

Why not the best?

Adapting OTP for the Enterprise

Traditional barriers to adapting the only known perfect cipher are melting – and with conventional cryptographic solutions displaying new and ominous vulnerabilities, the breakthrough could not be better timed.



THEON
TECHNOLOGY

Scott Bledsoe, Chief Executive Officer
Brian Anderson, Chief Marketing Officer
Joseph Mulvihill, Senior Technical Business Analyst
Theon Technology

Abstract

Information security hinges on effective cryptography deployable economically and at scale, but conventional cryptographic methods are increasingly threatened by malevolent deciphering, advances in higher mathematics, and quantum computing. Some widely adopted ciphers in place for decades, representing a heretofore mostly adequate level of “computational security,” are now vulnerable or will be imminently. The most formidable and secure class of cipher, the one-time pad or OTP, leverages a single-use high-quality key plus a reversible algorithm to encrypt cleartext data into ciphertext. Though acclaimed as uniquely uncrackable, OTP is often dismissed as an enterprise

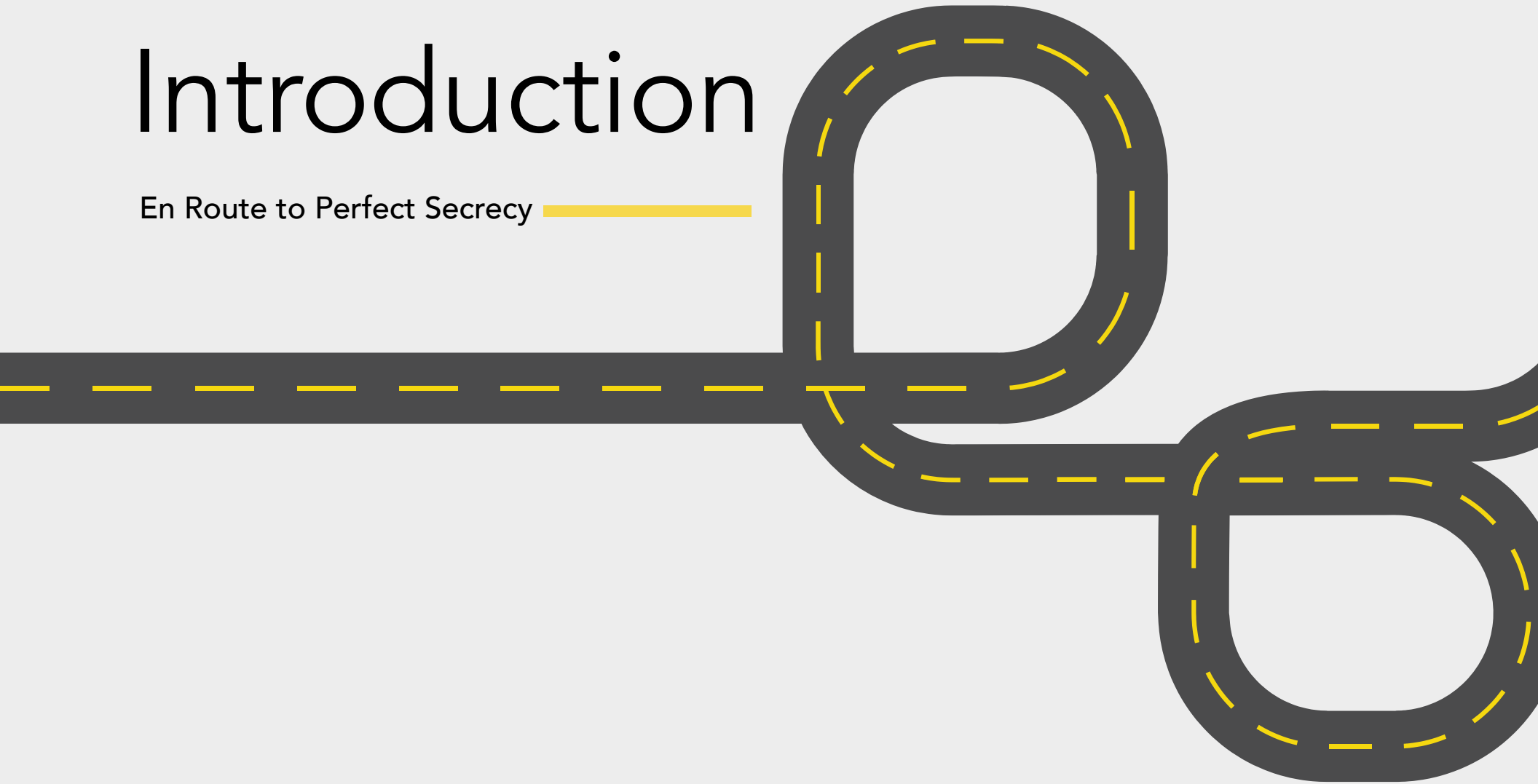
security option due to implementation challenges, primarily the requirement that the OTP key be of a size equal to the data it’s securing. Theon solves the challenge of distributing large cryptographic keys over distance with a breakthrough based on transmission of compact data parcels, “shared short secrets,” that enable secure reconstitution of keys and decryption of ciphertext. Key attributes of the only cipher ever deemed “perfect” is now practical for enterprise adoption. Tapping many inherent advantages of OTP while eliminating the biggest obstacle to adoption is a momentous step toward perfect secrecy – arriving at a propitious time.


