CS557: Cryptography

Modern Ciphers (Block cipher Modes of operations)

S. Tripathy
IIT Patna

Announcement

- Assignment-2: (Submit the handwritten Answers only) Deadline: 08-09-2024
  - (a) Explain neatly Linear Cryptanalysis on the Tiny SPN cipher discussed in class.
  - (b) Explain neatly Differential Cryptanalysis on the Tiny SPN cipher discussed in class

- Quiz-1 : No Quiz Today
  - Scheduled on 10-09-2024 (Mon) 5PM
  - Non Compensatory, so Pl do not request

Term project

Deadline

Topic Choose: 30th Sept 2024 (through Googledoc)

Final report and Slides: 10th Nov 2024 (tentatively)

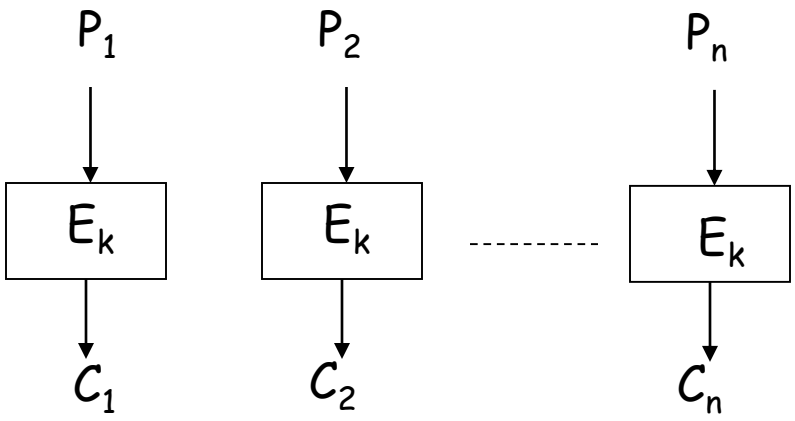
Topic: Related to Cryptography and cryptanalysis

- Must not be in the topics scheduled in class
- Choose a recent published work of your interest and fill the googledoc
- 2 students in a group
  - Ex: One can work on cipher while other on cryptanalysis
- Implement, Analyse and extension

