# Episode Book

EPISODE #6152

# Whatever Happened to the One-Time Pad?

| | |
|---|---|
| PUBLISHED | 20 October 2026 at 01:50 UTC |
| DURATION | 24:36 |
| LISTEN | myweirdprompts.com/episode/one-time-pad-today-62063/ |
| HOSTS | Corn, Herman, Larry, Hilbert |
| SCRIPT MODEL | anthropic/claude-sonnet-5.5 |
| VOICES | chatterbox-regular (chatterbox-local) |
| PIPELINE | V5.10 |
| BOOK GENERATED | 20 October 2026 at 07:46 UTC |

## SYNOPSIS

A banker published the first one-time pad in 1882 and told readers to erase the numbers after use. Shannon proved in 1949 that it's mathematically unbreakable. So why has almost every attempt to actually use one failed? This episode follows the pad's real lineage — Vernam's repeating tape, the Soviet duplicate pages that cracked Venona, SIGSALY's fifty tons of vinyl key records, the Moscow-Washington teletype, and Ana Montes's diskettes — to the uncomfortable conclusion that the cipher was never the weak part. Then we ask what replaced it: fill devices that courier a few hundred bits of AES key instead of a pad as long as everything you'll ever say, and quantum key distribution, which reproduces the physics but not necessarily the discipline.

# TRANSCRIPT



### Corn

Daniel wants to know what became of the one-time pad. Not the paper version in the spy novels, but whatever descends from it today: a key that arrives by a separate road, sometimes with no internet anywhere near it, and that works exactly once and then stops existing.



### Herman

The answer has a shape that surprised me. The lineage is real and it's well documented. The current products are not. Most of the famous names in it are either dead, or are something that sounds like a one-time pad and is not one.



### Corn

Give me the paper version first, quickly. We've done numbers stations here before, so I don't want the whole tour.



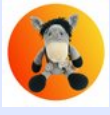
### Herman

Quickly, then. The idea is older than people think. A banker named Frank Miller published a codebook for telegrams in eighteen eighty-two, and his preface tells you to erase the shift numbers once you've used them. A computer scientist, Steven Bellovin, dug that up only in twenty-eleven. Then in nineteen eighteen and nineteen, Gilbert Vernam at AT&T patents a teletype machine that combines each bit of the message with a bit from a punched tape. Joseph Mauborgne at the Army Signal Corps looked at it and said the tape should be completely random and never repeat.



### Corn

So Vernam built the engine and Mauborgne told him what to put in the tank.



### Herman

Fair. Vernam's own tape was a loop, so it repeated, so it was breakable. The random, non-repeating part is Mauborgne's contribution.



**Corn**

And the combining step. Say it so I can follow it with my eyes closed, which is how I follow most things.



**Herman**

Two ways, and they're the same idea. The teletype way is called XOR. You line up a message bit and a key bit. If they match, the result is zero. If they differ, the result is one. The useful part is that if you do it a second time with the same key bit, you get the original back. The key undoes itself.



**Corn**

And the paper way?



**Herman**

Letters become numbers, A is zero up to Z being twenty-five. The key says shift by seventeen. Your letter is D, which is three. Three plus seventeen is twenty, which is U. If the sum runs past twenty-five, it wraps around like a clock, which is what modular addition means. The receiver subtracts seventeen and gets D back. Now the trick is that if the shifts are truly random, then U could have been any letter at all. Every possible message of that length is equally likely. There's nothing to crack.



**Corn**

Unless the shift number gets reused.



**Herman**

That's the Venona story, and it's the cautionary tale. In nineteen forty-two the Soviet pad factory shipped a large number of duplicate pages. The figure I've seen is around thirty-five thousand, probably wartime pressure on production. An Army cryptanalyst, Richard Hallock, noticed the reuse. Over the following decades roughly twenty-two hundred messages were read, some of them years after they were sent. The nineteen forty-four traffic was the most exposed, with about half of it recovered.



**Corn**

Half. From a system that is mathematically unbreakable.