CONTENTS

Introduction	4
P is for Pad, as in Paper	8
Forget One-Time Passwords, Remember OTP	11
The Four OTP Pillars	13
Outrunning Deprecation	16
The Unique Needs of Enterprise Environments	20
The Theon Solution	22
Conclusion	26

Introduction

En Route to Perfect Secrecy 





Here's a shot of conventional wisdom regarding cryptography. The most formidable and desirable digital security cipher – an encryption technique with roots going back hundreds of years; a technique proven impregnable by the celebrated “father of the information age,” Claude Shannon¹ – cannot be applied usefully at scale in enterprise environments. At a moment in history when the world needs the very best cryptography it can get, standard thinking says a modern business with modern demands must settle for something less. Still good, mind you, serviceable, but suboptimal. The best is out of reach.

Then again, conventional wisdom has a way of persisting and persuading until something arrives to sweep it aside. In the middle of the 20th century the president of IBM famously predicted, “I think there’s a world market for maybe five computers.”² American auto executives once proclaimed only a few eccentric customers would want quirky, tinny little foreign cars. Sometimes conventional wisdom begs to be nullified.

Here we are to do the job. This brief, friendly discussion will make you a fast-track expert on the iconic


cryptographic tool in question – a tool misunderstood by many. It is the so-called Holy Grail of secret-keeping techniques: the one-time pad, or OTP for short.

**The essential need-to-know
about an OTP cipher: it means
higher-quality cryptography.**

Information security in the digital era revolves around effective cryptography. The essential need-to-know about an OTP cipher: it means higher-quality cryptography.

Cryptography depends on secure marriages between sturdy, go-to algorithms used for encrypting data and secret keys. The algorithms are widely employed, so the keys must carry a lot of water – more so as demand soars.

Today there are too many weak keys in the wild – that is to say, at work in real-world environments. No resource on earth is more valuable now than data, the “new



oil,” but the pace of security upgrades frequently lags spiking urgency and data-volume curves. Some old ciphers get deciphered. Some don’t scale well. Even when keys are proven inadequate and taken off the market, they can linger on mission-critical duty. One recently marketed series of keys, products of older software but offered in 2020, was cracked “instantly” in 2022 by German researcher Hanno Bock – not with a quantum computer, but using the factorization method developed by Pierre de Fermat in ... 1643. Indeed: A nearly 400-year-old decoding tool consigned a modern cryptographic key to the trash bin.³

How many similarly weak keys are in use right now, lending a literal sense of false security? It’s impossible to estimate. But with more shortcomings exposed in last-generation cryptography as time passes, it’s fair to conclude our digital infrastructure faces a yawning risk-management crisis.

Now more than ever, with virtually all our most important secrets stored on computer networks while cyber pirates lurk and probe and phish, it matters how you generate your cryptographic keys. At the very

least, you want a large, complex alphanumeric string that is used once and only once, then disposed of.

Volume requirements have led to reliance on random number generators, or RNGs, to issue keys by the boatload. Inventive some RNGs may be – hardware-based ones might reference the unpredictable on-off behavior of local fans, or human user mouse movements – but they can also be problematic. Exert enough computing force examining the apparently random number strings RNGs produce, and buried patterns can emerge. Those keys can be vulnerable, all the more so with the emergence of quantum computing and the code-cracking threat it presents in the hands of malevolent players.

An OTP cipher is better. It leverages a single-use high-quality key plus a reversible algorithm to encrypt cleartext data into ciphertext. Come decryption time, the process runs backwards, decrypting the ciphertext back to the original cleartext.

So far as is known, when ciphertext is encrypted using a high-quality OTP key created under a few

fundamental, time-honored rules, it can't be cracked by brute force. The generalized quantum threat to cryptographic standards, however imminent or fierce, recedes here. Properly executed, OTP enables uncrackable encryption.

Yet for all its natural virtues, and despite looming threats to popular cryptography methods, OTP has not typically been adopted at scale. The single biggest obstacle: In conventional practice, the key must be of a size equal to the data it's securing. If you are keeping a 200mb secret, it means a 200mb OTP key. Yes, storage is cheap, but still; an enterprise might have millions of giant files worth protecting. And when you want to put that sensitive file in motion – transmit it from one locale to another – you typically must transmit the key as well.

It's been historically unwieldy. Imagine owning a suitcase-plus-lock that can hold 30 pounds of shirts and socks. Good news: your suitcase is invulnerable to break-ins. Your shirts are safe and secure. Bad news: the suitcase weighs as much as your clothes -- another 30 pounds. You're lugging a total of 60 pounds down

Concourse B. A lot of people would opt for a little less secure bag and travel a lot lighter.

