EPISODE 492

[00:00:00] AH: It's probably a waste of time introducing you. I'm sure all the SpyCast listeners know you are. So how has it been since you left the Spy Museum?

[00:00:08] VH: No, I mean, there's always nostalgia for what you left. I mean, I spent six and a half years at the Spy Museum. So it's not like something that you manage up and move away from. Fortunately, there's always ways to work together in the future. And it's not like I've been gone for long. A lot of what I'm trying to do here at the Cryptologic Museum is based on experience and from information and knowledge of what we did at the Spy Museum. So there is a lot of harkening back to the last six and a half years. And I've even taking a group through the museum to kind of show what we did and how we did it. And I'm taking another one through coming up with the same idea in mind, as I say, "Alright, how can we emulate this museum that had a ridiculous amount of money in a massive building in our tiny little space with no budget? How can we find a way to steal some of the good ideas that make them cheap, if not free?" Whereas they were certainly not when we were putting together the Spy Museum?

So yeah, no, I mean, it's certainly bittersweet. It's always fun to see. I've been obviously following along with SpyCast and seeing the kind of guests that you're getting, and some of them made me a little jealous. I'm like, "Ah! I would have loved to have that person." So it's always one of these things where it's nice to be tackling a new challenge, which is obviously is. I don't regret a minute of those six and a half years. So it's hard not to look back and miss it a little bit.

[00:01:25] AH: One of the things that I'm learning taking over SpycCst is it's kind of like you're doing rehearsals for a player, but every rehearsal is filmed and released into the world. There's no you learn all the lines and you practice it and then you go on stage. You're just on stage from the get go. And then you kind of make your mistakes and learn from them and move on.

[00:01:45] VH: I think that we're in a position now where we've established ourselves as SpyCast of being a professional podcast that gets good guests and knows what they're doing. It adds a human element to it, right? Where we're people to, and there are times when we misspeak, and there are times when we make mistakes. And we're on primetime news, right?

Where there're sponsors involved. And there're commercials and other things like that. We're doing 50 things at once. You look at some of the podcasts out there where, literally, all that person does is the podcast. Their job title is like podcast host. And I think people understand that I, and then now, you, Andrew, had 500 other things that we were doing. SpyCast is one of them. But it's only one of many things.

I did SpyCast for years while we were building a new museum, and now you're doing the same thing where you're trying to expand upon the museum that's been built and do all these other things and deal with COVID and 900 other things. And you're not being paid just to do the podcast.

[00:02:45] AH: For our listeners, could you just tell us a little bit more about your new role and about the museum?

[00:02:50] VH: So I am the Director of the National Cryptologic Museum, which is the museum, which is part of the National Security Agency. So different intelligence agencies have their own museums. CIA tends to be the most famous, because they've been around the longest, I guess. But we are the only ones that is completely open to the public. Yes, you can go to the FBI experience, but you have to get kind of special permission from the congress. Some people can go to CIA, but they've got to get on Langley first.

We, you can just drive up and pull in and walk in the door without any special permission, without any reservation, without anything. We're completely open to the public. We're right outside the wire at NSA. Now, that being said, we're not open right now, though, listen to this podcast and jump in your car, we're still dealing with COVID restrictions. And during COVID, which we'll certainly talk about, we haven't just been sitting on our hands. We've taken this time to do a full-fledge renovation of the museum for the first time since it opened in the 90s. If you've been here before, it's going to be completely different when you come back.

[00:03:45] AH: And one of the interesting things I think about that museum is that it plays quite an interesting role, because like you said, a lot of other places are closed off to the public. To many people, the NSA are being seen as even more secretive and mysterious. How do you balance being part of the NSA with your editorial?

[00:04:07] VH: Sure.

[00:04:07] AH: Some people could be skeptical and say, “Well, is it just the kind of propaganda arm of the NSA or something?”

[00:04:14] VH: One of the things that's important – There're a lot of answers to that question. That's a really great multifaceted question. And it is kind of ironic that we are the one completely open museum and we are attached to arguably the most secretive agency in the world, right? The NSA used to stand for no such agency. It didn't even exist until recently. But I think that the advantage to that is just about everything we put on display is new to people, right? It's not one of these things where it's, “Oh, I saw that in a movie.” Or, “Oh, there're 10,000 movies about CIA, and there's a handful about NSA, and most of them are garbage, where NSA officers are running around shooting people.” I promise you that doesn't happen.

If you looked at the clientele and the people who work here at NSA, they don't look like guys in black suits running around shooting people. They look like people you'll find at Gamestop or at computer conventions and other things like that. We are the nerds of other nerds. Like no other intelligence agency cut out-nerd NSA. We win. We top the list across the board. A wonderful thing is there's no dress code at NSA, which is one of their selling points when they recruit people. So it's not a bunch of people walking around in suit. It’s literally people walking around in like slippers and Misfit shirts and with beards halfway down their chest. That's the agency. And it's kind of wonderful that it’s so quirky.

And I think that we are a kind of a quirky response to that, too. Again, you have this closely guarded agency that has a very public museum. And I think that one of the things that allows us to do that is that we are not the NSA museum. I know I said we're attached to the NSA. We are. I worked for NSA. Everyone here worked for NSA. But the museum doesn't focus on the history of NSA. It focuses on the history of cryptology. Anyway, well, that's kind of being a little nitpicky there. No, I mean, cryptology is the making and breaking of codes and ciphers. That's 99% of what NSA does. We are that museum, which actually allows us to show things that predate NSA, that go outside of NSA. We have very little on display if it was just from 1952 to the present, which is when NSA existed. We wouldn't have some of our better artifacts going back into World War II, in World War I, and even going back to kind of the Revolutionary Period and even earlier than that. So we are the Cryptologic Museum. And so that's where we don't necessarily cover issues that are specific to whether you want to call it whistleblowers or leakers. We don't cover the bad guys. We’re really kind of focused on some the –We’re more of a technology museum. But that's where someone would come into play when they're talking about a cryptologic history story versus something like an individual. And they're talking about one person or not that has some kind of information that they gave away that has nothing to do with cryptology.

