Lecture 6 DES Key Schedule and Decryption :-
In last lecture we have learned about DES, Feistel networks which contains S-Box Expansion Box and P Box.

Now there are certain important things we are still left with :-

1. Key Schedule
2. DES Decryption
3. DES Security
4. DES alternatives.

DES is 56 bit cipher or 64 bit?
Actually **PC-1** => Input is 64 bit but output is 56 bit. Question why ? Professor doesn't know. Actually DES PC-1 internally remove bit 8,16,24,32,40,48,56,64 and as per DES these are used as parity bit.
So whatever you put in these 8 bits is ignored.

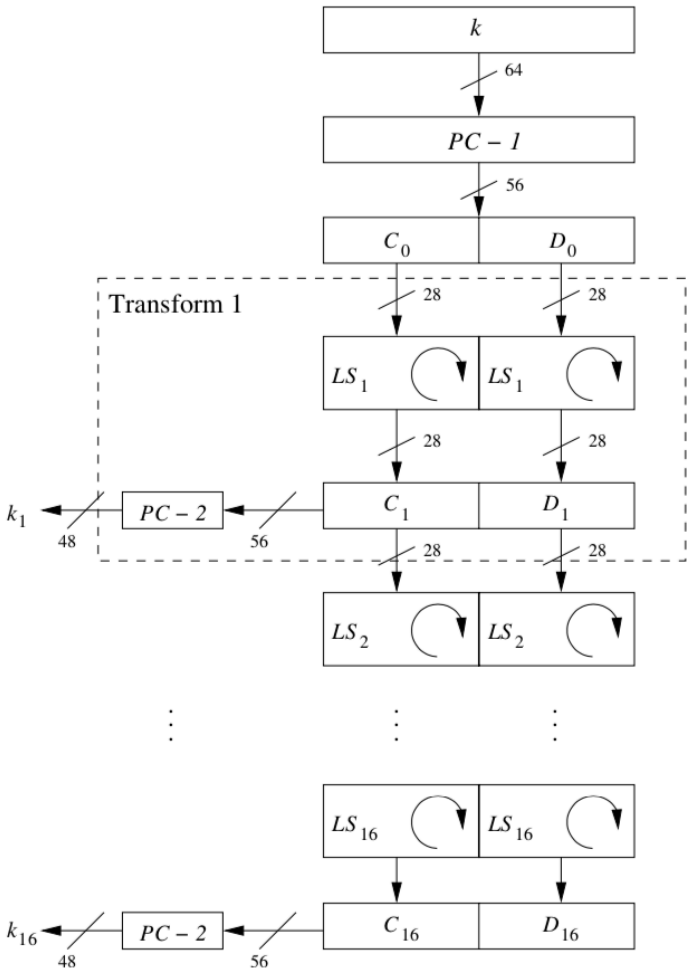


Fig. 3.14 Key schedule for DES encryption

DES is actually 56 bit.

the parity bits are stripped in the initial *PC* – 1 permutation.

Key schedule or Sub Key =>
In the next step, 56 bit key is split into 2 halves, C0 and D0 and then feed into LSi.

