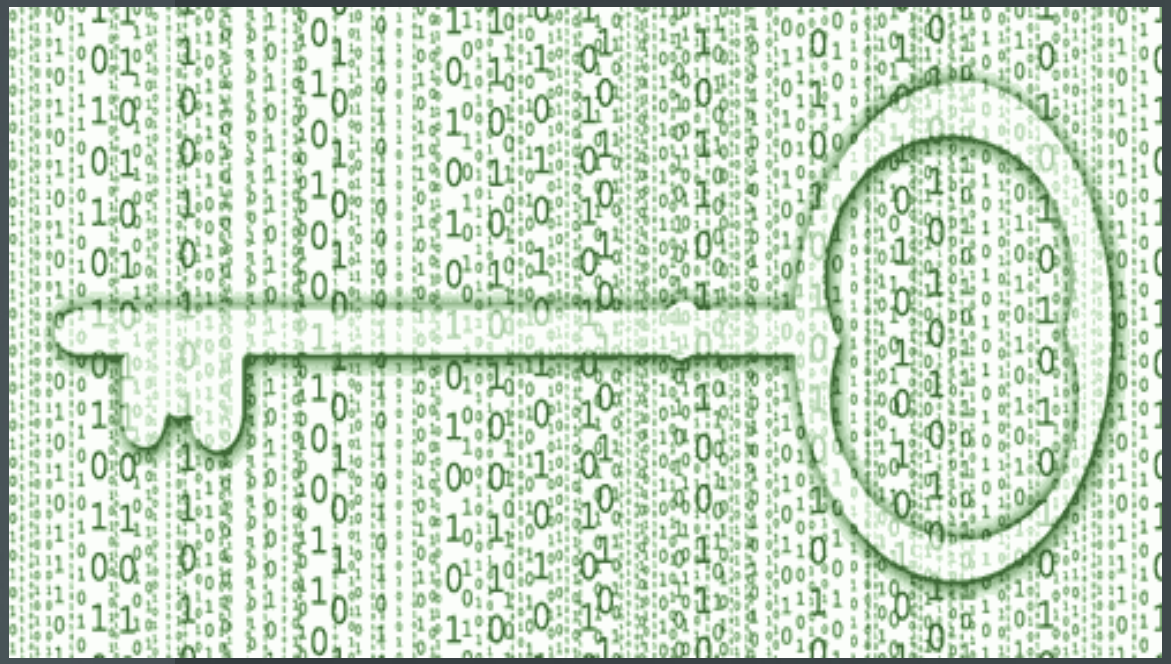
# Differential Cryptanalysis of Simplified DES

- UCSB CS290g




- Anjini Shukla
- Manish Goyal

# Outline

- What is Cryptanalysis
- Differential Cryptanalysis(DC)
- Simplified DES (SDES)
- DC of SDES
- Capturing the Key
- Conclusion

# Cryptanalysis

*What is Cryptanalysis*

It is the analysis of a cryptographic system to find the plain-text.
Some information is required to perform the cryptanalysis.

*Differential Cryptanalysis*

Study of the impact of difference in inputs on the difference in outputs

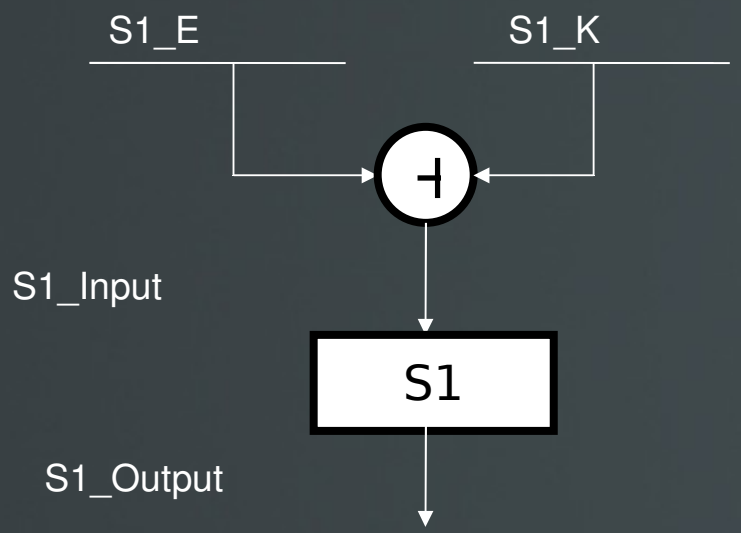
- DES does not exhibit pseudo randomness in differential output
- Key does not have any influence on the differential  ouput