[00:06:52] AH: And what's your vision for the museum? So here at the Spy, there's an entry point for people from a variety of different perspectives, people that are interested in technology, people that are interested in human stories, people that are interested in international politics. How was the material displayed the Cryptologic Museum before it closed? And how do you want it to be displayed when it reopens?

[00:07:16] VH: When I took over, and this museum did such an exceptional job of being a good museum despite having zero resources. Like they've been around since the 90s, and they did what they could to get across this message that cryptology is important. That it has historical importance. That it has made a difference throughout history. But in many ways, it was a bit of a grandma's attic setup to where there was just a lot of artifacts everywhere. There were a lot of things to look at, a lot of words on the wall, a lot of noise.

And so I kind of walked in, and from the very beginning I was thinking of just kind of a very important signals intelligence adage. And that's separating signals from noise, right? You go back to Wilberto Willstater writing about Pearl Harbor and the idea of what the failures were, because there's so much noise, and they couldn't pull the signals out of the noise. And they couldn't figure out what was actionable intelligence, versus just gobbledygook.

I felt as though you walked in this museum and it was just noise everywhere. And that's one thing if you're trying to hide the fact that you don't have cool stuff. But what made it problematic for me, at least in my mind, was that the artifacts this museum has our extraordinary, ridiculously good, one of a kind, the first ever, the only thing in existence, the kind of artifacts that most museums would dream of having one or two of, and we have dozens and dozens of them. The problem is you couldn't find them, or you didn't know what they were. You didn't know that they were significant, because they were in cases with like six or seven other things, mostly just window dressing.

And so my concept more than anything else is less is more, is the idea that we want to separate the signal from the noise. Get rid of the noise altogether, and make it a very straightforward basic experience. Everything you look at is going to be something important. That's kind of the mantra that we have, right? The idea is no matter what direction you're looking in, you're looking at history. You're looking at a key artifact in cryptologic history, whether it's a machine that broke an important code, or it's a cryptologic machine that protected important people, or it was a machine that allowed for conversation between like Churchill and Roosevelt, for example, or if it was a particular piece that helps our nuclear command and control capabilities. Everywhere you look is going to be something important. And I think that's what we're trying to do here, is to separate the nonsense from the interesting stories.

And then once we do that, kind of think the Marine Corps model, we're going to break it down to build it back up. And at some point, we might get to the point where we're going to make it a little less Spartan than it's going to be when we reopen. We're adding AV that may not be ready by the time we reopen. We're doing stuff to the infrastructure that may not be ready by the time we reopened, which is going to be a dynamic museum. And that dynamism is also something that we hadn't done before. The museum very static. And if you'd been to it five years ago, if you'd been to 10 years ago, you realize that a lot of things didn't change.

So what we wanted to do was to build in the opportunity for changeable exhibits for temporary exhibit space, and to make contact and relationships with our partners, whether it's through the IC, other intelligence agency museums, or even within the building, right? I think one thing that hadn't been done to the extent that could have is to exploit the kind of things that NSA does that haven't been really shown as well as they could have been beforehand.

So we're trying to do what we can to make coming to this museum not only an experience when you come the first time, but also something we're like, “Hey, come back in a couple months. It's going to be very different. There's going to be cool new things on display that you hadn't seen this time.” And so there's a reason to stop in again.

[00:10:47] AH: Talking about breaking things down to build them back up. One of the things that I love about SpyCast, and this better than me, is that there's a really interesting mix of people that are in the IC, or that are super knowledgeable about it. And then there's other people that are more casual listeners and do something completely different. So could you just break down some of these terms and help us understand the relationship between them? So, cryptology, crypt analysis, code breaking, code making, help the new comer understand this.

[00:11:18] VH: Yeah. It's a lot of funny ways of saying that since the beginning of time, people have communicated, right? There's kind of premise number one. We all understand that. And eventually got to the point where your communications became important to your adversaries. If you can listen into the communication between two people and gain a tactical or strategic advantage, you're going to do so. In that case, it becomes important that you hide what you're actually communicating, right? So you find a way to protect it. In the old days, you might send a writer along with your message with a gun so that people couldn't steal your information. That didn't always work. So you found ways to hide the actual message that you're sending. In some cases, you turn it into a code, and a code basically is where you're replacing one word with another. And then you may have a code book that kind of translates that code back into English or whatever language you're talking about.

Cryptology is slightly different, in that you are not working out of a codebook. So it's not a one for one replacement of a single word with another word. Like, for instance, a code might be where every time I see my name, Vince, instead it's the color red. It’s a very basic code. But roll with me on this one, right? Or wherever there's Andrew inside of our message, it's going to be purple. And then we'd have a book that would actually tell us that. So we would actually know how to go back and forth and determine that.

Cryptology is where you're taking a message and you're turning it into something completely different. In some cases, you're turning it into other letters, where you're scrambling the letters with a machine like the Enigma. In some cases, you’re turning them into numbers, or as an alphanumeric code. In some cases, you're doing that, and then you're doing the other thing. In some cases, you're turning them into symbols. In some cases you’re turning into completely unreadable information. Like in the digital age, we're turning into ones and zeros and the new encrypting systems with that.

The simplest way to put this is that when we are using cryptology, we are taking messages and information and trying to hide it from our adversaries. Now, on the other hand, our adversaries are doing everything they can to break our cryptology, to decrypt our information. And that's a cat and mouse game that's now gone on for thousands of years and will continue on for the rest of human civilization as one side tries to hide their information and the message that they're sending from the other. And this is something that it's not just governments doing this. This is something the trickles down in everyday life. This is something that we understand when we're watching sports, for instance.

