Perfect Security…

Security is mostly a superstition. It does not exist in nature, nor do the children of men as a whole experience it. Avoiding danger is no safer in the long run than outright exposure. Life is either a daring adventure, or nothing.” – Helen Keller

Security via incomprehensible complexity, exists via groups which have fallen prey to groupthink, conformity, and irrationality when individuals suppress their independent judgment to align with the majority, the result is the "madness of crowd" or snake oil security that comes with no proof of security. This post aims to set the framework for perfect security for the first time in human history.

The problem with the world and security, is that the Intelligent people are full doubts, while stupid ones are full of confidence.

It should be noted that this post limits the scope to a digital world coupled with information security (INFOSEC), even though perfect security has a much wider scope including COMSEC, TRANSEC etc and more general CYBER security, and potentially physical security. One immediate pitfall is assuming a secure cipher means a secure system, one will note the proof of security provided in the references below apply to the entire INFOSEC solution not just the One Cipher.

Perfect security implementations demand the same rigor we apply to classical ciphers – constant-time code, masking, fault detection, careful code review and testing on real hardware. A theoretically information Theoretic Secure-secure cipher offers little comfort if a hacker can simply read your secrets via a timing leak or glitch your device to bypass its security. Solid engineering and diligence are mandatory to realize the promise of Information Theoretic Security (ITS).

In summary, the arrival of an Information Theoretic Secure cipher is a milestone to celebrate, but security professionals must approach perfect security adoption with eyes wide open. The ciphers alone won’t save a digital world unless they are implemented correctly and redesign systems around them.

The clock is ticking for data with long confidentiality requirements – think medical records, intellectual property, state secrets, critical infrastructure schematics, etc., that must remain secure across several decades. Every year that goes by without Information Theoretic Security increases the window of vulnerability for this long-lived data.

A key concept here is “secrecy lifetime” – how long the confidentiality of a given piece of data must last. You should categorize your data and systems by secrecy lifetime: if it’s more than a few years, that system should be high on your Information Theoretic Security transition list.

Organizations, especially in critical infrastructure and government, should treat the Information Theoretic Security migration as a present-day project, not a future contingency.

Perfect Security

- Definition: The highest possible level of security, where there is absolute zero statistical correlation between the encrypted message and the original plaintext.
- Unbreakable: An attacker has no advantage, and their probability of success is equivalent to pure guessing or a true random number, regardless of how much computing power, or time they have.
- INFOSEC: When perfect security is applied to information, the result is termed a perfect security solution (refer to appendix).

Axiom: Perfect security always comes with a 'verifiable proof' of its security, if no proof then its just another peddled snake oil-based security claim.

Security through obscurity works because it takes time to defeat obscurity. The effectiveness of encryption, for example, is measured in the amount of time it takes to break it, not that encryption is unbreakable. We inherently understand that the processing power of a computer in just a handful of years will be able to break in a few minutes what would take hundreds of years today.

In an era where the quantum threat is no longer a distant possibility but an impending reality, the concept of perfect secrecy emerges as a critical security standard. Perfect security is the highest level of security because it guarantees permanent security because it's unaffected by advances in mathematics or computing power.

Is there such a thing as perfect cybersecurity? Until now the answer has always been No…
But with the proven existence of Information Theoretic Security the answer is now YES!

$$C = M \oplus K$$ ← The ciphertext (C) is constructed by XOR-ing the message (M) with a random key (K)

$$p(M = m|C = c) = p(M = m)$$ ← The ciphertext provides no information about the message.

$$I(M;C) = H(M) - H(M|C) = 0$$ ← Equivalent: zero mutual information between the message and ciphertext

Axiom: Unit today Perfect security has been impossible in practice, due to implementation challenges with key management. The development and deployment

of the worlds first, and only, "Information-theoretic secured Key Management System', changes the world forever.

Perfect security represents the gold standard in cryptographic security. Grounded in Claude Shannon's pioneering work, perfect secrecy ensures that encryption remains invulnerable, even in the face of unlimited computational power. It is not just a defence mechanism but a potentially definitive solution—one that eliminates the need for continuous algorithmic updates and provides mathematically unassailable security.