No wonder conventional wisdom says OTP keys, the most formidable, most secure class of cryptographic key, can't be scaled in the manner enterprise environments require – even though the margin of protection they afford is sorely needed.

With old-school cryptography under pressure from new forces, not only quantum computing but advances in higher mathematics and more sophisticated kinds of cyberattack, a secure civilized world needs to bring its A game. Happily, though, as we said up front, conventional wisdom doesn't come with a lifetime guarantee.

Read on to see why it's expiring in this case – and how enterprise-wide security implementations inspired by OTP can absolutely, positively be viable.



P is for Pad, as in Paper

Like so many principles upheld in modern cryptography, OTP is rooted in predigital days. The P in OTP refers not to some hunk of computer hardware, a keypad or touchpad, but the literal pad of paper used by pencil-scratching keepers of secrets, encoders and decoders, decades before UNIVAC was a gleam in anyone's eye.

The idea of encrypting secrets utilizing alphabetic substitution – with a helpful key provided to an authorized decoder – goes back to 50 B.C. and Julius Caesar, who issued coded orders to his field generals that way. Fast-forward to the 1460s when the Italian Renaissance polymath Leon Battista Alberti went Caesar one better. He invented not only the polyalphabetic cipher but, in constructing a physical cipher disk he called *Formula*, machine encryption itself. Alberti went down as the founder of Western cryptography,⁴ though two subsequent cryptologists, Giovan Battista Bellaso and the French diplomat Blaise de Vigenère, improved on his work. Vigenère's complex cipher scrambled secret data, or plaintext, into ciphertext using 26 distinct cipher alphabets plus a key phrase. It endured for centuries.⁵

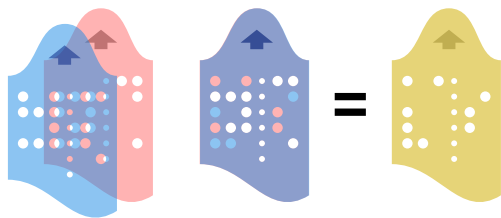
Confederate spies in the U.S. Civil War resorted to the Vigenère cipher, but they seem to have relied on only three key phrases to decode most messages: "Manchester Bluff," "Complete Victory," and "Come Retribution." Careless or not, the practice of using standard keys repeatedly proved costly – a point to remember. Union cryptographers quickly deciphered

the opposition's plaintext communications.⁶ Around the same period, English mathematician Charles Babbage cracked the Vigenère cipher by taking note of buried, repetitive patterns in the ciphertext⁷ – remember that point, too – and it fell out of use.

But it did not take long for inventive souls to address these newly exposed flaws in the Vigenère cipher. What if the key to decrypting ciphertext was not a constant, like "Come Retribution," but changed all the time? Perhaps with each use? And what if the key was not a meaningful phrase, reducing its effectiveness against good guessers, but random gibberish? Wouldn't that be more effective?

Credit for originating the one-time pad, the brilliant answer to those questions, is generally assigned to Gilbert Sandford Vernam, an AT&T Bell Labs engineer, and Joseph Mauborgne, a colleague and captain in the U.S. Army Signal Corps. In 1917 they co-developed a cipher that combined plaintext with a stream of random numbers of equal length. The one-time-use idea was Vernam's, the randomness idea was Mauborgne's, but their resulting brainstorm is known to this day as

the Vernam Cipher.⁸ (Some claim their thunder was stolen decades earlier, in 1882, by California banker and encryption enthusiast Frank Miller. Miller, laboring to secure telegraphic communication among banks, authored an ambitious codebook revolving around one-time use of random keys. In any event he finished out of the money, historic recognition-wise.⁹)



Vernam Cipher. Source: cryptomuseum.com

The modern OTP, was quickly leveraged, on multiple sides, as a vital weapon of 20th century espionage. (In World War II, had German intelligence used OTP keys to encrypt communications, the code behind the famous Enigma machine would in all likelihood remain uncracked by the Allies, and the outcome of the conflict might have been different.¹⁰) Single-use OTP keys were distributed on literal paper pads – the Soviet KGB waged the Cold War using pads so small, they fit inside a walnut¹¹ – or recited over shortwave radio “number stations” in spooky, emotionless voices

to field agents scribbling frantically by moonlight.¹²

In the digital age the paper pad is out of the picture, but the security advantages of an OTP cipher are more relevant than ever. And while in analog days the physical transfer of key data to a decryption point was the only way to make the OTP cipher work, a new technology era offers new opportunities. We can rethink OTP and ways to leverage its natural advantages digitally – without diluting them.