2. **LSi ->**

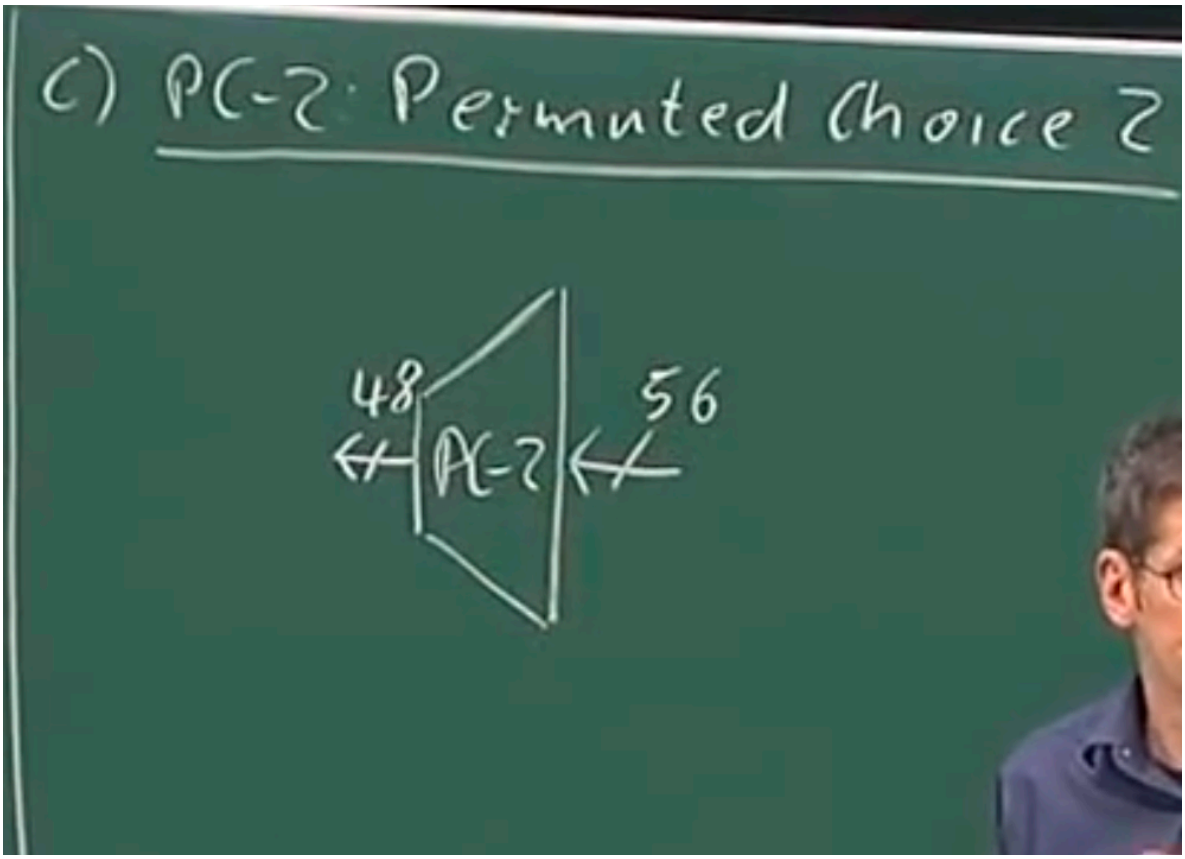
Left Shift from 1 to 16 for each round. (It is actually left rotate) Now question is how many bits shift ?
1 position shift for I=1,2,9,16
2 position shift for all other.

Question :- Why 1 position shift for some and 2 for others?
Question :- Key schedule is within one block what about key generation for next block.
Total number of bit positions shifted is following :-
4 round shift by 1 and 12 round shift by 2 position => 28 shifts > which is the size of C0 and D0.

As you can see we have C0 to C16 which is 17 iterations so we can conclude that C16 is same as C0 as we have rotated all 28 bits.

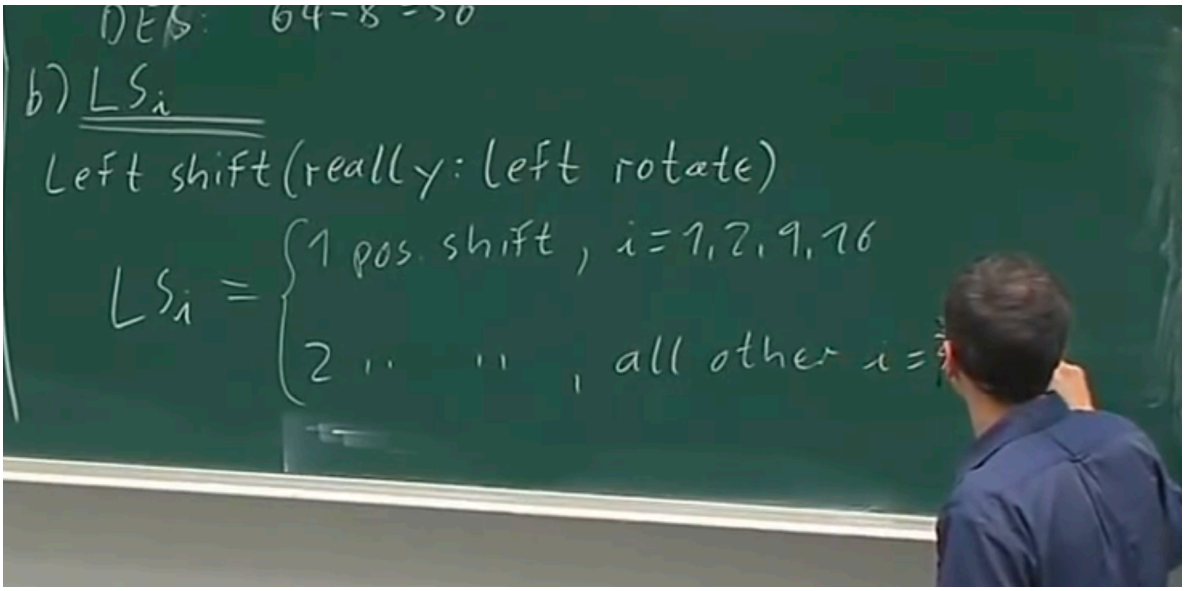
So C0 = C16 and D0 = D16, this is needed in Decryption.

