THEON
TECHNOLOGY

Cryptography’s End

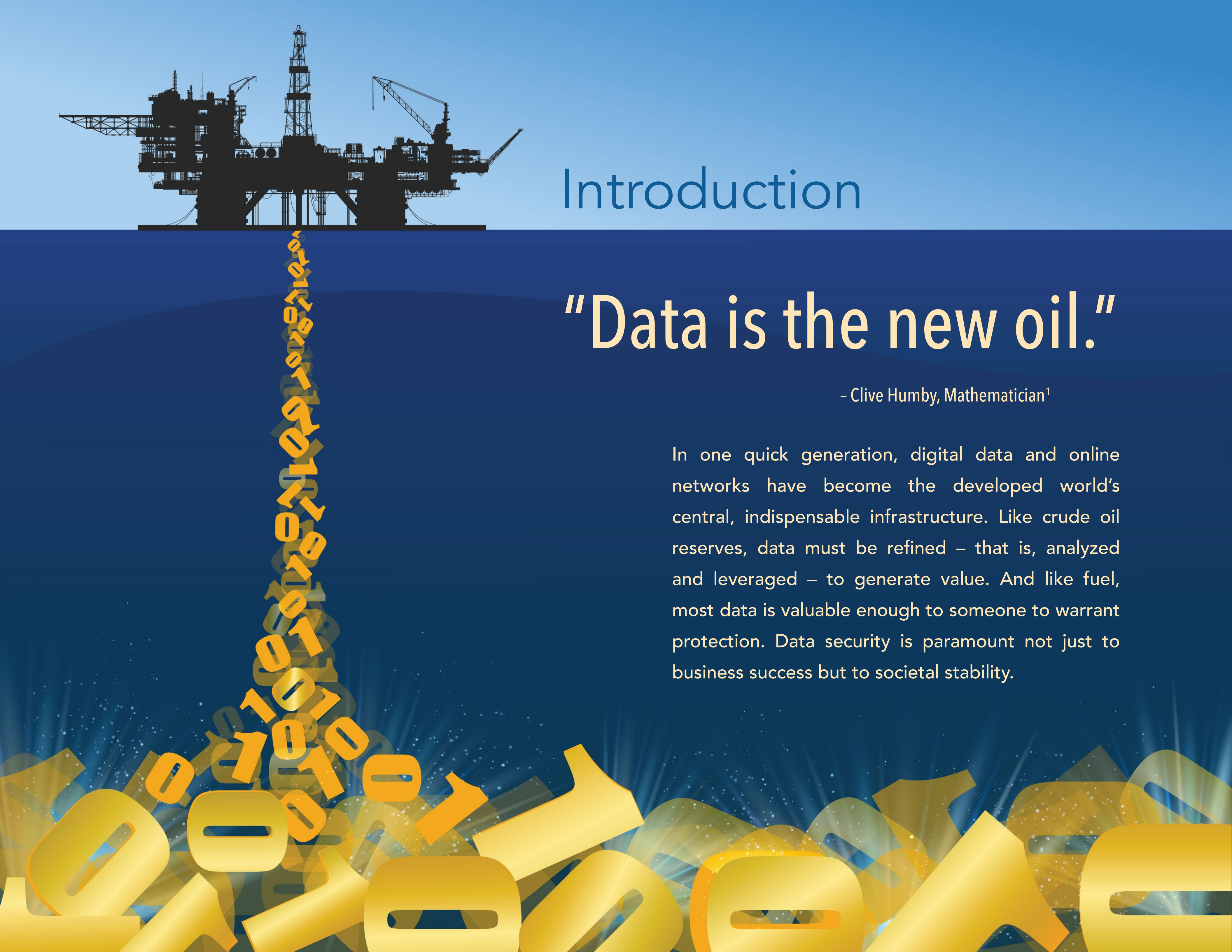
The technology behind keeping information secret is essential to human affairs. But in the digital era, a standard security paradigm with century-old roots is on its last legs, overwhelmed by advanced mathematics and mushrooming volumes of data. **Securing our future requires a sea change in our approach to cryptography.**

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

Abstract

Traditional cryptography, the art and science of securing data, has intellectual roots in the pre-digital era and is now proving inadequate. To achieve functionally adequate and economical data encryption, we have developed and clung to a default paradigm of common-use algorithms combined with complex public and private keys. But numerous factors suggest the old order's technological benchmarks are exhausted. These factors include the exponential expansion of data volume, steady advances in higher mathematics, and the emergent code-breaking potential of quantum computing. Ciphers revered as perpetually invulnerable should not be counted on to remain as such into the future; this threatens the foundations of digital security, therefore economic and societal stability. A new technological framework is required to securely generate cryptographic keys resistant to challenges from quantum computing in malicious hands. The quest continues for an encryption solution that addresses the limitations of status quo technology and can be deployed economically and efficiently at scale. Theon Technology offers an approach that mitigates the problems that have arisen as old protocols collided with new and daunting volumes of diverse sensitive information. It generates high-entropy, quantum-resistant keys at scale with speed and economy, setting a new standard for software-based cryptography and representing a decisive step toward the goals of quantum-proof encryption and perfect secrecy for businesses.

CONTENTS



Introduction

“Data is the new oil.”

– Clive Humby, Mathematician[1]

In one quick generation, digital data and online networks have become the developed world’s central, indispensable infrastructure. Like crude oil reserves, data must be refined – that is, analyzed and leveraged – to generate value. And like fuel, most data is valuable enough to someone to warrant protection. Data security is paramount not just to business success but to societal stability.

The data-oil analogy coined in 2016 by data scientist Clive Humby, who leveraged customer data to build a powerhouse loyalty program for Britain's Tesco supermarket chain, is echoed often enough to have become an article of faith in the world of information science: a kind of soothing mantra. Everyone nods. But the analogy goes only so far. Global crude oil reserves are in decline, requiring more inventive and costly extraction efforts. In contrast, global data volume expands at a dizzying geometric rate; information is increasingly easy to harvest and stockpile.

