☰ 🔊 Listen ▶

The Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a widely used symmetric-key block cipher used for secure data encryption. It was established as a U.S. Federal Information Processing Standard (FIPS) in 2001 and has become a global standard for securing sensitive data. AES operates on fixed-size blocks of data and supports key sizes of 128, 192, and 256 bits, making it a versatile choice for various security applications.

AES uses a substitution-permutation network (SPN) structure that consists of several rounds, with the number of rounds determined by the key size. In each round, AES applies a series of transformations, including substitution (using S-boxes), permutation (through a shifting operation), and mixing (using a mathematical operation known as the Mix Columns step). These operations provide both confusion and diffusion, ensuring that plaintext data is transformed into ciphertext in a way that is resistant to cryptanalysis. The specific number of rounds used varies depending on the key size.

AES offers a balance between strong encryption and computational speed, making it suitable for a wide range of applications, from securing data during transmission (e.g., in HTTPS connections) to protecting sensitive information on storage devices. AES has withstood extensive cryptanalysis efforts and is considered a reliable and robust encryption algorithm, making it a cornerstone of modern cryptography.

The RSA Algorithm

The RSA cryptosystem (named after Ronald Rivest, Adi Shamir, and Leonard Adleman) implements a public key algorithm using prime numbers and modular arithmetic. To implement the RSA algorithm, a person selects two (large) prime numbers, p and q. The person then computes $m = pq$ and releases m as public knowledge. For any plaintext message to be encrypted, a sender represents the message as a number x between 0 and $m – 1$. This is achieved by converting the number from base 26 (letters) to base 10. Finally, one selects the public key by choosing an integer e that is relatively prime to $(p – 1)(q – 1)$ and releases it. Encryption is performed by exponentiation mod m: $y = x^e$. Mod m then becomes the cipher text. Note that this is done via a computer using the public information e and m. To decrypt, the recipient uses his or her private key d, where $ed = 1$ mod n. By Fermat’s little theorem, a person calculates $y^d = x^{ed} = x$ mod m. The security of the algorithm is based on the difficulty of determining p and q from the public information m and e.