MY WEIRD PROMPTS

Podcast Transcript

EPISODE #253

The Future of Privacy: Quantum Threats and Backdoors

Published January 19, 2026 • Runtime: 24:05

https://myweirdprompts.com/episode/quantum-encryption-privacy-backdoors/

EPISODE SYNOPSIS

In this episode, Herman and Corn dive into the rapidly evolving landscape of digital privacy in 2026. They discuss the reality of quantum-resistant encryption, explaining why companies like Apple and Signal are moving toward lattice-based math to defend against future threats like "Harvest Now, Decrypt Later." The conversation also peels back the curtain on signal intelligence, revealing that while the math remains strong, endpoint compromises and metadata analysis provide government agencies with plenty of ways around the shield. From the technicalities of NIST standards to the political battle over "Chat Control" in the EU, this episode is a comprehensive look at the front lines of the modern crypto wars.

DANIEL'S PROMPT

Daniel

I’d like to get your thoughts on the state of consumer encryption in 2024. What do you make of the claims regarding quantum-resistant encryption, and considering the capabilities of signals intelligence, can we assume that major entities already have backdoors into everything we use?

TRANSCRIPT

Corn

So, Herman, I was sitting in the kitchen this morning, and Daniel was telling me about this deep dive he's been doing into encryption. He actually sent over a voice memo for us to dig into today, and it's a big one. He's looking at the state of consumer encryption right now, in early two thousand twenty-six, and he's specifically curious about two things that feel almost like science fiction but are actually very real. First, this whole wave of quantum-resistant encryption that's being marketed to us, and second, whether we should just assume that major intelligence agencies already have a backdoor into everything we do.

Herman

Herman Poppleberry at your service, and man, Daniel really knows how to pick a topic that gets my gears turning. This isn't just about privacy anymore; it's about the fundamental math that keeps our modern world from collapsing. If you think about it, every bank transaction, every private message, every medical record relies on the assumption that certain math problems are too hard for a computer to solve. But that assumption is getting a bit shaky, or at least, we're preparing for the day it finally breaks.

Corn

It's interesting you say it's shaky. To the average person, encryption feels like this invisible shield that just works. You see the little padlock icon in your browser, or that notification in your messaging app that says your chat is end-to-end encrypted, and you move on. But Daniel's question about quantum resistance suggests that the shield might have a shelf life. He specifically mentioned seeing these ten-dollar-a-month Vee Pee Enn services claiming they offer quantum-resistant encryption. Is that just marketing fluff, or is there some substance there? Because we don't even have a functional, large-scale quantum computer capable of breaking current encryption yet, right?

Herman

You’re right on the second part. We are still in the era of Noisy Intermediate-Scale Quantum computers. Just last year, in late two thousand twenty-five, we saw some incredible breakthroughs in error correction, but we still don’t have a cryptographically relevant quantum computer. However—and this is the huge however that most people miss—there is a strategy called Harvest Now, Decrypt Later. Intelligence agencies and well-funded bad actors are likely capturing encrypted data right now, even if they can’t read it. They’re just storing it in massive data centers, waiting for the day a quantum computer is powerful enough to crack it. If you’re a government or a high-value target, a secret that’s revealed in ten years could still be devastating. Think about diplomatic cables or long-term corporate strategies. That data is being vacuumed up today.

Corn

That’s a chilling thought. It’s like a time capsule of your private life that’s just waiting for the right key to be invented. So, when a company says they are quantum-resistant today, what are they actually doing? Are they just using bigger keys, or is the math fundamentally different? I mean, how do you even build a lock for a key that doesn't exist yet?

Herman

It’s fundamentally different math, Corn. We’re moving into what’s called Post-Quantum Cryptography, or P-Q-C. The National Institute of Standards and Technology, or N-I-S-T, has been leading this charge for nearly a decade. They finally finalized the first set of standards in August of two thousand twenty-four. We’re talking about algorithms with names like M-L-K-E-M, which was formerly known as Kyber, and M-L-D-S-A, which was Dilithium. These aren’t just tweaks to old math. Most of the encryption we’ve used for the last thirty years—things like R-S-A or Elliptic Curve Cryptography—relies on the fact that it’s incredibly difficult for a classical computer to factor large prime numbers or solve discrete logarithm problems. It would take a supercomputer longer than the age of the universe to crack a strong key. But a quantum computer? A sufficiently powerful one uses something called Shor’s algorithm, which can slice through those specific math problems like a hot knife through butter.

Corn

So if Shor’s algorithm is the hot knife, what are these new N-I-S-T standards made of? Are they just a thicker block of butter?

