AES (Advanced Encryption Standard) is a widely used encryption algorithm that supports various key lengths. However, the standard key lengths are 128, 192, and 256 bits. Using a key length of 24 bits is not recommended as it is too weak and can easily be cracked. In fact, it is no longer considered secure and should not be used for any serious encryption purposes.

That being said, if you still want to implement a simplified AES algorithm with a 24-bit key length for educational purposes, you can do so using the following steps:

Key Expansion: The first step is to expand the 24-bit key into a set of 192-bit round keys. To do this, you can use a key expansion algorithm similar to the one used for 128-bit keys in AES. However, you will only need to generate 12 round keys instead of 10.

Initial Round: The plaintext is XORed with the first round key.

Rounds: A total of 11 rounds are performed, where each round consists of the following operations:

SubBytes: Each byte of the state is replaced with a corresponding byte from a fixed 256-byte table called the S-box

ShiftRows: The rows of the state are shifted cyclically by different offsets.

MixColumns: Each column of the state is multiplied with a fixed 4x4 matrix in a special algebraic field.

AddRoundKey: The state is XORed with the round key.

Note that the MixColumns operation is slightly different from the one used in AES due to the shorter key length.

Final Round: The final round is similar to the other rounds, except that the MixColumns operation is omitted.

The resulting state is the ciphertext.

Again, it's important to note that using a 24-bit key length for AES is not recommended and should not be used for any serious encryption purposes.