- Block Ciphers

Modes of Encryption

ECB Mode

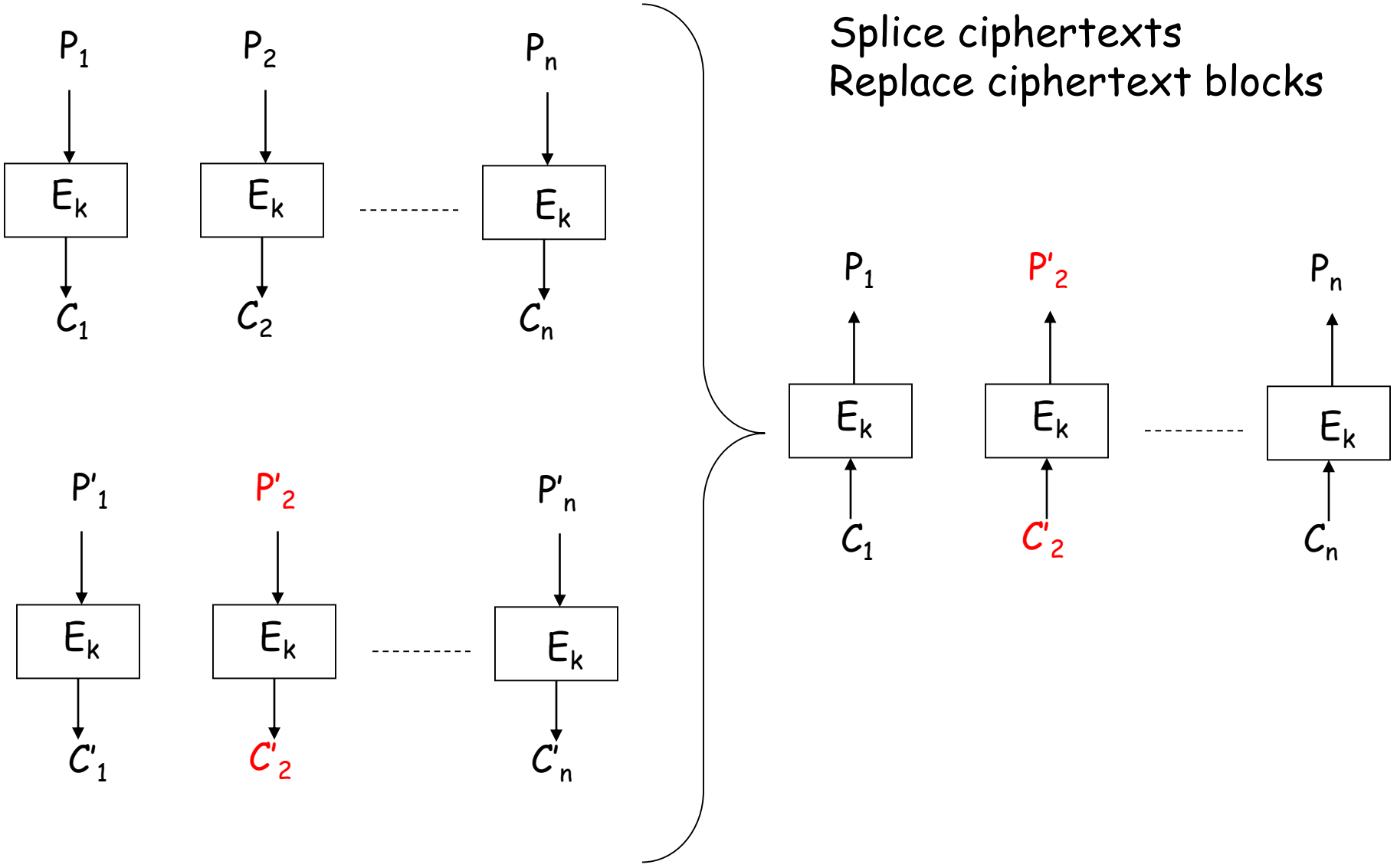


Problems?

Two identical plain text blocks produce two identical cipher blocks

Blocks can be rearranged or modified

ECB Mode


P1
P2
Pn
Ek
Ek
Ek
C1
C2
Cn
P'1
P'2
P'n
Ek
Ek
Ek
C'1
C'2
C'n
Splice ciphertexts
Replace ciphertext blocks
P1
P'2
Pn
Ek
Ek
Ek
C1
C'2
Cn

Ex. :

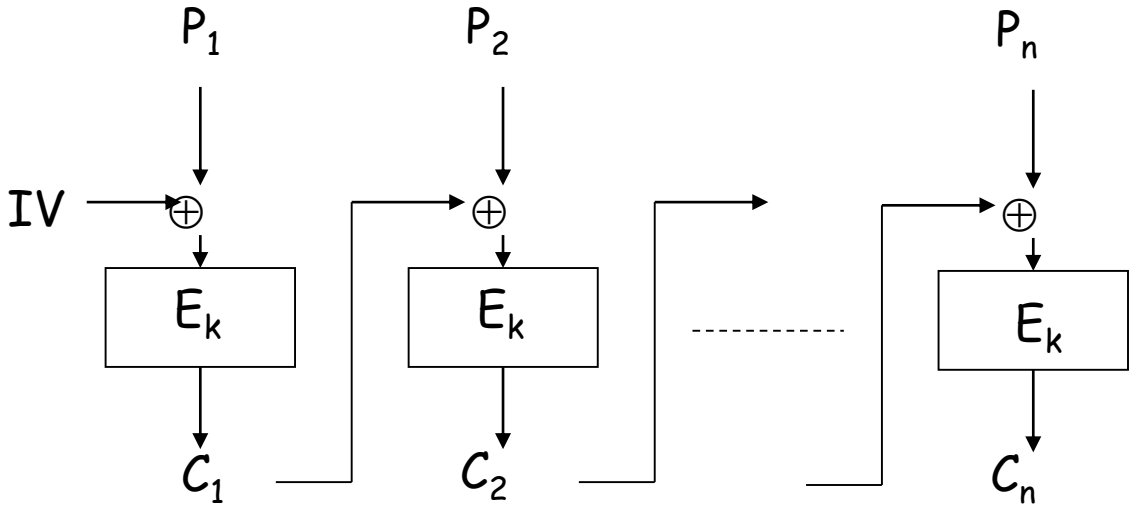
What happens in the following structure?