One of the things that I've always kind of pushed, and this almost made it into the Spy Museum, and perhaps it'll make it into the Cryptologic Museum, is the idea that you can't watch baseball without seeing cryptology, right? When the third base coach is sending in signs science to the batter, that third base coach is encrypting a simple communication. And even as simple as the catcher is sending in signs to the pitcher. That catchers encrypting information. It's being sent to the pitcher, and the other team is trying to figure it out. And if you're like the Astros, you can figure it out and transmit it back so you have a strategic advantage. Most teams aren't that bold. So they try to find ways to steal signs and be a little less ridiculous about it.

But that's the same thing that nations are doing, right? We're sending information. When the president sends information to his cabinet, when information is being sent from one general to another, we don't want our adversaries to read it. And so they find ways to encrypt that. Nowadays, it's usually digital encryption or even going into quantum computing encryption. Back in the day of handwritten letters, they would use more basic, less technologically advanced systems to make the message unreadable, unless you have a key or unless you can find ways to break the code.

[00:14:59] AH: Some people with intelligence more generally, their point of view is that, in the grand scheme of things, intelligence doesn't make that much of a difference. Do you have a good example from the history of cryptology where some important event or some important set of events or historical process has been impacted by cryptology?

[00:15:21] VH: Yeah, I mean, I'm not a naval historian, so I can't – But there are naval historians that say the Battle of Midway is the most important naval battle in history, the most impactful naval battle in history. I'm not going to weigh on that, because my expertise is somewhere else. But it's certainly an important one, right? It turns the tide of the Pacific War. The Japanese were rampaging all over the Pacific up until that point. The battle right before that, the Battle of Coral Sea was kind of a tie. It was the first time anyone had like tied the Japanese during this time. But the Battle of Midway was absolutely consequential and that, at that point forward, the Japanese were on the defensive and the allies for pushing them back until the end of the war.

And Midway only happens the way that it does is because we break the Japanese codes. An organization with a US Navy called OP-20-G, which was the Navy codebreaking team. Many of them were stationed in Pearl Harbor at place called Station Hypo. And they were able to break the Japanese naval codes that we had called JN25. And that had given us the order of battle and who was coming to Midway long before the battle began. And we were actually able to set a trap for them at Midway. In the end of that battle, we had completely annihilated the forces on the battlefield and sank a bunch of very important ships, including aircraft carriers.

But most importantly, we had killed a whole lot of their veteran pilots, and killed a whole lot of the veteran air crews. And at that point, they never really recovered from that, and they really spent the rest of the war going backward. That's one of the great battles where you can say, A, cryptology had a direct impact on who won and lost that battle. And B, that battle itself – It's been productive a decisive battle all the time, right? You can't pick up a military history book without being like, “This is the decisive battle blah-blah-blah.” It's hard to argue against Midway being a decisive battle. It was the Japanese on offense up until that point. And then from that point on, they were on defense. That was the turning point of the Pacific War. And it was all because of code breaking.

[00:17:18] AH: I'm also not a naval historian. But if memory serves me correctly, Admiral Yamamoto, the Japanese admiral, he was killed as a result of them breaking JN25 as well. So you could argue that that’s another important contribution.

[00:17:32] VH: There are two crypto linguists, which is a fancy word for a cryptologist, who’s also a linguist. Two Japanese experts, Joe Rochefort, and a man named Red Lasswell. And they both worked at Station Hypo. And they both were instrumental in breaking JN25. It was Lasswell actually, who was a marine officer, who broke the Yamamoto message and went to the Navy leadership and said, “I know exactly where Yamamoto is going to be. He's going to be on this plane. This is their flight path. This is the time they're going to be flying.” You make the decision. This is intelligence, right? So intelligence officers don't tend to make policy. Now it's your turn to make the decision about what you're going to do with this information, but here's where he's going to be.

[00:18:11] AH: So I guess this would have been the equivalent of Admiral Nimitz being called an important naval commander.

[00:18:18] VH: Yeah. I mean, Nimitz, or MacArthur, or an Eisenhower, right? Think about particularly in the Japanese case, they had some very good naval commanders. But Yamamoto had basically planned the whole war. And so you're taking out the guy who was the top dog. And you can argue day in and day out and about the ethics of this. And you can argue all you want about whether this is an assassination or whatever else. That's not my job. My job is to tell the history, and the history was that code breaking led directly to his death.

[00:18:47] AH: With code breaking as well, like let's try to zoom in on JN25. Let's use JN25 as an example of cryptography. Tell us about what was that? How did they break it and so forth as a kind of case point of how the secret communications that you mentioned there later used?

[00:19:07] VH: Yeah. I mean, if you think about the codes that you might get in like a back of a newspaper or one of those kind of books that you take on a long drive somewhere, those are ones that you sit down and maybe in a couple hours you're able to break them through substitution and trial and error and maybe some frequency analysis if it's kind of advanced. These codes are not things that you're going to break in an afternoon. These are ones that were worked on for months and months and months at a time.

One of the advantages actually, and this is somewhat ironic, was that because the Japanese were so successful in the early months of the war, because they were running around at such a high operations tempo throughout the Pacific, they gave American codebreakers a ton of information on how to break their codes. They're successful. They were running around. They were fighting everybody and they were talking all the time, because they had to. They had communicate in order to keep this operation tempo very high. By communicating, by using the JN25 code, they were giving us example after example after example of how the code worked. And when you put this kind of stuff into the right people's hands, and the right people being – There are some people that just natural born cryptographers. The idea is that they're good at puzzles. They've got the language background to help them do it. They're in a position where they have a lot of help to kind of work their way through these different codes. They can eventually get there. And that's exactly what happened, is they were able to use a multitude of different techniques to break this code, from analyzing things in depth, which means when you've got a ton of variations of the same code, you can kind of compare them to see if any kind of similarities pop up, if there are any kind of key differences, if there are any trends, right? Because if a code is not a one-time pad, which is something you use once and never again, it will eventually get beyond the point of randomness.