And while tactical security measures protecting oil tank farms and pipelines have not required much evolution, established data encryption techniques are increasingly vulnerable.

Digital information is disturbingly easy to steal. Severe cybersecurity breaches have become so frequent in this era, they are now practically expected, like the occasional freeway wreck: an irritating but tolerable cost-of-doing-business surtax levied by the modern digital world. But flawed prophylactic cybersecurity is not the crux of the problem, nor the focus of this discussion. The real issue is cryptography: the aging technologies we typically use as engines for encrypting and decrypting information.

Advances in mathematics, and to some extent the assistive factors of artificial intelligence, deep learning and deep neural networks, plus emergent quantum computing, threaten the aging foundations of status quo cryptography. Not to mention fateful choices made by managers and users alike as they weigh security priorities against the sirens of convenience and expediency. (Ajay Banga, the outgoing executive chairman of Mastercard, has said secure data can be as effective a wealth generator as oil: "[T]he prosperity that oil brought in the last 50 years, data will bring in the next 50, 100 years if you use it the right way." But he warns in the next breath that consumers prefer convenience over security.[2]) Add the likelihood of fiercer privacy regulations in the 2020s and a vivid case emerges for change.

Almost every aspect of daily life is evolving – has either become digital or grown more so – but not our basic intellectual approach to keeping secrets.

Effective cryptography is intrinsic to everything from buying a pizza with your smartphone to the security of nation-states. We are never as secure as we think, but particularly not at this crossroads of exploding data volume, clear and present threats to the old order, and a certain level of structural complacency. It is time for cryptography's end as we have known it. A paradigm shift is overdue.

But while cyber theorists tend to gloomy pronouncements, the outlook presented here is, ultimately, anything but pessimistic. New cryptographic technologies are imminent. They are poised to usher in a new era of far less vulnerable, far more economical information security.

The Two-Thousand-Year-Old Protocol

Cryptography, the art and science of securing data, is an ancient pursuit. Julius Caesar was a devotee.

Directing faraway military campaigns from Rome, Caesar did not trust the messengers who delivered instructions to his generals. Around 50 B.C. he devised an early encryption stratagem, the so-called "shift by 3" cipher described by Suetonius in a historical account, *The Twelve Caesars:*

> If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so, with the others.[3]

The Caesar Cipher was a straightforward monoalphabetic substitution cipher. Its efficacy depended on symmetric key tables employed at both ends of the messenger's run.

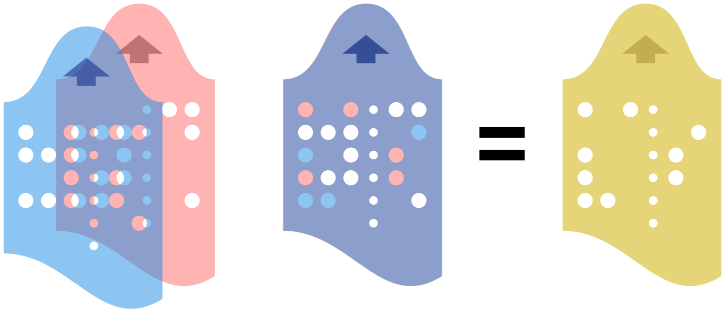
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

Caesar encrypted his orders using his table, and a loyal functionary in the battlefield decrypted them using an inverse table. To a breathless courier, the data looked like gibberish – useless to an enemy spy without the encryption and decryption keys.

There are basically two ways to keep a secret. One, hide the sensitive information where prying, unauthorized eyes won't find it. Two, render the secret unintelligible, so even if they find it, those eyes won't know what they're looking at. Cryptography is mostly about rendering data indecipherable to unauthorized eyes. It is remarkable how the basic approach of Caesar's shift cipher and other, similar tools persisted for millennia despite evident bugs. Data was only as secure as the encryption keys used; steal them, and you've not only acquired the data but broken the system. And with time, trial and error, a patient code-cracker could usually deduce the cipher's structure.

Fast forward two thousand years from Caesar's wars to World War I, and we find ciphers in use Caesar would have recognized. In 1917 Gilbert Sandford Vernam invented what came to be known as the Vernam Cipher, a sort of Caesar's Cipher on steroids. Vernam took sensitive data and overlaid it with an outwardly random series of polyalphabetic characters; his advance was used to encrypt military teletype messages.[4] As in ancient Rome, Vernam's encryption system depended on encryption and decryption keys at both ends of the transmission, though it was an order of magnitude more complicated.

It took a collaborator of Vernam's, U.S. Army Capt. Joseph Mauborgne, to elevate the Vernam Cipher to breakthrough status. Mauborgne reasoned that if Vernam's encryption and decryption keys were



Vernam Cipher. Source: cryptomuseum.com

impermanent – if they contained short-lived random elements, algorithmic keys that changed for every transmission – its cryptographic powers would be more substantial still.

Although they never used the term, Vernam and Mauborgne had invented a foundational cryptographic technology still in mainstream use in the 21st century, where it is regarded by many, inaccurately, as a modern advance: the one-time pad, or OTP.[5] OTPs also figure in today's dual-factor authentication (2FA) protocols. When a brokerage firm sends a one-time random digit series to your smartphone to enable authorized account access via your laptop, it is a sidelong homage to Vernam and Mauborgne. When an undercover intelligence agent in the field tunes a shortwave radio to an open frequency to transcribe lists of digits recited from points unknown, in the middle of the night, with eerie, mysterious solemnity – "numbers stations" remained a communications channel for spy agencies well into the digital era – that is more or less the same encryption idea at work. The data is decipherable to the recipient with the OTP key; to eavesdropping shortwave band surfers, it is merely spooky.