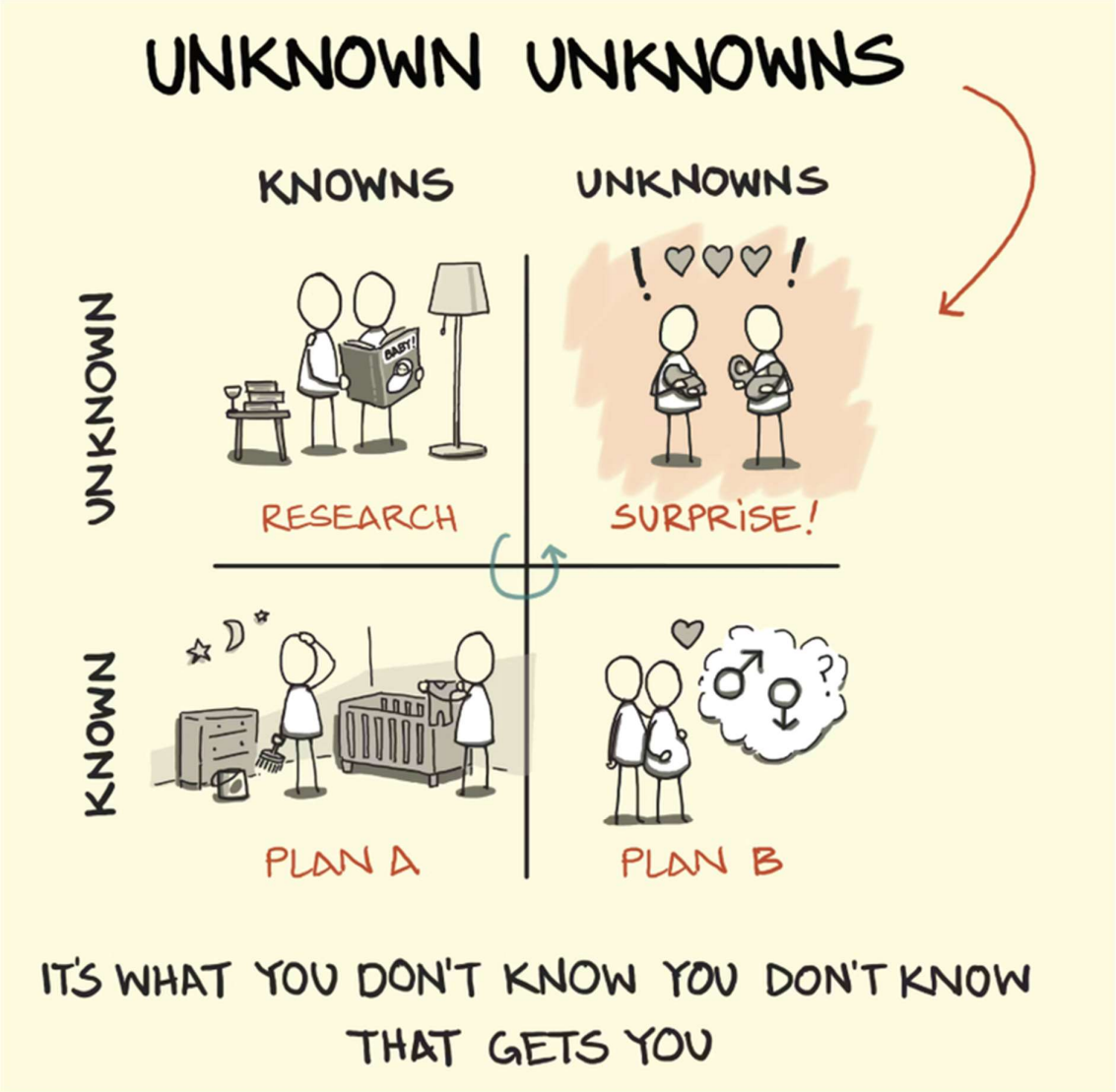
Kerckhoffs' Principle states that the security of a cryptosystem must lie in the choice of its keys only; everything else (including the algorithm itself) should be considered public knowledge.

Kerckhoffs' principle is a foundational design philosophy for classical and modern cryptography that enables information-theoretic security by ensuring that a system's security can be proven to be based on the strength of the key alone, making it resilient against analysis of the algorithm.

