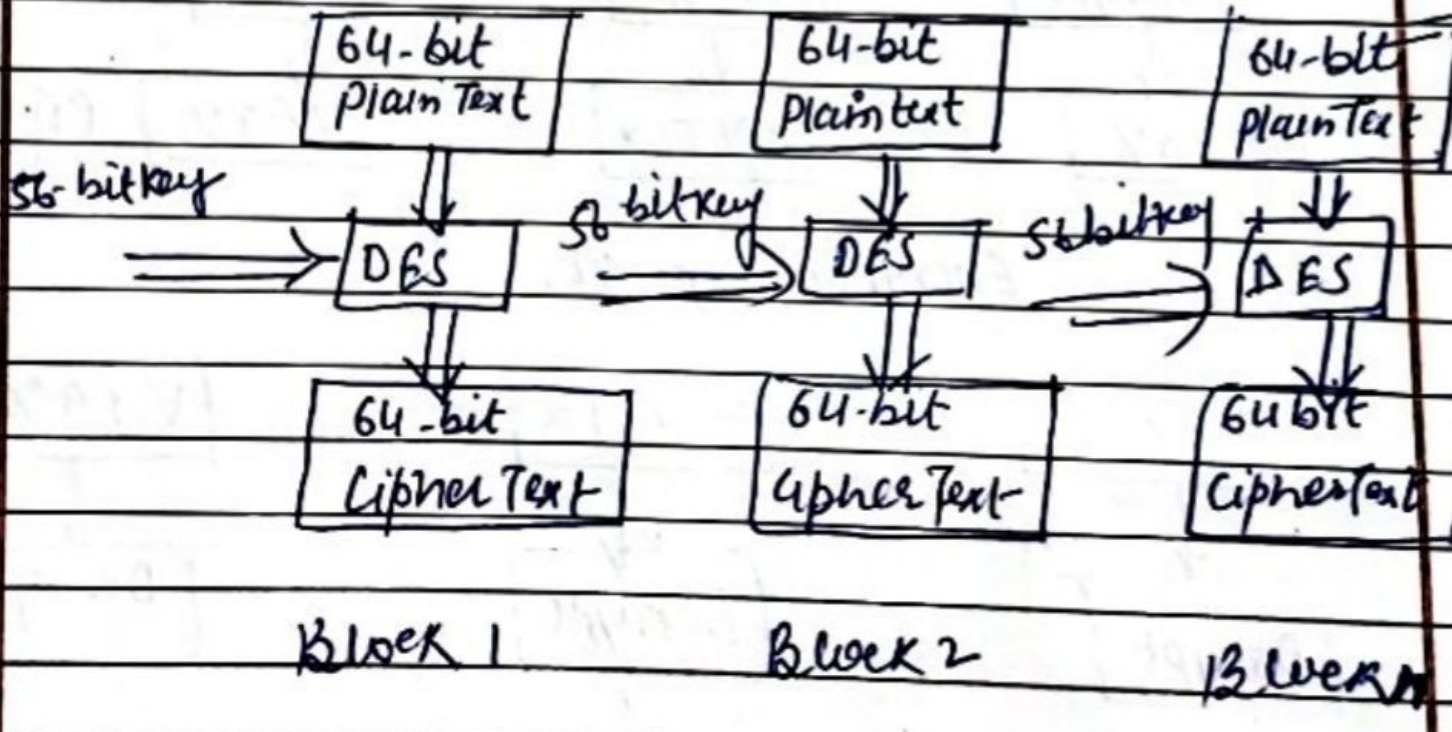
2.1 Data Encryption standard (DES)