Conventional wisdom to this day enshrines the Vernam Cipher OTP as the only encryption algorithm with perfect security. Mathematician-inventor Claude Shannon, who aided the Allied effort in World War II with cryptography advances and later fathered the field of information theory, held that the Vernam OTP was unbreakable if the keys employed were "truly random, as large as the plaintext, never reused in whole or part, and ... kept secret."[6] Other, lesser cryptographic algorithms were viewed as computationally secure, but theoretically soluble given sufficient time and resources.[7]

But the theory of the Vernam Cipher's invulnerability was framed a long time ago, prior to the dawn of mainstream computing, and in the past few decades the digital world has changed beneath our feet.

Cryptography Meets One and Zeroes

Until late in the 20th century cryptography was primarily a national security concern, used for war, spycraft, and to protect state secrets. Business interests had extensive use for secrecy, but much less for keeping secrets on computers – the secret Coca-Cola formula could be, and was, rendered in plain English and stored in an Atlanta bank vault. To the public, computer secrecy was even more abstract and distant. Savings passbooks were pencil-and-paper affairs.

The democratization and socialization of computing starting in the 1970s, and parallel changes in communication methods, changed all that. As more sensitive information went digital, protecting it via cryptography gradually became a broad, egalitarian concern. Within a few decades the developed world grew dependent on the security of digital data.

But core cryptographic principles remained anchored in an earlier, pre-digital, comparatively slow-paced era. Some digital technology standards that serve as pillars of network security today offer disquieting echoes of the pillars of ancient Rome. They would certainly be familiar to Vernam, Mauborgne, and Shannon.

The syntax and architecture of digital information echo Julius Caesar's brainstorm for securing military secrets. Whether at rest, in use, or in transit from one location to another, all of it is stored as binary code: long strings of ones and zeroes. As in Caesar's day, when a sensitive piece of data warrants protection, it is scrambled into ciphertext using an encryption algorithm. An authorized user or program employs a decryption algorithm to access it. This standard

> "The only way to prove an algorithm is secure is by publicly disclosing it and letting really, really smart people beat on it for years. That's why, if you look at the algorithms we're using, they've been out there for 15, 20, 30 years."
>
> – Dr. Eric Cole
> Former CIA Cybersecurity Officer
> Author, *Cyber Crisis*

procedure protects data in transit in particular; data in motion has traditionally been regarded as exposed to the highest risk.

Because developing good encryption and decryption algorithms is so complex, it is not feasible to create a fresh one for each nugget of digital data requiring security – no more feasible than a high-volume manufacturer of door locks designing millions of unique physical mechanisms. Instead, digital cryptography does what door lock makers do: pair a standard algorithm with cryptographic keys. A cryptographic key is merely a companion string of numbers – theoretically random numbers – that, when applied, unlocks the mystery of a particular string of ones and zeroes, making ciphertext legible. When the same private key is used for both encryption and decryption, it's called a *symmetric* cryptographic method.

Decades after conception, modern digital cryptography still revolves around a marriage of algorithmic locks and mathematically complex numerical keys.

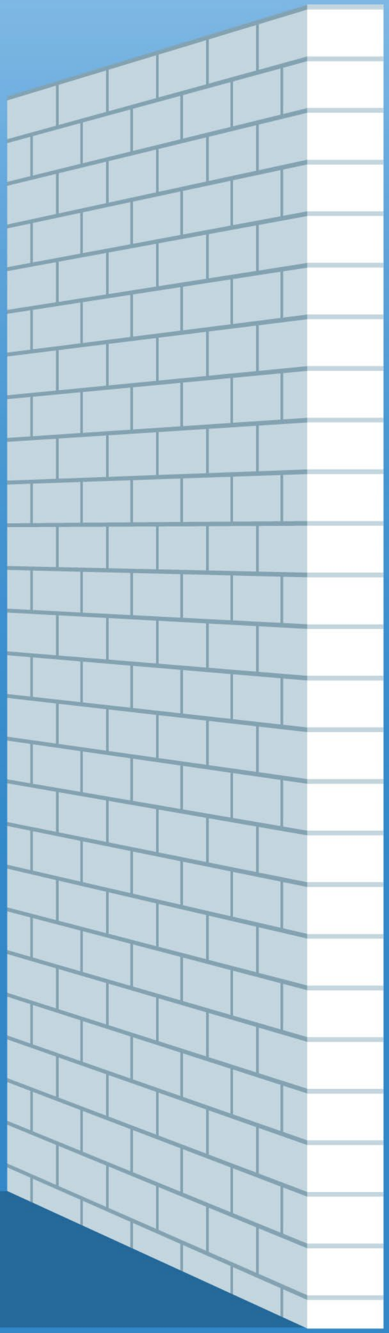
Within the established cryptography paradigm, there have been incremental advances to cope with both burgeoning volumes of data and the increasingly common practice of transmitting it from place to place. Probably the most notable is public key infrastructure (PKI), developed in the mid-1970s and generally attributed to Whitfield Diffie and Martin Hellman of Stanford University. (Some suggest the British intelligence services created PKI first, though they apparently did nothing with the breakthrough.[8]) With PKI there are two keys for encryption and decryption. One is public, for all the world to see, while the second remains private, married to the public one via a very complex mathematical algorithm – an approach that became known as *asymmetric* cryptography. This model enabled good security with what was generally seen as acceptable, manageable risk.

PKI today is indispensable. With the explosion of the consumer internet, which obviously put a good deal more sensitive data in motion, PKI became the foundation for the secure sockets layer (SSL) and transport layer security (TLS) approaches to web server and browser security. (PKI is also at work in digital signatures and document signing, digital identity authentication, and so on.) Common, name-brand algorithms used to generate public keys and keep internet activity moving with reasonable security include Rivest-Shamir-Adelman (RSA), Elliptic curve cryptography (ECC), and digital signature algorithm (DSA).[9] There is no need to unpack their technicalities in this discussion, but RSA *et al* are fixtures along the digital highway – the equivalent of Sunoco pumps and McDonald's on interstate road trips. If they were unavailable, you'd miss them.