Herman

Ha! No, they're more like a block of diamond. Instead of factoring primes, these new algorithms use things like lattice-based cryptography. Imagine a multi-dimensional grid of points—we're talking hundreds or thousands of dimensions. The math problem is to find the point in that grid that is closest to the origin, but you're given a slightly "noisy" or offset starting point. This is known as the Shortest Vector Problem. It sounds simple when I say it, but in high-dimensional space, even a quantum computer struggles to find the answer efficiently. There's no known quantum algorithm that can "shortcut" a lattice problem the way Shor's algorithm shortcuts prime factoring. So when those Vee Pee Enn companies claim they are quantum-resistant, they are likely just implementing these new N-I-S-T standards, specifically M-L-K-E-M. It's not that they've built a quantum computer; they're just using the new shield that's designed to withstand a quantum sword.

Corn

Okay, so it's legitimate math, even if the threat is still a few years off. And some of the big players have already made the jump, right? I remember reading about Apple and Signal doing something similar.

Herman

Exactly. Apple was a major pioneer here. In early two thousand twenty-four, they updated i-Message to a protocol called P-Q-three. It was a massive deal because it wasn't just about the initial handshake; it was about what they call "level three security." They implemented a system where the keys are constantly rotating using post-quantum math. Signal followed suit with P-Q-X-D-H, and just last October, in two thousand twenty-five, Signal announced something even more advanced called S-P-Q-R, or the Sparse Post Quantum Ratchet. They're basically wrapping our current encryption inside a second layer of this new lattice-based math. It's like wearing a bulletproof vest over your chainmail. If one fails, the other might hold. It's a hybrid approach, which is the gold standard right now because we still trust the old math for classical attacks, but we want the new math for the future quantum ones.

Corn

That makes sense. It's a belt-and-suspenders approach. But let's get into the second half of Daniel's concern, which feels much more immediate and, frankly, more cynical. He's looking at signals intelligence, or S-I-G-I-N-T, especially given where we live here in Jerusalem and the technological capabilities of the regional powers. He mentioned seeing intercepted communications between groups like Hamas and wondering: if these groups are using encrypted apps, how is the intelligence community getting those transcripts? Does it mean the encryption is broken? Does it mean there's a backdoor that the N-S-A or the Mossad has a key to?

Herman

This is where the gap between public perception and technical reality is the widest. When people hear that an intelligence agency intercepted a message, they immediately think, oh, they must have a master key or they've cracked the code. But in reality, it's almost never about breaking the math. Breaking the math is the hardest, most expensive way in. It's much easier to go around the encryption. If I want to read your mail, I don't try to invent a machine that can see through the envelope; I just bribe the mailman or pick the lock on your mailbox.

Corn

Like the difference between trying to pick a high-tech lock on a front door versus just climbing through an open window in the back.

Herman

Exactly. There are three main ways intelligence agencies get in without needing a backdoor in the encryption protocol itself. The first is endpoint compromise. This is the big one. If I can put a piece of malware on your phone—something like the Pegasus spyware from N-S-O Group, which is still very much active in two thousand twenty-six—I don't need to break your encryption. I can just see the message on your screen before it gets encrypted, or read it from your device's memory after it's been decrypted for you to read. Your phone is the weak point, not the app. We've seen "zero-click" exploits where you don't even have to tap a link; just receiving a specifically crafted image over i-Message or WhatsApp can compromise the entire device.

Corn

That's terrifying because it feels like there's nothing the user can do. If the device itself is compromised, the encryption is just theater. What's the second way?

Herman

The second way is metadata analysis. This is what people really underestimate. Even if the content of your message is a scrambled mess, the N-S-A or the Mossad can still see who you're talking to, when you're talking to them, how often you communicate, and where you are when you do it. If a suspected operative calls another suspected operative every night at ten p.m. for exactly five minutes, you don't need to know what they said to know they're collaborating. Metadata is often more valuable than the data itself because it's easier to analyze at scale with A-I. In fact, a lot of the "intercepted" transcripts we see in the news are actually reconstructed from a combination of metadata and other human intelligence, or they come from the third way: implementation errors.

Corn

Implementation errors? You mean the developers just messed up the math?

Herman

Not necessarily the math, but how they built the house around the math. You can have the most secure vault door in the world, but if you build the walls out of drywall, it doesn't matter. A classic example is the Encro-Chat or Sky E-C-C cases from a few years back. These were “secure” phone networks used almost exclusively by organized crime. The authorities didn't break the encryption; they actually infiltrated the server infrastructure or found a flaw in how the keys were managed. In the case of an app called Anom, the F-B-I actually ran the entire company! They built the “secure” app themselves and marketed it to criminals, then just sat back and read every message because they had the master key from day one. That’s a supply-chain backdoor, and it’s much more common than a mathematical one.