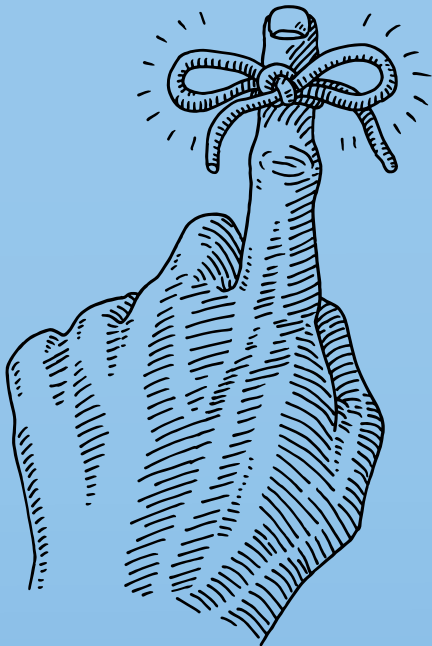
How do we generate an OTP-class key today that is deeply complex and entirely devoid of buried patterns, therefore a step ahead of regular RNG-produced keys? And when we’re protecting data in motion using OTP principles, we know the protocol requires identical keys, as large as the size of the protected file itself, to exist at the originating and receiving ends – the points of encryption and decryption. But how do we plant it in both locations?



It takes a little more than a shortwave-band numbers station.

Forget One-Time Passwords,

502745



Remember OTP

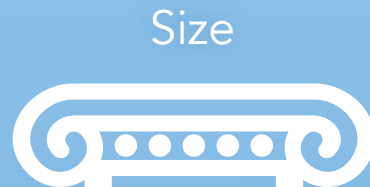
A brief pause here to knock down a common misconception. Type “OTP” into a search engine, and chances are the results will be front-loaded with chatter about one-time passwords. You probably have experience using one-time passwords, also known as two-factor or multi-factor authentication (2FA or MFA). You want to view your credit card statement? The provider texts a one-time, fast-expiring numerical code to your mobile phone.

One-time passwords have vulnerabilities OTP keys don’t share. Those short-lived numerical codes aren’t even encrypted. They’re simple and compact, usually five or six digits, whereas OTP ciphertext is very long and complex. They can be compromised by device or wireless network security flaws, malware infections, or interception bots that trick their targets into surrendering tokens. Because they’re relatively simple to implement, new rollouts of one-time passwords keep coming despite all these problems. (They project the *idea* of security, anyway.)

But the alarms are legion. NIST, the government-run National Institute of Standards and Technology advised organizations back in 2016 to wean themselves away from SMS-centric two-factor authentication.

Many people, and even some widely distributed technical literature, confuse these simple, flawed one-time passwords with the OTP that inspires leading-edge cryptography. Don’t. All OTP keys have in common with one-time passwords is that they authorize access to sensitive data. Familiarity with one-time passwords shouldn’t provoke qualms about OTPs. Store them mentally in separate folders.

The Four OTP Pillars



Claude Shannon, inventor of information theory, proved mathematically in 1945 that when an OTP key displays four critical, defining attributes, the related encrypted ciphertext is uncrackable – even when an adversary applies unlimited, brute-force computing power to the task.¹³ This, said Shannon (who, like Gilbert Vernam and Joseph Mauborgne, worked for Bell Labs), was the way to perfect secrecy.

Those four critical attributes are:

- 1 Genuine, intrinsic **randomness** – that is, the OTP key contains no discernible repeating patterns.
- 2 A key **size** at least equal to that of the plaintext it's protecting. Each byte of plaintext is encrypted by combining it with a corresponding byte from the equal-sized OTP key. (This is a giant upgrade in complexity and effectiveness from the antecedent examples like the Vigenère cipher, with its mere 26 cipher alphabets.) Shannon stipulated

that there must be as many possible keys as there are possible ciphertexts; therefore, the key material must be comprised of as many bytes as the ciphertext.¹⁴

- 3 **Uniqueness.** The OTP key is used just one time, to encrypt one item of data, though it may be used multiple times to decrypt it. (Imagine a user wanting to read the same email attachment multiple times.) The key is never recycled to encrypt some other file. If you were to recycle an OTP key to encrypt multiple portions of plaintext, you could cross-analyze the two ciphertext files and, via triangulation, reveal the key. So, no two-time pads.

- 4 Finally, if perhaps obviously: the key must be kept **secret**. Like any encryption cipher.

Tick all four boxes, said Shannon, and the resulting ciphertext is impossible to decrypt or break. He made that assertion back when Truman was president, but it endures today. What is more, no competing encryption technique has yet proven the equal of OTP.

Yet meeting all Shannon's requirements for perfect secrecy is harder than it sounds. Fall even a little short, and security may suddenly be a lot less perfect. As was noted earlier, it is difficult to generate truly random numbers; RNG outputs sometimes conceal embedded clues that, if surfaced, can enable unwanted deciphering. Having to generate keys as big as the files they're securing means obvious scalability and practicality challenges. Whether the data is in transit or at rest, you have to manage twice the volume of data. Transmitting big OTP keys from one place to another poses risk in itself – no network is immune to hacks and breaches – and discarded keys may be vulnerable to forensic recovery.

All these factors have in the past combined to discourage widespread, broad-scale adaptation of OTP principles at the enterprise level. With cybersecurity decision makers perpetually balancing the safety of their data against economic pressures and entreaties from budgeteers to do more with less, a practical argument gained favor: Perfect security is a stretch that doesn't cost out. It's actually okay to settle for pretty good.