In long-standing theory, these expressions of the standard cryptographic model deliver functionally adequate computational security. But in practice the vulnerabilities are numerous and growing more acute.

Hitting the Wall

Few aspects of human activity have failed to undergo an intrinsic, atomic-level paradigm shift in our lifetimes. Cryptography is among them.



Compared to our forebears a century ago, we grow, process, and preserve food today, manufacture industrial products, plan and manage our cities, and travel long distances in utterly different fashion. In all those cases the technologies and systems at work would be science fiction to a time traveler arrived from a century ago; imagine what a World War I biplane ace would make of a stealth fighter. Yet a reasonably adept mathematician or spy from the roaring Twenties would recognize familiar principles in today's cryptography. As we have said, the Vernam Cipher is alive and well in today's common-use OTPs.

Multiple factors suggest the old order, a standard benchmark in digital affairs for fifty years, is finally exhausted. Seven are especially pertinent to this discussion. Individually and in concert, these seven trends, developments, or facts of life make the case for the inevitable end of cryptography as we have long known it.

1 First, as the world discards analog data storage practices at scale and uploads everything, consider the exponential expansion of digital information volume. In 2010 the world created, copied, captured, or consumed two zettabytes (10^{21}) of digital data. Just eleven years later, in 2021, it was 79 zettabytes. The projected volume in 2025: 181 zettabytes.[10] Today, in one short week, we create, copy, or consume a new mountain of digital data equivalent to everything that existed in 2010. The security demands are staggering.

Ever-cheaper computing power and ever-faster digital networks reduce barriers to managing larger digital files; the days of waiting impatiently for downloads to complete are coming to a close. Yet old-school OTP solutions don't scale with the same elegance as servers and network performance; protecting a 100MB file requires an equal-sized 100MB cryptographic key.[11] And as those digital files grow larger and more complex, it becomes an ever-greater computational challenge to create keys of the required equal size. Greater resources are diverted to key generation.

2 Second, imposing volumes of data, combined with eternal pressures for economy and efficiency, often result in real-world security practices that fall somewhere short of best practices. As in ancient Rome, digital information is only as secure as its cryptographic keys. Decode or steal them, and you have stolen the data itself -- as surely as a pickpocket in a hotel lobby who steals your room-access keycard has in the same moment also stolen the laptop you left upstairs. In the realm of practical data management, we are not stamping out new encryption and decryption algorithms at a rate concurrent with expanding data volume, so we need more and more keys. Unfortunately, an oft-chosen alternative is to make greater, repeated use of a finite set of keys. Identical keys may knowingly be used to lock up large volumes of data; worse, those keys are often stored within easy reach of the sensitive information they protect, that is, on the same server. They are too easy to locate. It's like owning a car that can only be started via a sophisticated anti-theft keyfob with rolling codes, but leaving the fob taped to the windshield in a busy supermarket parking lot.

> "The problem with cryptography is, the secrecy of the cipher text is only as secure as the secrecy and robustness of the key. We want a unique key for every single message. We want it long; we want it robust. We want to store it in a separate location."
>
> – Dr. Eric Cole
> Former CIA Cybersecurity Officer
> Author, *Cyber Crisis*

3 Third, brilliant adversaries are out to get those keys. Cyber criminality has evolved into a highly professionalized, for-profit global industry. Sensitive data is under unprecedented siege, and the threat is not stoned hacker-gamers in dorm rooms. It comes from innovative, well-compensated black-hat players, perhaps working as proxies for nation-states pursuing industrial espionage or strategic cyber warfare, including attacks on critical infrastructure. Conventional wisdom used to hold that data in transit is at greater risk compared to data at rest or in use, but today's drumbeat of ruinous server breaches indicates there is little comfort in drawing that distinction. Data at rest is stolen all the time. Cybercrime is projected to exact a global toll of $6 trillion in 2021, with 15% per annum growth through 2025, to $10.5 trillion. If cybercrime were an economic nation-state, that growth curve would make it the third largest on earth, after the U.S. and China.[12]

4 The fourth challenge: mathematics marches on. Like computing capabilities, the state of mathematics is evolving rapidly, far beyond the state of the art when standard cryptographic models took hold. Strides in math enable concrete technological advances in one sector after another, from defense to pharmaceuticals to climate change, but virtuous scientists hold no monopoly on math advances, let alone security advocates. Anyone can play; benign advances can be leveraged in pernicious ways. Higher-level math makes the old pillars of cryptography look more precarious. Shor's algorithm, for example, discovered in the '90s by American mathematician Peter Shor, performs exponentially faster large-integer factoring. Standard cryptography, and therefore online security itself, assumes that factoring integers composed of more than one thousand numerals is for practical purposes impossible. Shor's algorithm suggests otherwise – at least, in combination with the fifth factor that threatens the cryptography status quo: quantum computing.[13]

Massive computing power, quantum-level power unimagined by 20th century information theorists, is ever more accessible – to malefactors as well as righteous data guardians. These increased capabilities pose an existential threat to the old order. A quantum computer of sufficient horsepower that runs Shor's algorithm might be capable of defeating public key infrastructure mainstays like RSA. That would be a traffic-stopper, as it were. Daniel L. Bernstein, computer scientist at the University of Illinois at Chicago, states:

> Assume that large quantum computers are built, and that they scale as smoothly as one could possibly hope. Shor's algorithm and its generalizations will then completely break RSA, DCA, ECDSA, and many other popular cryptographic systems; for example, a quantum computer will find an RSA user's secret key at essentially the same speed that the user can apply the key.[14]

5 There's an additional potential concern. Contemporary cryptographic keys – remember, they're merely simple, if ever-longer, strings of numerals – are routinely created using random number generators, or RNGs. But RNGs can be problematic. Computers operate empirically, executing the instructions they're given; they do not invent anything. Simulating genuine randomness has proven a surprisingly difficult computing task. Patternistic weaknesses may be buried deep within apparently random prime number strings produced by similar RNG "seeds." A quantum computer might make more straightforward work of revealing those patterns. Already, in one case involving (largely unregulated) cryptocurrency, a "blockchain bandit" made off with millions by guessing victims' weak private keys generated by RNGs.[15]

(In technical terms, randomness is *entropy*; you want all the entropy you can get. Some computer applications generate entropy by glomming onto local hardware inputs like fan operation or mouse movements. Even so, with quantum computing coming on strong, potentially offering a big break to cyber pirates out to break RNG-generated cryptographic keys, a more skeptical view of standard RNG solutions is justified.)

