The DES Encryption Algorithm

Ahmed Ibrahim
201204361

Babikr Elnimah
201204005

Mohammed Sheikh
201205380

The DES Encryption Algorithm

Ahmed Ibrahim
201204361

Babikr Elnimah
201204005

Mohammed Sheikh
201205380

The DES Encryption Algorithm

Ahmed Ibrahim
201204361

Babikr Elnimah
201204005

Mohammed Sheikh
201205380

History:

-For a period of time, as of not long ago DES (Data Encryption Algorithm) was the primary encryption algorithm for encrypting data.

-DES is a product of a research project ran by IBM (International Business Machines) in the late 1960's

-This research eventually lead to the creation of a encryption cipher known as LUCIFER

-In the early 1970's IBM decided to commercialize
LUCIFER

LUCIFER:

-The commercialization of LUCIFER resulted in a large number of adjustments

-These changes were not done entirely by IBM alone

-In the early 1970's IBM decided to commercialize LUCIFER

LUCIFER:

-The commercialization of LUCIFER resulted in a large number of adjustments

-These changes were not done entirely by IBM alone

-A number of outside consultants were recruited by IBM

-However the major contributor in terms of technical contribution was the NSA

-The resulting altered version of LUCIFER was proposed to the NBS (National Broad of Standards) as an answer to their call for a new national encryption standard.

-In 1977 the altered version of LUCIFER was dubbed DATA ENCRYPTION STANDARD – DES (FIBS PUBS 46) and adopted by NBS as its

as an answer to their call for a new national encryption standard.

-In 1977 the altered version of LUCIFER was dubbed DATA ENCRYPTION STANDARD – DES (FIBS PUBS 46) and adopted by NBS as its name sake