And so you get to where if you're using the same code over and over again, it is technically breakable. And the more that you use it, the more examples that you hand over to the Americans and the allies, the more likely it is it's going to get broken in the end. So this is not some more to what the British did against Enigma. They weren't building massive machines to kind of helped them turn out information step by step. A lot of this is pencil and paper. A lot of what was happening at Station Hypo where people just brute forcing their way through these codes. JN25 wasn't an alphabetic substitution cipher like Enigma. So it wasn't substituting letters for letters. It was actually using a five number system to actually replace letters with numbers. And so you had to go and you basically would have a page full of numbers. And then to look at these numbers and understand that there was a pattern somewhere. Impossible just to look at and pick up the pattern off the top of your head, but if you had enough of the examples of these things, if you had enough ways to put them next to each other and see the similarities are, see what the differences are, then eventually you can start checking things off and working at it piece by piece. And that's literally what they did 24 hours a day, seven days a week. They just chunked away at these messages. And in some cases, they were able to use important worldwide events to help them figure it out, right? If there was a bunch of coded messages coming from a particular ship that had just fought in a very particular battle, then you could kind of say, “All right, we know that Guadalcanal just happened.” The word Guadalcanal is in these messages, multiple places, probably. So let's use that knowledge. And let's see if we can't figure out how they're actually laying out this word like the Guadalcanal. Let's see if there are similar numbers that pop up in multiple messages so that we can do that.

That's kind of similar to one of the ways that Enigma was broken, because if you track things like weather ships, the weather ships use the Enigma machine. Weather ships in World War II in German Nazi, weather ships in World War II, they're not different than anyone telling the weather, right? They’re not all that different from your weatherman on the TV telling you the weather. They start with the weather for Tuesday, April 12th is – Well if you know that's the first sentence of the report, then you already have the clear text. You can actually say, “All right, I've got this plain text. Let me work backwards and see what this turns into as far as code.” Those little hints allow them to kind of churn their way through this information.

It's hard to imagine this because we're sitting here going, “Man, after about 20 minutes of that, I'd probably get frustrated and pissed off and be like, “Just give me a rifle. I'm going to go fight the front.” But the patience of these guys and – Not guys. Some tons of women work on this as well. Over 10,000 women work on this as well. The patience of these people to sit there day in and day out and just stare at coded messages. And just try to figure out. The bigger trick there also is that the messages are all in Japanese. So it's not like you can stare at these messages and pick out English words that are being written in it. So it's almost a code on top of a code. Japanese coded messages. I couldn't do it. So I have a lot of respect for the kind of patience that goes into the seemingly futile pursuit of breaking these codes because they got them. It wasn't a futile. They were able to figure them out. It really turned the tide of the war.

[00:24:11] AH: So you mentioned frequency analysis there. We're talking about things like the fact that he is the most common letter that shows them the English language. So you would look at the currencies of V and then you would look at the currencies of the least used letter. And then you would kind of have a graph or a chart and then you would use that to try to unpack the puzzle. Is that right?

[00:24:32] VH: Yeah, I mean, every language has its own quirkiness, right? To where, in English, you're right, E, is the most frequently used letter, A's T's, S. Is the Wheel of Fortune or letters, right? The ones they give you at the end of Wheel of Fortune. They're the most common letters in the English language. And then you look at Q’s and Z's and others that are the least common. You also have common two letter words, right? N, on of, to, all those that there's only a handful of them that exists in human language. And then you have doubles, where letters appear next to each other, like double LL, double NN, OO, EE. There are only a certain amount of those.You don't tend to see a lot of double Q's. That helps you to tackle some of these very simple codes, not all of them. But ones that are kind of a one for one that aren't, well, called progressive.

The Enigma is progressive. Frequency analysis does not work against the Enigma, because if you hit an A and it becomes a Q. The next time you use an A, it doesn't become a Q again. It becomes an R, or whatever. And if you have an A again, it doesn't become an R again. It becomes a J, and so forth. So you can't actually look for frequency. But if it's a one for one, it's like a shift cipher, where you just kind of shift the alphabet a little bit. Or if you're replacing at random one letter with another letter and it stays consistent throughout the message, then you can use frequency analysis, and there's very few codes that can't be broken that way in about a half an hour or less, because English has tendencies.

Now, if the message is in another language, then your tendencies change. But there are still tendencies in other languages, right? Every language has its own little unique quirks. And if you're able to work – If you have knowledge of those unique quirks, then frequency analysis can help you break a lot of the more basic codes, particularly the tactical codes, right? Ones that are being sent on the battlefield, because you don't have time to go through this long process, really hardcore encrypting something. And so people are like, “Well, whatever. If they don't break this in 20 minutes, it won't matter anyway, because the missions over at that point. We've already attacked or whatever. So I'll send in a relatively simple code.” Well, you better hope that someone good doesn't get a hold of that, because they might be able to break it in about five minutes and then you're in trouble.

But yeah, frequency analysis is something that was not invented but perfected by American code breakers in the early 20th century. Now, the rest of the world figured this out also. But people like William Freedman, Elizabeth Friedman were exceptionally good at coming up with frequency analysis. They looked at – They created sharks. They created different ways of tackling codes to make it much, much easier for code breakers to take them down.

[00:27:00] AH: We could easily do a whole podcast on this. I find it personally fascinating. One of the ways that I think about is that with JN25 and Enigma, it’s like the world's most difficult crossword puzzle. But for JN25, by using frequency analysis, you can get in crossword puzzle the three letter word that gives you your N. And then when you get that N, then it's just painstakingly building the rest out. Whereas with Enigma, one of the ends was that a letter would never be the same letter after it had been enciphered. So if you typed an A, it would never come out as an A. Would you agree with that?

[00:27:42] VH: Right. I mean, one of the advantages. One thing that kept the Enigma more secure is that it never encrypted a letter as itself, right? Like you said, an A never becomes an A, which means that there are only 25 other options that that letter could become. And really what's interesting about if you want to think about brute force attacking Enigma, the way we had a crossword puzzle or a simple code in the back of some book, it would take longer than the universe will continue to exist. The sun will have burned out, before we have time to finish doing that like one by one. The amount of different ways that Enigma can encrypt a letter is 10 to the 114th power, which is an astronomical number. And I don't mean that figuratively, I mean that that's more than there are stars in the known universe. That's about one with 115 zeros after it.