A 2021 World Economic Forum summary warned:

> When will quantum computing break cryptography? This is a question often asked but unfortunately a specious one, because it frames the threat to be in the future. For data that will require protecting for decades, the threat is today. The impact is in the future. Data considered securely protected today is already lost to a prospective quantum adversary if stolen or harvested now.
>
> All data – past, present, and future – that is not protected using quantum-safe security will be at risk. It threatens the digital infrastructure on which modern societies rely. All critical infrastructure, transactions and processes relying on cryptography that are not quantum-safe could be compromised, causing widespread disruption. As the quantum threat exists today, governments and business shouldn't delay action.[16]

At any rate, care should be taken not to assume that only plentiful, accessible quantum computing power will eventually threaten traditional encryption. New mathematical approaches to large-integer factoring will be perfected that do not depend on quantum horsepower. They will run on standard computers anyone can leverage. That threat may be even more alarming, but it is not yet adequately recognized in the mainstream.

6 Which brings us to the sixth way standard cryptography is hitting the wall: complacency.

At a Gartner IT symposium in late 2021, one key analyst dismissed the state of quantum computing as "embryonic at best," and one breakout session was titled, "The CIO's Strategy Guide to Navigating the Quantum Computing Hype." The advice to large enterprise organizations was to form small working groups of no more than five to eight people. Gartner analyst Chirag Dekate predicted any value to be delivered by quantum technology lay a minimum of ten years in the future. "Quantum is not a general-purpose technology and quantum computing cannot solve all known problems," he said.[17] But it can certainly become a generally *disruptive* technology and will likely be capable of *creating* known problems.

There is a natural human tendency, of course, to dismiss dangers that cannot be qualified as clear and present. Few expect their homes will be burgled until it happens to them. Despite regular security crises, everyday corporate complacency about prophylactic cybersecurity persists: as the 2010s ended, multiple credible surveys found most leaders felt their IT infrastructure was sufficiently protected,[18] even though a Ponemon study found 53% of IT practitioners didn't even know if their cybersecurity solutions were working.[19] And of course the cryptography industry itself has clung to an familiar, aging paradigm – assuring itself, and us, that a revered cipher of yore, considered unbreakable at birth, will be invulnerable in perpetuity. In this way defenders of the established order are like futurists of the early 20th century who could not foresee iPads or 747s, only larger, fiercer steam locomotives.

It is typical for such complacency in human affairs to be shattered only by catastrophe. It would be better if cryptography's state of the art were advanced via other, less jarring means.

7 The seventh and final way cryptography as we know it is hitting the wall is in the political and regulatory realm. The battle to balance digital security with privacy is a pivotal issue of the 2020s; there is debate at high levels of the U.S. government about reining in big technology firms, possibly by making

their proprietary algorithms subject to oversight and approval. Privacy initiatives like the European Union's GDPR (General Data Protection Regulation) present not only compliance hurdles but data sovereignty challenges, as sensitive data crosses international borders and falls subject to different secrecy and security rules in different jurisdictions.

More private citizens are wary of data abuse or misuse: 79% told a 2019 Pew Research Center study they were "not too" or "not at all" confident that companies will admit mistakes and take responsibility if they misuse or compromise personal information. 69% doubted firms would use their personal information in ways they would be comfortable with.[20]

These developments suggest that whatever security reforms occur in response to all the prior problems discussed will need to survive tumultuous critical scrutiny from a mosaic of overlapping political overseers. And of course, a security framework that does not inspire user confidence is no security solution at all.

The Next Wave is Building

Now for some good news. Traditional cryptography is vulnerable in the current digital era, its inherent flaws and limitations have put it on the road to inadequacy, but there are clear and heartening alternatives going forward. We have cause for optimism.

The best guarantor of societal security is a technological framework for securely generating cryptographic keys that are protected from unauthorized access or disclosure – and resistant to challenges from quantum computing in unauthorized hands, running powerful factoring algorithms that function as malicious pattern detectors and code-crackers.

The quest to achieve better encryption is not a brand new one. An older alternative protocol, 3DES (for "triple data encryption standard"), dates from 1998; it was a good-faith shot at improving on vintage PKI-founded algorithms for generating public keys, like RSA and DES. 3DES became a go-to solution in finance and payment scenarios including credit card transactions, but the digital realm has changed so utterly since the 1990s, 3DES is now rated weak and *en route* to retirement.[21]

Though it does not yet command center stage in the encryption arena, a cottage industry of so-called post-quantum cryptography solutions is at work today, supported and encouraged by NIST, the U.S. National Institute for Standards and Technology. NIST issues recommendations of stronger, more secure encryption algorithms and coordinates the establishment of post-quantum cryptographic standards.[22]

There are many approaches to choose from. Three in particular have drawn recent interest.

1 Homomorphic encryption (or FHE, for "fully homomorphic encryption") offers some promise – and far greater resistance to being blown open by quantum computing power. The core concept is to permit use and manipulation of data while it remains encrypted, concealing sensitive details from parties without a need to know. Like today's standard encryption protocols, the homomorphic approach uses a public key to encrypt data – but in the standard scenario a user must decrypt the information, or even download it to work on it locally. These transitions ramp up risk.

