to look for those kinds of number patterns after we already saw the key.

The 3rd condition is: The whole key, or even parts of the key, must never be reused. Kaczynski violates this rule by repeating his key after using up to 9,072 numbers from the various phases of reading his grid. But that's still a very large amount of ciphertext being generated before the key starts to repeat.

[2] Period 19, Fibonacci, Game Theory, Nash Equilibrium

So it would still be hard for codebreakers to take advantage of the repeating key by looking for patterns. Especially if they didn't know the size of his key. But I wonder: What If codebreakers didn't have the key, but suspected he was reusing the numbers in different directions?

Could they make a guess about the grid of numbers, then rearrange it to undo the different reading directions? Maybe certain patterns would emerge if they guessed the right directions and grid size. It's definitely a long shot. But, I think it's worth studying further.

Code II decryption

Now, that brings us to his second coding system, called Code #II.

This system is simpler to use, and it also seems to eliminate the security problems we saw in Code #I.

Instead of using and reusing a grid of numbers, Kaczynski used two notebooks, called Notebook A and Notebook B. Each one has a long series of numbers. One series is his ciphertext, and the other is a one time pad. But in this case, the pad is as long as his message, which satisfies these two security conditions for one time pads:

1. The key (or pad) must be as long as the plaintext message

3. The whole key, or even parts of the key, must never be reused.

Like his first system, Code #II also has its own List of Meanings that is used to translate numbers back to plain text. So, with the two notebooks and the list of meanings, we can decipher his messages.

Let's work through an example.

Here we have the two Notebooks, A and B, each with its own series of numbers.

We start with the first number from both notebooks. We are going to do a special kind of subtraction, called modulo 100 subtraction.

One way to do it, is to see if the first number is smaller than the second number. If it IS, then we add 100 to it, BEFORE subtracting. So here, 36 is smaller than 38, so let's add 100 to 36, which makes 136. Then 136, minus 38, is 98.

Now we move to the next pair of numbers from the notebooks. 86 is bigger than 58, so we can just subtract them, which gives 28. Same with the next pair: 49 minus 39 is 10. Then, 22 is smaller than 88, so we have to add 100 to it. Then 122 minus 88 is 34.

Let's continue this simple subtraction procedure for the rest of the numbers...

Now we're done producing this new sequence of numbers, which is the original cipher with the pad removed from it. What's left is a simple substitution cipher. To get the final message, let's look up the numbers in the list of meanings, just like we did for Code #I.

98, stands for the entire word WHO. 28 stands for S. 10 stands for A. 34 is Y 28 is S and 42 is a space between words.

Let's keep going with this simple substitution process...

The last two numbers also stand for entire words. 43 stands for ABOUT. And 89 means THIS.

Now we have the final message: "Who says crime doesn't pay? I feel very good about this."

That was a simple example. Kaczynski probably would have thrown in some intentional mistakes, foreign words, and meaningless punctuation, like he did in his first coding system.

Code II encryption

Encrypting a message is similar to how it works for his first code system. First, we replace letters, words and punctuation with numbers from his List of Meanings...

Then we get the notebook with the list of numbers used as a pad. Then, instead of subtracting numbers, we're going to add them. But if the result is 100 or larger, we're going to subtract 100 from the result. For example, 98 plus 38 is 136. It's bigger than 100 so subtract 100 to get 36. Let's keep adding pairs of numbers, and we'll subtract 100 whenever a sum gets too big.

And that's it! We now have two number sequences. We can put our cipher sequence in Notebook A. And the pad sequence in Notebook B.

Code II security

This second code system seems much more secure than his first one. Mainly because the key is as long as his plaintext message. And as far as I know, he doesn't reuse any of it like he does for the first system. But I haven't seen the entire pad.

Are there any patterns in his pad of numbers, like we saw in the grid he used for the first code? If accurate guesses can be made about some of the patterns, a codebreaker could unlock fragments of his message without using the key. But I think it would still be extremely difficult.

In the end, investigators were very lucky to find the keys and instructions.

Reporting on FBI decryption efforts

Towards the end of 1997, newspaper articles reported on FBI codebreaker Michael Birch's work to decipher Kaczynski's journals as part of his criminal trial.

The articles were rather dismissive of the difficulty of the task. This one claims, "Experts says cracking diary's numeric code isn't difficult."[1][2]

Yeah, that's true - I've shown the steps in this video, and they really aren't that hard to perform as long as you've got the key, and you're careful about keeping track of what you're doing.

The article goes on: Code experts say Kaczynski used a "hand code" that would have been relatively easy to break, even without the key...

I think that's definitely not true. Sure, we saw some weaknesses in his code system, but his codes are still extremely secure.

It would be very hard, if not impossible, to reconstruct those very long sequences of numbers needed to decode the journals.

This book claims an FBI cryptologist said that it was a code that "no one, not even NASA computers, could have broken."[3]

At any rate, the case against Kaczynski was solid, his fate sealed in large part by the detailed confessions extracted from his deciphered journal.

> "I sent a bomb to P.S. Wood, president of United Air Lines"[4]
>
> "My projects for revenge are expensive."[5]
>
> ... I sent a bomb to a computer expert ...[6]
>
> ... [I] must succeed, must get revenge ...[7]

On January 22nd, 1998, Kaczynski finally pleaded guilty to avoid the death penalty and a lengthy trial.

---

[1] Star_Tribune_Sat__Dec_27__1997
[2] The_Messenger_Sat__Dec_27__1997
[3] Harvard and the Unabomber
[4] Star_Tribune_Wed__Apr_29__1998
[5] Chicago_Tribune_Wed__Apr_29__1998
[6] UnaBomber Secret Code Cracked after 10 years
[7] UnaBomber Secret Code Cracked after 10 years

The Department of Justice has just accepted a plea of guilty, for life in prison without the possibility of parole, from Theodore Kaczynski. The Unabomber's career is over.[8]

[8] USA: SACRAMENTO: UNABOMBER TRIAL: TED KACZYNSKI PLEADS GUILTY

Conclusion

Clearly very intelligent, Kaczynski moved from a successful and impressive career in mathematics and academia, towards an isolated life, in which he unfortunately devoted his talents to terrorizing those he believed to be destroying the environment and developing technology.

He had enough knowledge and skill to develop sophisticated bombs that could be mailed and triggered by his targets opening the packages.

And he had enough knowledge to create a virtually unbreakable code he could use to hide his secrets.

We might STILL be puzzling over the contents of those coded journal entries, if he hadn't left the instructions laying around in his cabin.

I think prosecutors had plenty of evidence against Kaczynski even without those decrypted messages. But the treasure trove of deciphered confessions sealed his fate.

I still wonder: If we hadn't found his keys, could anyone have unlocked his secret messages?

His system was extremely secure but had a few weaknesses.

I think a mathematician or professional cryptographer should investigate this question, especially since it could help with similar problems and maybe help unlock other unsolved ciphers.

Thanks again for watching! Help me keep the channel going by clicking the Thumbs Up and Subscribe buttons.

And leave your comments and questions below. Let me know what you want to see in future episodes.

Bye for now!

David Oranchak
The Unabomber's Codes
Feb 3, 2023

YouTube
This transcript is published here mainly to help people find the video when searching for analysis of Ted's cryptography. But, it can also be used to see where documents are referenced and remembering the instructions at a glance.