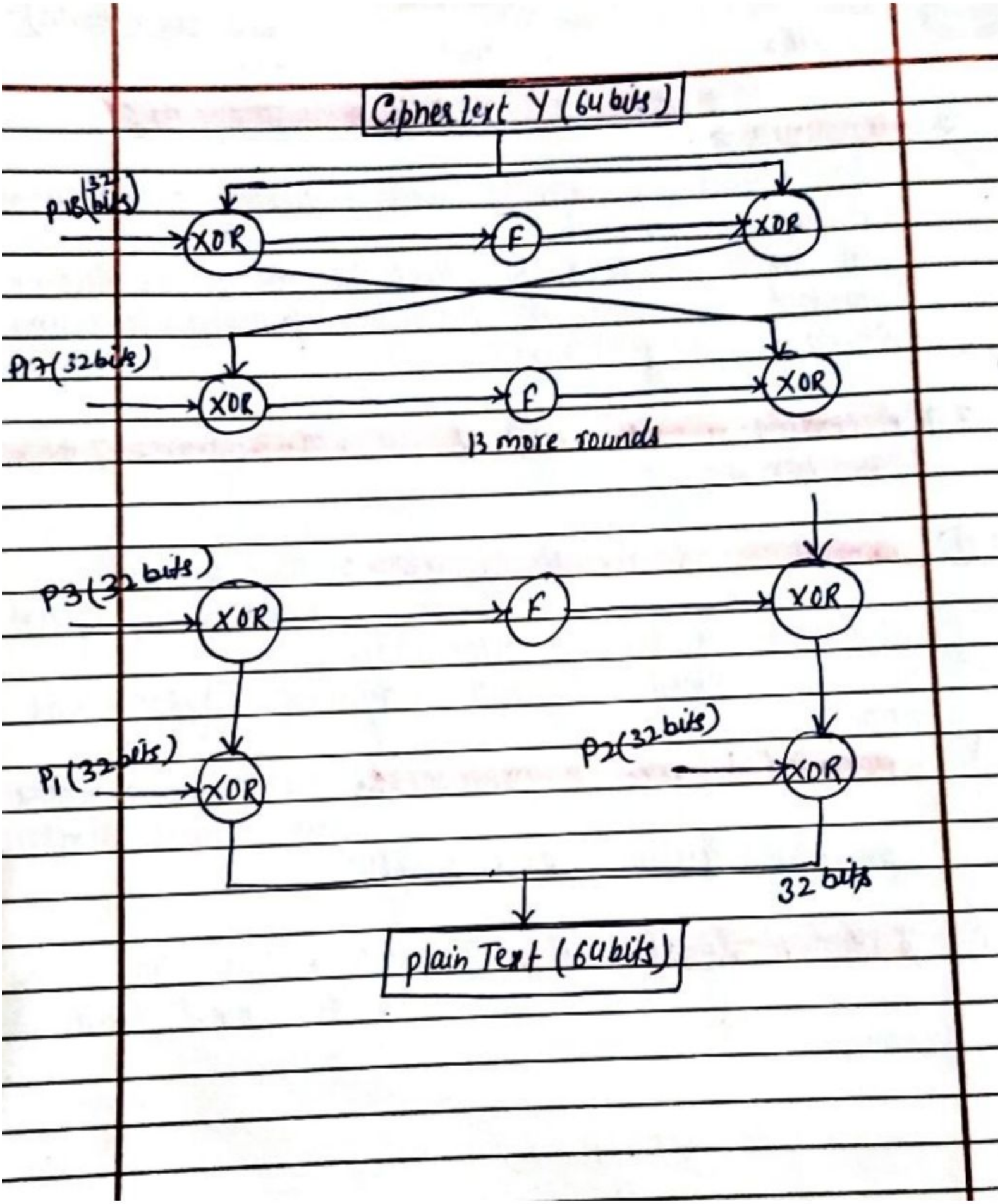
Data Encryption standard (DES) is also called as the data encryption algorithm
DES is generally used in the ECB, CBC or the CFB mode.

The Oregin of DES go back to 1972 when in the US the National bureau of standard now known as the National Istitute of standard and Technology

2.2 Structure of (DES) :-

How Does it works




Ciphertext Y (64 bits)
P18(32 bits)
XOR
F
XOR
P17(32 bits)
XOR
F
XOR
13 more rounds
P3(32 bits)
XOR
F
XOR
P2(32 bits)
P1(32 bits)
XOR
XOR
32 bits
plain Text (64 bits)

2.7 Bent function

2.7.1 **Definition** :- A bent function is a special types of boolean function. Bent function are named so because they present maximum possible distance from all linear and affine function

2.7.2 **Properties**

⇒ A bent function can be defined as a boolean function

$$f = Z_2^n \to Z_2$$

⇒ $f(x_1, x_2) = x_1 x_2$ and $G(x_1, x_2, x_3, x_4) = x_1 x_2 \oplus x_3 x_4$ are the simplest example of bent function.

⇒ The sequence of value $(-1)^{f(x)}$ with $x \in Z_2^n$ is called a bent sequence.

⇒ Bent function and bent sequence have equivalent properties.

2.4.4 S-Box Design

① **Balanced Component function** :-

The component function of substitution box be balanced in the manner that message bits.

Purchase the Notes

100₹

Per semester
(All subjects)

Notes (Hand written) ✅
Most Questions ✅

All Branches

Min 100%
amount will go
into charity ⭐

For specific
Subject - 50₹

UPI ID -
sahilkagyan337@ybl

Er Sahil ka Gyan

🔥 Steps for getting NOTES and Most Questions -

👉Do payment using UPI ID -

sahilkagyan337@ybl

👉Take screenshot of transaction and send me on Email -

ersahildrive@gmail.com

Then finally access all Notes and most questions 🔥

Scan & Pay Using PhonePe App

SAHIL KHAN