Contents

QUESTION 1

```
%Implement a function that will generate the specific subkey Ki when the following parameters
%are passed as inputs to the function: a 56 bit key and the index i.
% FUNCTION CREATED IS CALLED subKey
k0 = "F0CCAAF556678F";
index = 1;
key = subKey(k0,index)
```

```
key =

  Columns 1 through 13

     0     0     0     1     1     0     1     1     0     0     0     0     0

  Columns 14 through 26

     0     1     0     1     1     1     0     1     1     1     1     1     1

  Columns 27 through 39

     1     1     1     1     0     0     0     1     1     1     0     0     0

  Columns 40 through 48

     0     0     1     1     1     0     0     1     0
```

QUESTION 2

```
%Calculate the number of unique subkeys for the following 64-bit keys (ignore the parity bits
%in your calculations) and classify the keys:
% FUNCTION CREATED IS CALLED uniqueKey
k1="1F1F1F1F0E0E0E0E"
[uniqueSubKeys,classifyKey] = uniqueKey(k1)
k2="1FFE1FFE0EFE0EFE"
[uniqueSubKeys,classifyKey] = uniqueKey(k2)
k3="1FFEFE1F0EFEFE0E"
[uniqueSubKeys,classifyKey] = uniqueKey(k3)
```

```
k1 =

    "1F1F1F1F0E0E0E0E"


uniqueSubKeys =

     1
```

```
classifyKey =

    "Weak keys"


k2 =

    "1FFE1FFE0EFE0EFE"


uniqueSubKeys =

     2


classifyKey =

    "Semi-weak key pairs"


k3 =

    "1FFEFE1F0EFEFE0E"


uniqueSubKeys =

     4


classifyKey =

    "Possibly weak keys"
```

QUESTION 3

```
%Implement a function that will produce two 32-bit output blocks, given a 64-bit input block,
%the index of the round (i ∈ {1, 2, ..., 16}) and the 48-bit subkey Ki.(The whole round must be implemented.)
% FUNCTION CREATED IS CALLED LeftRightofDES
input = "0123456789ABCDEF";
index = 16;
k0 = "133457799BBCDFF1";
mode = "encrypt";
[left,right] = LeftRightofDES(input,index,k0,mode)
```

```
left =

  Columns 1 through 13

     0     1     0     0     0     0     1     1     0     1     0     0     0

  Columns 14 through 26

     0     1     0     0     0     1     1     0     0     1     0     0     0

  Columns 27 through 32

     1     1     0     1     0     0
```

```
right =

  Columns 1 through 13

     0     0     0     0     1     0     1     0     0     1     0     0     1

  Columns 14 through 26

     1     0     0     1     1     0     1     1     0     0     1     1     0

  Columns 27 through 32

     0     1     0     1     0     1
```

QUESTION 4

```
%Using the functions of 1 and 3, implement the Data Encryption Algorithm (DEA).
% FUNCTION CREATED IS CALLED DES, Key, feistel, sBox
% As it is encryption: mode = 'encrypt'
input = "0123456789ABCDEF";
k0 = "133457799BBCDFF1";
mode = "encrypt";
output = DES(input,k0,mode)
```

```
output =

    '85E813540F0AB405'
```

QUESTION 5

```
%Implement the decryption algorithm as well.
% As it is encryption: mode = 'decrypt'
input = "85E813540F0AB405";
k0 = "133457799BBCDFF1";
mode = "decrypt";
output = DES(input,k0,mode)
```

```
output =

    '0123456789ABCDEF'
```

Published with MATLAB® R2021a