**Herman**

It stayed unbreakable. Nobody broke it. They exploited a factory error, which is the mathematically precise way to say the lock was fine and the door was open. Claude Shannon proved it in nineteen forty-nine. For perfect secrecy the key has to be random, at least as long as the message, secret, and never used twice. Miss one and you don't get a weaker pad. You get a different cipher.



**Corn**

Every condition on that list is something a human has to do on a Tuesday afternoon.



**Herman**

Would you trust yourself with it, Corn? You'd be the one generating dice rolls for a month, and I've watched you decide a lunch order.



**Corn**

I'd get through about four pages and declare them random enough.



**Herman**

That's the real cause of most pad failures. Not the math. Tedium.



**Corn**

Then the humans are the part that's broken, as usual.



**Herman**

Now, the numbers stations are the other half of the old picture. A shortwave transmitter reads out groups of digits to nobody in particular. Anyone can listen, and only the agent holding the matching pad can read it. It's one-way and it's anonymous, because the receiver never transmits anything.



**Corn**

That tedium is why I never made it as a spy. Is there a documented case of someone actually receiving one of those broadcasts?



**Herman**

Ana Montes, the Defense Intelligence Agency analyst arrested in two thousand and one. She received orders from Cuba on shortwave, messages of around a hundred and fifty five-digit groups. And here's the twist I love. She didn't decrypt them with a paper pad. She used a laptop and diskettes supplied by the Cuban service. A software pad.



**Corn**

Which sounds like progress and was, I assume, a mistake.



**Herman**

A paper pad you burn, and then the key is gone. A diskette leaves traces. When the FBI copied her hard drive, they could recover plaintext that was supposed to have vanished. People who studied the case point out the Cubans digitised the pad and lost the one property paper gave them for free.



**Corn**

They upgraded it into evidence.

L

### Larry

Tired of random numbers that stay random only until somebody asks where they came from? Introducing the Burn After Reading Box, the monthly subscription that delivers a fresh, hand-shaken bundle of unbreakable digits to your door, in a plain brown envelope with a bonus decoy envelope that's also brown! Choose your tier. Bronze Chaos gives you one hundred digits that are only mostly random. Silver Entropy gives you five hundred digits and a certificate that says the word truly. And our top tier, Platinum Cosmic, delivers digits personally selected from the background hum of the universe by a man in a lighthouse. Every digit is guaranteed for single use, and so is your cancellation form! To cancel, simply write your request on a page of your own pad, deliver it by hand to our lighthouse between the hours of three and three-oh-four in the morning, and then watch it burn, because we do not accept copies, and we do not accept refunds, and we do not accept that you were ever a member. The Burn After Reading Box. Your secrets, subscribed.



### Herman

I have that subscription, actually. It's left me unable to throw away any paper with a number on it. The recycling takes me four days.



### Corn

Anyway. SIGSALY.



### Herman

Yes. This is the first place the digital lineage is genuinely, documented-ly there. July nineteen forty-three, the first call between Washington and London. It was a voice scrambler, and the key was noise. They recorded the noise from mercury-vapor rectifier tubes onto phonograph records. About twelve minutes of key per record, two turntables at each terminal, one playing while the other was cued. Each terminal was forty racks of equipment, over fifty tons.



### Corn

Fifty tons, to keep a conversation private. I've been in meetings that weighed more and said less.



**Herman**

Before the delivery, one detail. The noise wasn't the voice. The speech was digitised into coarse levels, and the noise record was added to those levels, so the sound that crossed the Atlantic was hiss. Anyone intercepting it heard weather.



**Corn**

A transatlantic phone call that sounded like a kettle.



**Herman**

A kettle with a key. The point is the delivery. The records were pressed in very small numbers, sources disagree on whether it was a pair or three per segment, and then the masters were destroyed. You shipped a record to London, you shipped the matching one to Washington, and each side played its copy once. After that it was scrap. That is a pad that happens to be made of vinyl.



**Corn**

And the next stop is the telephone that wasn't a telephone.



**Herman**

The Moscow to Washington hotline. Signed in Geneva in June nineteen sixty-three, live by the end of August. People assume it's a red phone. It was a teletype. The messages were encrypted with a one-time pad on a Norwegian-built machine, the ETCRRM II, and each country made its own key tapes, five-hole punched tape, and sent them to the other through its embassy abroad.



