EPISODE 490

[00:00:01] AH: I'm really looking forward to discussing more about code breaking and about the types of things that both of you have been up to and about your book. But I guess I just wondered, how did you both meet? How did you both begin to work together and to collaborate on this stuff?

[00:00:15] ED: Well, we met at not too far away at the National Security Agency's Cryptologic History Symposium, and I believe Klaus had organized a dinner and had invited various speakers there. And I think that's where we first met. Right, Klaus?

[00:00:33] KS: Yes, it was in 2009 at the pre-conference dinner. Yes, that was an unofficial dinner I organized. No. No. Sorry. It wasn't. The second time was organized by me. But the first time was organized by **[inaudible 00:00:47]**, a Dutch crypto history expert. So he is the one who brought us together.

[00:00:53] ED: And we just got talking and got talking and got talking. And then sometimes when we were traveling, like would you be going to the Voynich Manuscript Symposium in Italy. And again, we're just like, "Oh, you're here and talking and talking and talking." It was just a very natural fit.

[00:01:10] AH: How many code breaking experts are there out there along the lines of both of you? So I'm not talking about people that work for the NSA and so forth, or GCHQ, but just like the code breaking community, like both of you. What are the numbers? Are we talking hundreds, thousands, millions, or a few dozen?

[00:01:32] KS: Well, at this conference where we met, there are usually like 200 people also. But it's not only about code breaking. It's also mainly about crypto history. And well, to be honest, I'm not a hardcore code breaker. I'm more interested in the history or in the background, and I write about code breaking. And I've written this book together with Elonka. But I'm not the kind who spends all the code breaking. I'm more the journalist type.

[00:02:05] AH: Some of our listeners could very well be experts in this, but some of them weren't. So just to start off, one of the things that we look at here at the Spy Museum is the difference between codes and ciphers. Can we just start off by telling us what the differences between both of them?

[00:02:23] ED: Sure. So codes, you need a codebook. So you'll generally have each word will have some sort of representation, like the word Apple might mean battleship. And a cipher is where you can do a one-to-one on different letters. So a B would be something. An A would be something. A t would be something. So a cipher is more adaptable to different things that you want to say. But it's also easier to crack. Because a codebook, you really kind of need that book in order to crack what's going on, unless you have a lot of cipher text to work with, and then you can start guessing what means what?

[00:03:05] AH: So the book *Codebreaking: A Practical Guide*, that's mainly looking at paper and pencil code breaking, right? Could you break down what the differences between paper and pencil code breaking and where we are now?

[00:03:21] KS: Yes. Well, today, the computer-based methods are used for encryption. So for example, if you use a web browser, or a smartphone, or something similar, you always use encryption without even knowing it. And the algorithms used by these programs or by these hardware tools are modern mathematic encryption algorithms, very hard to break. This is not what our book is about. Our book is about traditional encryption from the last 500 years. And we use computers for code breaking. So we use computer tools for, let's say, counting the letters in a text or things like that. But the book is not about breaking the encryption used by a smartphone or something like that.

[00:04:10] AH: When does that shift from paper and pencil to the modern techniques? When does this take place? Are we talking about – Are we going back to Enigma during World War II? Or are we talking about the advent of modern digital computers? Or give us a rough timeline of the shift.

[00:04:28] KS: Well, basically, the era of paper and pencil encryption lasted until, let's say, 1920 or 1930. And from then on, at least four important encryption tasks machines were used like the

Enigma, or there were plenty of others. And around 1970 or so, the computer or electronics took over this task. So the era of computer-based or electronic encryption started around 1970 roughly.

[00:05:02] AH: So Julius Caesar would have been using the same types of technology as Ulysses S. Grant. But when we get to the 20s, it becomes electromechanical. And then in the 1970s, it becomes digital. Is that correct?

[00:05:18] ED: Well, the pencil and paper methods were quite different between Julius Caesar and the Civil War.

[00:05:23] AH: Give us a sense of why.

[00:05:25] ED: Well, Julius Caesar tended to use a very simple system called the Caesar Cipher, where you have a basic alphabet, and then you're just shifting everything by three in the alphabet. Whereas in the Civil War, they might have been using something where you’re putting letters into grids and then writing things with symbols. So it's a whole order of magnitude difference.

[00:05:47] AH: Okay. And in your book, you start off the substantive part looking at the Caesar Cipher. Is the Caesar Cipher the building block of all cryptography or code breaking?

[00:06:01] KS: I wouldn't call it a building block, but it's the most basic encryption technology. Well, at least in code breaking, it's something like the foundation. If you know how to break a Caesar Cipher, you can go to the next step. It's something like a first step in code breaking.

[00:06:18] AH: Okay.

[00:06:19] ED: There were systems that were much older than that. For example, about 500 years earlier, the Greeks used a system that was called a Scytale. And it involves taking a stick and wrapping leather around it. And that goes back to about 500 BC.

[00:06:36] AH: Okay. Wow! One of the questions that I had just thinking about the 1970s and then digital computing, and code breaking becomes much easier with the assistance of computers. So I guess one of the questions that I had was why did it take so long for them to break the Zodiac codes? Maybe this is like a beginner's stupid question. But couldn't you just load that all into a computer? And the computer would do the work for you? Or why did it take so long?

