AES(Advanced Encryption Standard)

More about AES encryption can be found here:

1. https://www.n-able.com/blog/aes-256-encryption-algorithm
2. https://www.comparitech.com/blog/information-security/what-is-aes-encryption/

In [26]:
```
#Importing Libraries
import hashlib
from Crypto import Random
from Crypto.Cipher import AES
from base64 import b64encode, b64decode
```

In [27]:
```
#Test data
data='fc5841de-bdcf-4a22-86f2-f7b75c964412'.encode("utf8")
data1='Hello World'.encode("utf8")
```

In [28]:
```
#Encryption Part
from Crypto.Cipher import AES

#32 Byte Encryption Key for AES 256
key = b'Sixteen byte keySixteen byte key'
cipher = AES.new(key, AES.MODE_EAX)

nonce = cipher.nonce
ciphertext, tag = cipher.encrypt_and_digest(data)
```

In [29]:
```
#View Encrypted Text and Length of Encypted Key
print(ciphertext)
print(len(ciphertext))
```

```
b'\x9a\xe5\x8b^\xc0\x93\xaa\x1e\xc3(\xcc\xd6\x13\xb9\x7f\x98\x02\xfc\xb3`"d~\xad\x9f\x
fc\x8af\xcb\xe1Q\xd5B&\xa6\x1e'
36
```

In [30]:
```
#Decryption: require key and (nonce, ciphertext, tag)
#32 Byte Encryption Key
key = b'Sixteen byte keySixteen byte key'
cipher = AES.new(key, AES.MODE_EAX, nonce=nonce)
plaintext = cipher.decrypt(ciphertext)
try:
    cipher.verify(tag)
    print("The message is authentic:", plaintext)
except ValueError:
    print("Key incorrect or message corrupted")
```

```
The message is authentic: b'fc5841de-bdcf-4a22-86f2-f7b75c964412'
```

In [ ]:
```
```