**Corn**

Why a pad at all? Why not just agree on a good cipher?



**Herman**

Because that would have meant swapping cipher designs, and neither side wanted the other to see how it encrypted anything. A pad needs no secret method. Mathematically it's the same for everybody. All the secret is in the key you hand over, and each side only needs to trust the tape it made itself. I'll say plainly that I haven't seen the embassy courier procedure described in detail anywhere I'd trust. The embassy part is what's reported.



**Corn**

Two superpowers who agree on nothing, agreeing that the only thing safe to mail each other is random punched tape.



**Herman**

The teletype circuits were cut in nineteen eighty-eight. Fax had been added two years before.



**Corn**

Okay, so what carried it forward? That's what Daniel's actually asking. If a government wanted a pad today, who sells it?



**Herman**

There's one company with a documented line of them, an Austrian firm called Mils Electronic. Founded in nineteen forty-seven as Reichert Elektronik in Trier, moved to Mils in the sixties. They made random key generators and mixers. The M E six hundred could output punched tape, floppy disks, paper for hand pads, even memory cards. The M E eight hundred wrote to floppy or EPROM chips. The idea was always the same, two copies of the key medium exist, each is used once, each is destroyed.



**Corn**

And Mils is...



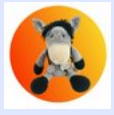
**Herman**

Restructured in July twenty-seventeen. Dissolved in twenty-eighteen.



**Corn**

Seventy-one years. The company outlasted most of its customers' secrets.



**Herman**

I couldn't confirm any current government product that uses a physical pad as key media. There's a patent for a self-erasing physical key that I've seen mentioned, but I have no sign it's a product. If someone out there still does it, it isn't marketed. I'd rather say that than hand you a nice story about a vault somewhere.



**Corn**

Then what's the stuff everyone does carry around? Because I assume there are soldiers with a key in a little box.



**Herman**

There are, and this is the distinction that matters for Daniel's question. The US system is called EKMS, and now KMI. At the bottom of it you have a fill device, first the DTD, the Data Transfer Device, which holds on the order of a thousand keys, keeps an audit trail, and encrypts the keys at rest. Its successor is the Simple Key Loader. A person carries it to a radio, plugs it in, and loads the key.



**Corn**

Couriered key. Separate road. Used offline. Sounds like a pad.



**Herman**

It's the same logistics and a different mathematics. What gets loaded into the radio is a short key for a symmetric cipher, something like AES, a few hundred bits. The radio stretches it, with an algorithm, across gigabytes of traffic. Its security is computational. It's secure because nobody knows how to break the algorithm in practice. A pad's security



### Herman (continued)

is informational. A pad is secure because the ciphertext simply doesn't contain enough to recover the message, no matter how much computing you throw at it.



### Corn

So the loader is the pad's grandchild by way of the courier, and a cousin by way of the math.



### Herman

Yes, that's the lineage and the break in one line. What survived was the delivery. What changed is how much key you carry. A pad is as long as everything you'll ever say. A fill is a few hundred bits that you stretch.



### Corn

Hm.



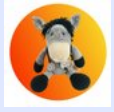
### Herman

Let me ask you something, Corn. If you were handed the pad for a whole year of messages, where would you keep it?



### Corn

In the one place nobody searches. My brother's sock drawer, which is a lawless region.



### Herman

Funny, and that's the actual answer people gave. Booklets in ballpoint pens, picture frames, walnuts, and a Stasi travel kit. The storage was always the weakest link.



**Corn**

I notice we still haven't reached a thing that's both digital and a real pad.



**Herman**

The nearest candidate people reach for is quantum key distribution. The second channel is physics, photons whose state can't be copied or read without disturbing them, and the receiver finds out about the disturbance. The most famous demonstration is the Chinese satellite Micius, in twenty-seventeen, which delivered key between a ground station in China and one in Austria, over seven thousand kilometres. Then came the video call between Beijing and Vienna, which a lot of coverage described as one-time pad encrypted.



**Corn**

I was about to say that.



