The Days Before Crypto Wars — Rethink the Kerckhoffs' Legacy

Good afternoon, everyone. It's a privilege to be here on the ETHDenver stage.

I'm Sun Peng, a Master of History and the author of the first article in the *Find Cypherpunk* research series, *Biography of Auguste Kerckhoffs*. The title of my speech today is *The Days Before Crypto Wars — Rethinking the Legacy of Kerckhoffs*.

At First, who is Kerckhoffs?

Modern cryptography emerged in the 1950s, and by the 1970s, with Diffie-Hellman key exchange and RSA, we entered the era of public-key cryptography. That same period—the '1960s and '1970s—was a time of civil rights movements, counterculture, and peak activism in Europe and the U.S. The birth of public-key cryptography and the cypherpunk movement carried the cultural DNA of that era, setting the stage for the "three crypto wars" and civic movements since the 1990s.

So, when it comes to the pioneers of modern cryptography, we might trace back to Claude Shannon, the father of modern cryptography. His paper, *A Mathematical Theory of Communication in Secret Systems*, based on information theory, introduced "the enemy knows the system" as a security assumption for analyzing a system's safety. But what many don't realize is that this concept was Shannon's refinement and synthesis of earlier ideas. The true originator was Auguste Kerckhoffs, a Dutch linguist and cryptologist from the late 19th century.

In early 1883, Kerckhoffs published **Military Cryptography**—and laid out his famous "Kerckhoffs' Principle": a system "should not require secrecy, and it should not be a problem if it falls into enemy hands."

What circumstances led Kerckhoffs to propose this groundbreaking principle? What's his story? Allow me to take a moment to share his journey.

Auguste Kerckhoffs was a relentless seeker of knowledge. Born in 1847 in the Netherlands to a well-off family, he grew up surrounded by learning. At 20, he studied philosophy and natural sciences in Leuven, Belgium. After graduating, he taught English and German in France, while diving into languages—modern and ancient—alongside math, history, and archaeology. In 1873, at 26, he pursued German classical linguistics at Bonn and Tübingen universities in Germany, earning his doctorate. Seven years later, he joined the Paris Anthropological Society, immersing himself in archaeology, religious studies, and cryptography.

This intellectual diversity shaped his cryptographic work. Before modern cryptography, classical cryptography was a humanistic field, intertwined with linguistics and archaeology. In the very year he joined the Paris society, Kerckhoffs published *Military Cryptography*.

If you know cryptography's history, you'll recognize it's always been a child of war. *Military Cryptography* was born from the Franco-Prussian War. Evidence suggests Kerckhoffs had ties to French military leaders. In 1870, that war ended in France's defeat. Prussia's victory owed much to cracking French codes, while France was unprepared. The field ciphers of the time relied on polybius square—a system so fragile that knowing its mechanics meant breaking it. The telegraph made interception and decryption even easier. Kerckhoffs noted that France's wartime codes were so weak, "even the least experienced analyst could find the key in an hour."

After the war, France followed Germany's lead, establishing a modern general staff focused on intelligence and decryption. With telegraphs transforming communication, Kerckhoffs didn't chase more complex ciphers. Instead, he offered a guiding principle: separate the "general system" from the "specific key." A system could be secure even if fully known, as long as the key stayed secret. That's the Kerckhoffs' Principle. For those of us in Crypto, it's astonishing to think this idea emerged 140 years ago.

This principle sparked a movement that lasted nearly a century, reaching its peak with public-key cryptography. Kerckhoffs' insight still guides us. Take Bitcoin's ECDSA and Schnorr signature algorithms—they rely on the "discrete logarithm" problem, assuming no polynomial-time solution exists in certain groups. Their security hinges on practical, not absolute, difficulty—a direct echo of Kerckhoffs' "practical security."

He also made cryptanalysis the only reliable test for military ciphers, a method that endures. The late 20th-century open-source software movement is a prime example.

Eric Raymond, a key figure and author of *The Cathedral and the Bazaar*, reframed Kerckhoffs' Principle: "Any security design that doesn't assume the enemy has the source code is untrustworthy; never trust Closed source." Since then, civilian cryptography has followed this openness. An algorithm is only deemed secure after surviving relentless attacks from a public, hardcore cryptographer community.

Under Kerckhoffs' influence, French cryptography thrived from the late 19th century to World War I—a golden age.

Let me share one final story about Kerckhoffs. His principle champions openness, mirroring his own spirit. He was a pioneer in the Volapük movement, a 19th-century push for a universal language, reflecting his internationalist ideals. Tragically, in 1903, at 68, he died in a train accident while vacationing in Switzerland.

For over a century, he faded from memory. Then, in 2020, two cryptologists from École Normale Supérieure in Paris, Rémi Géraud-Stewart and David Naccache, wrote his biography. Visiting his grave, they found it neglected—simple and untended. On behalf of the global cryptography community, they rebuilt his tomb and urged French authorities to recognize its historical value, ensuring it isn't lost to time.

That's Kerckhoffs' story. He bridged science and humanities in an age of polymaths. His legacy, born from 19th-century national conflicts, shines with a cosmopolitan vision.

Kerckhoffs' cryptographic triumph was inseparable from his era—politics, war, and culture shaped him. Today, cryptography remains entwined with politics, society, and human rights. Isn't Crypto's ethos of openness and sharing also a borderless, global ideal?

As the core value of Crypto gradually fades today, we should take a step back and revisit the pioneers of cryptography. As Karl Kraus said, "Origin is the goal." If Crypto has become nothing more than a casino, and if all the builders feel lost and powerless about the current state of the industry, we should consider whether we need to look back. Let's reflect on how Crypto has come to this point, and why the original Cypherpunks started this century-long struggle. What was their goal? How do they feel about Crypto's current development? And do we still retain our original vision? Ultimately, Crypto helps Crypto, and in the face of the Leviathan, I firmly believe that those who stay true to their roots will still lead Crypto forward and continue its development.

OK, that’s all from me. Thanks for your listening, and a heartfelt thanks to Primitives Lane and its founder, Yao Xiang, for inviting me.