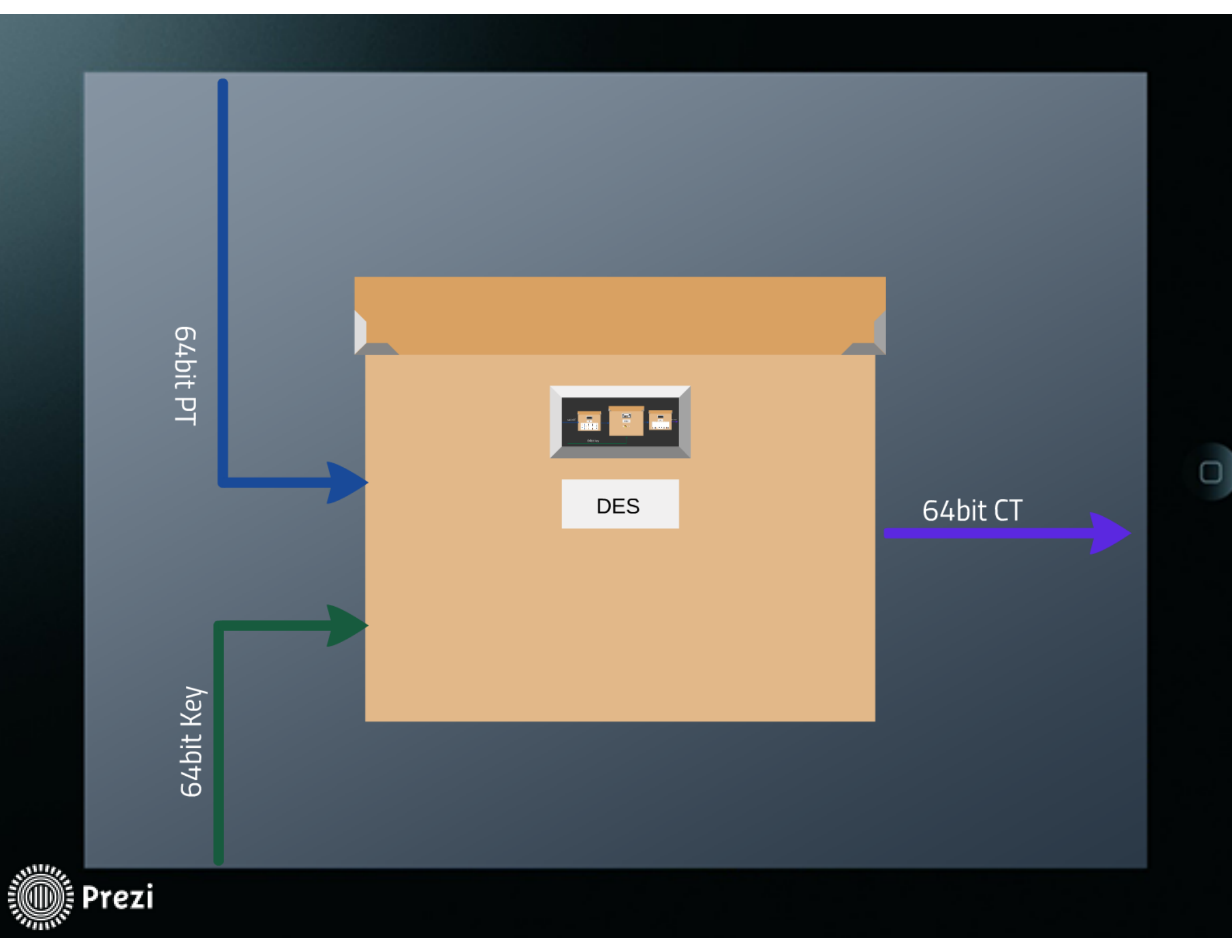
The DES Encryption Algorithm

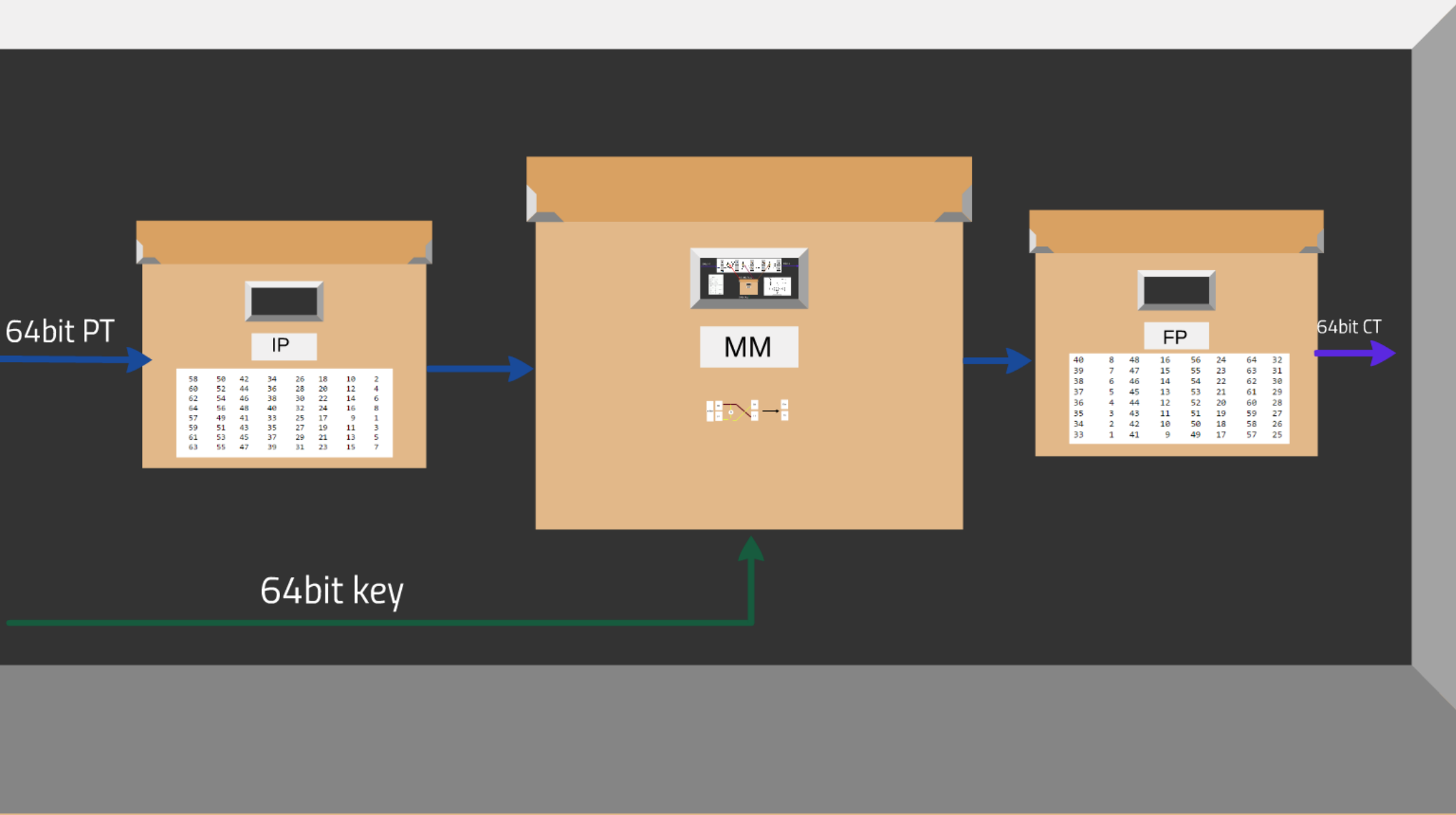
Ahmed Ibrahim
201204361

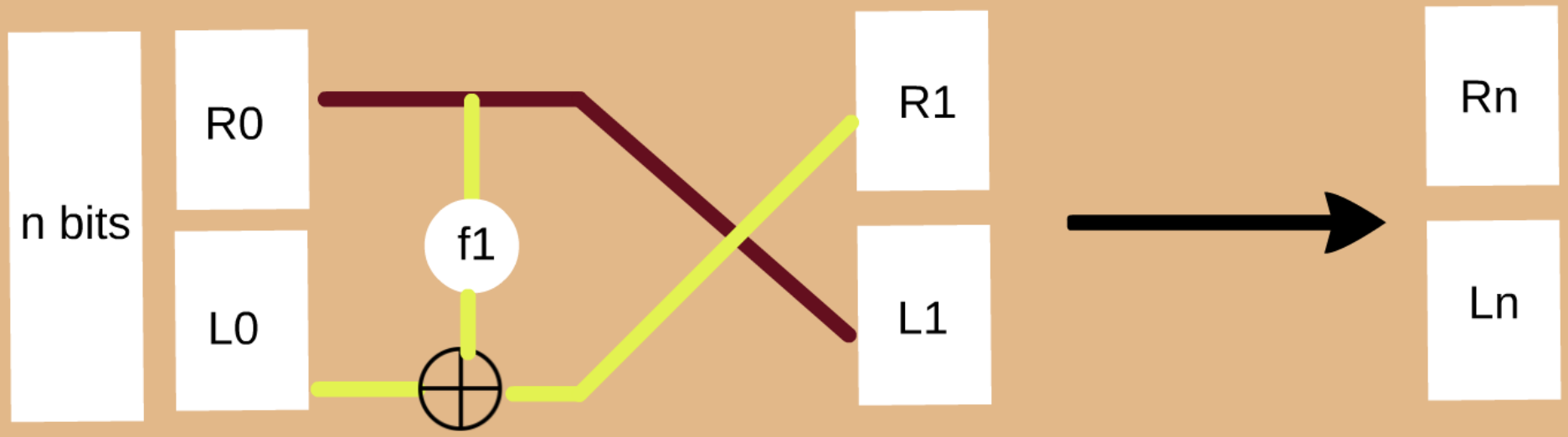
Babikr Elnimah
201204005

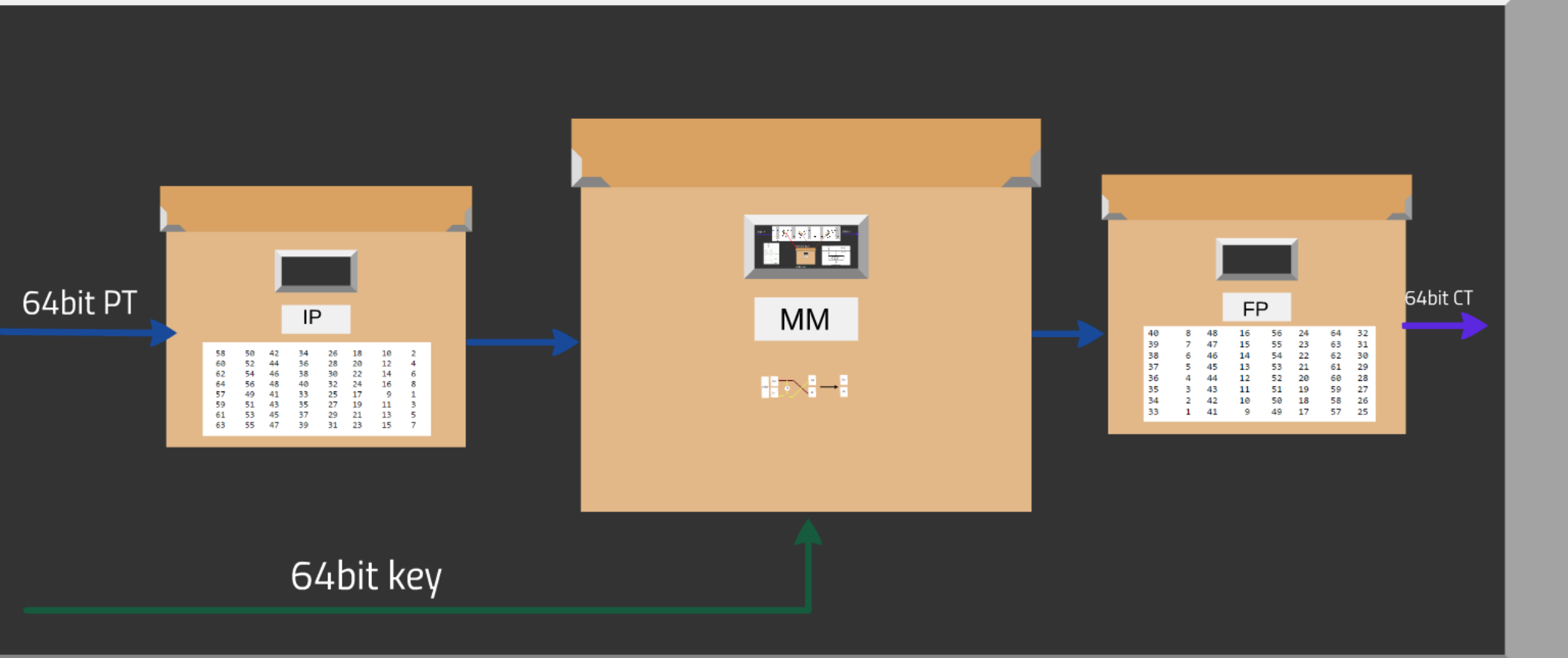
Mohammed Sheikh