**Herman**

The call wasn't a pad. It was AES with a one hundred twenty-eight bit key, and the quantum key was used to reseed that key every second. Seventy-five minutes of video, about two gigabytes, and it consumed only around seventy kilobytes of quantum key in total. The true pad, XOR and all, was used on two small pictures, about five kilobytes each, out of a hundred-kilobyte key batch.



**Corn**

So the satellite got to say the words one-time pad and used them on two thumbnails.



**Herman**

Which is still genuine, and the demonstration is real. The key distribution works. But the satellite itself was a trusted relay. It held both halves, so in principle whoever controlled it saw the key. And the ground network, the Beijing to Shanghai backbone, over two thousand kilometres, has about thirty trusted nodes along the way, each holding the key in the clear for a moment.



**Corn**

A secure channel where thirty-odd boxes in a row have to be honest.



**Herman**

NSA doesn't buy it. Their published position is that they don't recommend QKD for national security systems unless its limitations are overcome. The list is specific. It gives no source authentication, so you need either public key cryptography or preplaced secret keys to prove who's on the other end. It needs special hardware and dedicated fibre or line-of-sight links. Trusted relays add cost and insider risk. And its security is described as implementation-dependent rather than assured by the laws of physics. They recommend post-quantum algorithms instead.



**Corn**

The preplaced key is my favourite bit. The quantum pad needs an old-fashioned pad to prove it's talking to the right person.



**Herman**

It does, in a small way. Hmm, though I should narrow that. The authentication key can be short and reusable, so it's not a full pad. But the principle's the same, a secret that had to arrive by another road before anything started.



**Corn**

Which brings me to air gaps, because Daniel mentioned them. Machines with no internet. I suspect they're not as gapped as the brochure says.



**Herman**

Two separate things. First, the defensive hardware. A data diode is a one-way link enforced in the physical layer, typically a fibre with a transmitter on one side and only a receiver on the other. Data can go in. Nothing can go back. A real diode can't do acknowledgements, so the commercial versions add software on each end to fake the conversation.



**Corn**

A numbers station is a data diode made of radio.



**Herman**

It is, and it's nice because the sender can't even know whether you got the message. But the other half is the bad news. Stuxnet crossed the gap at Natanz on a USB stick, through a flaw in how Windows displayed shortcut files. How the stick physically got in is reported both ways, an insider or a dropped drive, and I wouldn't claim to know which. And a researcher at Ben-Gurion University, Mordechai Guri, has spent years showing air-gapped machines leaking out by other means. Fan noise. The blink of the disk light. Heat. Even the SATA cable acting as a radio antenna at around six gigahertz.



**Corn**

So the cable that carries the data is also a broadcast tower.



**Herman**

And a one-way delivery of a pad on a drive is the same thing as sneakernet. The pad only has to cross the gap once. But that means the gap has to be clean at that moment, and the thing carrying it in is the weakest part.



**Corn**

What Daniel flagged is bothering me. Decrypts exactly once. The word once. Who enforces it? When the Cubans put the pad on diskettes, the once was just a promise.



**Herman**

Right now it's a policy. Zeroisation, burning the page, destroying the second tape, a fill device wiping a key after use. These are procedures. A person or a circuit does them and you trust it. Nothing about the key itself prevents a second reading.



**Corn**

And you'd want a key that can't be read twice.



**Herman**

That's theory, and I want to mark it as theory. In two thousand eight Shafi Goldwasser, Yael Kalai and Guy Rothblum described what they called one-time programs. A program that runs on one input, once, and then can't run again. Software alone can't do it, because software can always be copied. So they proposed a tiny hardware token, a one-time memory, that holds two secrets and hands over exactly one of them, then destroys itself. As far as I know the token has never been built. Matthew Green wrote as much in twenty-twenty-two. And the quantum angle is the no-cloning idea, that a quantum state can't be copied, which would make once a law of physics rather than a rule of the office. That's a research direction, not something you can buy.



**Corn**

So the burning is still a person with a lighter.



**Herman**

Yes, a person with a lighter, or a zeroise button which is the same person in electronic form.



**Corn**

Then why isn't everyone using these? Mathematically perfect, delivered by courier. And I'm the sloth, so I'll be the one who says the word unbreakable makes me twitchy.