PC-2 —>

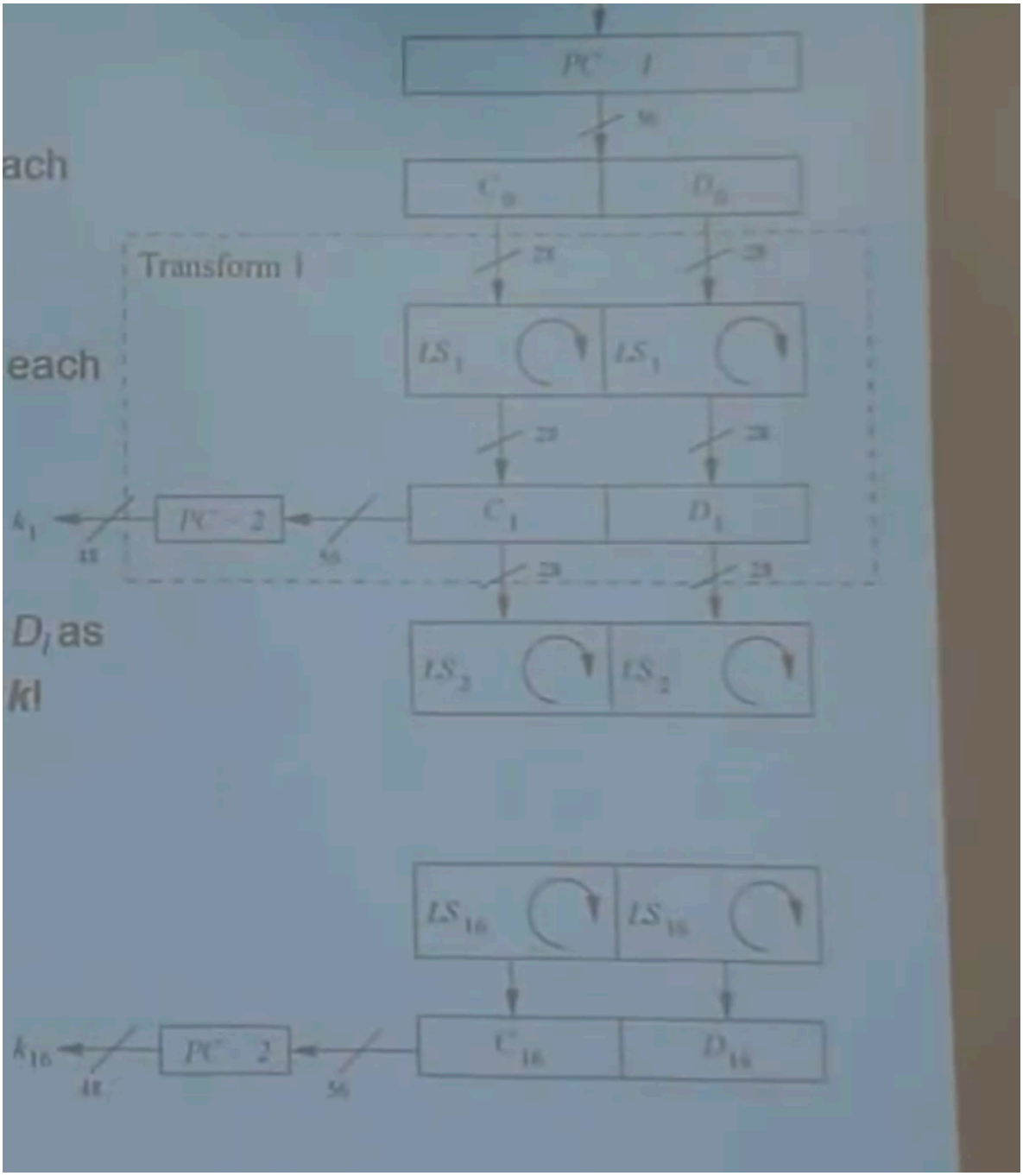


Here also 8 bits are dropped. The remaining bits are permuted. In PC-2 it is only permutation, there are no maths/Grates etc. only cross wiring.and cross wiring is very specific to each round.