`

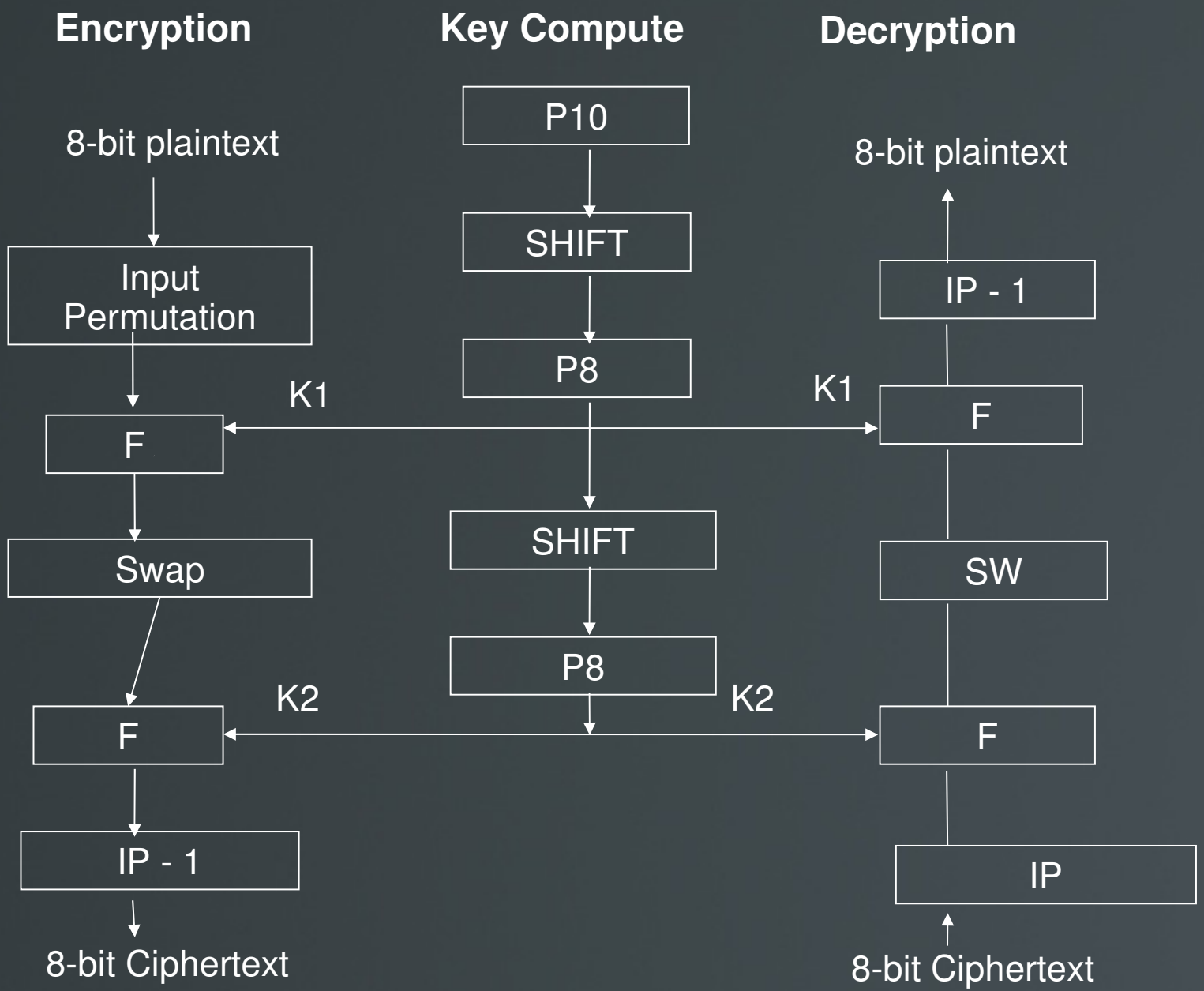
# Differential Cryptanalysis

The Differential Input to the S-box remains same regardless of what the Key is