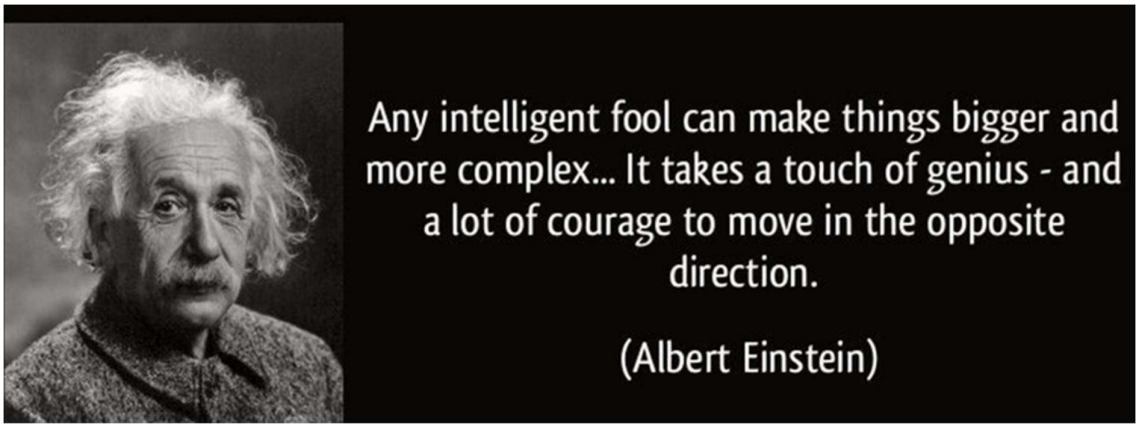
Axiom: Information-theoretic security, coupled with Kerckhoffs' Principle, means ciphers and algorithms self-deprecate to ensure the secrecy and sufficient entropy of the shared secret to prevent knowledge or guessing by a third party (attacker).

We face dangers every day, from stolen corporate and financial information to interference with the political processes that our countries rely upon. With the universal availability of Perfect Security for the first time in human history, humanity has an opportunity to become greater than who we are today.

Perfect security provides a level of security that is not dependent on the computational difficulty of breaking algorithms or understanding the world. unknown, unknowns. This approach resists future technological advancements, including those in quantum computing. For organizations concerned about long-term data protection, perfect security presents a solution that is designed to withstand the test of time.



There’s no shortage of studies and reports of cryptanalysis breaking the unbreakable, but there is no concept of any cryptanalysis attacks on perfect security, as Information-theoretic secured means a system's security is guaranteed by the principles of information theory and hence is proven secure against all posable attacks, even with unlimited computational power, resources and time, as long as the key remain secret..



One Cipher: to rule them all

"One cipher" refers to the Authenticated Encryption with Associated Data (AEAD) adaptation of the classic Vernan cipher[2] a theoretically unbreakable encryption method using a truly random key the same length as the message, used only once and then discarded, making it perfectly secure.

Its is called the one cipher as it represents a single, perfect, versatile, or universal cipher method that could handle all cryptographic security needs. It represents a humorous twist from J.R.R. Tolkien's famous line for the One Ring ("One Ring to rule them all, One Ring to find them...") from *The Lord of the Rings*, but with an absence of a secret back door.