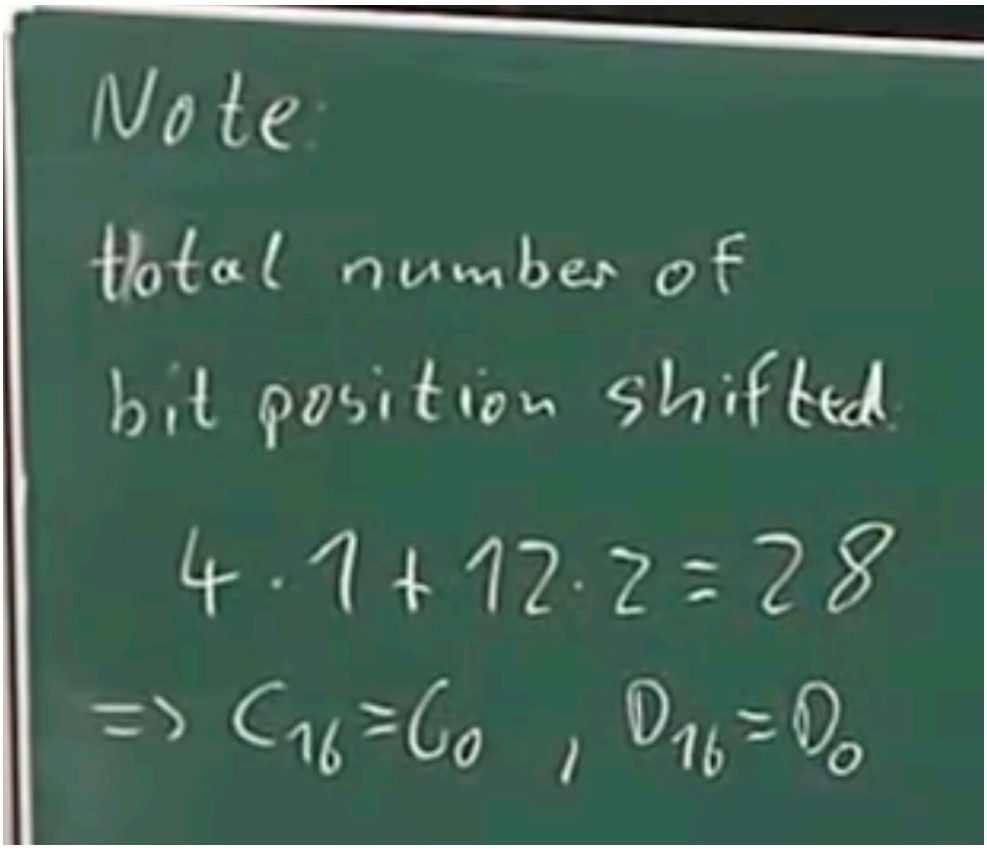
For F function, this 48 bit key is done by PC2.



For rounds i=1,2,9,16 => left rotate for one bit and others left rotate for 2 bits.