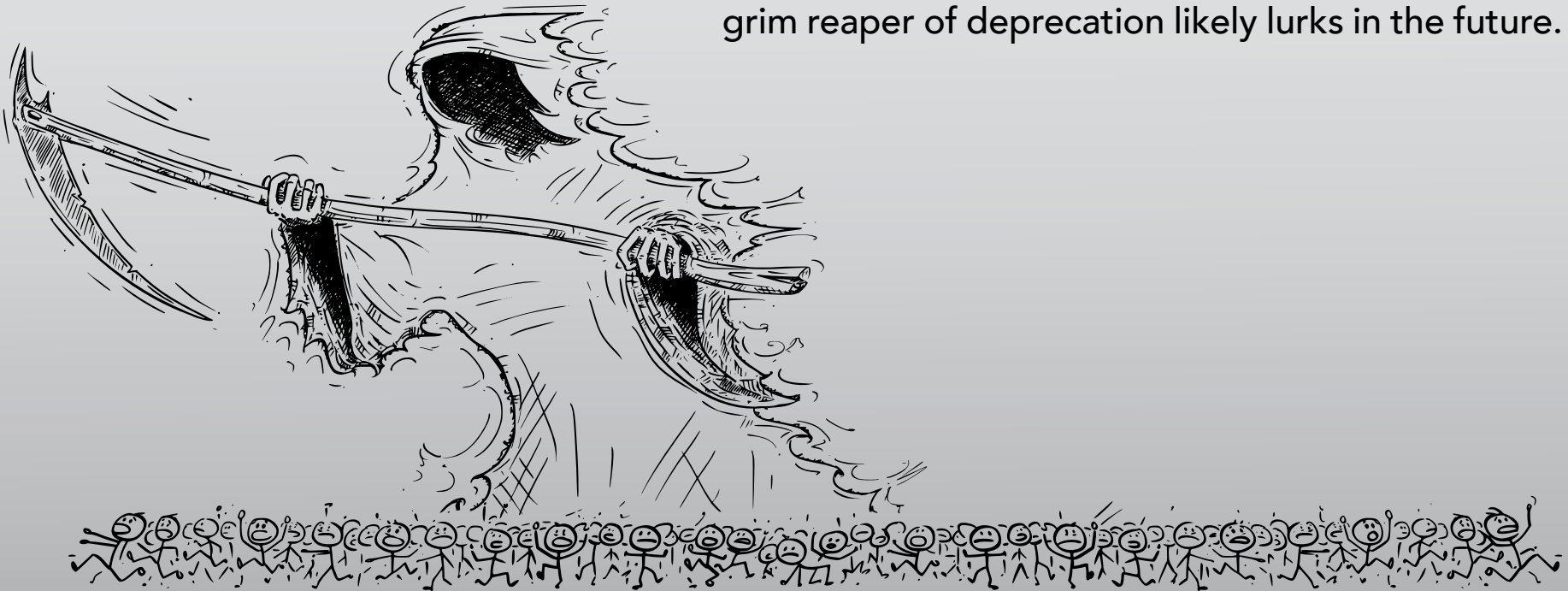
Backed by gee-whiz stats designed to make pretty good seem good enough to risk managers, the concept took hold of an imperfect but acceptable level of "computational security." Scientists Timothy J. Shimeall and Jonathan M. Spring, both of Carnegie Mellon University, wrote in 2013:

"Perfect secrecy is impractical to implement. There are enough potential operational difficulties that provide the adversary an attack vector that the defender's effort is often better spent on something besides the one-time pad key management problems. Therefore, modern cryptography suffices with what is called computational security... [A]s long as the cipher is well designed, the adversary must try all the keys – actually, half the keys on average – to break the encryption. For a random 256-bit key, this would currently take all the computing resources of the world running for more time than the universe has existed so far. This is generally considered sufficient."¹⁵

In the 2020s, however, a lot of conventional wisdom is suddenly up for review.

Outrunning Deprecation

When a once-effective cryptographic key solution loses its edge and is packed off to the metaphorical attic, it's said to have been deprecated. Usually, it's not that the solution deteriorates organically; it's that the threat landscape changes, growing fiercer. Adversarial computational power and higher-math theory get more powerful and complex; most cryptographic keys do not. For solutions born to deliver pretty good "computational security," the grim reaper of deprecation likely lurks in the future.



The prospect of quantum computing power in malevolent hands raises the stakes.

Security mavens place mordant bets about when “Q-day” will arrive, that is, the day a quantum computer deciphers once-serviceable keys, upends all security assumptions, and effectively breaks the internet. “If they reach their full scale, quantum computers would crack current encryption algorithms exponentially faster than even the best non-quantum machines can,” warned the journal *Nature* in early 2022.¹⁶

Putting quantum disruption aside for a second, though, routine advances in conventional, “classical” computing have exposed vulnerabilities in one key protocol after another.

Widely deployed asymmetric public key exchange algorithms, known generally as PKI (public key infrastructure), employ one public key and one private key linked by a mathematical algorithm. PKI has kept global internet transactions going since the 1990s. All sorts of everyday digital connections rely on public key encryption. The best-known example is probably RSA, conceived in 1977 but now considered past its sell-by date – deprecated! – in part because its keys are generated using prime numbers.