[00:07:10] ED: Well, it wasn't one cipher system from beginning to end. It was a combination of systems. And it required three different people actually working in different parts of the world. We had Europe, and America, and Australia. And they were brainstorming. There have been people, thousands of people brainstorming on it for decades. But, finally, this group brainstormed the right combination of techniques. And it was their ideas, and it was computers, both. And they started teasing something out and like, "I think we got something." And then they managed to tease out the rest of the message, but it took over 50 years.

[00:07:51] AH: Wow! So that's something that you can do as well. You can have a combination of systems. Or is a combination of systems really only decipherable immediately to the person that makes up the combination of systems? Am I right in thinking it's not really designed to communicate? It's more just designed to embed something that you want to keep secret. Is that correct?

[00:08:16] ED: Right. I mean, a good code or a good cipher is generally something that's used in wartime, where someone has a message that they are encrypting. That is then sent to someone who might be in the middle of a battlefield, who then, in the chaos of a battlefield, needs to be able to decrypt that message fairly rapidly. So you want a good system to encrypt and then decrypt the message. These complex systems like the Zodiac did are not really good for battlefield conditions. He was trying to make something very difficult to solve.

[00:08:52] AH: Wow! For the listeners, help them understand how the rest of the book unfolds. So at the beginning, you have the section where you lay some of the groundwork and then you enter just the Caesar Cipher. Obviously, your book is 500 pages. So we can't cover everything. But give us a sense of the evolution of the pencil and paper cipher. Let's just walk up to the middle ages to start with.

[00:09:19] KS: Yes. Well, it started with simple letter substitutions. For example, somebody would replace every letter of the alphabet with a symbol, a symbol that looks spectacular. Of course, that didn't make the encryption more secure. But perhaps, 700 years ago, that impressed somebody. But then from the simple letter substitution, systems evolved to so called nomenclatures. That means not only letters were substituted, but also common words. And the number of words that could be substituted with one table grew.

In the 19th century, finally, there were entire books, code books that contained code words for each word of language. But in parallel, there were systems that didn't replace letters, but changed the order of letters, the so called transposition ciphers. There are many different ways how to implement such transposition cipher. And there were ciphers replacing two letters at once, or even three levels at once. So there were different ways. Of course, this may still exist. But these are very important until, let's say, the beginning of the 20th century. And these are – Well, basically, in our book we cover everything that was important in this time of the paper and pencil ciphers. And our goal was to give solution approaches to all these systems you encounter in practice.

[00:10:59] ED: And one of the unique things about our book is that instead of just discussing it abstractly, we use actual examples, actual encrypted postcards, actual encrypted newspaper ads, actual messages that spies used, or prisoners used. So we show what they did, what kind of system they used, and then how to decrypt that.

[00:11:22] AH: One of the things that I loved about your book is that it's very easy to follow because, I think, for a lot of people, they just think code breaking and they just think it's going to be very complicated mathematics, or algebra, or something like that. But you actually lay it all out. And if you follow up, as you have laid out with the examples, it's not as difficult as you may think, right?

[00:11:47] ED: Thank you. That was our goal.

[00:11:49] KS: Yes, sir. That was the goal. Yes, exactly.

[00:11:52] AH: Okay. Well, that was an easy one.

[00:11:58] ED: Easy question.

[00:11:59] AH: So just to go back there, what's a transposition cipher?

[00:12:03] ED: A transposition cipher is where you keep all the original letters of the plain text. You're just scrambling them in some predetermined way.

[00:12:12] AH: Okay, and what's the opposite?

[00:12:15] KS: Well, the opposite would be substitution cipher. For example, that would mean I replace the A with a C, and the N with a P, and D with, let's say, an L. That would be a substitution cipher. And the transposition cipher would be starting with the N, then taking the A, and then the W, and then the E, and so on. But one disadvantage of transposition ciphers is that if the message is short, like only one word, it's easy to break. There are certainly not many transposition ciphers, not many ways to encrypt the word Andrew with a transposition cipher. But of course, if you have 100 letters in your message, it gets really difficult if you use a good transposition cipher.

[00:13:03] ED: And there are a couple other methods. So you have substitution transposition. You also have something called a concealment cipher, like steganography, which is a way of hiding a message in a way that it's not entirely clear that there is a message. For example, kids will often know way of writing something on a piece of paper and lemon juice, and then holding it over a candle. Or there's an old method, thousands of years ago, Herodotus talked about one message where they needed to send a messenger. They knew he would be searched. So how to send him where he didn't have a message, but there was still something in writing? So they took a messenger and they shaved his head and then they tattooed a message on his scalp, waited for the hair to grow back, and then sent him across enemy lines. And then there're some other things like abbreviation ciphers, but those are the primary methods.

[00:13:57] AH: From the paper and pencil era, do you have something that particularly caught your interest or something that you're like, “Wow! That's so cool.” Yeah, I don't know. Do you have a favorite?

[00:14:11] KS: We recently wrote a research paper about Playfair cipher. So that has certainly become one of our favorites. We wrote this paper with four other experts. And some of these others who took part improve the world record in breaking Playfair cipher. So the shortest Playfair cipher text that has ever been broken is, I think, 26 letters long. And with the person who set this world record, we wrote this research paper, which was really interesting.

[00:14:49] ED: In our book, we have what's called a made up puzzle. So we hid puzzles within the book about puzzles. Like there are secret messages about like Morse code somewhere. Or there's a little shorthand message that’s next to an image. And you have to solve all these different messages to get to the end.