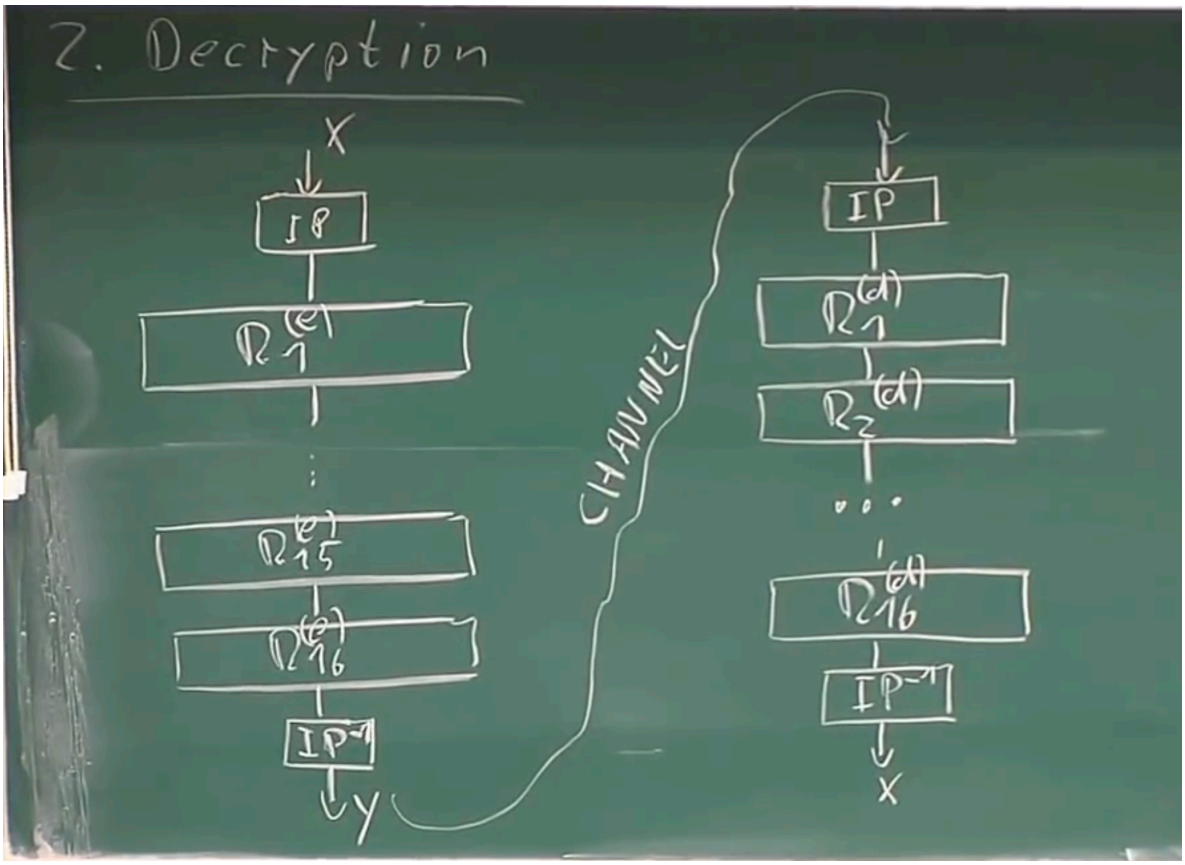
Rotation happens only in C0 and D0 ie bits are not rotated between both of them as there is a hard boundary.



More information on PC2 :-
Output of PC2 is the SubKey for F function. In this method 8 bits are dropped ie they are not connected through.