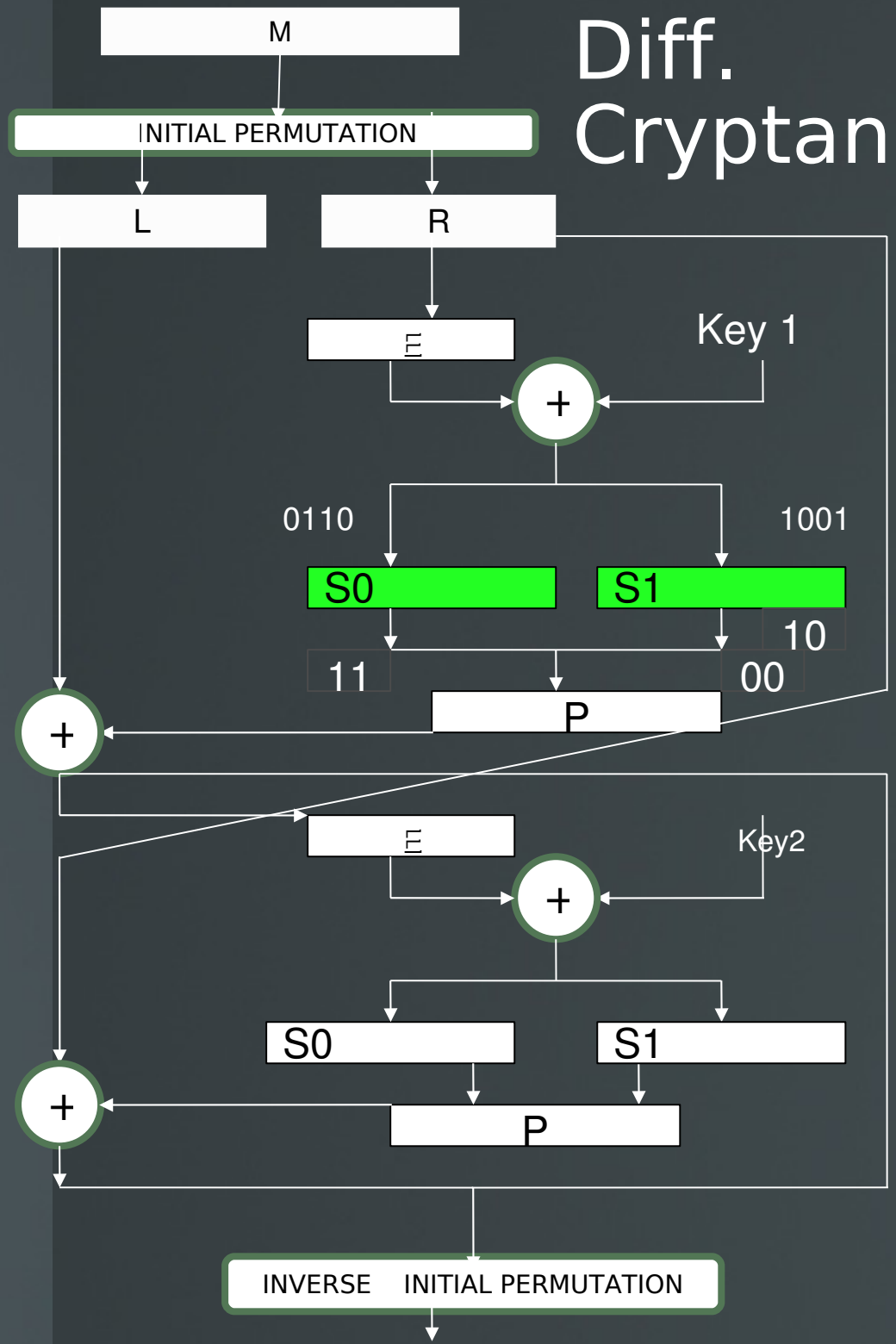
S1'_Input = S1_Input ⊕ S1*_Input
= (S1_E ⊕ S1_K) ⊕ (S1*_E ⊕ S1_K)
= S1_E ⊕ S1*_E
= S1'_E