So you can understand why the Germans were confident, were confident that their machine would never be broken. I mean, it's standard sense, it was unbreakable. They just didn't count on that mathematics was moving as quickly as it was, that we would be able to get our hands on multiple Enigmas and codebooks to understand how it works, and actually how it did what it did, which gave us insight into how to break it. And it didn't count on the fact that modern technology would be able to keep up with that speed by creating machines that could work through these possible permutations very, very quickly. Like one machine that we have here at the museum, a Bumbe. That's what they call it. A B-U-M-B-E, which was not a computer, but a mechanical machine that was able to work through different potential Enigma combinations very, very quickly, much, much faster than a human could. That was not something that the Germans were thinking about when the Enigma was put into play. That's not something that they thought about even at the end of the war. They did not believe that Enigma had been broken until much, much after the war was over.

[00:29:30] AH: With both of them, JN25 and Enigma, again, just for the newcomer to cryptology, how would you describe JN25? And how would you describe Enigma? In cryptological terms, what was Enigma and what was JN25? And what are some of the differences?

[00:29:49] VH: Like I mentioned before, I mean, Enigma was a progressive alphabetic cipher. So essentially, it was you typed a letter and then you got another letter out of the machine. And the machine encrypted that letter in multiple ways. It's sent it through a plug board. It sent it through rotors. It sent it to a reflector. The wiring, and depending on which rotors that you put in that day, would give you a letter in return. So you hit A and you would get J. And it didn't just go from A to J, it went through this system. The electrical current went through a system of movements throughout the machine, which eventually produced your J.

And then you just typed like on a typewriter. So you would type your message out. It would encrypt it for it. And then you would send your message via Morse code to your recipient who had the same settings for their enigma. And they were able to type the letters in and get the plain text back. It was that simple, right? It was about user friendly as it gets. It's just you type onto a machine. It was a QWERTY keyboard. You typed your information, whatever the code was into the machine, and you got your plain text back. It was as simple as that. It’s about as user friendly as it gets.

So JN25 worked somewhat differently than Enigma. It didn't take one letter and encrypt it into another letter. It wasn't like a machine that did it that way. Essentially, what it did, it would turn letters and words into five digit numbers, one through nine, sometimes zero. Zeros don’t pop up all that much, but they're in there. So you've got 10 possible digits. Five of them that replaced each word, or in some cases, letter.

And what this did was it added a layer of encryption, because not only were you – You weren't just changing a letter to a letter, but you're changing to a letter to a series, or a word to a series of numbers. And these series of numbers would have had an additive added on to them, which meant that there was a five digit number that you added to the five digit number once you had already encrypted your word or your letter.

So you couldn't just look at these and figure out what does 17493 turn into, because 17493 doesn't turn in anything. It's 17493 minus whatever additive was added on to it after it had been encrypted. So your first step as someone trying to decrypt this was figure out what the additive was. And once you did that, that took away one layer of encryption. At that point, you were still stuck with a page full of five digit numbers that you had to figure out how did these turn back into not English words, but Japanese words? And how do we go about decrypting that? So it's not something that I wish on my worst enemy. That has to be the most tedious work on the face of the planet. It's just kind of just chugging through these one by one, step by step.

And the crazy part about all of this, with Enigma especially, is that you could break that day's Enigma. You can figure out the rotor setting for that day’s Enigma. You can figure out the plug board setting for that day's Enigma. But at midnight, it all changed, because every single day, the rotor settings change, the plug board settings change. And in some cases, the wiring and actually what rotors were used inside the machine change. So you're going to start that all over again at midnight doing the same work that you just did for the last, let's call it year, to try to break this.

Now, once you've figured out how the system worked, you can actually build machines that will help you do it a lot faster, and actually build machines that will help you read the messages a lot faster. So in the case of the four rotor Enigma, where we built the Bumbes for the four rotor Enigma because the British didn't have the additional capability at that point of the war to do it. Once you figure out the rotor settings, which was the Bumbe does for you, then you can actually plug that into an analog of the Enigma machine. So a machine that you build that has the same functionality as the Enigma, and then just churn out the messages so fast, much, much faster than a human sitting there with an Enigma could do. That means you're reading messages much more quickly or looking for the good stuff, and you're pulling out actionable intelligence much faster than you would have otherwise. But that takes time, right? That's not something you build in the beginning. That's something you build as you go along. There're very gradual improvements to the systems. There're very gradual improvements to the training of the personnel. At the beginning, they didn't know what the hell they were doing. But as the war carried on, they started getting much better at doing this.

So by the end of the war, they're reading these messages almost in real time. So the German general is getting information, and the Americans are reading it right along with them. And that's not a good way to win a war if you're the Germans when the Japanese. If your information is being so compromised, that it's being read almost in real time by your adversary, you're probably going to lose that fight.

[00:34:23] AH: And one of the things that it seems to me – And tell me if you would agree with this analogy. With JN25, it's easier to get in, relatively speaking. But then when you're in, there's no extra additional layers to go through. Whereas Enigma is more like the wall and the Game of Thrones. Like it's extremely difficult to get inside. But when you're inside, then the kingdom is open, because there was a series of rules and logics to it. So when you're in, you're. Is that right?

[00:34:59] VH: That's a pretty damn good analogy. I mean, you look at JN25, there's somebody in the military we call defense in depth, where you set up multiple layers of defense in case your outer layer gets breached, the bad guys can't just run in and capture the princess. You've got multiple layers of defense. And that that's what the Japanese were counting on.

And you're, right? Enigma was the wall. Enigma was the impenetrable wall that no one's ever going to get through. But once we did, and once we understood how the machine worked, and once we understood how life was opened, once you're able to get the rotor settings for that day, then the game was over for the Germans. I mean, look at the life expectancy of a German submariner during the war. Something like 75%, 80% of German submarines were killed during the war, and it had everything to do with finally deciding to take them out. And we knew exactly where they were because of breaking the German Enigma machine. So that demonstrates that you don't count too much on your communication security, because sole to this day, there is only one unbreakable code. And that's the one-time pad.