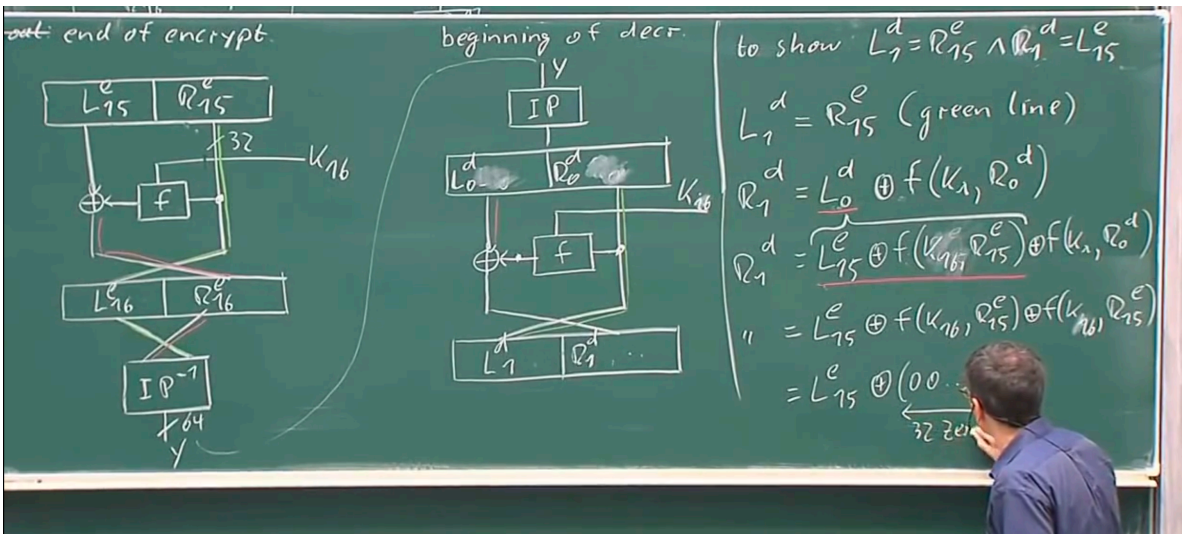
2. **Decryption :-**

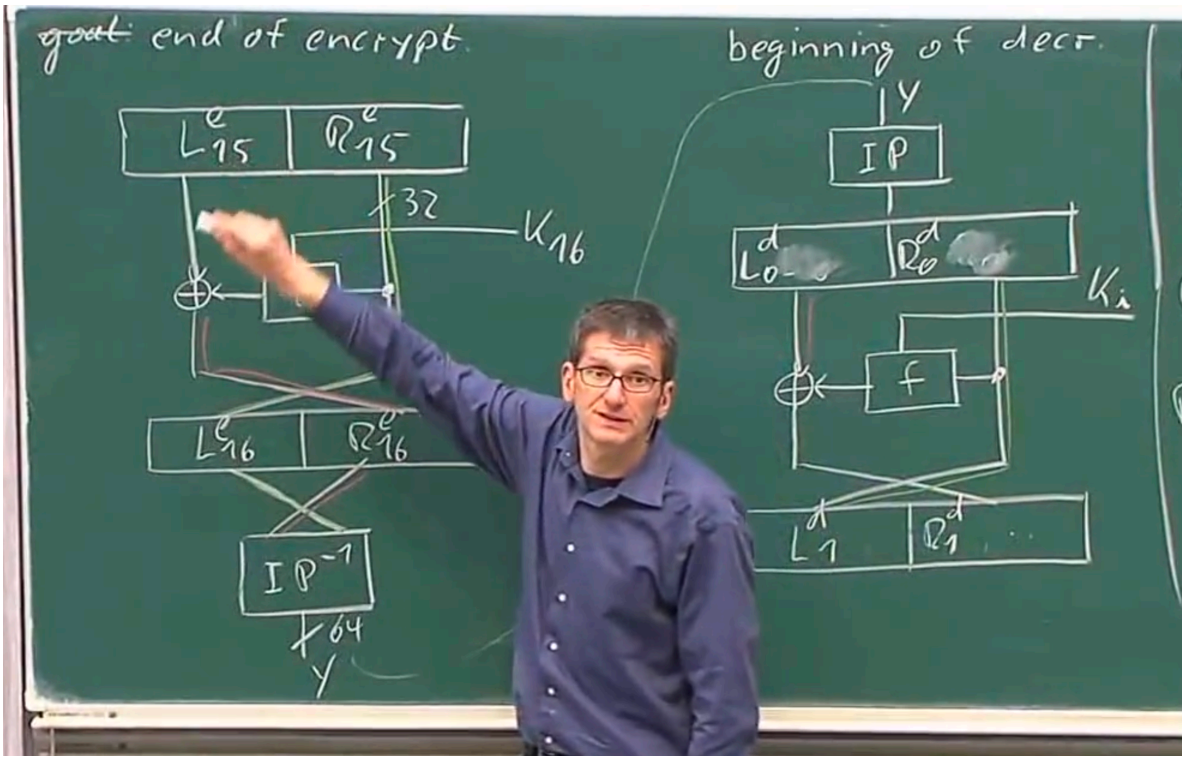
Recalling Encryption :-



So each decryption round is inverse of encryption round. Ie r1 decryption is inverse of r16 encryption.decryption goes down and encryption goes up.

Goal is to show that r1 decryption will undo r16 encryption and so on.
So as we thought R1 decryption will take key of k16 reason is key for R16 encryption takes key of k16.