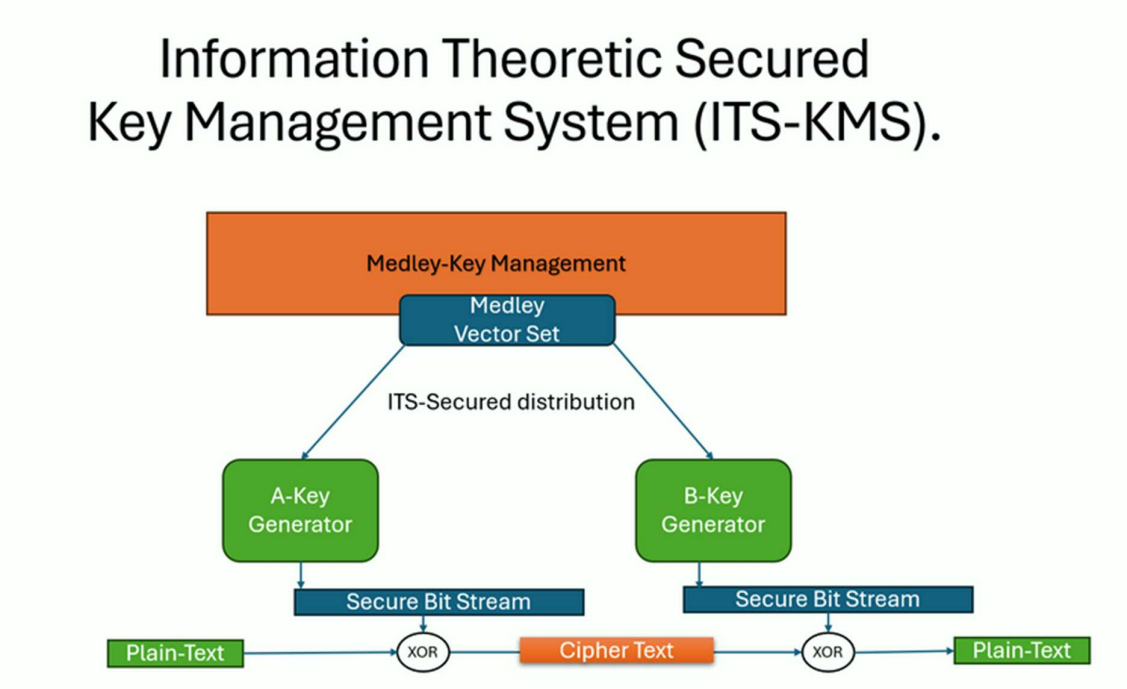
Axiom: The One Cipher makes all other ciphers obsolete, as anything more complicated then XOR just adds risk and complexity for no real benefit.

Given a chose between perfect security and insecure complexity, choose the proven, perfect security, via the One Cipher for all use cases today and though to the end of time.

The Solution...

The main problem with Vernam Ciphers (One-Time Pads) before the existence of an ITS-KMS is the extreme impracticality: you need a truly random key the exact same length as the message, which must be securely exchanged beforehand and then securely destroyed, making key management a logistical nightmare for large-scale communication, though the *theoretical* system offers perfect security if implemented perfectly. The availability if the ITS-KMS changes this for all time and makes the One cipher possible.

The One Cipher is just a part of the complete Information Theoretic Security solution; the key innovation is the ITS-KMS as shown below which makes the One Cipher the universal cipher for all time.



How it Works

1. The Medley ITS-KMS generate the medley vector set.
2. The Medley vector set is ITS securely distributed to each party A/B.
3. The end system use a Key Generator to generate a cryptographically secure bit stream or secret key stream. The key stream is set equal in length to the information object
4. The resulting ITS secured cipher text is transmitted via any media to party B.

Party B uses the medley vector set to regenerate the secret (cryptographically secure bit stream) and recover the plain text.

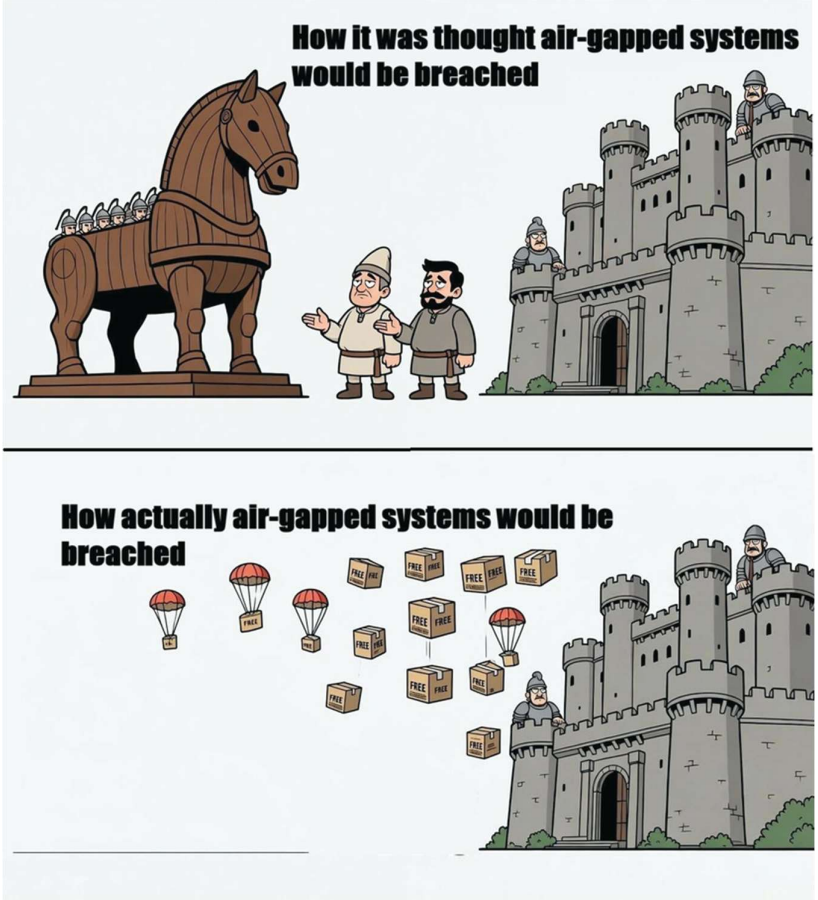
The snap below shows the ITS secured distribution to the two end points A/B Secure Identities:
A: 0199742c945df39f3755625147de290cc06d895f2830
B: 0199b2d2f90f5741f72cc0de4681c4a428367d5ea751

