Program-18

#include <stdio.h>

#include <stdint.h>

static const int IP[] = { 2, 6, 3, 1, 4, 8, 5, 7 };

static const int PC1[] = { 2, 4, 1, 6, 3, 9, 0, 8, 5, 7 };

static const int PC2[] = { 5, 2, 6, 3, 7, 4, 9, 8 };

static const uint64\_t KEY = 0x0000FFFFFFFFFFFF;

uint64\_t permute(uint64\_t input, const int \*table, int size) {

uint64\_t result = 0;

int i;

for ( i = 0; i < size; i++) {

result |= ((input >> (64 - table[i])) & 1) << (size - 1 - i);

}

return result;

}

void generate\_subkeys(uint64\_t key, uint64\_t \*subkeys) {

key = permute(key, PC1, 56);

int i;

for ( i = 0; i < 16; i++) {

uint64\_t shifted\_key = (key << i) | (key >> (28 - i));

subkeys[i] = permute(shifted\_key, PC2, 48);

}

}

int main() {

uint64\_t subkeys[16];

generate\_subkeys(KEY, subkeys);

int i;

printf("Generated Subkeys:\n");

for (i = 0; i < 16; i++) {

printf("K%d: 0x%012llX\n", i + 1, subkeys[i]);

}

return 0;

}