“Because algorithms like RSA rely heavily on the fact that normal computers can’t find prime factors quickly, they have remained secure for years,” said Lane Wagner, founder of Qvault.io. “With quantum computers breaking that assumption, then it may be time to find new standards.”¹⁷

Although quantum capabilities are not yet commonly deployed, RSA and other flavors of asymmetric key encryption, such as ECC (elliptic-curve cryptography) and its cousin ECDH (elliptic-curve Diffie-Helman), have already proven vulnerable to breakage by other means. We’ve long known that RSA keys produced using prime numbers that are too close together are susceptible to exposure via Pierre de Fermat’s factorization method – Fermat, remember, being Hacker of the Year back in 1643.¹⁸ But here come quantum computers to raise the risk factor. Mathematician Peter Shor (yet *another* Bell Labs guy) showed in 1994 that a quantum computer should be able to factor large numbers into primes at a comparatively blistering pace. Shor’s algorithm proving as much, and Lov Grover’s database-search quantum algorithm (1996),¹⁹ thereby wrote an effective epitaph

for RSA and its ilk – even though, in the ‘90s, practical quantum power remained a white-board idea.

DES (the Data Encryption Algorithm), like RSA a product of the 1970s, was a fine example in its day of the other main type of encryption solution, the symmetric approach – so called because it uses one private key at both ends of the encryption-decryption routine. DES was only a 64-bit algorithm, however – mighty when conceived, but less so as years passed and ultimately deprecated. Some upgraded to Triple DES, featuring three 56-bit keys, which became a cornerstone of the electronic payments industry, but in the 2010s deprecation came for 3DES too.

Much of the world migrated to another symmetric protocol, AES (Advanced Encryption Standard). AES was adopted as a U.S. government security standard in 2002.²⁰ AES, particularly AES-256 with more bits comprising a fixed-block-sized cipher key, is thought to be at least quantum-resistant. AES-256 is considered at least potentially viable post-quantum, because no quantum attacks have been discovered since its publication in 1998.²¹

Good, but something short of absolutely, positively “uncrackable,” Claude Shannon’s exclusive designation for OTP. For nearly half a century almost all cryptographic key protocols have landed with fanfare, enjoyed a season of adequacy, but then slid toward obsolescence. The cycle is plain: What was once thought impressively secure ends up deprecated and unloved.

The exception is OTP. In contrast to conventional encryption, OTP is seen as immune even to brute-force attacks. The typically large OTP key sizes dwarf 64-bit or 256-bit keys. Unfortunately, this strategic advantage is simultaneously a pragmatic obstacle to high-volume enterprise deployment of OTP or OTP-inspired cryptography.

To inoculate against the quantum challenge, you want a next-generation symmetric encryption solution that packages key superior qualities of OTP, the undisputed optimal cryptographic cipher, but solves for those giant-key drawbacks. Such an advance would move enterprise environments a big step closer to perfect secrecy.

The Unique Needs of Enterprise Environments

It's not only quantum computing and demolition-bent algorithms undermining time-honored cryptography solutions. Look also at exponential growth and complexity of enterprise environments navigating digital transformation.



The digital files that require protection grow bigger and more complex all the time – and the total global volume of sensitive digital information is expanding exponentially. Not very long ago, in 2010, the world created, copied, captured, or consumed 2 zettabytes (10^{21}) of digital material. In 2021: 79 zettabytes. The prediction for 2025: 181 zettabytes.²² The entire volume of digital data that existed globally in 2010 is today created anew in a single five-day workweek. An organization serious about cybersecurity in the 2020s needs to protect far more data, more vigorously, than ever before – which means reappraising old solutions. A washing machine installed in 2010 may make ominous thumping sounds in the spin cycle but probably still works. In all likelihood, a cryptography solution installed in an enterprise environment in 2010, sufficient in pragmatic terms at the time, is ominously ill-suited now. Quantum threats and that fierce deprecation schedule aside, modern data volume and workflow circumstances conspire against it.

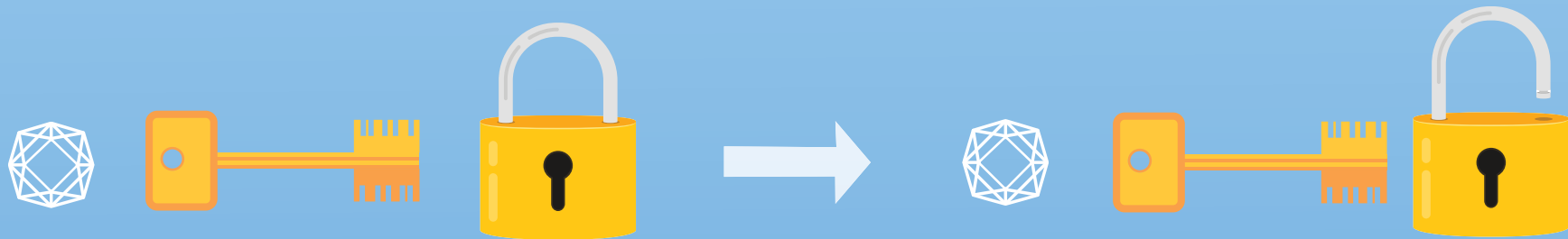
And beyond all *that*, real-world enterprise security practices in the real world often fall somewhere short of