[00:15:06] AH: What is a Playfair cipher?

[00:15:08] KS: It's a cipher that encrypts letters pairwise. So first, you need a certain table. And with this table, which is quite simple, you can substitute the letters of a plaintext pairwise. You always have to look this pairs up in the table. And when you use this system, you can encrypt just any text you want. And the system was invented in the 19th century. Well, with today's means, it's possible to break it. But before the computer age, it was quite secure if the cipher text wasn't too long.

[00:15:47] ED: So it's a little difficult to describe Playfair and just an audio medium. But imagine if you have a grid, it's a five by five grid, and you write the letters of the alphabet, and it's A through Z, and you combine, say, the I and the J. So you have 25 in this grid. And then you would come up with a word you wanted to encrypt, for example, the word hello. And so you'd look on this grid, this five by five grid, you'd look for where the H is and where the E is. So you have a pair. And the H and the E are going to be corners of a rectangle. And then you look for the two letters that are at the opposite corners of the rectangle, and those become the pair of letters in the cipher text. And then you go to the next pair in hello, H-E, then, well, L-L. So forget the double L. Go L-O, and you look for where the L is and where the O is. And those are corners of a rectangle. And you take the letters that are at the opposite corners of the rectangle, and you go on pair by pair. And there're some other rules for what to do if they’re on the same line or if you had doubled letters. But that's it in a nutshell.

[00:16:52] AH: Wow! It would be good to focus in on some of the famous ciphers from history. Let's focus in on a couple of examples. So I know in the book you discuss Mary, Queen of Scots. You discussed Edward Elgar. You discussed all kinds of people. Help us just focus in on a couple of examples. And let's analyze them.

[00:17:15] KS: Well, I think the most famous encrypted document is the Voynich manuscript. That's an encrypted book probably from the 15th century. It's a unique piece. A script or a writing system is used that is unique. And, well, it has 230 pages. And so far, it's simply not possible to read this book because nobody has broken the encryption, if it is an encryption of at all. Of course, it could also be just nonsense, gibberish, or it could be just an ordinary writing. But it could also be encrypted. But this encryption has never been broken, although very many people have tried. That's a very famous one.

[00:18:00] ED: Another very famous system that is solvable is what's called the Freemason cipher, which they didn't invent, but they were the people most commonly who used it. And it basically looks like a tic-tac-toe grid, followed by an X and another tic-tac-toe grid. And imagine a tic-tac-toe grid where there's a dot in each of the nine sections of the grid. And, again, you would write letters in each of those sections. So for example, if you had a tic-tac-toe grid and you put an A in the upper left hand corner, then an A would become that corner. The right angle of the lines would become an A. And then a B would become like the U shape of the next. And, again, I'm waving my hands in the air. It's difficult to do on a podcast. But the Freemasons use this routinely to communicate between lodges, and even on tombstones. If you go to some of the Freemason tombstones, you can see this cipher on their tombstones. And other people would just use it, because it's a simple system to learn. So children might use it. And postcards were very commonly encrypted. So if someone wanted to send a postcard and they didn't want their family and the postman and everyone else reading the postcard, they might use the Freemason cipher to encrypt what they wanted to say.

[00:19:20] AH: And I just want to go back to the Voynich manuscript. What time period are we talking about here? Who was Voynich? Or is that just the name of the book? Yeah, help us just understand what's going on there a little bit more, please.

[00:19:34] ED: Sure. It's a book that is over 500 years old. We've radiocarbon dated it to the early 15th century. It's called the Voynich manuscript because it came to modern attention when a Polish book dealer named Wilfrid Voynich purchased it in the early 1900s, I believe. And we don't know what it says. It has hundreds of pages in a script we don't recognize, with an alphabet we don't recognize, with pictures of plants we don't recognize, and other pictures that they might be astrological drawings. And there're many small drawings of what looks like tiny bathing tubs with women in the bathing tubs. But it's just this very mysterious – It's called the world's most mysterious manuscript. We have no idea what it was for and no idea what it says.

[00:20:35] AH: That sounds immediately to me like something where there must be a lot of theories or conspiracy theories about what exactly it is. Tell us about some of them.

[00:20:46] KS: Well, some say that the Voynich manuscript was written by extraterrestrials. Meanwhile, there are at least 60 solutions. So there extremely many people who claim to have solved the Voynich manuscript. Then about every year, two or three new ones are published. It's quite annoying. And it's impossible to look at all these solutions. But none of these solutions has ever been accepted by the research community.

[00:21:18] ED: There are people who claim that it is in pretty much any language you can imagine. That it's in Latin. It's in Arabic. It's in, I don't know, Hungarian, all these different languages. And there are people, as Klaus said, who think that it's extraterrestrial. There're people who think that maybe it has something to do with alchemy. Maybe someone was looking for that Philosopher's Stone. And so they were writing things in code. One of my favorite theories is that someone may have been selling medicinal ointments. So you got to think this is 1400s. This is maybe 100 years after the black plague. People are kind of more interested in health or buying something to make themselves healthy. And if someone were to sell an ointment, the price of the ointment would be directly related to the rarity of the herbs that were in the ointment. So if you had this mysterious book with pictures of herbs that no one recognized, you could say, “From far away, very expensive, very expensive.” But in truth, we just don't know. We don't know.

