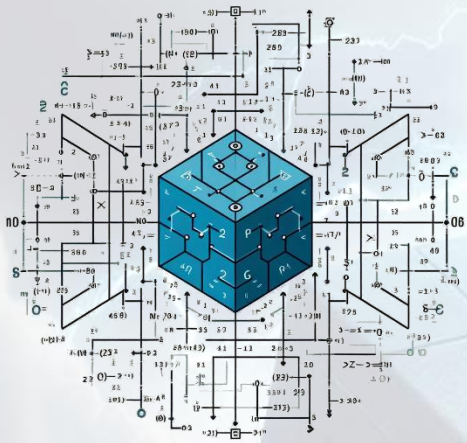
Aging of AES (Encryption Standard)



AES encryption is one of the most widely trusted methods of protecting data. It was adopted by the U.S. Gov in 2001. AES is a symmetric-key algorithm that uses the same key (up to 256-bit) for both encryption and decryption.

But how secure is AES encryption in practice? Can it withstand attacks from hackers and adversaries who want to break into our systems and steal our secrets?

In this whitepaper, we will explore the design and security of AES encryption, as well as some of the challenges and threats that it faces in the modern world.

Cipher aging is the gradual weakening of encryption over time due to advancements in computing power and cryptanalysis techniques. This is crucial for cryptography as it ensures our data remains secure even as technology evolves.

Born from a global competition in 1998, Rijndael's algorithm emerged victorious for its security and efficiency. By 2001, NIST declared it the new U.S. encryption standard, christened AES. Widespread adoption followed across the government and beyond in 2002, solidifying AES as the world's dominant encryption shield.

Key space is the total number of possible encryption keys in a cipher. A larger key space makes brute-force attacks exponentially harder, protecting your data even as computing power increases. AES offers varying key sizes, like 128, 192, and 256 bits. E.g., cracking AES-128 requires 2^{128} attempts—virtually impossible! Theoretical attacks like Bernstein and Krawczyk targeted reduced versions of AES, emphasizing the proper implementations and continued vigilance is crucial for optimal security in the ever-evolving tech landscape.

Quantum computers hold the potential to revolutionize—and threaten—cryptography. Grover's quantum algorithm could drastically accelerate the search. This means even vast key spaces, once considered impenetrable, could become vulnerable.

Three factors that determine the age of cipher

One, Moore's Law: computing power doubling every few years could eventually crack its 2^{128} key space, just as it did with DES's smaller key space. Two, hidden flaws: though resilient, a cryptanalyst's jackpot could drastically shorten its lifespan. Unfortunately, examples exposing cryptanalyst success are often kept under wraps for security reasons. Still some known examples include Enigma, RC4, GSM cipher, MD5 collisions, SHA-1, etc. Finally, disruptive technologies, like AI, quantum computers and Groover's algorithm, potentially shrink life of many ciphers.

What is the expected age of AES from 2024 perspective?

In reality, answer depends on many uncertain factors, such as the development pace of new technologies (esp. quantum computer) and discovery of new attacks (esp with help of AI). Based on our survey from dozens of domain experts, the probability of AES-128 surviving until 2040 is about 60% and AES-256 surviving 2040 is about 60%.

Aging is a reality. A diversified encryption strategy is the key to ensure secrets remain safe even as the clock ticks on current ciphers.

Sara Malik <smk@PakCrypt.Org> is an InfoSec professional in PakCrypt outreach program.