With the ITS encrypted Medley vector sets for each end point.
AKey:U1WjzfQmzVvrDarcPmMqPJL7G/qDiLZjVJD5XkTk6RUAWEEorttusnxNowbkwFCve
Ocxd1zgvrHZbZBkL/6YxwR/Nft6LmhrvbmIsg8Eq73JoxERsCT3DbUrzgO5gaCK|ID:0199b
2d2f90f5741f72cc0de4681c4a428367d5ea751
BKey:JjPywgWHfbwUnvNuKXCD3k2FxCbrVJuuQ5vsZn3W1yBFTCDxcpwjdBThbA4UTb0T
beZcNTXCpzGdXxB7UaGJd23No+RnmmEEZYFqvaHdLAn6sEh2s6Wm/nM8w2lIuHy+

```
  "Devices": "ID:0199742c945df39f3755625147de290cc06d895f2830, Key:U1Wj
zfQmzVvrDarcPmMqPJL7G/qDiLZjVJD5XkTk6RUAWEEorttusnxNowbkwFCveOcxd1zgvr
HZbZBkL/6YxwR/Nft6LmhrvbmIsg8Eq73JoxERsCT3DbUrzgO5gaCK|ID:0199b2d2f90f
5741f72cc0de4681c4a428367d5ea751, Key:JjPywgWHfbwUnvNuKXCD3k2FxCbrVJuu
Q5vsZn3W1yBFTCDxcpwjdBThbA4UTb0TbeZcNTXCpzGdXxB7UaGJd23No+RnmmEEZYFqva
HdLAn6sEh2s6Wm/nM8w2lIuHy+",
```


The entire system and all components are Information Threptic Secured and come with a proof of security.

Let the adventure begin…



References

1. An information-theoretic secure, key management system…
2. Information-theoretic security…
3. Security Proof
4. The unknow, unknowns or snake oil security…

Notes

1. “Perfect security” and “information-theoretic security” are used interchangeably and trace back to a 1949 publication by Claude Shannon. At its core,

information-theoretic security means that there is zero statistical dependence between the encrypted (observable) message and the secret plaintext message. Without statistical correlation, intercepting the encrypted message yields no advantage – the attacker's success probability is equivalent to pure guessing.

2. Classical ciphers and cryptographic algorithms (both public-key and symmetric) provide security proofs based on the infeasible computational complexity of an eavesdropper who attempts in decoding an encrypted message without a knowledge of the secret key.
3. Gilbert Vernam invented the system and patented it in 1919 (US Patent 1,310,719) for teleprinters, the formal *proof* of its perfect secrecy came much later from Claude Shannon in his 1949 paper, "Communication Theory of Secrecy Systems".
4. SHANNON Paper: Communication Theory of Secrecy Systems
5. Medley - Key Management and associated Key Generators are supplied only as a managed service, or licenced directly to OS developers, to guarantee correct implementations in accordance with their design.
6. New survey reveals $2 trillion market opportunity...
7. A uniform random function generates outcomes where every possibility within a given range (or set) has an equal chance of being selected, creating a flat probability distribution, unlike other functions that might favour certain numbers (e.g., a bell curve). It's defined by a minimum (a) and maximum (b) value, with a constant probability density of $1/(b-a)$ for continuous variables or 1/n for discrete ones.
8. If a vulnerability ("zero-day") were discovered in a foundational technology like AES, it would have immense value and would likely be exploited covertly rather than published for public knowledge.
9. Hoax: to trick into believing or accepting as genuine something false and often preposterous.