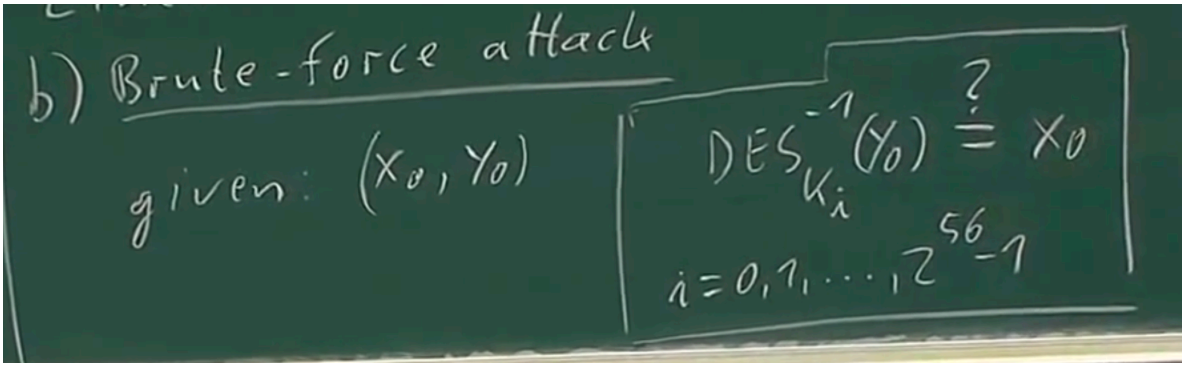


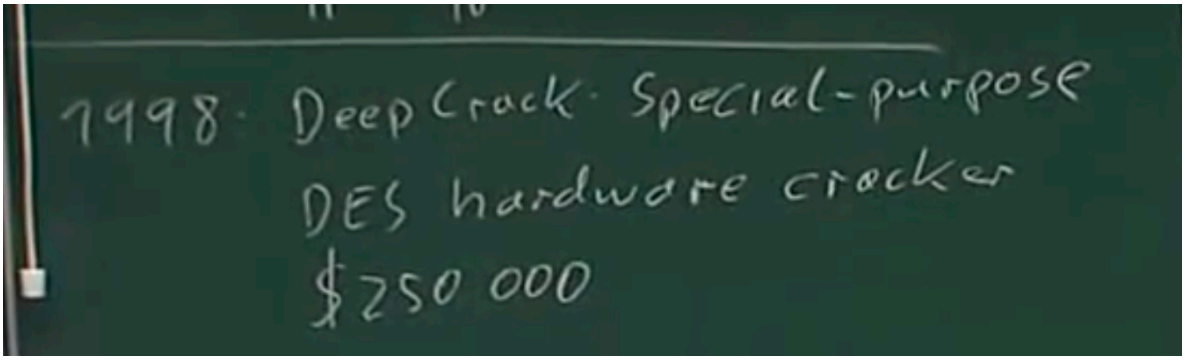
The remaining rounds will be similar.

3 : **Security of DES**

there are 2 family/principle of attacks against DES.

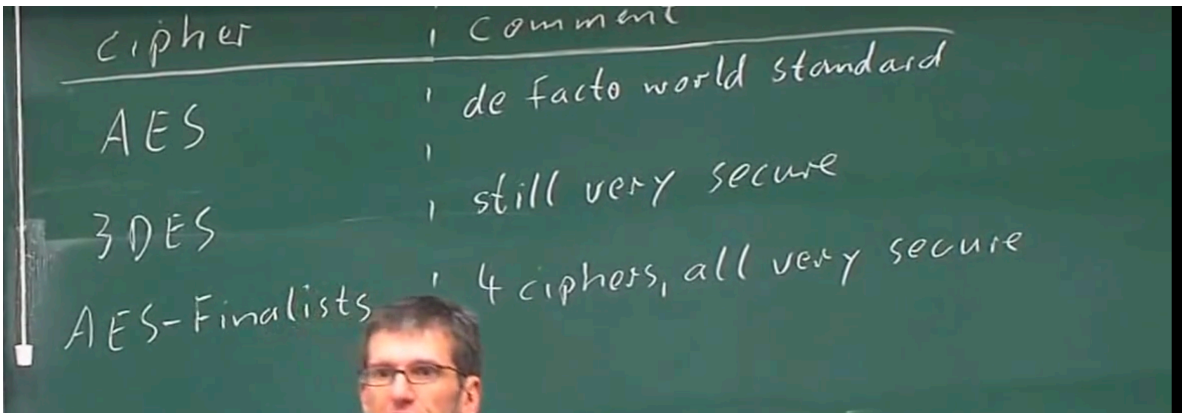
a) Analytical attacks
    Differential crypt analysis.
b) Brute force.





Des can be broken in days. (1.5 days.)

4. **DES Alternatives :**



AES is a very good algorithm. There is one drawback that it is not small in hardware. So German passport etc are using triple DES which is also very secure.

One more point Diffusion property is also called avalanche effect.