[00:22:23] AH: Is it Polish originally? Is that where it originally came from? Or do we not know?

[00:22:28] ED: It was purchased by Wilfrid Voynich in Italy at the place called the Villa Mondragone, which was south of Rome. The Villa Mondragone, you may have heard of that before, because that's where Pope Gregory declared the Gregorian Calendar in that particular place. But the monks there we're running low on funding, and we're discreetly selling some of the books in their collection. And that's where Voynich went. And he went through and he found it. He called this one – What did he call it? The ugly duckling. Because it was so different from everything else. You have these beautiful, illuminated manuscripts with gold calligraphy. And then you had this strange one with pictures of odd plants. And he spent the rest of his life trying to decrypt it and had no luck.

[00:23:15] AH: Have either of you ever tried to have a go at the Voynich manuscript?

[00:23:20] KS: Not really. So as I said, I'm more the journalist type. So I write about others deciphering it. But so far, nobody has been successful.

[00:23:32] ED: I've taken a look at it. And when you're cracking a code, you look for patterns. That's the first thing we look for, and trying to find out what are their letters that are commonly used in different places, or words that are commonly used. And one of the difficult things about the Voynich manuscript is the script is different. It’s in a cursive script. And we can't tell where exactly the letters are. For example, if you were to write in English the letter M, right? And an alien were to come in and look at it, they wouldn't know if that was one letter, if it was two letters, if it was three letters. They wouldn't know where one letter stopped and the other one started. So we have that problem with what we call Voynichese, the alphabet. But we have – It looks like a language. It seems to have word rakes, but it has no punctuation. So there're just all these questions about it.

[00:24:23] AH: Is there's something actually there or do you think there’s not something that can be broken?

[00:24:29] ED: I change my mind every day.

[00:24:32] KS: I'm not sure. But, meanwhile, I think that it cannot be broken. That it just contains nonsense. At least it would be very unusual, because encryptions from the 15th century can usually be broken quite easily today. The encryption techniques of the time were not very good. So it would be very unusual that a book with so much material to analyze from this time could not be broken would be very unusual.

[00:25:02] ED: The main theories are either it's a code, or it's fraud. For example, Emperor Rudolph II around that time was known for collecting curiosities and paying good ducats, gold ducats for it. So someone may have created a curiosity to sell to him from far away. It's also possible that there was someone who was just mentally ill and was scribbling. Now, the handwriting in the Voynich is beautiful, beautiful calligraphy. So either someone – If that's the theory, then someone who's mentally ill had beautiful calligraphy, or maybe he or she was a member of a wealthy family and scribbled a lot. And the family paid a calligrapher to take all these notes and write them out to where they looked like nice notes. Or maybe someone was trying to write in their language what they thought Arabic sounded like. I mean, there're all these different theories on it.

[00:25:58] AH: Are there examples from history where people have invented what looks like a code, but actually it's just like a big joke? It's just nonsense. It's just gibberish underneath it all? Are there any examples of that?

[00:26:12] KS: Yes. Well, there's a quite recent example in Germany, in Hamburg, in the river Alster, bottle posts were found, and they contained a text that looked like secret messages. Meanwhile, I wrote about this on my blog several times. And meanwhile, it is known who created these messages. And it was actually a mentally ill or mentally disturbed person. And it's very likely that these texts don't have a meaning. So there are some parallels with the Voynich manuscript, although it's certainly not the same, but some similarities.

[00:26:50] ED: Yeah. By bottle posts, he means that, for years, they were finding these bottles washed up along the riverbank that would have within the bottle usually a piece of cardboard, like a cigarette carton, that was covered with what looked like an encoded message. And they were showing up. I think we had what? Like seven or eight different bottles. And many people were trying to decrypt these until, as Klaus said, it showed up in the newspaper. And the reporter got a call from someone who said, “I know who made these.” And we found out that it was someone who was mentally ill.

[00:27:25] AH: Are there examples of this kind of stuff being used surrounding like historical events where someone's trying to lead someone off in a false direction and they give something that looks very difficult to decipher, but it's actually just nonsense? I guess almost like cryptographic disinformation or something? Are there examples of that?

[00:27:49] KS: I wouldn't know.

[00:27:52] ED: I mean, definitely, disinformation is part of spy craft. The whole D-day invasion, there were all sorts of things of ways that the allies were trying to confuse the Germans as to what was going on. Now, whether it involved codes that were deliberately not solvable, I would say no. Usually, it's the opposite, where there is a code that we think the enemy has solved. And so we will put messages in it that they think are real, but are not, because we know that they can solve, if that makes sense, kind of going around and around.

The whole battle in the Pacific Ocean in World War II, the Battle of Midway, kind of involves something like that, where we could read some of their messages. And we knew that they were planning an attack, but we didn't know where the attack was going to be. And so we deliberately sent a message, we, being the United States, saying, “Well, we think it's this island.” And so that island sent a message saying that they were having trouble with their water purification plant. And then in the code that we could crack, we heard them say, “This island AF. AF is short of water.” That way, we knew that AF meant midway. And so we knew that's where the Japanese fleet was going. And so we could send our fleet to meet them there.

[00:29:17] AH: That allowed the American Navy to defeat a larger and more experienced Japanese Navy, right?