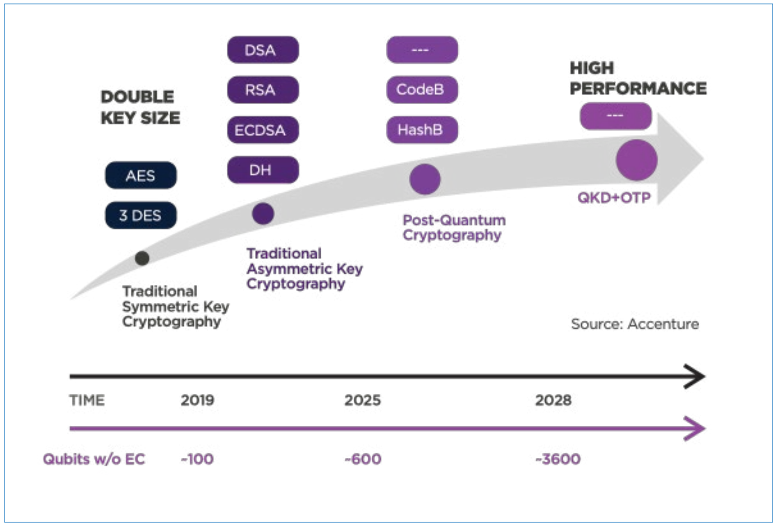
"Homomorphic encryption can be used to simplify this scenario considerably," says a consortium of businesses, government agencies, and academics dedicated to promoting standards for homomorphic encryption, "as the cloud can directly operate on the encrypted data, and return only the encrypted result to the owner of the data. More complex application scenarios can involve multiple parties with private data that a third party can operate on, and return the result to one or more of the participants to be decrypted."[23] The inherent challenge, as the consortium concedes, is a rash of competing schemes: "Homomorphic encryption is already ripe for mainstream use, but the current lack of standardization is making it difficult to start using it."[24]

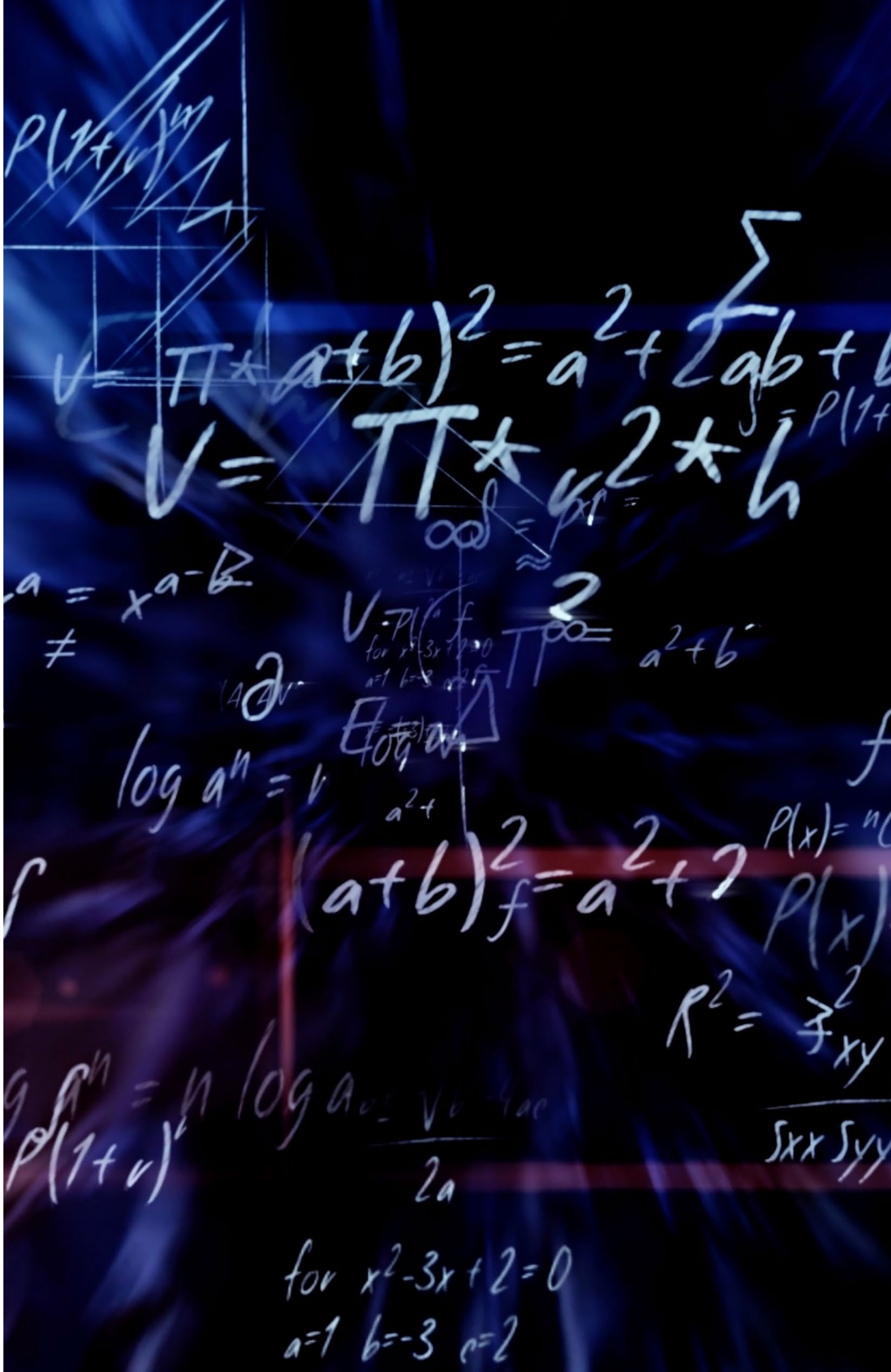
2 Polymorphic encryption represents a different approach: it departs from traditional methods by treating different data types in different ways. Conventional encryption-decryption processes remain the same whether they are applied to an email, a video, or the blueprints for the next Ford F-150; only the key lends an element of uniqueness. With the polymorphic approach the algorithm changes with every use – in response to the category of data it's keeping secure. One advantage of some expressions of polymorphic encryption is that data is subdivided into chunks, each with its own unique key. Enthusiasts of polymorphic encryption say this creates an advantage versus traditional encryption: multiple sets of ciphers and keys that can be processed in parallel, as opposed to a block of data encrypted with one key.