best practices. It took a mighty, decade-long campaign – and a high-profile parade of breaches and failures – to get cybersecurity elevated from a nuisance for the I.T. boiler room to a boardroom priority. But even now enterprise SOC's (security operations centers) are short-staffed; security software may be procured in a blind panic and deployed haphazardly or not at all; cryptographic keys are reused or stored, cheek by jowl, up against the material they're securing. A high-value next-generation encryption solution has to be more secure, truly quantum-resistant, and built to anticipate future data volumes and system complexity. But it should also help protect organizations from themselves.

So the quest for better cryptography for the enterprise is no fashion statement, or Pavlovian response to the Gartner hype cycle. It's not hype-driven; it's propelled by real, structural needs.

The Theon Solution

The future of cryptography starts with shared short secrets.



The Theon methodology for generating symmetric keys means not having to transmit entire, large-size OTP keys from one locale to another. Solving the challenge of distributing a big key in a symmetric private-key situation retires the biggest single barrier to enterprise deployment of OTP-inspired cryptography. Consequently, Theon adapts key aspects of the one-time pad encryption technique, the only technique ever deemed “perfect,” and for the first time makes them practical for enterprise adoption.

A pair of shared short secrets, relatively small parcels of data, is used at each end of the transaction to generate large, identical keys independently. The shared secret is not the key; in a way, it’s the key to the key. Theon utilizes industry-leading methods for securely exchanging these well-protected short secrets. Authorized parties at both ends of a data-sharing transaction then use the data to reconstitute the key via a Theon-patented method.

This OTP-inspired solution surpasses the AES series of symmetric encryption protocols, even AES-256, in important ways. AES jams its cipher key into a fixed

block of bits: 256 bits for AES256. An OTP key is of a size equal to the ciphertext it protects. 10MB file? 10MB key. Key size varies every time. And this methodology leaves earlier symmetric ciphers like DES, 3DES, and AES in the dust. In fact, it leaves the whole idea of good-enough computational security in the dust.

In the introduction we compared OTP to a theftproof suitcase-plus-lock that holds 30 pounds of clothes – but the suitcase itself weighs 30 pounds too, making the total 60-pound package a chore to haul through the airport. Think of the Theon solution as the equivalent of checking your bag – with the assurance of reclaiming it, using your unique claim check, on the carousel at the other end.

It’s important, also, to underline the quality of the numbers used in the Theon solution to generate these very large, complex, OTP-sized keys.

We have noted the vulnerabilities, however well-concealed they sometimes are, in polyalphanumeric keys generated in high volumes by random number generators, or RNGs. Cryptographic protocols that

rely on these numbers have been proven vulnerable to brute-force computing attacks – that is, where the adversary computer basically tries every key on the keychain, then every key in the building, then every key it can think of until a prize is unlocked. When keys are the product of prime numbers, it creates additional exposure; Shor's algorithm is hard evidence of that. So – and this is how we started this whole discussion – key quality matters, now more than ever.

Theon generates a secret, irrational, high-entropy number that cannot be factored, then leverages its non-repeating, non-terminating mantissa – the series of numerals to the right of the decimal point. The mantissa becomes the key – a very lengthy and complicated numerical sequence, with a starting digit determined by a special secret offset.

So that's the encryption end of things. When encrypted data is sent from one authorized set of eyes to another, that's where the short shared secret comes in. The authorized recipient leverages that data parcel and uses it to reconstitute the key, thereby reversing the

encryption process in mirror fashion and decrypting the file.

It's not possible to work backwards from a shared secret and decipher the mantissa playing the role of the OTP-sized key. Sure, if you know the irrational number involved, its mantissa swims into focus – but you don't. Just as with AES-256 and other last-generation approaches to cryptography, the key is secret. When you leverage an irrational number to generate the key as well as keep it secret, you're well on the way to a more successful model.

If you thought AES-256 was resistant to quantum brute-force attacks, sit down for this. With the Theon solution, there's no embedded, repeating pattern to hunt for. An adversary is reduced to pitching random guesses – and consider the vast size of OTP-style keys, always as big as the files they protect. Only knowing the key start to finish, first character to last, plus the special offset factor can lead to decryption. It's basically game over for quantum challenges.

Claude Shannon, founder of information theory, defined perfect secrecy as "the condition that observation of the signal by an eavesdropper does not provide any information about the secret message without any assumption on processing power and time."²³

A would-be thief can see the encrypted ciphertext go past and still have no clue what's in there. Shannon proved, mathematically, that this condition can only be attained if the secret encryption key is at least as large as the message itself.

This is that. Here are the key advantages of OTP, adapted and made practical for the enterprise. Suddenly there is a new best-in-class, forward-looking enterprise cryptography solution.