[00:36:08] AH: That's been really helpful. Hopefully, it will have given our listeners something to hang their hat on the comparison of JN25 and enigma. And I just want to go back now to

Cryptologic Museum. How much are you guys looking at the past? Are you going to be looking at news developments? Or like the Zodiac code was recently broken after a long period of time. Give us a sense of how this is all going to shake out.

[00:36:34] VH: We have never been able to keep up with current events before, because we just weren't dynamic. We're a very static museum. So there wasn't a temporary exhibit space. There weren't places to cover current events. That being said, you might have mentioned, like the one possible current event that we could cover here and like the breaking of the Zodiac code, because we are a museum that it's not going to give any classified information, because we are a government Museum. We are all government employees. We're not in a position to put up anything too recent, because anything too recent may have some real classification issues, particularly when we're talking about the kind of the magic words and intelligence and sources and methods.

Anything that we're thinking of from the last decade, methods could be a real problem, in this case to where we're not as sources specifically with the CIA really worries about their source side things. But in our case, we're very technologically-based. So methods comes into play. And so the last thing that we want to do is even hint anything that the agency is doing to gather information from whomever in order to keep this country safe. Forget the keep this country safe. That's a little fluffy. Let's call to keep our leadership informed, because that's what intelligence agencies do. The leadership is the one that's going to keep the country safe. But the NSA is not going to allow us, and we wouldn't try, to give away any of the nation's secrets just because of the museum. So it's difficult for us to do anything current. So we tend to be more focused on the history side of things.

Now, one thing that's interesting, and one thing that is going to be unique moving forward, is because the pace of technology is so rapid, that we may actually be able to show things that are more recent, because they become obsolete. Even things from five years ago had become obsolete because of the rapid pace of technological change. So you might actually run into some stuff and might be like, “I can't believe you’re showing me this supercomputer from 15 years ago.” Like, “Yeah, well, your iPhone does all the work the supercomputer did 15 years ago,” and this is the size of half a room, and your iPhone fits in your pocket. So yeah, we can show you this, even though this was really, really important in 2005. It certainly isn't 2021. So that's one thing that does potentially allow us to show more recent things, is because we are a technology based agency for the most part.

But yeah, it's hard. It's hard to do anything current because of sources and methods and because of the idea that NSA is just as secretive as the other intelligence agencies and for good reason. These are things that our adversaries would love to know what we’re doing. And so we're not going to – We don't have delusions of grandeur here at this museum. We don't think we're important enough to give away any national secrets. So I wouldn't count on seeing anything super recent. But the minute we have connections throughout the building and the minute something becomes declassified, we jump all over it.

[00:39:23] AH: And just on the topic of the museum and its relationship to NSA, what’s some of the other intelligence agencies? Their museums, it’s almost like a means to internal communications or institutional knowledge is like a very internal function, like the CIA museum is a case in point. How does the National Cryptologic Museum function? Is it also for internal matters? Or is it mainly public-facing? Or is that both?

[00:39:53] VH: We have an added mission, and that's the external side, right? So you're right, CIA Museum is mainly for VIPs or for people who work at CIA to get to know their history. Because most people working in intelligence agencies don't have the time to sit back and read books about intelligence agencies, because they're busy doing intelligence work. And so these museums can certainly serve as a means for them to learn their history, to learn the legacy of those that came before them. We are certainly part of that as well. A lot of our visitors when we're open are people who come over from NSA proper. People who are starting their jobs in NSA and saying want to learn the history of the agency before they do, or starting a cryptologic career and want to learn the history of cryptology before they do.

I think the one difference between us and them is that we do have an outward looking perspective as well, that we are open to the public. That we kind of are the gateway to the National Security Agency for the public. This is an agency, again, that was no such agency 25 years ago. And there's a kind of a push for transparency that predates this generation of people. It certainly predates any kind of scandals or anything like that. It was just the idea that if we were going to be an agency that has the trust of the American people and has the trust of

Congress, then we need to become more transparent where we can, that we are a response to that. We are very much, and I just talked about this, that once something becomes public, when something becomes declassified, then we'll have it out there to show the public. That's our mandate at this point, is to show the public what we can about what the agency does, and about what cryptology is.

[00:41:24] AH: I know that you can't speak on behalf of the NSA, but just in terms of the museum, give us a sense of how cyber has been or has not been a threshold that the field of cryptology has crossed. Like give us a sense of how that has played out in the museum today and how you see it playing out in the museum and the future.

[00:41:44] VH: There was an internal debate about the cyber fall to the cryptologic field. I mean, yes, you're breaking encryption when you're kind of in the cyber world. It's algorithmic. So essentially, there are algorithms. You have a sender and a receiver when it comes to cyber, and you're trying to make sure your communication is only read by your receiver and not intercepted along the way. Sure, I mean, that that does fall on kind of the same ideas as what we're talking about here. It's very difficult, as you know, to have a museum that focuses a lot on cyber. There're not a lot of three dimensional artifacts when it comes to cyber. So you can have old computers on display that don't work anymore. And I'm not making fun of it. That was what I did at the Spy Museum, right? We got some computers that we know were instrumental to some old cyber attacks. And you can build a very cool infinity room where you can kind of get inside the computers, which is obviously what the Spy Museum did.

We're having a lot of conversations about what do we do when it comes to cyber, because the director of NSA is also the commander of Cyber Command. Your listeners may or may not know that. He's got three hats, actually. He's the commander of Cyber Command. He's the director of NSA, and he's the director of what's called a central security service, which is all the different secret organizations within each branch of the military are all kind of brought together under this one umbrella command. And General Nakasone, who’s the director of NSA, is a commander of that as well.