3 An intellectual cousin to polymorphism is quantum key distribution (QKD), wherein a unique quantum connection between two authenticated users creates a secure channel for data transmission. If an interloper attempts to intrude, the system senses the trespass and generates error messages. QKD is an intriguing initiative, but perhaps a costly one.

This is not a conclusive list of possible next-wave approaches to cryptography. In the derby to supersede conventional methods, other entrant technologies jockeying for critical mass and legitimacy include lattice-based, multivariate, and hash-based cryptography; supersingular elliptic curve isogeny cryptography; and symmetric quantum key resistance. The field is fragmented.

The quest continues for an encryption solution that overcomes the flaws of RNG-sourced number keys with perhaps suboptimal entropy; is effective across the gigantic, diverse, fast-expanding digital dataverse; resists current challenges from higher mathematics and eventual challenges from quantum computers; and can be deployed economically and efficiently at scale.





Where the Quest Leads

Theon Technology employs an advanced mathematical equation to propagate truly random, high-entropy cryptographic keys at scale leveraging proprietary software. A cryptographically secure random number generator (CSRNG) exploits the proven properties of large irrational numbers. The results from Archimedes, Theon's CSRNG, expose the security flaws that may be present in current RNGs – apparently random numbers that conceal predictable submerged patterns; those numbers' vulnerability to decoding algorithms – and render them comparatively obsolete.

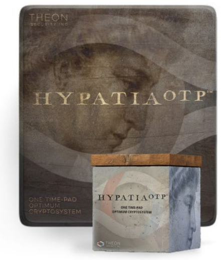
The Theon approach to next-generation cryptography mitigates the problems that have blossomed as old protocols collided with new and daunting volumes of diverse sensitive information. In typical security environments today, as we have said, a single key is used to encrypt a large volume of data, or the same key is used repeatedly to secure different data repositories; this practice, a consequence of managing large data volumes with limited resources, is a crucial enabler for attackers. Theon's **Archimedes** can generate keys at scale with speed and economy, discouraging this detrimental practice.

The high-entropy keys supplied by Archimedes anticipate the twin challenges of mathematical advances and quantum processing power and are designed to frustrate them. Theon represents a decisive step toward the goals of quantum-proof encryption and perfect secrecy for businesses.

The Theon cryptographic model is symmetric, leveraging a unique private key for both encryption and decryption – each unique item of encryption is encrypted with a different unique key. Paired with complementary third-party key management solutions, the Theon model also makes it easier to give up the expedient practice of storing decryption keys in proximity to the data they protect – the equivalent of leaving your keyfob taped to the hood of your parked car. Theon keys can easily be sequestered elsewhere. That is a high-value security feature in itself; most cyber attackers seek low-resistance targets.

Because Archimedes is software-based, the amount of computing hardware and processing power required to support key generation can be adjusted up or down as needed. Hardware-based RNGs require greater power and physical resources to generate more keys, and once that hardware is duly committed, it remains so. There is no ramping down. With Archimedes, far less hardware need be consigned to supporting effective cryptography.

OTPs – one-time pads – may have been born before digital computing, but they continue to represent an unbeatable cryptographic standard. Like cryptographic keys, however, OTP files can be large and unwieldly. Another Theon innovation, **Hypatia OTP**, reduces the bandwidth required to support OTP key transmission; a lower volume of data is managed and communicated, making it feasible to deploy OTPs for added security across more use cases.



Theon technology sets a new standard for software-based cryptography. It is an order of magnitude more secure than even the symmetric cryptographic models of the past. Yet it is a recognizable successor – far from alien to students of cryptography. As politicians and regulators embark on the fraught task of trying to reinforce both security and privacy while reinforcing data sovereignty, assessing and critiquing candidate technologies as they go, the Theon approach should prove welcome. Theon represents a paradigm shift without the risk that comes with embracing the unknown. Pressure on private concerns to reveal algorithmic secrets may in some security scenarios be less consequential, as the key ingredients in the cryptographic formula are the high volume of high-entropy keys sourced from Archimedes.

> "Theon solved a problem no one else could: revolutionize OTP, make it integratable, and make it work with clients, servers, and businesses in an easy, scalable manner."
>
> – Dr. Eric Cole
> Former CIA Cybersecurity Officer
> Author, *Cyber Crisis*

The Stakes

Society has cast its lot with digital infrastructure; there is no going back. Data is indeed the new oil; the world is finding alternatives to oil, but the safety and steady availability of sensitive information determines the fate of nations, businesses, and individuals alike. Anticipating threats and keeping digital data secure is therefore critical to geopolitical, economic, and cultural stability.

The World Economic Forum urges data curators to adopt a culture of "security agility" and pivot to advanced technology before malicious quantum computing reaches critical mass: an event estimated to occur as soon as mid-decade.[25]

The threats to the status quo discussed here, posed principally by advanced mathematics as well as maleficent quantum coders, are not yet emblazoned on mainstream magazine covers. But they will be. When the issue crystallizes in the public mind, imagine the stampede to a cryptographic model that is, demonstrably, an order of magnitude more secure. Traditional cryptography will never again inspire the faith it did in prior eras. The costs of security lapses are too great; the stakes are now too high.

Some dissidents call for reverting to pre-digital business practice – taking data offline, disconnecting computers. But such impulses are far less salutary and productive than fixing cryptography. Failure to evolve means digital decline; if digital security leaders do not innovate and inspire confidence, the breakdown in public trust already underway will only deepen, and bad digital actors will only be emboldened. All sensitive online transactions are powered by faith in the system. An increasingly skeptical digital culture is bad for business.