[00:29:23] ED: One of the big problems, especially in sea battles, is that it takes time to get ships to a certain location. You can't airdrop them. You need time.

[00:29:34] AH: One of the famous examples that I know of is the Edward Elgar letter. Could you just tell our listeners a little bit more about that?

[00:29:43] ED: Sure. You're talking about the Dorabella cipher, I believe.

[00:29:47] AH: Dorabella, yeah.

[00:29:48] ED: So Edward Elgar's family in the late 1800s stayed with another wealthy family over the course of a vacation. And then afterwards, they sent thank you notes. And in one of these thank you envelopes, Edward Elgar enclosed a note in cipher for one of his friends there, a young woman named Dora Penny. Dora was his companion for years. So they just liked each other. And later on, she wrote – After he passed away, she wrote a book, I believe, called *Memories of a Variation*, where she talked about her time with him and what it was like being with this master composer as he was coming up with this music. And she had gone through her papers, and she found this note that she'd never been able to decrypt. And so she put it in her book saying, "Can anyone decrypt this?" so this note from 1897. And no one was able to decrypt it now. Here we are 100 years later, we still can't decrypt this little message. It looks like a small substitution cipher. So there're all kinds of, again, theories about it. Was it really a cipher? Was he just messing with her at the time? Is it related to music? We just don't know.

[00:31:04] AH: What are your hunches? Well, do you think that that's also nonsense? Or do you think that there's something there?

[00:31:10] ED: Klaus and I have very different opinions on this. I'll let Klaus go first.

[00:31:14] KS: Well, basically, it's not even sure that this message was even created by Elgar. Well, it probably was. But there are even people who doubt this. It's hard to say. Well, I would expect if a guy had sent this message to a woman who was not familiar, not really familiar with cryptography, I would expect that it is easy to solve, but apparently it isn't. So either it's simply a joke, which could be, or perhaps it's a very strange text, perhaps a text without vowels, or avoiding the letter E, which is the most common in English, or something like that. Apart from that, I don't know. It's a mystery.

[00:31:59] ED: My theory is that it was intended. It was written by Elgar. It was intended to be solved, but I think he made a mistake. And that is not entirely uncommon. There are mathematicians who have published codes in their books that were not solved. And then they kind of, “Oops, I forgot. I don't remember how I did it.” And, yeah, I think he made a mistake. Now, some of these, they can make a mistake, and it's still solvable. I have solved at least one code that had mistakes in it. But yeah, that's my theory on it.

[00:32:28] AH: And you spoke about how you both have a different opinion on this one. I guess that that made me think, is there any big divides within the world of cryptography and code breaking? Like what are some of the big debates or the big controversies at the moment? Are there any?

[00:32:49] KS: Well, right at the moment, there's certainly a discussion about the so called Somerton man. He is a man who was found dead at a beach in Australia in 1948, and he carried an encrypted note with him. Or he didn't actually carry it with him. But it was found in a book he had in his pocket until shortly before his death. But in this case, the debate is not really about the encrypted text. It's more about the identity of this person. He might have been a spy. He might have been a refugee, a fugitive. But what makes this story especially interesting is that he was never identified, which is very unusual, because the face of this dead body was published all over Australia, and later all over the world. But nobody identified this person, which is really strange. Perhaps the encrypted text would help to identify him. But honestly, I doubt it. It's probably not really helpful.

[00:33:51] ED: Well, and that's actually got a follow up to it from this year. Because, again, this man, this dead body, with no identification, no tags on his clothing, no one coming forward to say who he was, was buried in 1948. And they actually decided this year, in 2021, to dig him up to see if they can get any DNA off of him and see if they can help them figure out which part of the world he was from, or did he have any descendants. So that's definitely something that we're following closely right now.

[00:34:23] AH: What's the name of your blog post just in case any of our listeners want to check it out?

[00:34:29] KS: The blog is name cipher brain.

[00:34:31] AH: Cipher brain.

[00:34:33] KS: That's a term that was coined by a cryptologist named Herbert Yardley in the 1920s. He called –

[00:34:40] AH: The Black Chamber?

[00:34:41] KS: Yes, exactly. He wrote the book, *The American Black Chamber*. And in this book he describes what it takes to be a good code breaker. And apparently, it takes a lot, because there are very few of them. Even Herbert Yardley had trouble finding people who were good code breakers. And he said, to be a good code breaker, you need a cypher brain. And he knew hundreds or even thousands of people who worked as code breakers, but only very few of them were cipher brains. And so I took this expression as the title of my blog.

[00:35:16] AH: and that actually preamps one of my other questions. What does make a good cipher brain? What makes a good code breaker? Is it mathematical abilities? Or is it creative thinking, or both, or all of the above, or something else?

[00:35:34] ED: All of the above. Yeah, mathematics helps being able to think in many creative ways. Also, being very tenacious. Not wanting to give up. Just trying method after method after method. Some code breakers use computers intensively. I don't. I don't use computers. Every so often, I'll use a spreadsheet. But I'm the kind of person that likes to say just get a Scrabble set and dump the tiles and move the tiles around and see if that sparks something for me. So everybody uses different methods.