Name	Address	Design	Salary
Alice	Arunachal	director	32,000,000
Bob	Bihar	Secretary	21,000,000
Cathy	ChatishGhar	Assistant	21,000,000

Each field is of fixed block size (say(1))

1. One can see which sets of employees have identical or similar salaries and
2. He can alter his own salary to match another employee with higher salary.

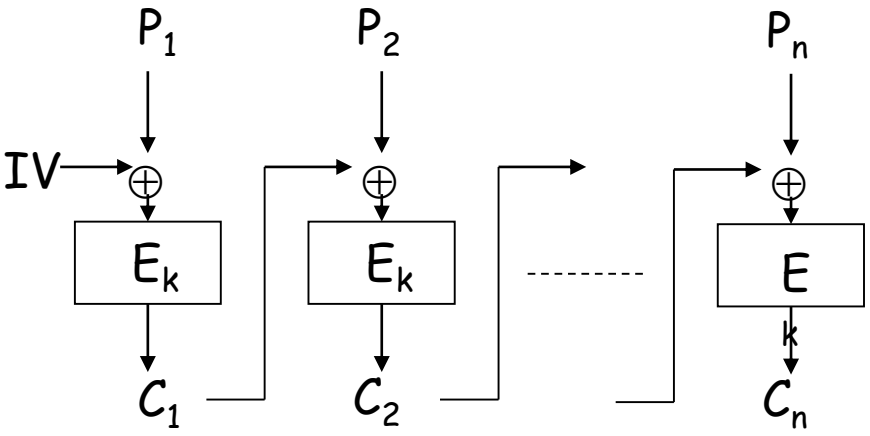
CBC Mode

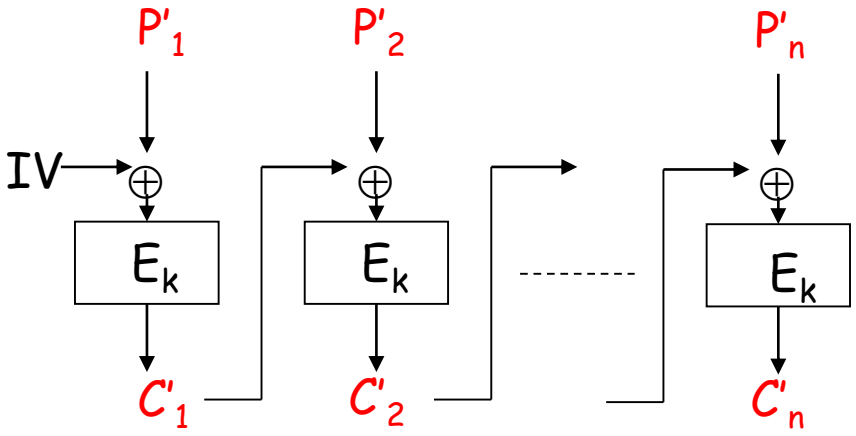


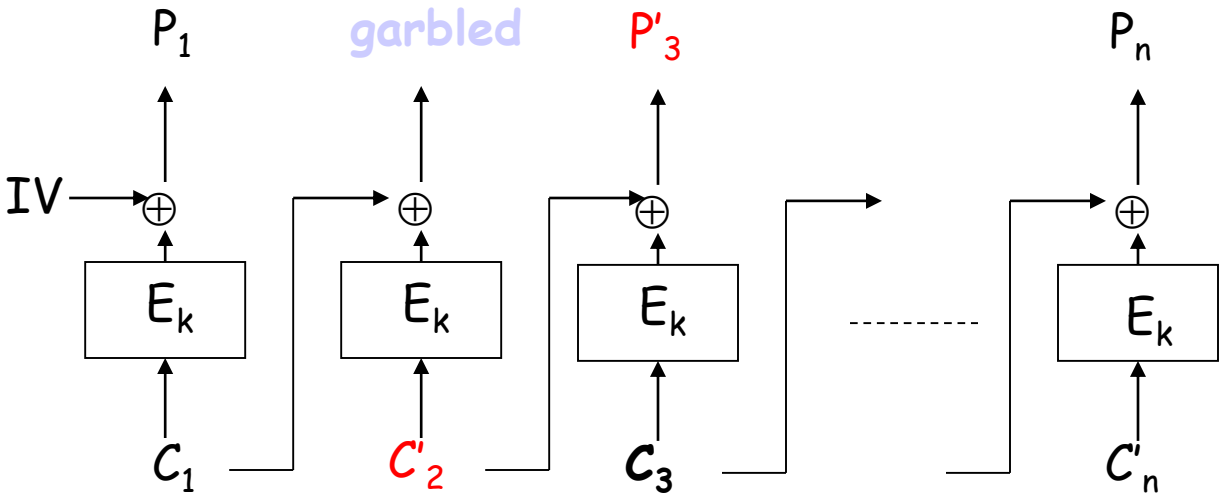
Two identical plain messages produce two different cipher messages.