# Simplified DES



# Diff. Cryptanal



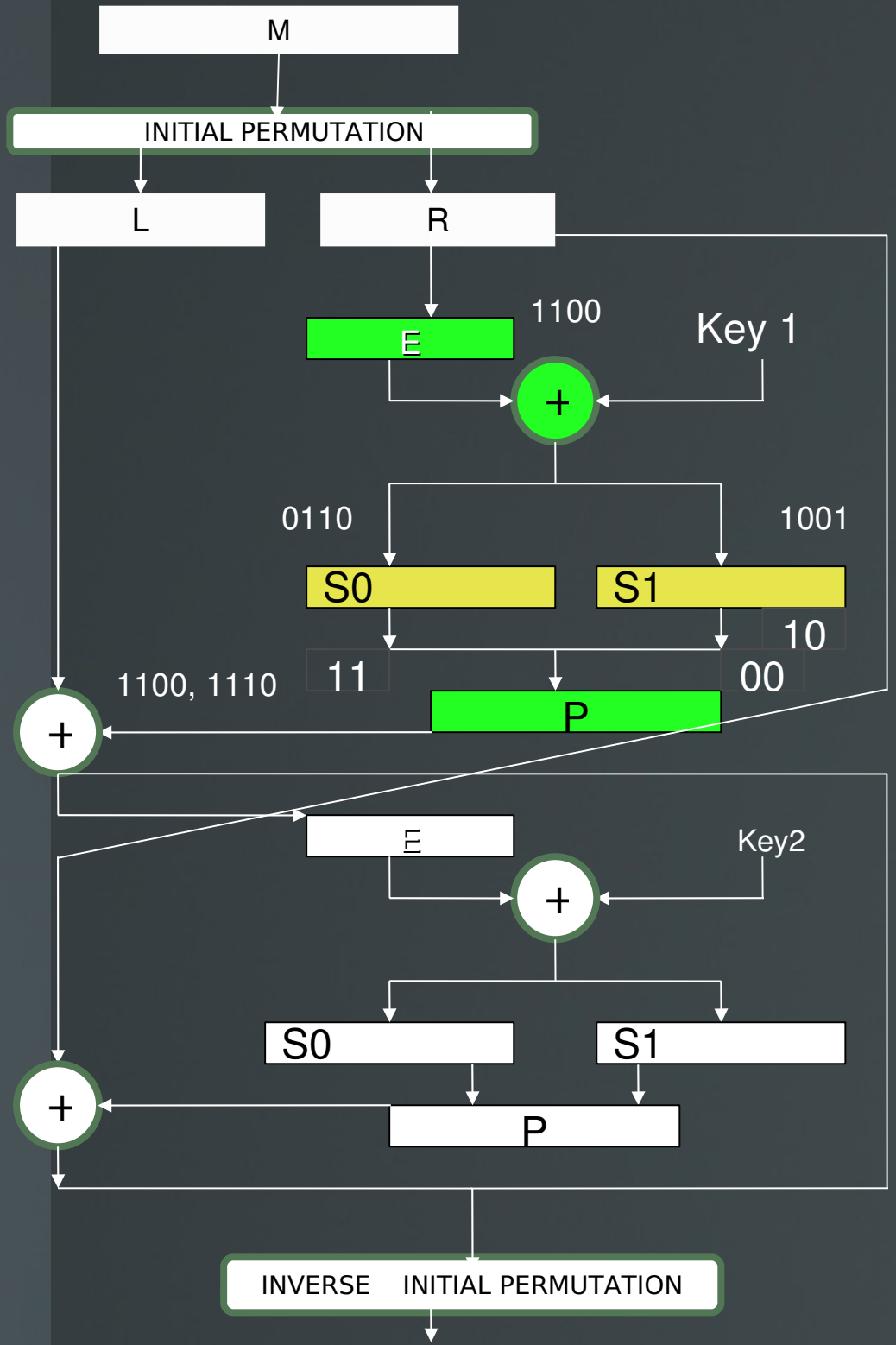

S0

| DX/DY | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 16 | 0 | 0 | 0 |
| 1 | 0 | 2 | 10 | 4 |
| 2 | 0 | 10 | 6 | 0 |
| 3 | 2 | 4 | 0 | 10 |
| 4 | 2 | 6 | 6 | 2 |
| 5 | 10 | 0 | 4 | 2 |
| 6 | 0 | 2 | 2 | 12 |
| 7 | 4 | 10 | 2 | 0 |
| 8 | 2 | 4 | 8 | 2 |
| 9 | 8 | 2 | 2 | 4 |
| 10 | 4 | 2 | 2 | 8 |
| 11 | 2 | 8 | 4 | 2 |
| 12 | 8 | 2 | 2 | 4 |
| 13 | 1 | 4 | 8 | 2 |
| 14 | 1 | 8 | 4 | 2 |
| 15 | 4 | 2 | 2 | 8 |