**Herman**

Fair twitch. Three reasons. One, the key must be as long as all the traffic you'll ever send. Not a hundred bits, as long as everything. Two, key distribution is the entire problem. Every pad you use has to be moved safely, which is exactly the problem you wanted to avoid. Three, and this is the one people forget, a pad gives you secrecy and no integrity.



**Corn**

Meaning?



**Herman**

Say an attacker knows you send a payment instruction, and knows the amount sits at a certain position. They can't read it. But with XOR, flipping a bit in the ciphertext flips that same bit in the plaintext. So they change the amount from one hundred to nine hundred without the key. The message decrypts perfectly. It's just a different message.



**Corn**

Perfect secrecy, zero tamper detection. A safe with a glass back.



**Herman**

The fix is a one-time authentication code, Wegman and Carter, nineteen seventy-nine. You compute a short tag from the message with a hash, then encrypt the tag with fresh key bits so the attacker can't forge it. It's information-theoretically secure, so it fits the pad. But it spends more key. The pad now has to cover the message and the tag.



**Corn**

So unbreakable means confidentiality only, and only if everyone behaved.



**Herman**

And that's why the consumer apps with a one-time pad in the name bother me. If the key comes from a password, or from a random number generator that expands a short seed, that's a stream cipher. It may be a fine one. It isn't a pad, because the key is shorter than the message by construction. The word is borrowed for its reputation.



**Corn**

How do you actually tell? Ask a normal person to check.



### Herman

Ask how long the key is next to the message, and how it reached the other person. If the answer is a short phrase, or a download, it isn't a pad.



### Corn

Under all of it there's still a person who says they burned the page. Who checks that?



### Hilbert

Nobody, and in Mrs. Okonkwo-Lund's case that was the first thing she asked me to do. Philippa Okonkwo-Lund, flat above the key cutter on the corner. She wants a receipt, so each evening I hand her the ash in a tin of Danish butter biscuits, the blue one, forty-one shekels. She is leaving her husband Barnaby the budgerigar. Barnaby is in a care home. The bird is called Councillor.



### Herman

Does the pad travel separately from the message?



### Hilbert

Gerald carries the message. Gerald is a man on a bicycle with a bell. I carry the pad, by a different road, on foot. We are not allowed on the same side of the street. Gerald's mother walks on the pavement behind him so nobody follows Gerald. She is eighty-one and has been followed by nobody for three weeks, and she has taken it badly.



### Herman

That is the correct design, a separate road for each. The hotline did it the same way.



### Hilbert

You're right about all of it, Herman. Pad by me, message by Gerald, one use, burn it. You said modular nine times, by the way, I got it down to six. Barnaby does the sum by hand. One digit a day, he is ninety-four. I turn the pages for him with my snout, because the claws tear them, and it leaves a mark. The message is fourteen letters. It comes to



**Hilbert (continued)**

nineteen days.



**Corn**

She changed her mind about the bird.



**Hilbert**

Three times. Gerald has delivered three messages. The second one says the budgerigar goes to the council. Barnaby is only partway through the first, and the pages already burned, so he cannot tell which page belonged to which message. He is working from the biscuit tin.



**Herman**

Position in the pad matters there. Each message has to start where the last one ended. If he slips one place, everything after it decrypts to garbage, and there's no going back because the used key is gone.



**Corn**

So if Barnaby misreads one digit on day four, the bird goes to the council by accident, and nobody can prove it wasn't intended.



**Hilbert**

Day five. Otherwise yes.



**Corn**

Nineteen days to carry fourteen letters, and the sum was never the slow part. That's the modern lineage too. Mils, the hotline, the loader, the photon link. The math was finished in nineteen forty-nine, and everything since has been logistics, moving the pad by a different road than the message.



**Herman**

Whether anyone builds a token that makes "once" a property instead of a promise is the thing I'd watch. Thanks to our producer, Hilbert Flumingtop, for keeping all of this sounding like it was recorded on purpose.



**Corn**

This has been My Weird Prompts. You can find every episode at my weird prompts dot com.



**Herman**

We'll be back soon.