This prevents Chosen plain text attack

Attack on CBC Mode - Splicing

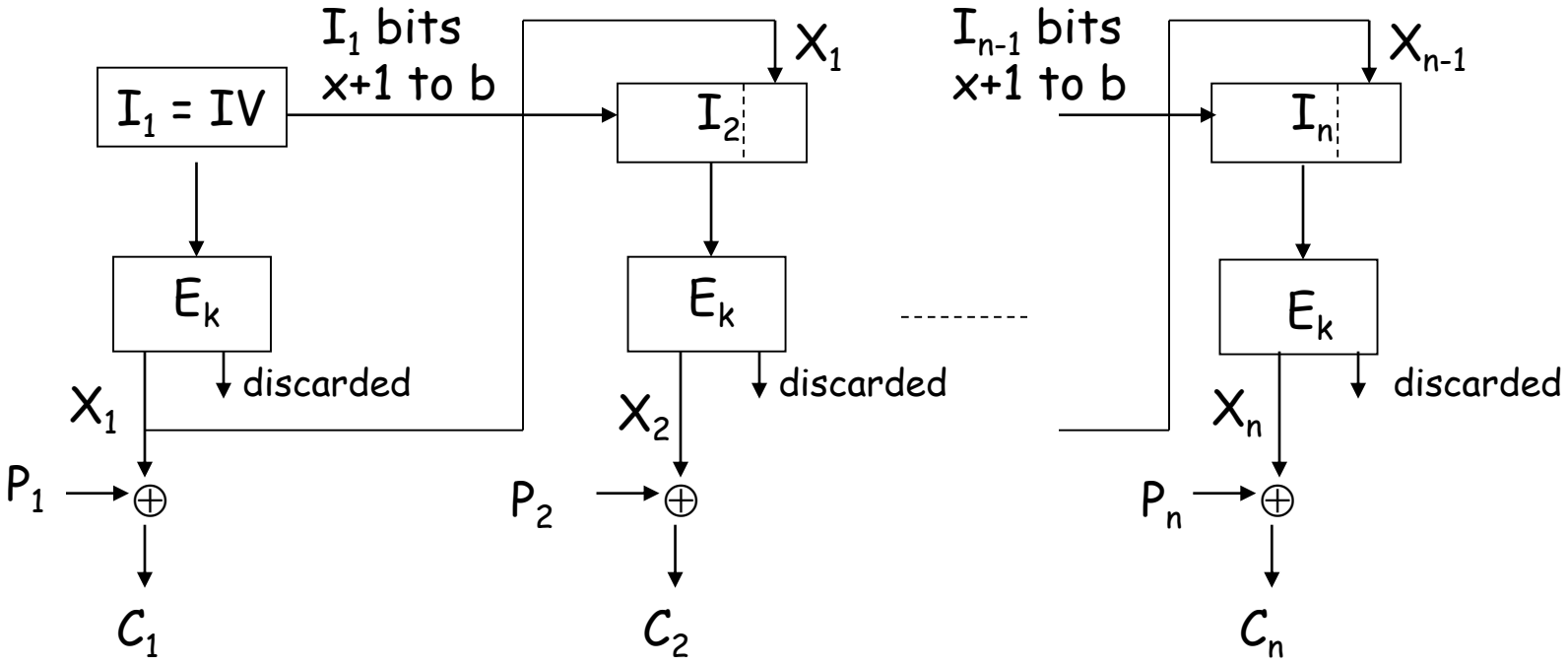






$c2 = c_2 + p_3 + p_3'$