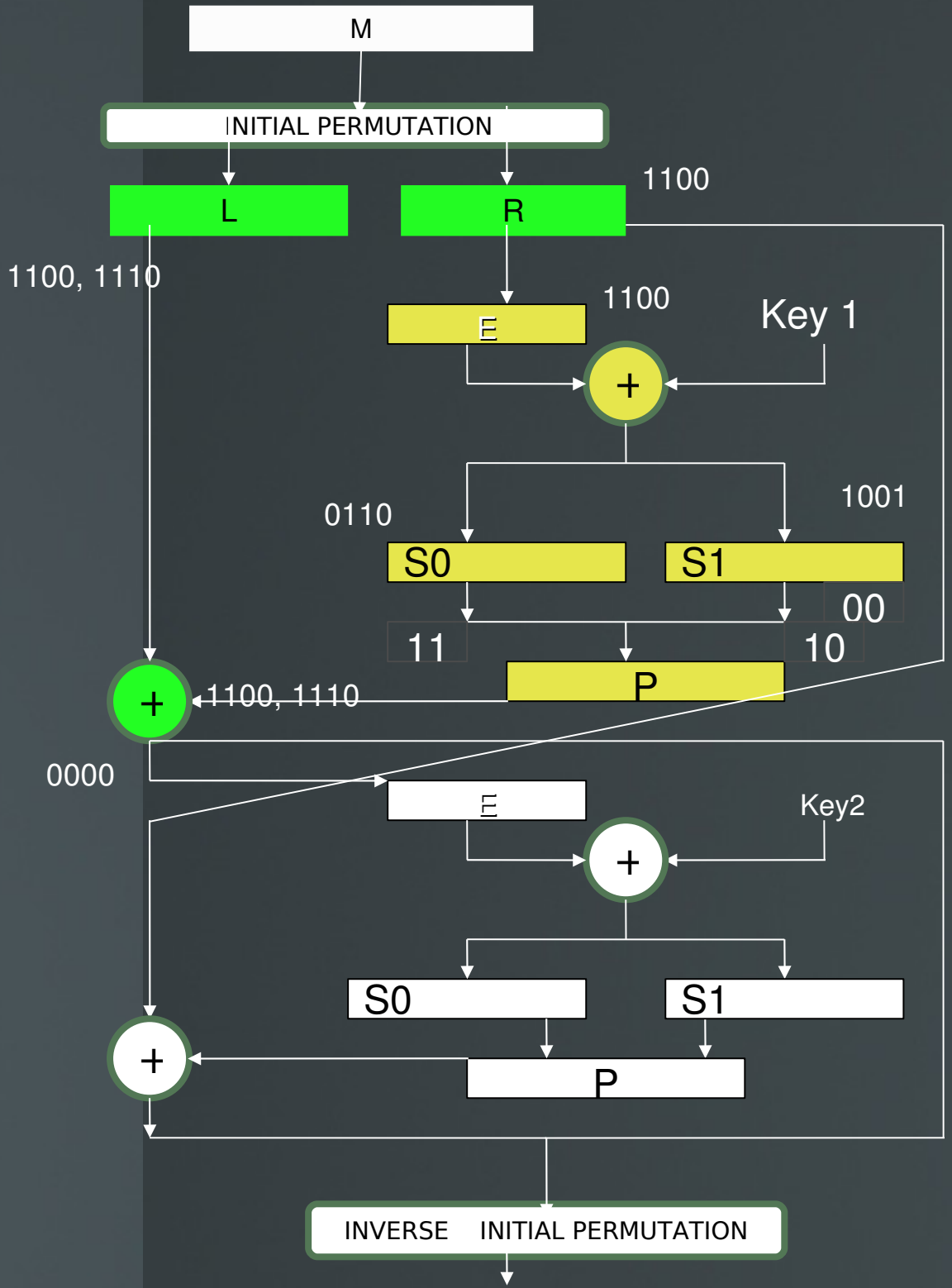
S1

| DX/DY | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 16 | 0 | 0 | 0 |
| 1 | 2 | 8 | 2 | 4 |
| 2 | 0 | 6 | 4 | 6 |
| 3 | 4 | 2 | 8 | 2 |
| 4 | 2 | 0 | 10 | 4 |
| 5 | 2 | 4 | 2 | 8 |
| 6 | 0 | 10 | 0 | 6 |
| 7 | 8 | 2 | 4 | 2 |
| 8 | 4 | 6 | 0 | 6 |
| 9 | 8 | 2 | 4 | 2 |
| 10 | 2 | 0 | 10 | 4 |
| 11 | 0 | 6 | 4 | 6 |
| 12 | 0 | 6 | 4 | 6 |
| 13 | 6 | 0 | 6 | 4 |
| 14 | 10 | 4 | 2 | 0 |
| 15 | 0 | 8 | 2 | 4 |