APPENDIX

What is Security

One of the more insane discussions I have regarding perfect security is to state cyber security or even perfect ciphers are not security and hence Information Theoretic Security is not relevant.

Security means protection from harm, danger, or threat, encompassing physical protection, and digital protection (cybersecurity). Traditional security is about risk

management and the acceptance of any residual risk that has no known counter measure to reduce to zero risk.

Axiom: security is fundamentally about both physical and cyber protection, as these two domains are deeply interconnected and rely on each other for comprehensive defence.

The problem with security is the unknown, unknowns this prevents a practical threat assessment and hence self-deprecates all Risk Assessments and hence security becomes a hoax detached from reality.

Today security is predicated upon "known knowns" — what's been observed, catalogued, and measured, via threat and risk assessments and penetration testing of defences. But the real danger lives in the "unknown unknowns" — risks we haven't even imagined. These aren't just blind spots. They are gaps in our mental models, born not from negligence but from the inherent complexity, emergence, and drift of digital systems.

The relationship between what we know, what we do not know, what we cannot know and what we do, a like to know determines the cognitive frame for security practice.

Welcome to today's real world of snake oil security.

The path forward…
Lets start with the ability of perfect security to store any and all information (INFOSEC), and guaranteed via a proof of security that this protection ensures an attacker has no advantage and their probability of success is equivalent to pure guessing or a true random number, regardless of how much computing power, or time they have.

So know we have protection against all unknown, unknowns as the attacker has zero probability of accessing the information even with infinite resources and time (harvest now attack latter).

No it does no matter to perfect security where the attack comes from or what part of the infrastructure is attacked perfect security guarantees that no attacks will be successful against any information.

So we have solved the digital protection (cybersecurity) part of the more generalised security problem, and only physical protection remains to be addressed.

The answer lies in this riddle:
If the information is protected against all attack vectors via perfect security does this not also include any and all forms of physical attacks?

The correlation between perfect security, Information and physical or cybersecurity is undeniable.

Axiom: Perfect security protest information against all forms of attack vectors both physical and cyber.

A well design perfect security solution, also includes protection against denial-of-service attacks and ransomware attacks which are a form of denial-of-service attack vectors.

"It's hard to win an argument with a smart person, but it's damn near impossible to win an argument with a stupid person" - Bill Murray.

Post Quantum is a Hoax

The latest hoax peddled by the greater fools of this world is known as Post Quantum Cryptography. Now based on this hoax is trivial to expose as peddled snake oil, simply look for the proof of security within any proposal and one will find, zip, zero none exist.

Axiom: if any PQC proposal does not come with a proof of its security then it is a waste of time and effort, as the One Cipher comes with a proof of security and hence represents Perfect Security as defined above.

Security Proof hoax

"The running theme seems to be that cryptography is a kind of Dark Magic, best left to anointed High Priests. Us mere mortals cannot hope to wield it safely without first becoming one of those vaunted Experts — a futile endeavour for those of us who know their place."

In cryptography, Shannon showed that perfect secrecy via Information Theoretic Security proofs. So called security proofs for all other complexity-based ciphers only prove that something is secure within a given model and set of known assumptions. There are many examples of provably secure schemes that admit attacks because those attacks were completely outside of that threat model and assumptions.

There is no mathematical proof that secure encryption systems can actually exist outside of those with a Information Theoretic Security proof or Shamir's Secret Sharing scheme, let alone that any specific cipher candidate is secure. At best, some encryption algorithms can be believed to be secure (for some notion of security) as long as some given mathematical problem remains intractable with existing knowledge against well defined, and hence limited, attack vectors.

We're using the wrong nomenclature. The term 'security proof' is misleading in that it gives you the impression that a scheme is, well… provably secure, when in fact outside of a vernan cipher this is never true. The peddled proofs that we see in day-to-day life

are more accurately referred to as *security reductions*. These take something (like a cryptographic scheme) and *reduce* its security to the hardness of some other problem — typically a mathematical problem, but sometimes even another cryptosystem. Symmetric encryption algorithms such as AES don't usually boast even that kind of proof.