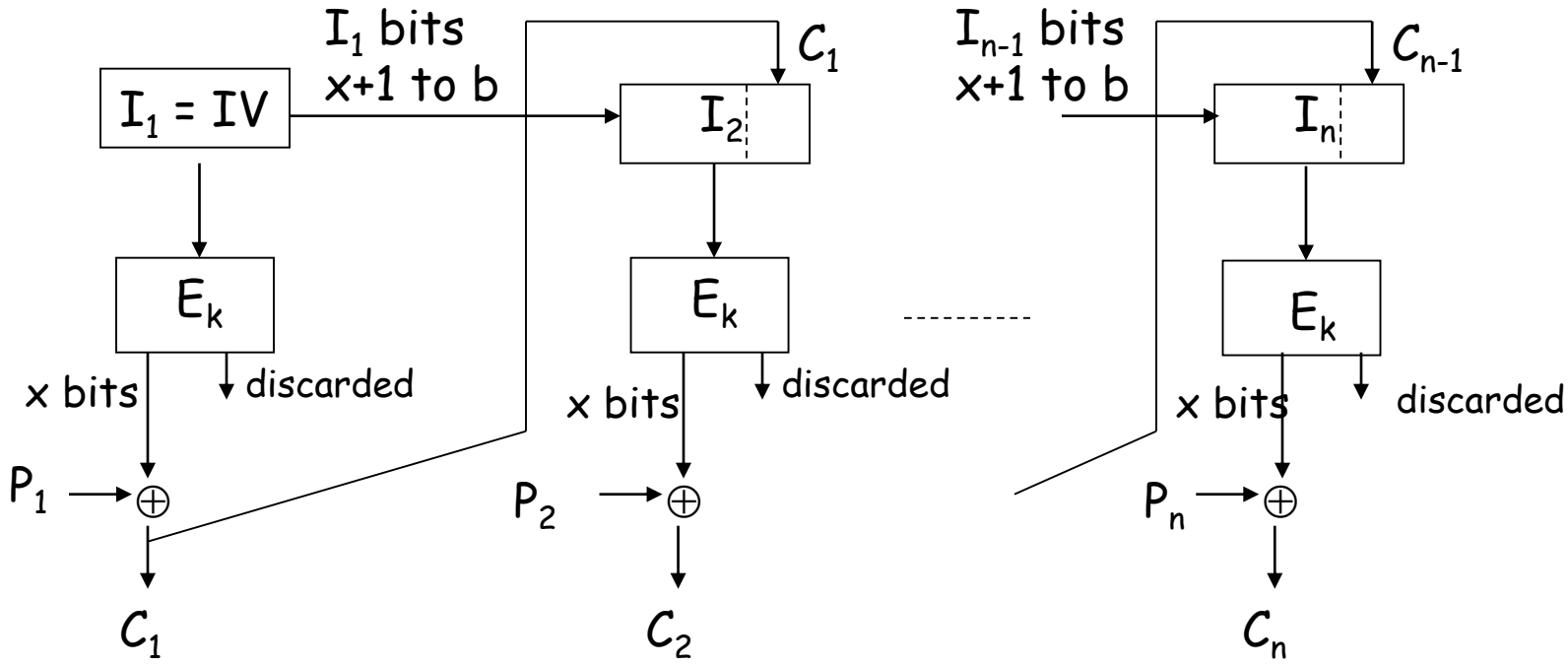
OFB Mode



X_j = leftmost x bits of the b bit output from the cipher
P_j is x bits
$I_j = I_{j-1}$ bits x+1 to b || X_{j-1}

