Practical 6\keyExpansion.py

```python
S = (
    ["63","7c","77","7b","f2","6b","6f","c5","30","01","67","2b","fe","d7","ab","76"],
    ["ca","82","c9","7d","fa","59","47","f0","ad","d4","a2","af","9c","a4","72","c0"],
    ["b7","fd","93","26","36","3f","f7","cc","34","a5","e5","f1","71","d8","31","15"],
    ["04","c7","23","c3","18","96","05","9a","07","12","80","e2","eb","27","b2","75"],
    ["09","83","2c","1a","1b","6e","5a","a0","52","3b","d6","b3","29","e3","2f","84"],
    ["53","d1","00","ed","20","fc","b1","5b","6a","cb","be","39","4a","4c","58","cf"],
    ["d0","ef","aa","fb","43","4d","33","85","45","f9","02","7f","50","3c","9f","a8"],
    ["51","a3","40","8f","92","9d","38","f5","bc","b6","da","21","10","ff","f3","d2"],
    ["cd","0c","13","ec","5f","97","44","17","c4","a7","7e","3d","64","5d","19","73"],
    ["60","81","4f","dc","22","2a","90","88","46","ee","b8","14","de","5e","0b","db"],
    ["e0","32","3a","0a","49","06","24","5c","c2","d3","ac","62","91","95","e4","79"],
    ["e7","c8","37","6d","8d","d5","4e","a9","6c","56","f4","ea","65","7a","ae","08"],
    ["ba","78","25","2e","1c","a6","b4","c6","e8","dd","74","1f","4b","bd","8b","8a"],
    ["70","3e","b5","66","48","03","f6","0e","61","35","57","b9","86","c1","1d","9e"],
    ["e1","f8","98","11","69","d9","8e","94","9b","1e","87","e9","ce","55","28","df"],
    ["8c","a1","89","0d","bf","e6","42","68","41","99","2d","0f","b0","54","bb","16"]
)

Rconst = [
    "00000000", "01000000", "02000000", "04000000", "08000000",
    "10000000", "20000000", "40000000", "80000000", "1B000000", "36000000"
]

def xor(a, b):
    return hex(int(a, 16) ^ int(b, 16))[2:].zfill(8)

def KeyExpansion(WordList):
    Index = "0123456789abcdef"
    KeyList = list()
    KeyList.append(WordList)

    for r in range(1, 11):  # 10 rounds
        row = []
        print(f'{r:^10}', end="")
        for i in range(4):
            if i == 0:
                word = KeyList[r-1][3]
                RotWord = word[2:] + word[:2]

                subWord = ""
                for x in range(0, 8, 2):
                    l = Index.index(RotWord[x])
                    m = Index.index(RotWord[x+1])
                    subWord += S[l][m]
                temp = xor(subWord, Rconst[r])
                print(f'{temp:^10}', end="")
                w = xor(temp, KeyList[r-1][0])
                print(f'{w:^10}', end="")
                row.append(w)
            else:
                w = xor(row[i-1], KeyList[r-1][i])
                print(f'{w:^10}', end="")
                row.append(w)
        print()

        KeyList.append(row)
```

```python

def main():
    wordrow = list(input("Enter Your Key (in format XXXX XXXX XXXX XXXX): ").lower().split(" "))

    # wordrow = ['2475a2b3', '34755688', '31e21200', '13aa5487']

    if len(wordrow) != 4:
        print("There must be 4 input keys")
        return

    for check in wordrow:
        if len(check) != 8:
            print("Each input key must be 8 hex characters long!")
            return

    print(f"{'Round':^10}{'t':^10}{'Key':^40}")
    print("="*59)
    print(f"{'0':^10}{" ":^10}", end='')

    for key in wordrow:
        print(f'{key:^10}', end="")

    print()
    KeyExpansion(wordrow)

if __name__ == '__main__':
    main()

```

```
Expansion.py
Enter Your Key (in format XXXX XXXX XXXX XXXX): 2475a2b3 34755688 31e21200 13aa5487
  Round       t                       Key
===========================================================
    0               2475a2b3  34755688  31e21200  13aa5487
    1      ad20177d 8955b5ce  bd20e346  8cc2f146  9f68a5c1
    2      470678db ce53cd15  73732e53  ffb1df15  60d97ad4
    3      31da48d0 ff8985c5  8cfaab96  734b7483  13920e57
    4      47ab5b7d b822deb8  34d8752e  479301ad  54010ffa
    5      6c762d20 d454f398  e08c86b6  a71f871b  f31e88e1
    6      52c4f80d 86900b95  661c8d23  c1030a38  321d82d9
    7      e4133523 62833eb6  049fb395  c59cb9ad  f7813b74
    8      8ce29268 ee61acde  eafe1f4b  2f62a6e6  d8e39d92
    9      0a5e4f61 e43fe3bf  0ec1fcf4  21a35a12  f940c780
    10     3fc6cd99 dbf92e26  d538d2d2  f49b88c0  0ddb4f40
```