Axiom: so, called complexity-based ciphers security proofs don’t actually *prove a cipher is secure at all*.

The worlds so called experts can provide mathematical *reductions* for the security of modern systems based on current knowledge and computational assumptions, but they cannot provide an absolute, unimpeachable *proof* of security against all present and future attacks in the real world, as cryptography relies on complex mathematical problems that are defined to be hard to analyse.

There are two ways to ensure security, either the secrecy depends on hiding both the algorithm and the secret key, or the algorithm is known to the adversary and only the secret key needs to be hidden. History has shown that the first one is not practical, and leads to greater security flows, as the amount of secret data to keep the secrecy is much larger if the algorithm is included. This was first explicitly stated as a fundamental principle in 1883 by Auguste Kerckhoffs [Kerckhoffs, 1883] and is generally called Kerckhoffs’s Principle; alternatively, and more bluntly, it was restated by Claude Shannon, the inventor of information theory and the fundamentals of theoretical cryptography in [Shannon, 1949].

Cryptographic algorithms, or more generally cryptosystems, are based on complex mathematical problems that are easy to state but have been found difficult to solve, the key is to prove that these complex problems are in fact unsolvable by an attacker with infinite resources and time. Traditionally, security proofs are asymptotic: it classifies the hardness of computational problems using polynomial-time reducibility. Secure schemes are defined to be those in which the advantage of any computationally bounded adversary to break the cryptosystem is negligible, but this is not a security proof as the probability cannot be reduced to absolute zero against the unknown unknowns which exist inside the real world.

The best any existing security proof aims at quantifying an upper bound on the probability of any (known) adversary to break the system studied. More precisely, a proof of security involves an upper bound on the advantage of the known adversary to break the system as a function of adversarial resources and of the problem size but cannot be considered as a formal proof of security.

All existing modern cryptography has no formal proofs of security but rather considers security properties in which known attackers may break the cryptographic algorithm

only with a small (negligible, but never zero) probability. In this context, cryptographic algorithms and security properties/assumptions are expressed as probabilistic assumptions. These so-called security proofs consist of bounding the probability of an event in such programs. Such proofs have been peer-reviewed for some decades, but since they are difficult to prove and to verify, fallacies keep emerging, as they have no known means to resist the unknown, unknowns of the real world in which they operate.

Axiom: There exists no known proof of security which has a zero residual probability for any modern cipher (with the sole exception of the One Cipher), against an unknown attacker regardless of how much computing power, or time they have.

Modern, widely used ciphers like the Advanced Encryption Standard (AES-256) are considered "secure" in a computational sense, meaning they have no publicly known attack vectors with current technology, but are not theoretically secure as there exist no formal proof of security. Given NIST crippled AES block size to 128 bits it is highly probable it can be brute forced or broken today.

In summary, the "proof" for all existing complexity-based ciphers (such as AES) is a conjecture that the cipher is a strong but deterministic pseudorandom function, supported by a lack of any published effective attacks, but this is not a proven proof of security.

At best we can only state that there is no published successful attack on AES, but then if an attack vector existed then most likely the attacker would keep this fact a secret.

<u>So called Security Experts</u>

The industry operates on the assumption that because so many experts have failed to find a practical attack, the algorithm is likely secure. But the vernan cipher proves beyond any doubt, expertise in mathematics and computer science are not prerequisites for proven security ciphers.

All modern-day ciphers including AES security, is a matter of confidence in the "madness of crowd" or snake oil security, not a single modern-day cipher or even PQC comes with any proof of security. The failure of many motivated individuals to find any successful attacks for a given cipher provides no evidence of its security.

In summary, there is no mathematical proof that *any* standardised (NIST) secure encryption system can exist, the security of ciphers like AES is based on the confidence in the 'madness of the crowd". It is highly unlikely that if any weakness was found that it would become public knowledge anyway due to the asymmetry between attackers and defenders and the resulting reward is targeted to attacker's.

Security experts did identify the possibility of a backdoor in the Dual_EC_DRBG algorithm in 2007, one year after it was standardized by NIST, but confirmation of the

NSA's involvement in creating an intentional backdoor did not emerge until the Edward Snowden leaks in 2013, in 2014 seven years after its standardisation NIST officially recommended against the use of the algorithm and began the process of removing it from its standards.