So cyber command, obviously, being as closely tied to NSA as they are, there is overlap obviously. We just struggle as a museum. And I think the Spy Museum did as good a job as he possibly could to portray cyber in a museum. The trouble you run into is a couple. One thing is what do you show? What three dimensional artifacts can you actually show? It's all ones and zeros. It's all within computers, or on the cloud, or wherever. But also, the minute you put up an exhibit, you want to try to keep it from becoming obsolete before it's even open, right? So you can cover cyber all you want. But it's moving so quickly, that the worry is that you spend months doing a cyber exhibit that is completely useless by the time you put it up. And so we're still trying to figure that out. I guess, the long and the short answer is we're still trying to figure that out. We know we work closely with our partners inside the building, that includes cyber command, to try to figure out what is the best way to kind of cover this issue. How much should we cover it? Should we spend a lot of time and a lot of real estate in the museum covering it? The answer to that is not so much. We're going to spend a lot more real estate covering the kind of standard topology. We're going to spend a lot more time and a lot more square footage in the museum looking at actual physical three dimensional artifacts, because it's much harder to do with cyber. But we're not going to ignore the topic altogether. We're going to do the best that we can to kind of present it to the public the best that we possibly can. And even then, we went into some real interesting classification issues about what we can't say that you can because of where we are.

[00:44:33] AH: How is the museum funded? And can visitors turn up for free or do they have to pay? Or is that going to change?

[00:44:39] VH: No. The museum is completely free. We are a US government run museum. So our money coming from the United States government through the NSA. There's no pay whatsoever. You just, again, drive up and walk in the door when we're open during our opening hours, and you're welcome to come in for nothing. We're in the kind of the same vein as the Smithsonian's where the museum is funded by your tax dollars. And I promise you, there's not a lot of tax dollars go into us. Maybe a half a penny of your taxes come to the museum, maybe. We certainly don't have the kind of budgets that air and space has or other things like that. That's fine. We're a small museum, and we do what we can with what we have. But no, there's no entry fee. You just can kind of come and learn the history and enjoy the artifacts anytime that we're open.

[00:45:22] AH: For our listeners at the Spy Museum, we'll have a pop up exhibit that features over a dozen of the National Cryptologic Museum's artifacts. And I was like a 10 year old boy who’s just been given a new BMX for Christmas when I saw some of that stuff. Can you tell our listeners a little bit more about some of the things that you sent over to DC?

[00:45:47] VH: Yeah, I mean, that's what I was talking about earlier of the fact that like we had all this stuff on display, but you couldn't find it, right? It was one of these things were like, “Hey, what is that? Is that what I think it is?” And it was. These are the cream of the crop. Basically we’re sitting around going, “Alright, we're not open yet. We're redesigning the museum. We don't necessarily need these artifacts to redesign the museum. We know how big they are. We know their dimensions. We know where they're going to go when the redesign museum opens. So how can we possibly use them to our advantage?

Look, I'll be perfectly honest. Our number one public affairs goal is for people to actually know we exist, because that is something that's not as – We're not as widely known as everybody else. So how can we possibly increase the people who have eyes on the fact that the National Cryptologic Museum is here and exists? And so of course, my immediate thought goes this time. Yes, I'm somewhat biased, but it's not like there's 10 spy museums, and I picked the one that I used to work at. You guys were at it. And said, wouldn't it be a cool way to partner up and put some of these artifacts on display so that not only the people going through your museum could see it. But of course, they would see where they came from. And maybe somebody would say, “You know what, next time we're here in DC, we're going to visit the Cryptologic Museum.”

People think we're so far from DC that you don't want to make the drive up here. We're closer to most of DC than Udvar-Hazy is, which is the Air and Space annex. Granted, they have a space shuttle, but we have some cool stuff too. I live right next to DC, like literally right next to DC, and I make it to work in 20 minutes. It's not that big of a drive. And again, you don’t have to pay for parking here. In Udvar-Hazy, you got to pay for parking. Here, even our parking is free. But what we gave at the Spy Museum, we try to give, and working with you, we try to give a kind of a broad history of cryptology going from some of the early period that we can cover, going back to the Revolutionary Period here in the United States, all the way up to his current as we could get. And included in that are everything from the purple analog, number one, which is the machine that we built. We, the United States, built in order to break the Purple Code, which is the Japanese diplomatic code, that led to us not only reading their 14 point message right before Pearl Harbor, where they essentially declared war. But also reading their diplomatic mail throughout the rest of the entire Second World War. And the machine we have was the one the original one they built, number one, to break the Japanese Purple Code.

We also have an Enigma machine. We have a lot of Enigma machines. But this one is pretty unique and that the rotor letters and the plug board letters are red. Like, “Oh, you got a red Enigma, great. Good for you.” But these particular enigmas were part of the variants. They created 24 enigmas and this is the only one left that were used in the highest levels of the German High Command. And by that, I mean, Hitler. So we call this Hitler's Enigma. It's likely that he, not himself, but messages that he was sending to his high command, whether it was Rommel, or Goring, or any of these was sent through this enigma. And again, this is the only one left in the world. So you're talking about a one of a kind artifact that you can only see right now at the International Spy Museum.

We also gave a little more recent artifact, which was the encryption system inside the Space Shuttle Challenger. So the Space Shuttle, as many of you know, didn't just fly missions for the good of mankind. There are military operations that the space shuttle was involved in putting spy satellites in the space and other things like that as well. So whenever you have military operations, DOD missions, you need to have encrypted communication. So the space shuttles themselves have encrypted communication system designed by NSA.

So one in Udvar-Hazy is probably still in it. But this one was in the Challenger, which of course exploded in 1986. And so this was the encryption system from the Challenger. We also lent a cipher wheel that is, as far as we know – And we know a bit, because we have communications with just about everybody. As far as we know, is the oldest existing cipher wheel on earth. And it was discovered very close to Jefferson's home in Monticello. It was discovered by an archaeologist. And they dated it back to late 18th, early 19th century. So you might be seeing where I'm going with this. And it just so happens to be of a design that Jefferson wrote about pretty frequently.

