AES (Advanced Encryption Standard)

AES (Advanced Encryption Standard) is a symmetric-key encryption algorithm used to secure sensitive data. AES is based on a substitution-permutation network (SPN) structure where the plaintext is divided into fixed-size blocks and each block is transformed using multiple rounds of substitution and permutation operations.

The AES algorithm involves the following steps:

1. Key Expansion:
   - Generate a set of round keys from the initial secret key using a key schedule algorithm
   - The round keys are the same size as the block size and are used in each round of the encryption process
2. Encryption:
   - Divide the plaintext message into fixed-size blocks (usually 128 bits)
   - Add the round key to the first block
   - Perform a series of substitution and permutation operations (known as rounds), each round consisting of four transformations: SubBytes, ShiftRows, MixColumns, and AddRoundKey
   - After the final round, output the encrypted ciphertext
3. Decryption:
   - Divide the encrypted ciphertext into fixed-size blocks (usually 128 bits)
   - Invert the last round of the encryption process by performing a sequence of inverse transformations: InvShiftRows, InvSubBytes, InvMixColumns, and AddRoundKey
   - Perform the inverse of each of the previous rounds in reverse order

The mathematical formulas used in AES algorithm:

- Substitution Box (S-Box): A nonlinear substitution function used in AES algorithm to provide confusion. In AES algorithm, the S-Box is a fixed lookup table.
- Permutation Box (P-Box): A linear permutation function used in AES algorithm to provide diffusion. In AES algorithm, the P-Box is a fixed permutation table.
- Round Key Generation: Round key generation algorithm is used to generate the round key for each round of encryption. It involves a combination of substitutions, permutations, AND, XOR operations.
- SubBytes: A substitution operation that replaces each byte of the block with a different byte, using the S-Box.
- ShiftRows: A permutation operation that shifts the rows of the block by a fixed number of bytes, for example, first row is shifted by 0 bytes, second row is shifted by 1 byte, etc.

- MixColumns: A linear operation that mixes the columns of the block using matrix multiplication by a fixed matrix.
- AddRoundKey: An XOR operation that combines the current block with a round key.

Example of JavaScript code for AES Encryption and Decryption:

```
// node-js
const crypto = require('crypto');

// AES Encryption
function aesEncrypt(secretKey, plaintextMsg) {
  const iv = crypto.randomBytes(16); // Generate random initialization vector
  const cipher = crypto.createCipheriv('aes-256-cbc', secretKey, iv);
  let ciphertext = cipher.update(plaintextMsg, 'utf8', 'base64');
  ciphertext += cipher.final('base64');
  return [iv.toString('hex'), ciphertext];
}

// AES Decryption
function aesDecrypt(secretKey, iv, ciphertextMsg) {
  const decipher = crypto.createDecipheriv('aes-256-cbc', secretKey, Buffer.from(iv, 'hex'))
  let plaintext = decipher.update(ciphertextMsg, 'base64', 'utf8');
  plaintext += decipher.final('utf8');
  return plaintext;
}
```

Another example:

```
// nodejs
const crypto = require('crypto');
const algorithm = 'aes-256-cbc';
const key = crypto.randomBytes(32);
const iv = crypto.randomBytes(16);

// Encrypt data using AES
function encrypt(text) {
    let cipher = crypto.createCipheriv(algorithm, Buffer.from(key), iv);
    let encrypted = cipher.update(text);
    encrypted = Buffer.concat([encrypted, cipher.final()]);
    return { iv: iv.toString('hex'), encryptedData: encrypted.toString('hex') };
}

// Decrypt data using AES
function decrypt(text) {
    let iv = Buffer.from(text.iv, 'hex');
```

```
    let encryptedText = Buffer.from(text.encryptedData, 'hex');
    let decipher = crypto.createDecipheriv(algorithm, Buffer.from(key), iv);
    let decrypted = decipher.update(encryptedText);
    decrypted = Buffer.concat([decrypted, decipher.final()]);
    return decrypted.toString();
}
```

Note:

This is a basic implementation of AES algorithm.