The advanced encryption standard (aes)

AES is the most-used cipher in the universe. It has high level of security and it is fast in software compared to its predecessors DES and Triple DES (3DES). NIST standardized AES in 2000 as a replacement for DES, at which point it became the world’s de facto encryption standard. Most commercial encryption products today support AES.

AES processes blocks of 128 bits using a secret key of 128, 192, or 256 bits, with the 128-bit key being the most common because it makes encryption slightly faster and because the difference between 128- and 256-bit security is meaningless for most applications. Whereas some ciphers work with individual bits or 64-bit words, AES manipulates bytes. It views a 16-byte plaintext as a two-dimensional array of bytes. AES transforms the bytes, columns, and rows of this array to produce a final value that is the ciphertext.

In order to transform its state, AES uses an SPN structure, with 10 rounds for 128-bit keys, 12 for 192-bit keys, and 14 for 256-bit keys. Each round consists of combination of 4 building blocks:

* **AddRoundKey -** XORs a round key to the internal state.
* **SubBytes -** Replaces each byte with another byte according to an S-box. In this example, the S-box is a lookup table of 256 elements.
* **ShiftRows -** Shifts rows.
* **MixColumns -** Applies the same linear transformation to each of the four columns of the state.

First 9 rounds use all 4 of these building blocks, and the last one uses skips MixColumns.

Another important part of encryption is called KeyExpanison. It produces unique key for each of rounds, using the same S-box.

To decrypt a ciphertext, AES unwinds each operation by taking  
its inverse function.

All of these operations contribute to security of AES, making it the most usable encryption algorithm in the world

1. **How many rounds does encryption algorithm have?**

Answer:10

1. **What are 4 building blocks of each AES round?**

Answer: AddRoundKey, SubBytes, ShiftRows, MixColumns

**Why does encryption need KeyExpansion?**

Without KeyExpansion, all rounds would use the same key, K, and AES  
would be vulnerable to slide attacks.