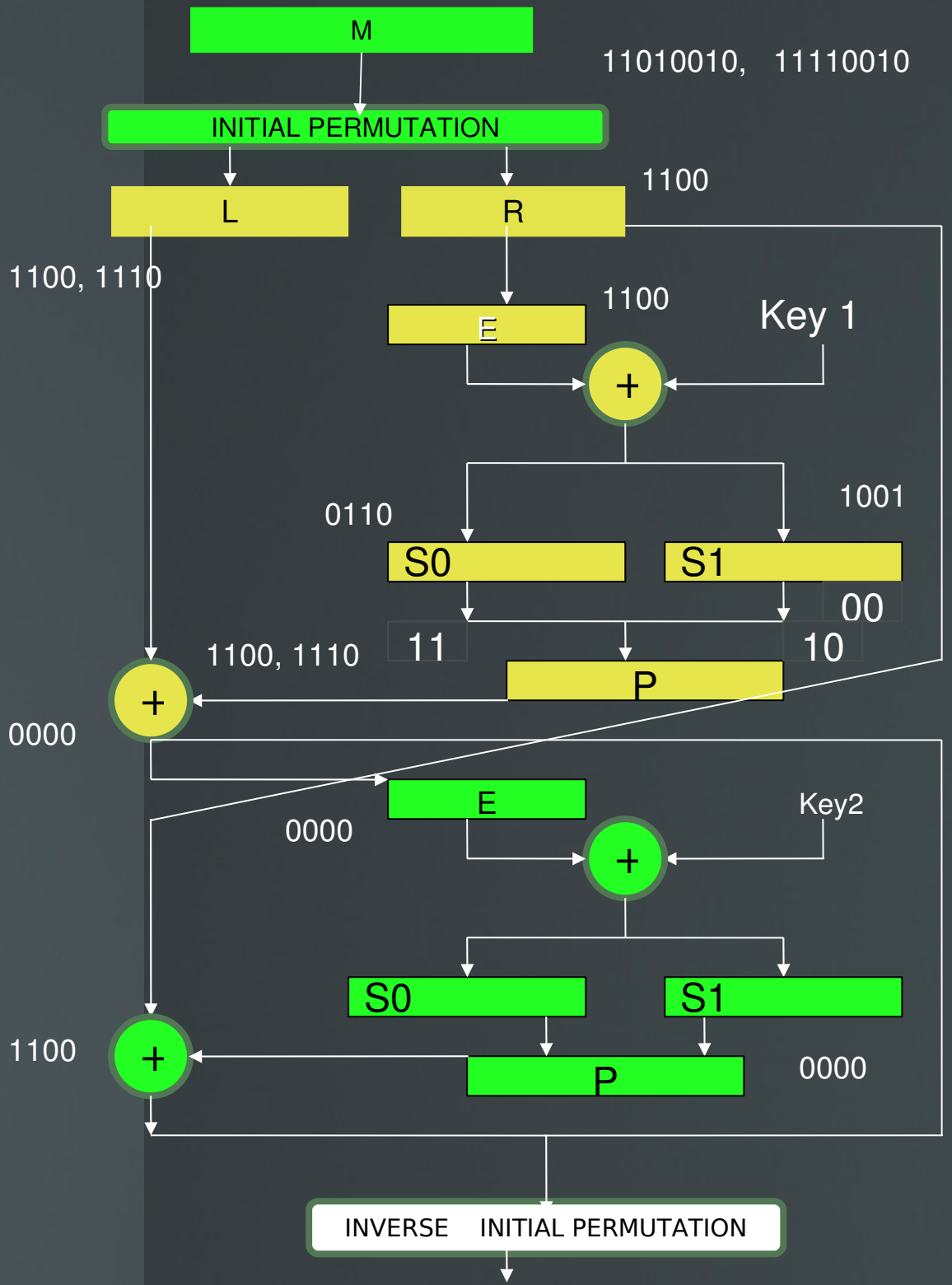
# Differential Cryptanalysis

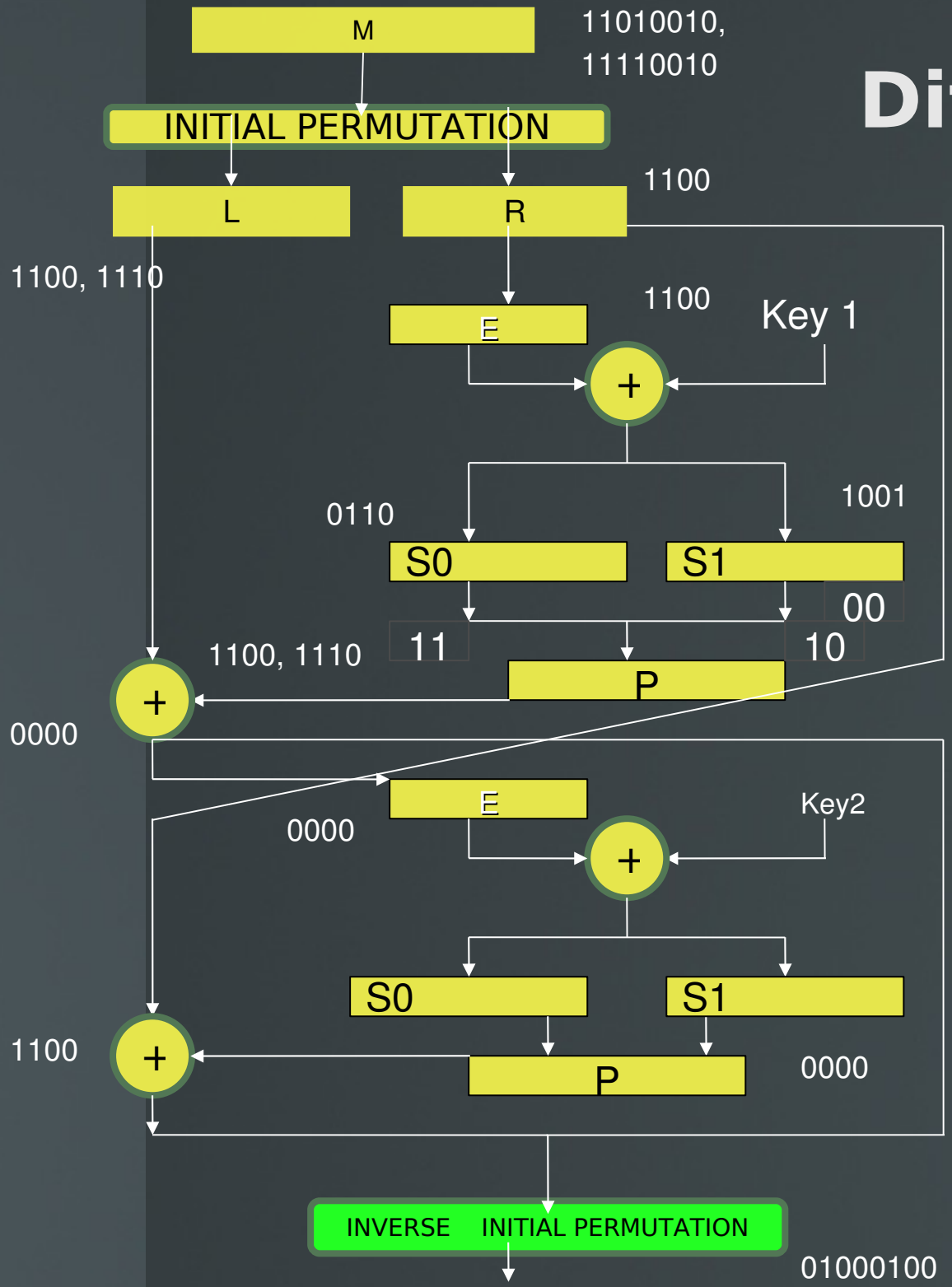


# Differential Cryptanalysis



# Differential Cryptanalysis






# Diff. Cryptanalysis

**del_C = 01000100**
**del_P = 11010010, 11110010**
**Calculate a Random P**

**P_1 = P ⊕ del_P1**
**P_2 = P ⊕ del_P2**

**C =Encrypt( P, K)**
**C_1 =Encrypt( P_1, K)**
**C_2 =Encrypt( P_2, K)**

**del__C1 = C_1 ⊕ C**
**del__C2 = C_2 ⊕ C**

**If del_C1 or del_C2 is = del_C characteristic has occurred, if not repeat the steps with different del_X and del_Y**

# Determining the Key

**Finding K1**

**- Select the Value of P that generated the differential characteristic**

**- Find the output of Expansion function**

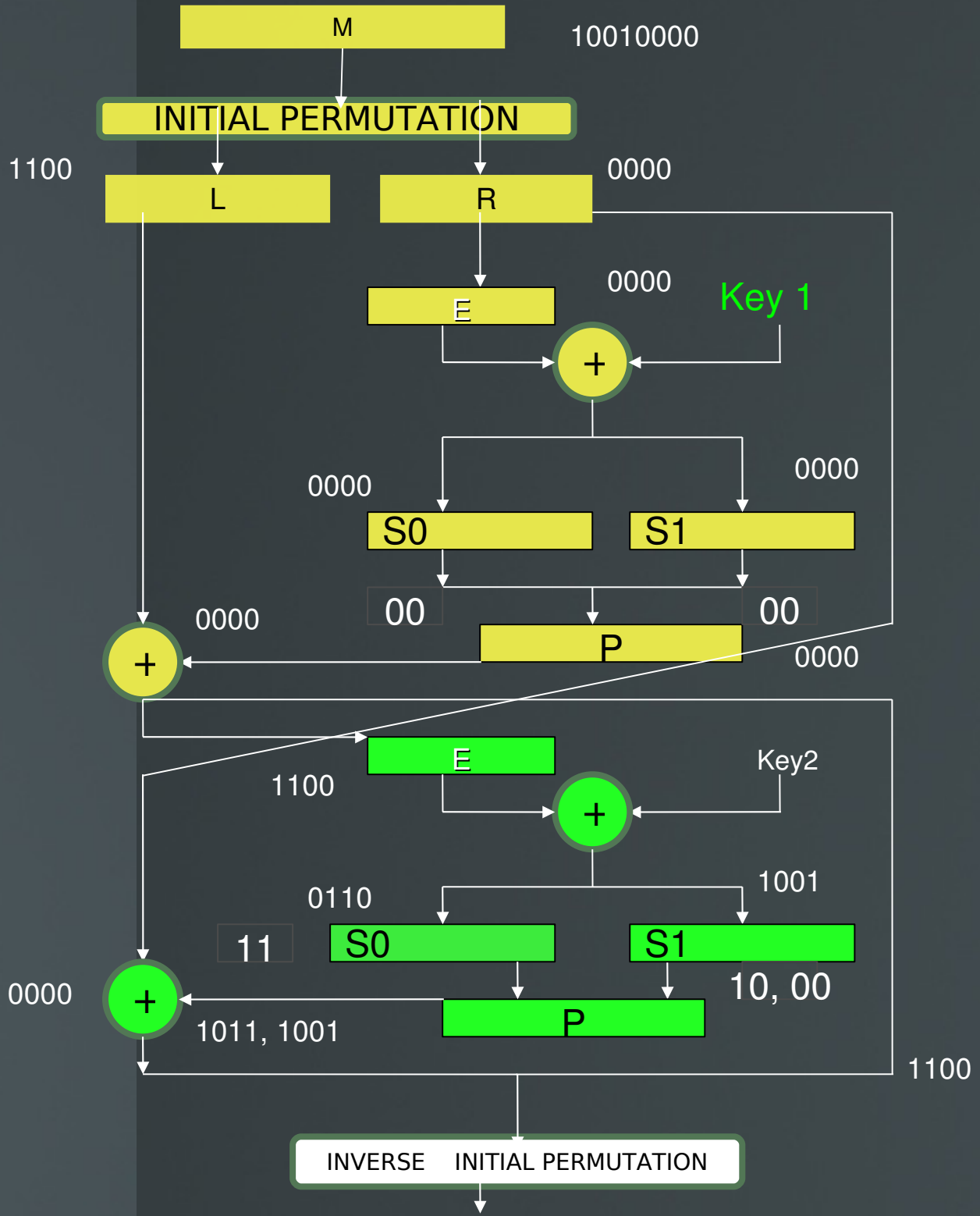
**- Identify the set of X values(X0, X1) that satisfy del_X and del_Y for  both S0 and S1.**