201205380

IMPLEMENTATION

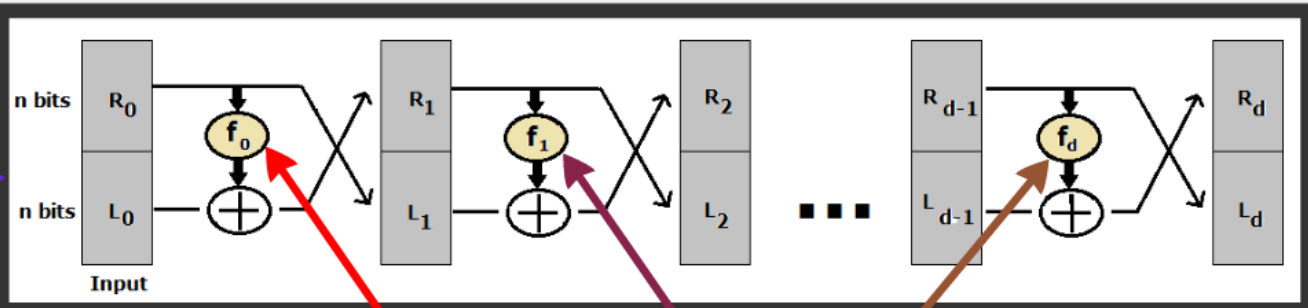

64bit PT
DES
64bit CT
64bit Key


64bit PT
IP
58 50 42 34 26 18 10 2
60 52 44 36 28 20 12 4
62 54 46 38 30 22 14 6
64 56 48 40 32 24 16 8
57 49 41 33 25 17 9 1
59 51 43 35 27 19 11 3
61 53 45 37 29 21 13 5
63 55 47 39 31 23 15 7
MM
FP
40 8 48 16 56 24 64 32
39 7 47 15 55 23 63 31
38 6 46 14 54 22 62 30
37 5 45 13 53 21 61 29
36 4 44 12 52 20 60 28
35 3 43 11 51 19 59 27
34 2 42 10 50 18 58 26
33 1 41 9 49 17 57 25
64bit CT
64bit key