Cryptography that rewards user confidence, on the other hand, is undoubtedly good for business. A recent McKinsey & Company report observed, "As consumers become more careful about sharing data, and regulators step up privacy requirements, leading companies are learning that data protection and privacy can create a business advantage."[26] Today that market intelligence manifests primarily in the steady demand for cybersecurity software solutions: Estimates of the global cybersecurity market opportunity were recently revised upward by MarketsandMarkets, from $217.9 billion in 2021 to $345.4 billion in 2026 – a Compound Annual Growth Rate (CAGR) of 9.7%.[27] But that emphasis will change as more comprehend the merits of intrinsically more secure cryptographic advances.

There are, as we said at the outset, two ways to keep a secret: Hide it from prying, unauthorized eyes, or else render it unintelligible. The first is an eternal, uncertain game of cat-and-mouse, but we know how to do the second. More formidable, economical, trustworthy cryptography means better privacy, a renaissance in public confidence, and a more serene and productive future.

Once the old cryptographic order served us well, but its day has passed. A new day is dawning. The ranks of those who see what is happening, and where the digital world is destined to head, are growing every day.

Visit
theontechnology.com

ENDNOTES

1. Michael Palmer, “Data is the New Oil,” ANA Marketing Maestros blog, November 2006. https://ana.blogs.com/maestros/2006/11/data_is_the_new.html

2. David Reid, “Mastercard’s Boss Just Told a Saudi Audience That ‘Data is the New Oil,’” CNBC.com, 24 October 2017. https://www.cnbc.com/2017/10/24/mastercard-boss-just-said-data-is-the-new-oil.html

3. Suetonius, The Twelve Caesars, A.D. 121. https://crypto.interactive-maths.com/caesar-shift-cipher.html

4. Security Encyclopedia, “The Vernam Cipher,” hypr.com. https://www.hypr.com/vernam-cipher/

5. Security Encyclopedia, “The Vernam Cipher,” hypr.com. https://www.hypr.com/vernam-cipher/

6. Shannon, Claude, “Communication Theory of Secrecy Systems.” Bell System Technical Journal 28 (4): 656–715., 1949.

7. MrBrownCS, “Vernam Cipher (One-Time Pad),” YouTube, 8 October 2018. https://www.youtube.com/watch?v=cpqwp2H0SNo&t=2s

8. Network Associates, *An Introduction to Cryptography*, 1990-2000.

9. “Public Keys and Private Keys in Public Key Cryptography,” Sectigo.com, 9 June 2020. https://sectigo.com/resource-library/public-key-vs-private-key

10. 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/

11. Theon leadership interview, 7 September 2021.

12. Steve Morgan, “Cybercrime to Cost the World $10.5 Trillian Annually By 2025,” Cybercrime Magazine, 13 November 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

13. “Shor’s Algorithm,” IBM Quantum Composer documentation.
https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm

14. Daniel J. Bernstein, “Grover vs. McElice,” University of Illinois at Chicago, 2010.
http://cr.yp.to/codes/grovercode-20100303.pdf

15. Stephen O’Neal, “‘Blockchain Bandit’: How a Hacker Has Been Stealing Millions Worth of ETH by Guessing Weak Private Keys,” Cointelegraph, 28 April 2019.
https://cointelegraph.com/news/blockchain-bandit-how-a-hacker-has-been-stealing-millions-worth-of-eth-by-guessing-weak-private-keys

16. Catherine P. Foley, Jay Gambetta, Josyula R. Rao, and William Dixon, “Is Your Cybersecurity Ready to Take the Quantum Leap?” World Economic Forum, 7 May 2021.

17. Veronica Combs, “Quantum Reality Check: Gartner Expects 10 More Years of Hype, But CIOs Should Start Finding Use Cases Now,” TechRepublic.com, 20 October 2021.
https://www.techrepublic.com/article/quantum-reality-check-gartner-expects-more-10-years-of-hype-but-cios-should-start-finding-use-cases-now/?ftag=TRE684d531&bhid=22821436205701382229251796262431&mid=13555776&cid=713531816

18. George Leopold, “Survey: Cyber Complacency Growing,” EnterpriseAI.news, 13 September 2016.
https://www.enterpriseai.news/2016/09/13/survey-cyber-complacency-growing/

19. “Ponemon Study: 53 Percent of IT Security Leaders Don’t Know if Cybersecurity Tools are Working Despite an Average of $18.4 Million Annual Spend,” BusinessWire, 30 July 2019.
https://www.businesswire.com/news/home/20190730005215/en/Ponemon-Study-53-Percent-of-IT-Security-Leaders-Don%E2%80%99t-Know-if-Cybersecurity-Tools-are-Working-Despite-an-Average-of-18.4-Million-Annual-Spend

20. Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, Pew Research Center, “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,” 15 November 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

21. Jasmine Henry, “3DES is Officially Being Retired,” Cryptomathic.com, 3 August 2018. https://www.cryptomathic.com/news-events/blog/3des-is-officially-being-retired

22. “Understanding the Upcoming NIST Post-Quantum Cryptographic Standards,” PQShield white paper, 10 February 2021. https://pqshield.com/whitepapers/understanding-the-upcoming-nist-post-quantum-cryptography-standards/

23. “Homomorphic Encryption Standardization” Introduction,” HomomorphicEncryption.org. https://homomorphicencryption.org/introduction/

24. Ibid.

25. Phil Quade, CISO, Fortinet, “The Quantum Computer Revolution: Here Tomorrow, So We Must Prepare Today.” World Economic Forum, 22 April 2021.

26. Venky Anant, Lisa Donchak, James Kaplan, and Henning Soller, “The Consumer-Data Opportunity and the Privacy Imperative.” McKinsey & Company Insights, 27 April 2020. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

27. *Cybersecurity Market with Covid-19 Impact Analysis by Component (Software, Hardware, and Services), Software (IAM, Encryption, APT, Firewall), Security Type, Deployment Mode, Organization Size, Vertical, and Region - Global Forecast to 2026*, MarketsandMarkets, June 2021. https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html