Conclusion

A new, superior generation of commercially viable cryptography is dawning, inspired by OTP. Theon is driving a paradigm shift that more than answers the escalating demands of enterprise security environments. It is hard to imagine today's complex digital world understood – or even dreamed of – by Alberti, Vigenère, Miller, Vernam, or Mauborgne, but this advance is entirely in their spirit.

Adapting the inherent advantages of the OTP model while eliminating the biggest obstacle to implementation is a momentous, fateful step on the road toward perfect secrecy.

Why not the best cybersecurity for the enterprise? Until now, conventional wisdom argued OTP-level security was too hard to implement. Fraught with operational difficulties, it saddled adopters with unwieldy key-management challenges. And besides, a pretty good level of “computational security,” a notch or two less shatterproof than OTP, was good enough. It always had been.

All that conventional wisdom is obsolete. The threat landscape has evolved, but now, so has the leading countermeasure. The best is now within reach.

Contact Theon Technology

info@theontechnology.com

Or visit

theontechnology.com

ENDNOTES

- 1 Tijmen van den Brink, Ralph Koning, Daniël Sánchez, and Maurits van der Schee, "One-Time Pad Crypto Systems," University of Amsterdam, 2006. <https://www.maurits.vdschee.nl/otp/>
- 2 John H. Lienhard, "Engines of Our Ingenuity No. 1059: Inventing the Computer," 1988-97, University of Houston College of Engineering. <https://www.uh.edu/engines/epi1059.htm>
- 3 Dan Goodin, "Researcher Uses 379-Year-Old Algorithm to Crack Crypto Keys Found in the Wild," Ars Technica, 14 March 2022. <https://arstechnica.com/information-technology/2022/03/researcher-uses-600-year-old-algorithm-to-crack-crypto-keys-found-in-the-wild/>
- 4 "Alberti's Cipher Disk," *People Behind Informatics* exhibition, University of Klagenfurt, Austria, 2003. <http://cs-exhibitions.uni-klu.ac.at/index.php?id=281>
- 5 "Le Chiffre Indéchiffrable," *People Behind Informatics* exhibition, University of Klagenfurt, Austria, 2003. <http://cs-exhibitions.uni-klu.ac.at/index.php?id=280>
- 6 Fred Cohen, "A Short History of Cryptography," *Introductory Information Protection*, 1987-89, 1995, All.net. <http://all.net/edu/curr/ip/Chap2-1.html>
- 7 Simon Singh, *The Black Chamber / Cracking the Vigenère Cipher*, simonsingh.net. https://www.simonsingh.net/The_Black_Chamber/crackingprinciple.html
- 8 "The Vernam Cipher," cryptomuseum.com. <https://www.cryptomuseum.com/crypto/vernam.htm>
- 9 Steven M. Bellovin, "Frank Miller: Inventor of the One-Time Pad," Department of Computer Science, Columbia University. <http://www.cs.columbia.edu/~CS4HS/talks/FrankMillerOneTimePad.pdf>
- 10 Anthony Thompson, "Writing the Next Chapter for the Historic One-Time Pad," CircleID.com, 5 May 2016. https://circleid.com/posts/20160504_writing_the_next_chapter_for_the_historic_one_time_pad

- 11 CipherMachinesandCryptology.com. <https://www.ciphermachinesandcryptology.com/pics/otpbooklet1.jpg>
- 12 Numbers Stations Research and Information Center,
<https://www.numbers-stations.com/articles/numbers-stations-listener-starter-guide/>
- 13 *Bell Labs Technical Journal*, 1949. Shannon's findings were classified and kept from public view for three years.
- 14 Timothy J. Shimeall and Jonathan M. Spring, *Introduction to Information Security: A Strategic-Based Approach*. Syngress, 2013.
<https://www.sciencedirect.com/book/9781597499699/introduction-to-information-security#book-info>
- 15 Ibid.
- 16 David Castelvecchi, "The Race to Save the Internet from Quantum Hackers," *Nature*, 8 February 2022.
<https://www.nature.com/articles/d41586-022-00339-5>
- 17 Lane Wagner, "Is AES-256 Quantum Resistant?" 10 September 2020.
<https://blog.boot.dev/cryptography/is-aes-256-quantum-resistant/>
- 18 Goodin, *Ars Technica*, 14 March 2022.
- 19 Wagner, "Is AES-256 Quantum Resistant?" 10 September 2020.
- 20 An accessible read on AES may be found here:
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- 21 "ONE TIME PAD (OTP)," Qrypt. https://docs.qrypt.com/data_at_rest/concepts/otp/
- 22 Arne Holst, *Volume of Data/information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2025*. Statista.com, 7 June 2021. <https://www.statista.com/statistics/871513/worldwide-data-created/>
- 23 Ertuğrul Güvenkaya, Jehad M. Hamamreh, and Hüseyin Arslan, "On Physical Layer Concepts and Metrics in Secure Signal Transmission," *Physical Communication*, 2017.
<https://www.sciencedirect.com/science/article/abs/pii/S1874490717300903>