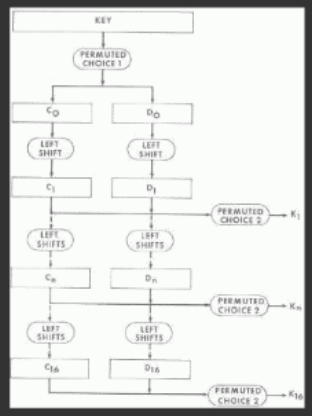



64bit PT
IP
58 50 42 34 26 18 10 2
60 52 44 36 28 20 12 4
62 54 46 38 30 22 14 6
64 56 48 40 32 24 16 8
57 49 41 33 25 17 9 1
59 51 43 35 27 19 11 3
61 53 45 37 29 21 13 5
63 55 47 39 31 23 15 7
MM
FP
40 8 48 16 56 24 64 32
39 7 47 15 55 23 63 31
38 6 46 14 54 22 62 30
37 5 45 13 53 21 61 29
36 4 44 12 52 20 60 28
35 3 43 11 51 19 59 27
34 2 42 10 50 18 58 26
33 1 41 9 49 17 57 25
64bit CT
64bit key

64bit PT

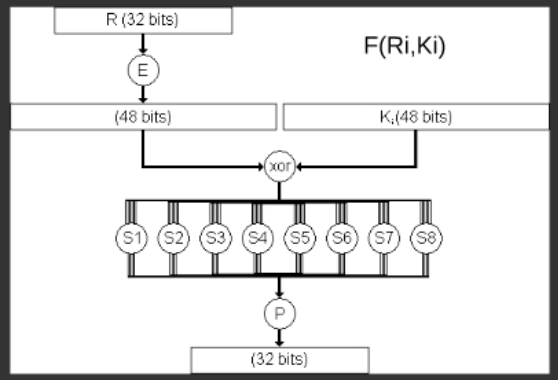


64bit CT

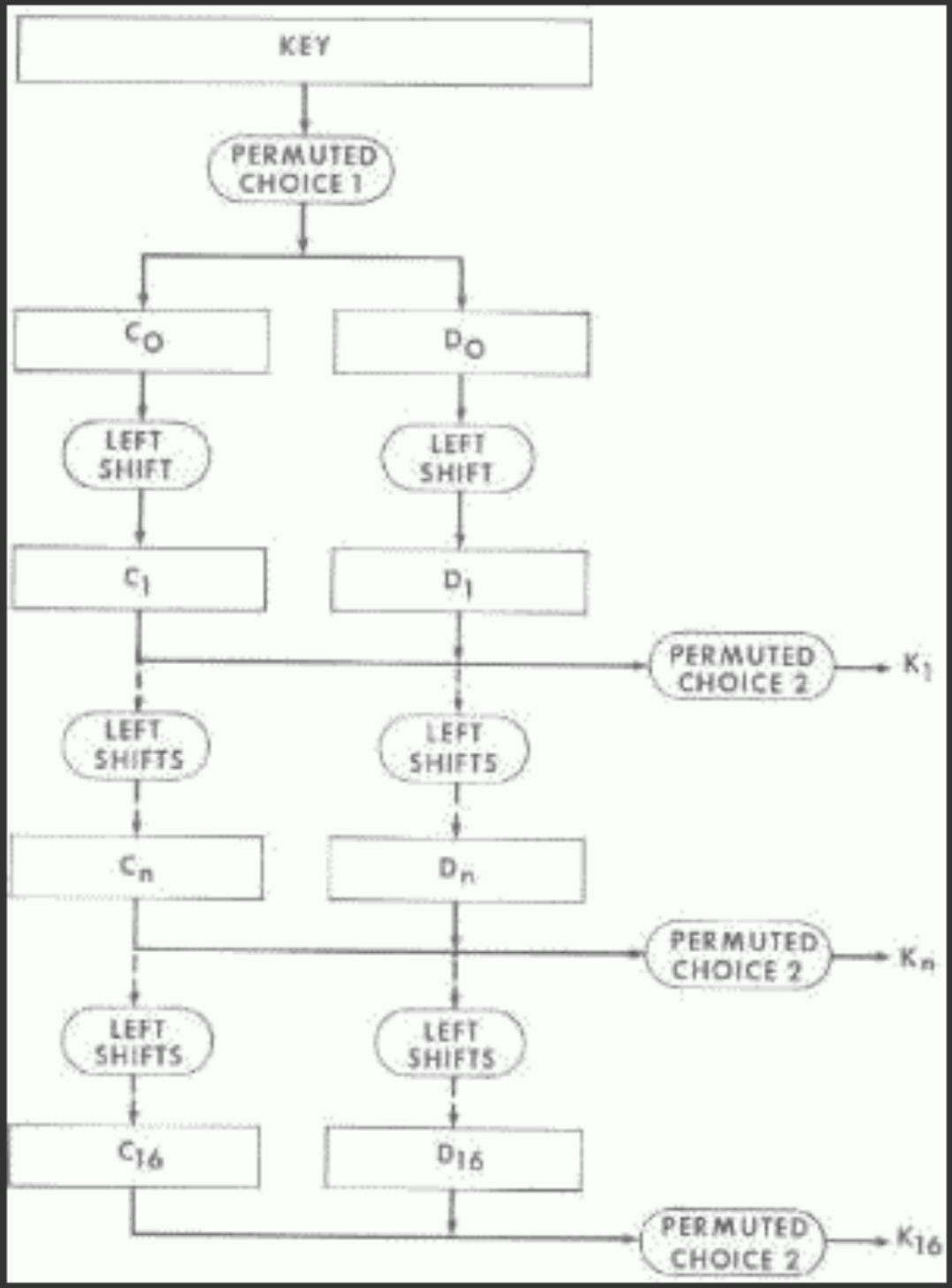


16 48bit keys

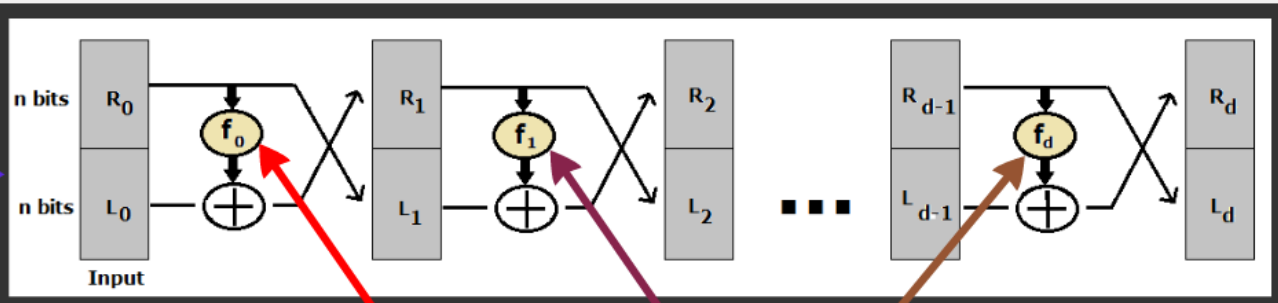
KP



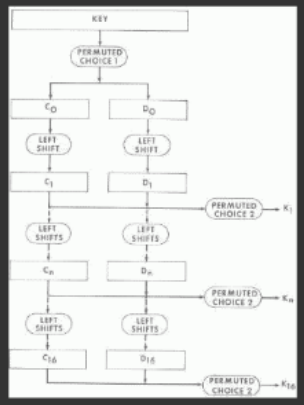
64bit Key


KEY
PERMUTED CHOICE 1
C_0
D_0
LEFT SHIFT
LEFT SHIFT
C_1
D_1
PERMUTED CHOICE 2
K_1
LEFT SHIFTS
LEFT SHIFTS
C_n
D_n
PERMUTED CHOICE 2
K_n
LEFT SHIFTS
LEFT SHIFTS
C_{16}
D_{16}
PERMUTED CHOICE 2
K_{16}