One of the codes I'm working on right now, unsolved, is a sculpture called Cryptos, which is at the center of CIA headquarters. And it's been 30 years. It's got four codes. Three of the four have been solved. The fourth has not been solved yet. And it's one of the most famous unsolved codes in the world. And it's just 97 characters at the very bottom. And it's my belief that because all the big code breaking minds and college educated folks have been working on it and have not solved part four, that it's going to be someone who comes in with lateral thinking. So it could be a child, it could be a chef, a gardener, someone who's looking at it a different way that may finally be the person that figures out how to take it apart.

[00:36:53] AH: And apart from the Voynich manuscript, is that Cryptos outside the CIA headquarters, is that the most famous one that hasn't been broken yet? Or what are some of the other ones that everybody's working on or everybody's excited to try to crack?

[00:37:09] ED: Well, I have a list of the world's most famous unsolved codes. And one I have at number one, again, is fairly controversial, because some people think it's solvable and some people think it's fraud. But I listed as the Beale ciphers, or the Beale papers, which is a pamphlet that was written in the late 1800s that has three encrypted messages in it. And one of them is solved in the pamphlet and used the Declaration of Independence as a way of solving it. The other two are not solved. And supposedly the pamphlet said these messages detail the location of a treasure of gold and gems that's hidden somewhere in Bedford, Virginia. But Klaus is of the theory that that one is not solvable. Again, my opinion changes. But yeah, there's the Voynich manuscript. There's the Zodiac Killer cipher. Though, as we spoke about that one, one of the messages, which is solved after 51 years. What else Klaus? What are other famous ones?

[00:38:09] KS: Yeah. Well, on my blog, the most popular stories are usually the ones about unsolved encryptions that are related to unsolved crimes. There are about half a dozen also of these cases. For example, there was a case in the 1990s, the McCormick case, in Missouri, in the state of Missouri. That's about a person who was murdered, and in his pocket, he had an encrypted text, and neither the crime nor the text has ever been solved. And there are a few other cases of this kind from the last 150 years. And these stories are extremely popular on my blog, because at least in theory, you can solve a crime just by solving a cipher you can retrieve from the Internet.

[00:39:03] ED: Another one that made the news in the recent years is about the pigeon. In England, someone was cleaning out his chimney, and he found the remains of a pigeon that had passed away. It was one of the carrier pigeons, one of the messenger pigeons from World War II. And it still had a message strapped to its leg. And this message was in code. And there are many people that have been working on that one, and some people saying it's solvable, some people saying it's not solvable. But that's another one that's big in the news.

[00:39:36] AH: Wow! So for the Zodiac cipher, there's three parts to it, and only one of them has been solved. The other two haven't?

[00:39:44] KS: There are four parts, and two have been solved.

[00:39:47] ED: Yeah, it's not so much – We're talking to Zodiac. Not Cryptos. If we're talking Zodiac, he sent multiple messages to newspapers. And the first message was solved very quickly by a puzzle solving a couple. I think they were a scrabble fan couple, and they solved it. Then he sent another lengthy message, and that was the one that took 50 years. And then there're some others that are very short. They're just two or three lines. We don't think they're parts of the first two. We don't know if they're going to use the same method or something else. But I just be cautious about calling them parts is what I'm saying.

[00:40:26] AH: On that note, actually, did either of you ever get law enforcement reaching out to you? The FBI? The police? What does this mean? Help us break some code. Yeah, can you talk about an example if you have,

[00:40:41] ED: Klaus was talking about the Ricky McCormick cipher. And that was of a body that was found in a cornfield in Missouri that had two messages, or two encrypted messages in its pocket. And the FBI tried for a while to solve these messages. The FBI has a unit called this CRRU. The head of the CRRU is a man named Dan Olson, who's very good at codes. And there's also the American Cryptogram Association, also very good at codes. But the FBI couldn't solve these. And eventually, they took the very unusual step of putting these messages on the front web page of fbi.gov asking for public help saying, “Can you solve these? Or have you ever seen anything using a similar system?” which also would have been very helpful to them. It didn't it didn't help. But yes, sometimes the FBI does reach out to the public.

[00:41:34] AH: And were you able to help in that case, Elonka?

[00:41:37] ED: No, I wasn't. I have spoken to various reporters about it. But no, it's not one that I solved. Most of the codes I've solved have been in the underground hacker subculture. The first big one I saw was called the Phreaknik three code, Phreaknik spelled P-H-R-E-A-K, like phone, phreaking, if anyone remembers that. And I went around cracking some other codes in the hacker scene. I actually cracked so many. I've been banned from competition.

[00:42:05] AH: Oh, really? Wow!

[00:42:07] ED: When they released it at the Atlanta convention, they put at the bottom of the code, "Past puzzle solvers are ineligible for prizes associated with this puzzle. Give someone else a chance, Elonka." And so I cracked that one too. And another big one I cracked was on the Cyrillic Projector. This was one that was on a sculpture at the center of the University of North Carolina in Charlotte. And decrypting, it came out to be extracts of classified KGB documents, not because it was a message from spies, but because the artist, Jim Sanborn, had access to documents that have been smuggled out of the Soviet Union. And one of them was a classified KGB document. And he used that text and he put it in this sculpture, which is now at University of North Carolina.