Corn

So, when Daniel asks if we can assume major entities have backdoors into everything, it’s not necessarily that there’s a secret button the F-B-I can press to read my texts. It’s more that they have an entire toolbox of ways to bypass the encryption without ever needing that button. But Herman, we have to address the legislative side. There’s been a lot of news lately about governments trying to force companies to build those buttons. I’m thinking about the E-U’s Chat Control and the U-K’s Online Safety Act.

Herman

Oh, you’re hitting on the real battleground of two thousand twenty-five and twenty-six. This is the modern “crypto war.” The E-U’s Child Sexual Abuse Regulation, or “Chat Control,” has been a rollercoaster. In late two thousand twenty-five, E-U ambassadors approved a revised proposal that pushes for what they call “voluntary” scanning. But don’t let the word voluntary fool you. They want to compel platforms to use something called Client-Side Scanning. Instead of a backdoor in the encryption, they want the app on your phone to scan your photos and messages against a database of illegal content *before* they get encrypted.

Corn

Wait, so the app itself becomes the spy? That sounds like a backdoor with extra steps.

Herman

That’s exactly what privacy advocates like Meredith Whittaker from Signal have been saying. If the app is scanning your data before it’s encrypted, the encryption is effectively bypassed. The U-K’s Online Safety Act has similar provisions. They’ve been in a standoff with Apple and WhatsApp for over a year now. The government says they need “lawful access” to stop terrorism and child abuse, and the tech companies say that if they build a way for the U-K government to get in, they’ve built a way for everyone to get in. It’s the fundamental law of cybersecurity: You cannot build a backdoor that only one person can use. If a door exists, eventually someone else will find it—whether it’s a foreign intelligence service, a rogue employee, or a bored teenager.

Corn

It’s a bit of a cat and mouse game, isn't it? We build better locks, they find better ways to pick them or just decide to take the hinges off the door. I want to go back to the human element Daniel touched on regarding the Gaza conflict. He was saying that if these are just regular phone calls, they aren't encrypted in transit, which is a huge mistake for any operative. But if they’re using voice over I-P, like WhatsApp or Signal calls, they are encrypted. If the transcripts are coming out, it suggests either the phone is tapped or, as you said, the implementation is being bypassed. But there’s also the psychological side, right?

Herman

Absolutely. In war zones, signals intelligence is as much about psychological warfare as it is about information. When an intelligence agency releases a transcript, they’ll never tell you how they got it. They want the enemy to wonder: Is there a mole? Is our software broken? Is the N-S-A listening to every word? Often, they might have just found an unlocked phone on a battlefield or used signal triangulation to find a location and then used a physical bug. But by letting the transcript leak, they sow distrust. It makes the enemy stop communicating, which is sometimes just as good as knowing what they’re saying. It’s the “panopticon” effect—if you think you’re being watched, you change your behavior.

Corn

That’s the nature of signals intelligence. If you tell people how you’re listening, they’ll stop talking that way. You have to keep the source a secret to keep the information flowing. It’s why the N-S-A is so famously tight-lipped. But Herman, what about the geopolitical side? We’ve talked a lot about the U-S and its allies, but what about China or Russia? Are they playing by the same mathematical rules?

Herman

That is a fascinating question. Math doesn't have a nationality, but the implementation certainly does. China has taken a very different path. While the West is focusing on Post-Quantum Cryptography—which is just better math on regular computers—China has been investing heavily in Quantum Key Distribution, or Q-K-D. They use actual quantum hardware, like their Micius satellite, to send messages using entangled photons. If someone tries to intercept the message, the quantum state collapses, and the sender and receiver know immediately that they've been compromised. It's physically impossible to eavesdrop on a Q-K-D link without being detected. It's incredibly expensive and requires dedicated fiber optic lines, but it's the ultimate end-game for security. We're seeing a bit of a balkanization of the internet here, where different power blocs are building their own "trust architectures."

Corn

So, to summarize where we are for Daniel: the quantum-resistant claims you see in apps today are real in the sense that they are using new, harder math, but they are protecting us against a threat that hasn't fully arrived yet. And as for backdoors, the math is likely solid, but the devices, the legislation, and the people using them are as vulnerable as they've always been. For the average person, the threat isn't necessarily a quantum computer; it's much more likely to be a phisher or a scammer using much simpler methods.