And so we put quotes around this, but we call this the Jefferson’s Cipher. We have no proof whatsoever that he used this particular cipher. But again, we know where we found it, we know what it's dated to. We know it is the design that Jefferson wrote about consistently. And we know that it is the oldest known cipher wheel of this type on the planet. So I like to think that he was sending messages on it. And it's in French too. Jefferson was at the Franco file. That kind of all comes together to be a really interesting story there. I mean, I can go through every one of them. But those are the kind of the highlights for me. The Code Talker Codebook is very cool.

[00:50:48] AH: There are just so many great ones there. One of my favorite ones is the Comanche codebook. So this is just a fascinating story. 17 Comanche men came up with this code based on the native language. 14 of them went to the European Theater. Many of them were on the beaches on D-Day in Normandy, and that Comanche code was never broken. It’s quite interesting to me that the Lorenz cipher was broken. So we have a Lorenz machine. The Enigma cipher is broken. JN25, the Japanese diplomatic code, but this Comanche code was never broken. So I think that's an amazing artifact. And also the hotline from the aftermath of the Cuban Missile Crisis.

[00:51:31] VH: The crazy things that I got here, and I went line by line through our holdings, essentially. Like what is our collection look like? And there are things that just jumped out that weren't on display at all. And I'm like, “We have this?” Yeah. And we have a piece from each side of the nuclear hotline that was put on in response to the Cuban Missile Crisis. And most people – I even watched a movie. It was been in a cover botch about the Penkoski case.

[00:52:02] AH: Oh, the carrier.

[00:52:04] VH: Yeah, the carrier, right? Through the Spy Museum. I get the code through the museum and I watched the movie. And at the end of it they talk about the hotline as a phone that was put up so that the leaders of each country could talk. And I'm yelling at the TV, “It's not a phone! It's a teletype.” And it is. It’s a teletype system that was set up so these two countries could communicate. Right now at the International Spy Museum, are a piece of the ally, the American side of that teletype, and a piece of the Soviet side of that teletype. The real ones, the ones actually that were there that made up the hotline. Well, that's the thing. Like people always ask, “Is this the real thing? The answer blanket is yes,” right. And that's one of the interesting things about the new Spy Museum, certainly. The stuff in that museum is all real. And everything here at the National Cryptologic Museum is real. We get it from the source. And so everything that you see going into the Spy Museum, inside that case is all real, absolutely.

[00:52:59] AH: So we got like over a dozen of the sort of top artifacts, but there are some that listeners are only going to be able to see when the Cryptologic Museum opens again. Some of my favorites are some of the early books that you have, the first printed book on cryptography and so forth. But could you tell our listeners a little bit more about some of the things that they can see when the museum opens up again?

[00:53:22] VH: Yeah, I mean, we did hold some stuff back not to be a jerk to the Spy Museum, just because there were certain things that just wouldn't work, because of size, and other things like that. I mean, the biggest artifact in the museum is also one of the most important we have. The only remaining US Navy four rotor Bumbe. So the machines that were created to break the four rotor submarine Enigma. They made over 100 of them during the war, but every other one of them was deconstructed and turn into gas trays, or God only knows what. We have the only one that still in existence. So you can come and see a fully – I don't want to say fully functional, because no one's turned it on in seven years. But a fully complete four rotor Enigma Bumbe during the war was used to find German U- boats and then eventually sink them.

The purple machine itself, no one's actually seen a fully intact purple machine, because the Japanese destroyed them all at the end of the war, but they didn't destroy them all that well. So we have a piece that only really the largest remaining piece of purple in the world that was pulled out of the rubble of the Japanese Embassy in Berlin after the war. And you can actually see a little bit about how it works. That to me is one of the more – The purple piece is as good as it gets from a kind of a nerdy history perspective. We also have a bunch of stuff from the Civil War, coded messages. We have another cipher wheel that was captured from the Confederate Army. That's really one of the only ones in existence that still exists like that.

We have a number of some of the early computers that NSA used, now fully into the kinetic computer world, but some of the early computers NSA used. Everything from kind of full-fledged analog ones, like the super computers. And one thing that we're – if you've been here before, a new gallery exhibit that we're opening up is focusing on nuclear command control. Most people don't really think about the fact that you hear that term all the time, like the nuclear codes, right? The football and all these other things. Well, who the hell do you think makes the nuclear codes? Well, if you're talking about making codes, you're talking about NSA, right? So nuclear command control is something NSA does. It's something that hasn't been covered. That's something talking about classification. That's tricky. But a lot of it's starting to become declassified. And so we can start showing some of the more interesting technology when it comes to keeping our nuclear weapons safe. Yeah, and then we're looking at space and other things too as well. So it's going to be pretty cool.

[00:55:44] AH: Well, I really look forward to seeing the new museum. For our listeners, you can come to the International Spy Museum and see some of the superstar artifacts from the National Cryptologic Museum. But just to close off, when you guys open up again at the end of this summer, just give any listeners and the DMV a better sense of the museum? How far are you from Washington? How far are you from Baltimore? What days are you open? Those sorts of things?

[00:56:10] VH: Yeah, we’re 20 minutes from DC. If you're on the east side of DC, we're 20 minutes. If you're on the west side of DC, we're 30 minutes. We're basically on 295. I would say, we're 60% of the way to Baltimore from DC. So we're a little bit closer to Baltimore. It's not a hard drive, but it's worth the trip. Look, if you're on your way to Baltimore from DC, you're crazy not to stop by if you've got time. But make the trip regardless, because it's worth your time. It's a museum that if you haven't been here before, you're going to get blown away by the kind of history that's on display here. And if you have been here before, you'll be even more blown away by the changes that have taken place, because it is an entirely new museum.

We're actually even changing our hours. But we're going to be a lot more user friendly when it comes our hours. It used to be we’d open like every other Saturday or the first and third of the month and only from this time to this time. We're going to become much more user friendly. But we're going to be open more than we were before. So it'll be even easier for people to come by. And there are people who couldn't come by because we're only open during like work times during the week. We're also going to fix that.

[00:57:11] AH: Thanks so much for your time, Vince.

[00:57:13] VH: No problem, man. Good to talk to you.

[END]