[00:43:00] AH: I think we've kind of touched on this I talked about. But say you get a code or a cipher, as someone that's broken all of these codes, help us understand like what the first steps are. So here at the Spy Museum, at the moment we have three Enigma machines. We have one from the Cryptologic Museum. And the way that I tried to describe it to people that were taking around is that imagine like a crossword puzzle, a very complicated crossword puzzle. And when you have one of those crossword puzzles, one of the places you can start is on a three letter word. You find a short word. You try to crack. And then that gives you an opening where you can look at other things. So I say like with the example of Enigma, the first three letter word does that. When you type in an A, it never comes out as the letter. When you type in a B, it never comes out as B, and so forth. So you're just looking for those small ways that you can gradually build up a picture. I don't know if you think that's a good example or not. But help us understand how your project. Is there like a system? Is there like a logic? Is there little Elonka's 12 steps to cracking a code? Yeah, help us get our head around that.

[00:44:22] ED: Well, first, I have to be humble here and say that I'm a lightweight. There are people who are far better at this than I am. And many of the bigger codes that I've solved, it hasn't been me alone. I've been part of a team that's done it. But I've helped by kind of gathering information together. Now having said that, I also need to say that one of the best code solvers in the world ever, I think, is the woman Elizabeth Friedman, who did not get enough credit during her lifetime. But her story is starting to come out. I believe you interviewed Jason Fagone and his book, *The Women Who Smashed Codes*.

Okay, having done the caveat of that. When I look at a code I'm trying to solve, the first thing that I do is I count. I look for the patterns. I do frequency analysis. I look, is it made of letters? Or is it made of symbols? If it's made of symbols, I'm going to make lists of those symbols and I'm going to convert the symbols to letters, because our brain generally processes letters better than it processes symbols. And, yeah, if it's got what looks like word breaks, I'll think what kind of language was it written in? Was it written in English, or French, or German? And research those kinds of languages and see what kinds of words were there. So small words, as you said, definitely can be a help, but making long lists of the letters that are there. When Elizabeth Friedman was cracking Enigma by pencil and paper, she would just get a huge piece of paper and just start writing things down. And you mentioned about the first words. One of the things that would help us in cracking Enigma, the crib, as we called it, would be similar words that would often be used. And in Enigma messages, for example, they might often have the words Heil Hitler. And so if we could look for that, then that would help us all things. Or if a message was sent from a place that we knew to be a weather station, and you would look outside and, "Okay, it's raining," then chances are pretty good that the word rain in German would be somewhere in that message. So those are the first things that come to mind.

[00:46:37] AH: When you say frequency analysis, you're just talking about how many times a particular letter turns up, or a particular symbol or something comes up. And this is based for English, the E is the most commonly occurring letter. So you look for what comes up the most often, and there's a decent chance that that's the letter E. Is that correct?

[00:46:59] ED: In English, absolutely. Yeah, you want to look for an E or a T. I also want to take a pause and say one thing. CRRU stands for the Cryptanalysis and Racketing Records Unit of the FBI.

[00:47:14] AH: And just out of interest, in German, what's the most frequently occurring letter in German?

[00:47:20] KS: It's also the E. E, then N, I, S, R, A T.

[00:47:26] AH: That's interesting to know. I just want to get on with another couple of questions. One of them was help us understand like this transition. So from the paper and pencil era, and then we go to the machines, and then we go to computing. So before we get up to just now and before we get up to pretty good privacy and quantum computing, I've always been quite fascinated by the one-time pad. Is the one-time pad, is that paper and pencil? Is the electromechanical? Is that computing? Or can it be theoretically all three? And just tell our listeners what a one-time pad is?

[00:48:09] KS: Well, first of all, the one-time pad is a method where you have a random sequence and you add this random sequence to your plaintext. And a one-time pad, if it is used properly, it cannot be broken, because every plaintext can be encrypted to every possible cipher text. So even if you have a suspicion of what the cipher text might be, you can't be short, because it could be anything else as well. So for the one-time pad to work properly, you need a key or a random sequence that is as long as the plain text itself, which means that you need a lot of key material. If you want to encrypt a thousand letters, you need a thousand random letters to encrypt them. And this makes, of course, the key management quite difficult. This is how the one-time pad works. And it's, in fact, all three. It was used manually before the Second World War. It was used with one-time pad encryption machines, electromechanical. And it also can be used with a computer. So the only or almost the only system that is provably secure, but it's not very convenient, because you need a very complicated key management. The name one-time pad is because you only may use each key once. This is why it’s called one-time pad.

[00:49:43] AH: And that's why it's unbreakable, because you use it one time and then you get rid of it and then you start again?

[00:49:47] KS: Yes, exactly. Yeah.

[00:49:49] ED: Unless they make a mistake, which some people did, and they would use the pad more than once, which was a big mistake, but would allow us to read some messages.

[00:49:58] AH: As a one-time pad, will that remain unbreakable even with – We hear of quantum computing and all of these other types of things? Even if you had the most powerful computer in history, you could still never break a one-time pad?

[00:50:14] KS: Yes. If it's used properly, it's impossible, for the simple reason that every possible plaintext can be encrypted to every possible cipher text. So even if you think you have the solution, you can’t be sure, because every other solution is possible as well.

[00:50:32] AH: Just to break it down, it’s tough with audio only, because we don't have the visuals. But just to give an example for our listeners to get their head around.

[00:50:42] KS: You have one random letter, or let's say we want to encrypt a text consisting of 20 letters, then we need a key consisting of 20 random letters. And then we add each letter from the text with a corresponding letter from the key. For example, if the first letter of the text is an A, and the first letter of the key is a B. A plus B would be like one plus two, would be three. That would be a C. And in the same way, you need to encrypt every other of the 20 letters. And if this key is really random and only used once, there's no possibility to break it.