Herman

Precisely. For ninety-nine percent of people, the current encryption we have—the stuff that isn't quantum-resistant yet—is still incredibly effective against almost every threat they will ever face. The move to quantum-resistant encryption is about protecting the future, not necessarily about fixing a broken present. We're building the sea wall before the tide comes in. But there's one more hurdle we should mention: crypto agility.

Corn

Crypto agility? That sounds like a yoga class for hackers.

Herman

I wish! No, it’s the ability of a system to quickly switch from one encryption method to another. The problem is that a lot of our infrastructure—banks, power grids, government databases—is running on code from the nineteen-nineties. Upgrading those systems to be quantum-resistant is a massive, multi-billion dollar headache. It’s the Wye-Two-Kay of cryptography. We have a deadline, even if we don't know exactly when it is, and we have a lot of old code to update before we hit it. If we do our jobs right, nothing will happen, and people will say it was all hype. But it only keeps working because of the massive effort going on behind the scenes right now.

Corn

It really puts things in perspective. We’re in this transition period where the old world is still holding on, and the new world is just starting to be built. Herman, before we wrap, do you remember that story about the Swiss company, Crypto A-G? I feel like that’s the ultimate answer to Daniel’s question about backdoors.

Herman

Oh, absolutely! That is the classic historical example. For fifty years, Crypto A-G sold encryption machines to governments all over the world—Iran, India, Pakistan, dozens of others. They thought their communications were secure. But it turned out the C-I-A and West German intelligence secretly owned the company. They had rigged the machines so they could read everything in real-time. That wasn’t a mathematical backdoor; it was a supply-chain backdoor. And in two thousand twenty-six, we have to ask: who owns the companies making our chips? Who owns the cloud servers where our data is stored? If you control the hardware, you don't need to break the code.

Corn

It’s enough to make you want to go back to writing notes in invisible ink and sending them via carrier pigeon. Although, as you always say, someone would just build a better pigeon trap.

Herman

Exactly! But that’s the beauty of it. The struggle for privacy is as old as human communication itself. We’re just doing it with more zeros and ones now. The fact that we even have this conversation is a win. Twenty years ago, strong encryption was considered a munition by the U-S government. Now, it’s built into every phone. We’ve come a long way, even if the shadows are getting a bit longer.

Corn

That’s a great point. Daniel, thanks for the prompt—it was a great excuse for Herman to go full nerd-mode on us. If you’re listening and you’ve found this dive into lattices and prime numbers interesting, we’d really appreciate it if you could leave us a review on your podcast app or on Spotify. It genuinely helps other curious people find the show.

Herman

Yeah, it really does. Stay curious, keep your devices updated, and don't believe every marketing claim you see on a ten-dollar Vee Pee Enn ad. There’s always more to explore. We didn't even get into the ethics of encryption in the age of A-I-driven surveillance, but maybe we’ll save that for episode two hundred fifty-two.

Corn

One step at a time, Herman. My brain needs a rest after all those multi-dimensional lattices. Thanks for listening to My Weird Prompts. You can find us on Spotify and at our website, my-weird-prompts-dot-com, where you can find our full archive and a contact form if you want to send us your own weird prompts.

Herman

Until next time, stay curious and keep your keys safe. This has been Herman Poppleberry and Corn.

Corn

Catch you in the next one.

Herman

Goodbye everyone!

Corn

So, I was just thinking about that Crypto A-G thing. How many companies today could be in that same position? We talk about the big tech giants, but what about the smaller infrastructure providers that the whole internet relies on?

Herman

That is the multi-trillion dollar question. When you look at the consolidation of the cloud—Amazon, Microsoft, Google—they are the infrastructure. If a government can compel one of them to provide access, they don't need a backdoor in the software. They just need a court order. This is why the fight for end-to-end encryption is so vital. It’s about making sure that even the service provider can't see your data, even if they’re forced to hand over their servers. If they don't have the keys, they can't give them away.

Corn

It’s the only way to truly decouple our privacy from the companies we use. It’s a marathon, not a sprint. And on that note, we’re out. Thanks again for joining us on My Weird Prompts.

Herman

See you soon!

Corn

One last thing, Herman—do you think Daniel’s going to start using a typewriter after listening to this?

Herman

Knowing him, he’ll probably just build his own encrypted mesh network in the backyard. Actually, that’s not a bad idea. Daniel, if you’re listening, let’s talk about that over dinner!

Corn

Alright, alright, let’s go. See ya!

Herman

Bye!