CFB Mode

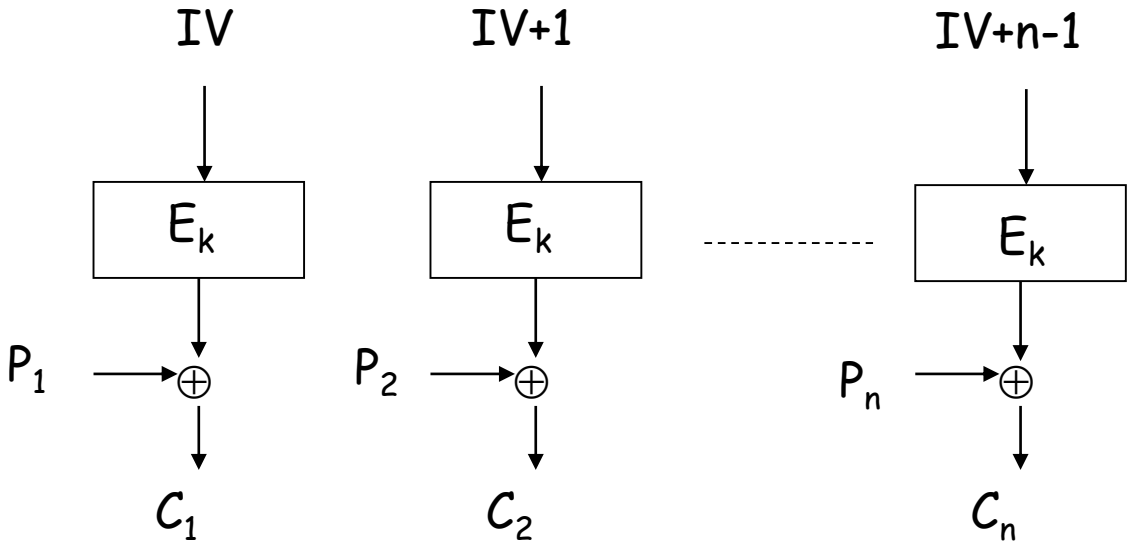
What happens if one cipher bit is changed?
What happens if one block is lost?



Cipher outputs b bits, the rightmost b-x bits are discarded.
P_j is x bits
$I_j = I_{j-1}$ bits x+1 to b || C_{j-1}

You can't generate a one-time pad in advance like OFB

CTR Mode



CTR have the following advantages:

- You can generate the one-time pad in advance.
- You can randomly access any block without decrypting all the preceding blocks

DES Attacks: Exhaustive Search

- Symmetry DES(**k'**, **x'**)=DES(**k**, **x**)'
- Suppose we know plain/cipher text pair (p,c)

```
for(k=0;k<2^56;k++) {
  if(DES(k,p)==c) {
       printf("Key is %x\n", k);
       break;
       }
}
```

- Expected number of trials (if k was chosen at random) before success: 2^{56}

Weak Keys

DES has:

- Four weak keys k for which $E_k(E_k(m)) = m$.
- Twelve semi-weak keys which come in pairs k_1 and k_2 and are such that $E_{k1}(E_{k2}(m)) = m$.

Weak keys are due to "key schedule" algorithm

Applying an Attack on DES

When attacking the cipher, try to determine key bits for first or last round, then repeat attack on reduced round version of the cipher

DES has 16 rounds, find round key for 1st or last round, repeat attack for 15 round version …

If same expanded key bits used in multiple rounds, fill in round key bits as they become known