[00:51:29] ED: He’s 100% correct. Another way I might describe it is if you have one of those memo pads that has glue along it. So you have multiple sheets. And each sheet would have 50 completely random numbers, completely random. And then you're trying to encrypt, say, the word code breaking. And you take the first number and do the C. And the second number and you add it to the O, and the third number you add it to a D. And someone else has their pad with the exact same numbers on the exact sheets, and they decrypt. And then you rip that sheet off and throw it away and never use it again. And the next sheet is a completely different set of random numbers. So there're only those two pads with those numbers. So another way that someone might do it wrong would be if they had, say, 20 pads that had the same numbers. But as long as you have just those two pads, it's unbreakable.

[00:52:29] AH: Just to come to the end, I just wondered, we've spoke about codes. We started off speaking about codes, and ciphers, and the difference between them. But you can also combine them, right? JN-25 was a code book, but then from an additive book, they would try to mask it by adding on an additional layer of security. From an expert's point of view, can you tell our listeners how JN-25 worked and how it combined both?

[00:53:01] KS: Yes. Well, JN-25 was a Japanese code in the Second World War. And on one hand, it was an ordinary code. So every word that had to be encrypted had to be looked up in this dictionary or codebook and replaced with another word. This is, or at least was a standard procedure. In addition, there was a second step, the so called super encryption. That means this coded text was encrypted in a second step. This was also a standard procedure, so nothing really new. But this made the system really secure. So an easy way would be, for example, to replace every word of a language with a number. And to make it secure and more secure, you add the current date to each number. So for example, if the word house is replaced with 123, according to a codebook, you might add 21, because today is the 21st. And you end up with 144. And if we do the same methods or same procedure tomorrow, it would be 145, because it would be the 22nd. And this additional step, super encryption, makes such code really difficult to break.

[00:54:23] AH: And sorry, what is super encryption?

[00:54:26] KS: It was not based on the date, but it was based on so called additives. So additional numbers that had to be added and that were provided in a key book. So this system was quite good and difficult to break, but the US code breakers managed to break it anyway.

[00:54:46] AH: When we get to the modern era, we mentioned Friedman, and a lot of people now are volunteering. When we get to the modern era, I guess like if you watch the movies and stuff, you get this idea that Alan Turing done Enigma single handedly on his own. And you mentioned, Elizabeth Friedman. Help us understand, in the modern era, is it more a case of a team as opposed to a single solitary genius that breaks a code? Or does it depend on the size and scale of the code? Or help us understand that?

[00:55:20] KS: Well, that's very different. There are cases where a single person broke a code without help from others. But in the case of Alan Turing, well, first of all, he wasn't the only person who worked on the Enigma. He had a team he worked with. And once the procedure for breaking the Enigma was known, the next task was to break such a large number of messages, because there were thousands or at least hundreds of messages every day. So in addition to a team of geniuses, it was also necessary to have machines. And it was necessary to have workers who operated these machines. These workers often didn't even know what they were doing, because everything was kept secret. But they were important, of course. So it took several thousand people to break Enigma messages on a regular basis.

[00:56:15] ED: And it's also worth pointing out that Turing based his work on information he'd received from the French who had received information from the Pols. So probably the first person to really crack Enigma was the Polish Marian Rejewski and two of his compatriots. So many people, as soon as they say Turing owns it, but don't forget the Pols.

[00:56:39] AH: Just to close off, I think it would be interesting if you told our listeners about – I thought it was very cute and very funny how your iPhone messages sign off, Elonka. It says, “Sent from my iPhone,” Tell us about it. It’s kind of cute.

[00:56:57] ED: Oh, yeah. You can say sent from my iPhone. I'm in Aruba or whatever. But I say, “Sent from my iPhone double ROT13 encrypted.” And ROT13 is an old Usenet thing where each letter would be shifted by 13 in the alphabet, 26 letters in the alphabet. So if it's double ROT13 encrypted, like an A goes to an N, an N goes to an A. So it looks exactly the same as normal English. So it's a cryptographer joke.

[00:57:30] AH: I had to do some giggling to get up, but I got it in the end. So maybe there're the makings of a cryptographer in me.

[00:57:37] ED: Yeah. Yeah. Yeah. Sounds like it.

[00:57:40] AH: Cipher brain, that’s your blog, Klaus. Do you have a website, Elonka? Or are you working on another book? Do you have talks on YouTube? Help our listeners engage with what you guys are up to a little bit more.

[00:57:54] ED: So my website is elonka.com. And I have a web page on the world's most famous unsolved codes. And I have an extensive set of pages on the crypto sculpture, so elonka.com/cryptos. Our book, the website is codebreaking-guide.com. In terms of YouTube videos, lots, lots and lots. We both speak extensively at many conferences, or we did before the pandemic. And we're doing a virtual book tour now. So our next talk will be at DEF CON, the big conference, hacker conference in Las Vegas. And we also speak at several others, the American Cryptogram Association, the ICCH, the International Conference on Cryptologic History and others.

[00:58:53] AH: Thanks so much for your time.

[00:58:55] KS: You're welcome.

[00:58:56] ED: Thank you. It was a pleasure.

[END]