Expertise in advanced mathematics and computer science do not a cipher expert make, as the vernan cipher clearly proves to all. Creating complex ciphers and then failing to prove their security is a well-trodden pathway for all snake oil security.

Axiom: Cryptography must be easy for every user to full understand its operation and complexity is the worst enemy of security.

"In theory, theory and practice are the same. In practice, they are not."

Stop creating complex versions of a predictable and deterministic PRNG key schedule, so called cryptographic experts simply do not exist.

Strategy

Implementing an ITS strategy is challenging in any IT environment, but critical infrastructure sectors face unique hurdles that make it both more difficult and more urgent. Sectors like energy, transportation, telecommunications, healthcare, and industrial control systems (ICS/SCADA in manufacturing or utilities) have a history of using long-lived equipment and protocols that were not designed with frequent crypto updates in mind. It's not uncommon for industrial control devices or embedded systems in these sectors to have 10- to 20-year lifecycles, with updates only applied during rare maintenance windows. Many operate under tight real-time constraints and with an overriding emphasis on availability and safety – meaning any change that could introduce latency or downtime is resisted. Fortunately, ITS solution has reduced constrains compared to existing solutions.

Axiom: critical infrastructure operators must start planning for ITS migrations now, because they are high-value targets for adversaries.

Another implication for critical sectors is the need for tailored migration playbooks. For instance, in the power grid sector, there are standards like IEC 61850 and IEEE protective relay protocols – sector-specific bodies should be updating those to include ITS options or at least not preclude them. The healthcare sector might focus on the PKI for medical devices (ensuring that existing certificates are deprecated and replaced by ITS solution). The aviation and automotive sectors will need to ensure future hardware (like next-gen aircraft communication systems or car onboard security modules) have the horsepower and tested libraries to do ITS, since those vehicles will be in service into the 2040s and beyond.

In short, critical infrastructure organizations face a "perfect storm" of long-lived tech, high stakes, and advanced adversaries. They should treat the ITS transition as part of

broader resilience initiatives (like safety system modernization and zero-trust networking). By doing pilot projects now and sharing lessons learned (perhaps through industry ISACs or coordination with agencies like CISA), they can avoid being caught off-guard. The worst outcome would be doing nothing and then, say, around 2030 when a quantum code-breaking capability seems imminent, scrambling to rip-and-replace crypto in systems that were never designed for it. Far better is to lay the groundwork gradually, starting today.

Stepping back, the ideal end-state is a system that can withstand the failure of any one component – including a cryptographic component – without catastrophic breach. This is the essence of resilience. Embracing zero-trust principles is one way to move toward that goal: assume that no single element (user, device, application) is inherently trustworthy and continuously validate using multiple signals. How does that relate to ITS? In a zero-trust approach, even if an adversary somehow breaks one element of the solution or impersonates one identity, they should not immediately get access to everything, because each transaction or session is verified independently (and often with context-aware policies).

Lastly

If you take a sheet of paper, write something on it, burn it and mix the ashes, one day we will be able to recover the information., this is the intuition based quantum computing threat.

Fully burned paper contains no structural information anymore, the molecules have been broken down, the ink is oxidized, the ordering is destroyed, there is nothing left to reconstruct, this is how perfect security works today.

Axiom: given a choice between one's intuition via the ignorance of the crowd and perfect security, why would any sane person choose intuition…

The point, with complexity-based ciphers that come with no proof of security, is we simply lack the understanding today to crack it, but we will eventually break complexity, as there is always order hiding in complexity, that nothing is truly chaotic or random, time eventually reveals hidden structure. Complexity is never real complexity but just a pattern we haven't discovered yet.

We confuse unfamiliarity with danger, we trust our intuition more than the physics and we assume something must be vulnerable simply because we do not understand it. Scepticism feels smart but it is often nothing more than a mental reflex meant to create false certainty where understanding is missing. That is the correlation I see over and over again, the less someone understands the more confident he sounds, not because

he is closer to the truth but because his mental model is too small for the reality he is trying to judge.

Intuition is the worst possible instrument to measure perfect security with; they mistake their own ignorance for insight.