64bit PT



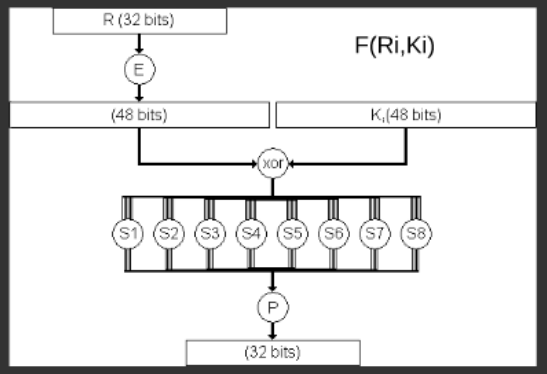
64bit CT

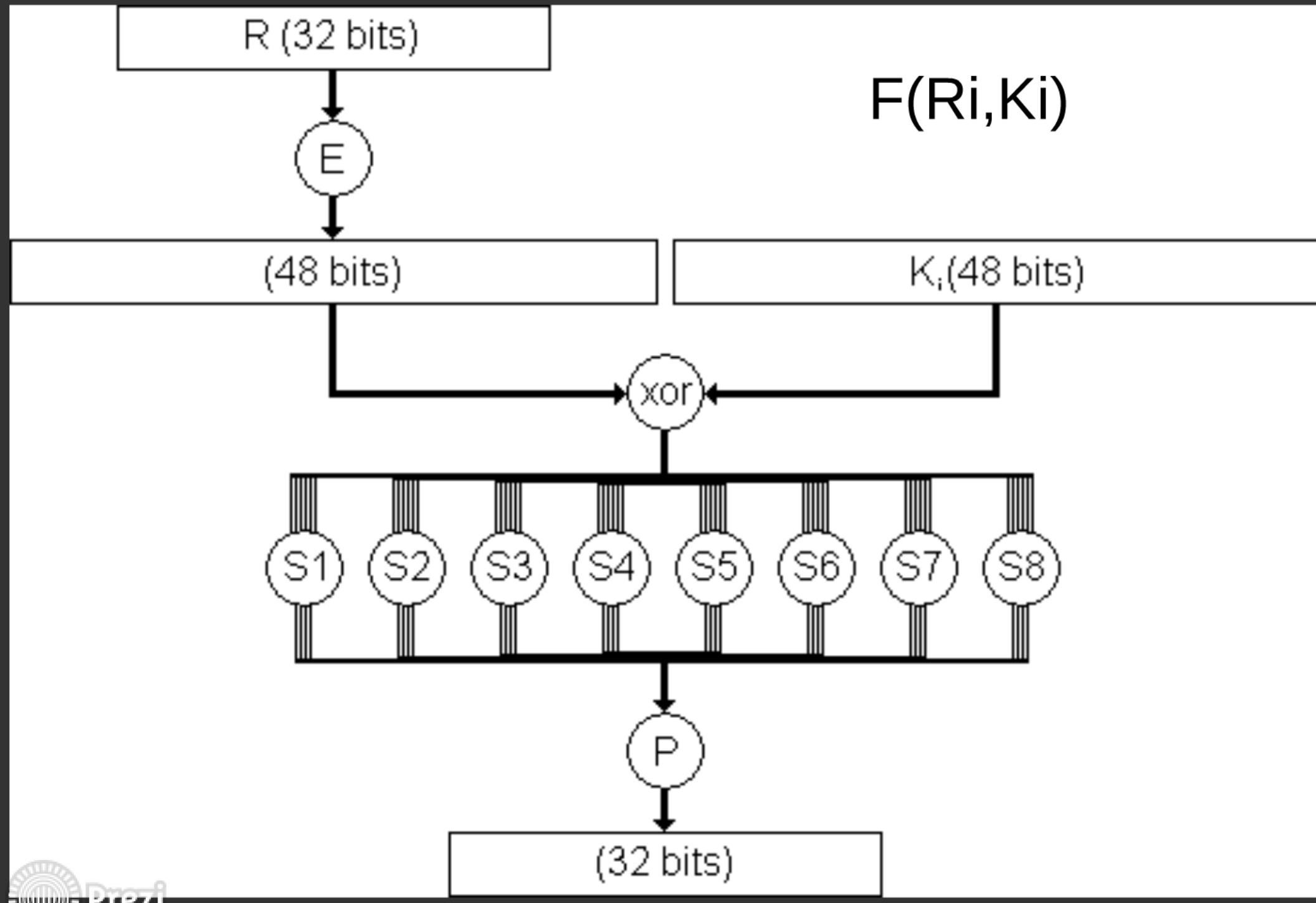


16 48bit keys

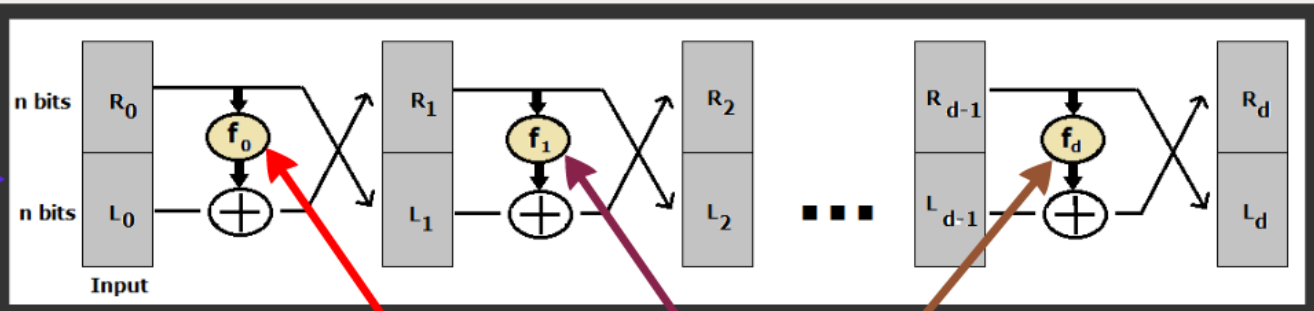
KP

64bit Key

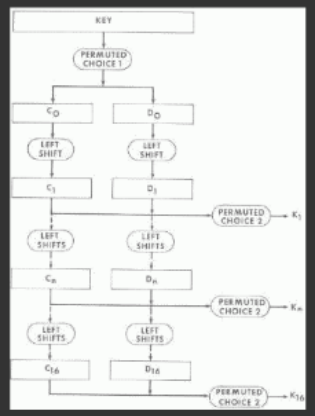



R (32 bits)
F(Ri,Ki)
E
(48 bits)
Ki(48 bits)
xor
S1
S2
S3
S4
S5
S6
S7
S8
P
(32 bits)

64bit PT



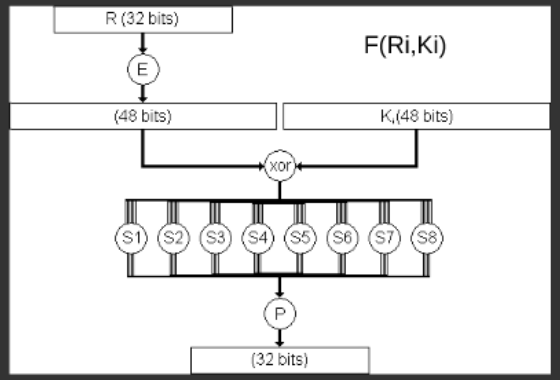
64bit CT



16 48bit keys

KP

64bit Key



A series of challenges were held in order to attempt to break DES

DES was broken on all challenges

Reason: The Fiestel network can not produce pseudo-random CT unless it receives pseudo-random keys

Brute forcing all possible keys is possible to achieve in a small amount of time


CMS
SEO
SOCIAL
in
PLATFORMS
DES v.s AES
-AES solved the brute force problem by giving the choice of 3 key-sizes (all larger than 56).
-AES does not use Fiestel networks

The DES Encryption Algorithm

Ahmed Ibrahim
201204361

Babikr Elnimah
201204005

Mohammed Sheikh
201205380