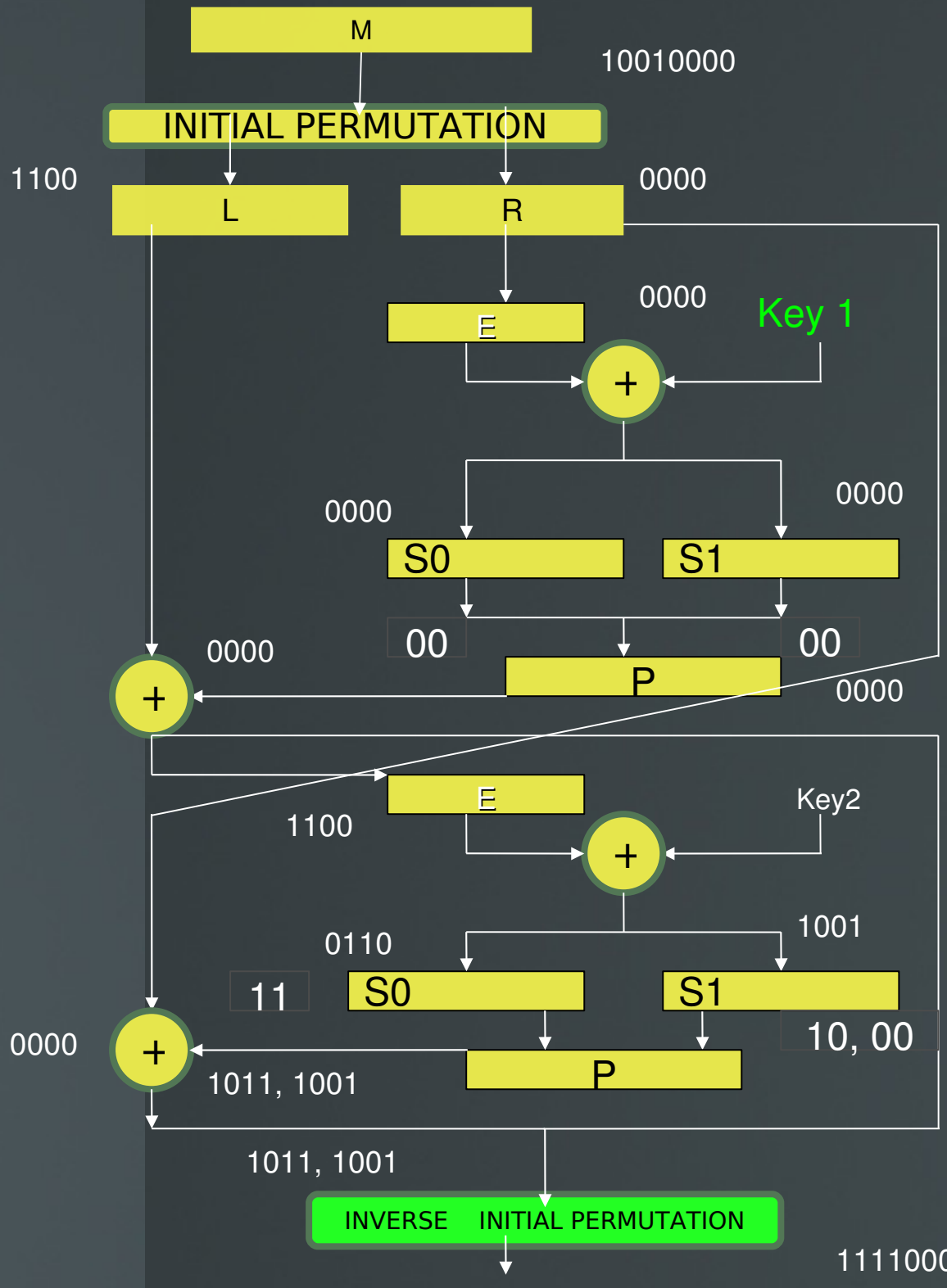
**- Left Half of K1 is El ⊕ X0, where El is the Left half of E, and X0 is the input to S-box 0**

**- Right Half of K1 is ER ⊕ X1, where Er is the right half of E, and X1 is the input to S-box 1.**

**- Iterate the above steps to find a Unique value of K1**

# Finding K2


M
10010000
INITIAL PERMUTATION
1100
L
R
0000
E
0000
Key 1
+
0000
0000
S0
S1
00
00
P
0000
+
0000
E
Key2
1100
+
1001
0110
11
S0
S1
10, 00
0000
+
P
1011, 1001
1100
INVERSE INITIAL PERMUTATION




**del_C = 11110001, 11010001**
**del_P = 10010000**
**Calculate a Random P**

**P_1 = P ⊕ del_P1**

**C =Encrypt( P, K)**
**C_1 =Encrypt( P_1, K)**

**del__C1 = C_1 ⊕ C**

**If del_C1 = del_C characteristic has occurred, if not repeat the steps with different del_X and del_Y**

# Determining the Key

## Finding K2

- Use Key1 to calculate the output of the first round and find output of Expansion function for round 2
- Identify the set of X values(X0, X1) that satisfy del_X and del_Y for  both S0 and S1.
- Left Half of K2 is El ⊕ X0, where El = Left half of E
- Right Half of K2 is ER ⊕ X1, where Er = Right half of E
- Iterate the above steps to find a Unique value of K2

# Key Captured...!!!

$$Key1 = K1_1, K1_2, K1_3, K1_4, K1_5, K1_6, K1_7, K1_8$$

$$Key2 = K2_1, K2_2, K2_3, K2_4, K2_5, K2_6, K2_7, K2_8$$

$$Key\ is = K1_1\ K2_6\ K1_6 K1_4 K2_4\ K1_8\ K1_2\ K1_5\ K1_3\ K1_7$$

# Conclusion

**This project demonstrates the successful use of differential cryptanalysis technique on Simplified DES.**

# Questions...!!