Linear Cryptanalysis of 3 round DES

$X[17] \oplus Y[3,8,14,25] = K[26] \oplus 1$, $p = 52/64$

Round 1

$X_1[17] \oplus Y_1[3,8,14,25] = K_1[26] \oplus 1$

$P_R[17] \oplus P_L[3,8,14,25] \oplus R_1[3,8,14,25] = K_1[26] \oplus 1$

Round 3

$X_3[17] \oplus Y_3[3,8,14,25] = K_3[26] \oplus 1$

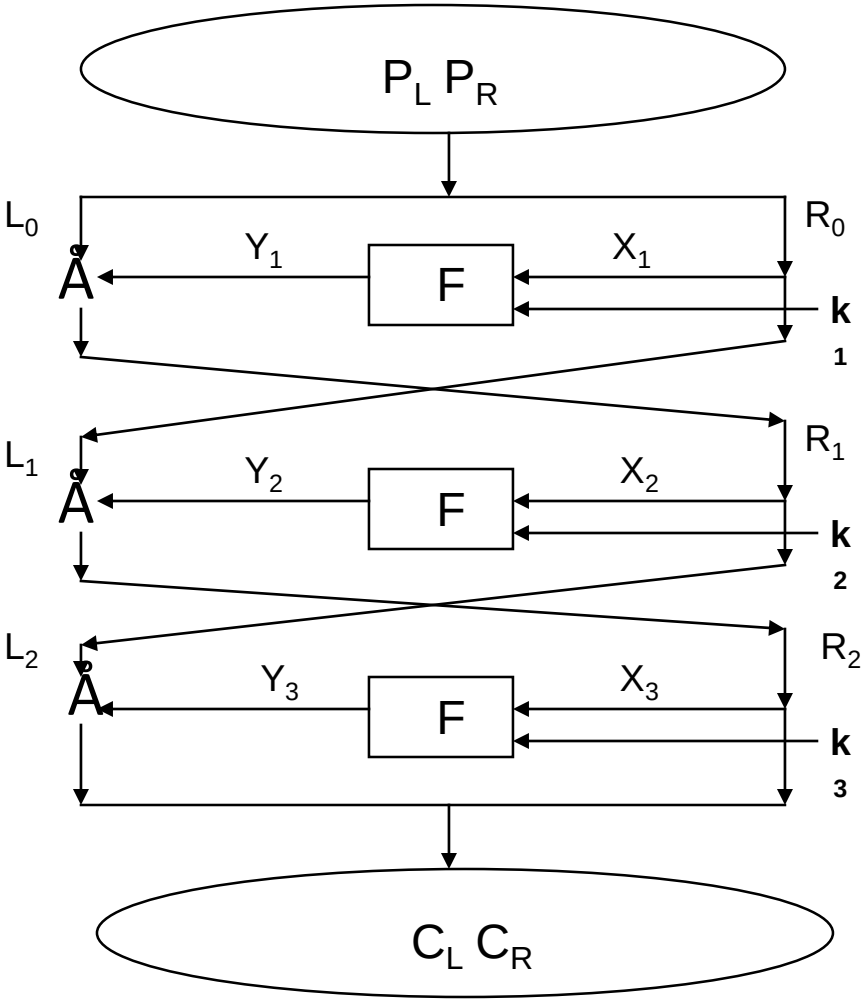
$R_1[3,8,14,25] \oplus C_L[3,8,14,25] \oplus C_R[17] = K_3[26] \oplus 1$

Adding the two get:

$P_R[17] \oplus P_L[3,8,14,25] \oplus C_L[3,8,14,25] \oplus C_R[17] = K_1[26] \oplus K_3[26]$

Thus holds with $p = (52/64)^2 + (12/64)^2 = .66$

for each pair compute the bit of the key take the value that occurs more times.



Matsui's Per Round Constraints

Label	Equation	Pr
A	X[17] $\oplus$ Y[3,8,14,25]=K[26]	12/64
B	X[1,2,4,5] $\oplus$ Y[17]=K[2,3,5,6]	22/64
C	X[3] $\oplus$Y[17]=K[4]	30/64
D	X[17] $\oplus$Y[8,14,25]=K[26]	42/64
E	X[16,20] $\oplus$Y[8,14,25]=K[25,29]	16/64

Matsui: Linear Cryptanalysis Method for DES Cipher. Eurocrypt, 98.

Linear Cryptanalysis on DES

Invented by Mitsuru Matsui in 1993.

16-round DES can be attacked using 2^{43} known plaintexts - get 26 bits, brute force the remaining 30 bits

$2^{43} = 9 \times 10^{12}$ = 9 trillion known plaintext blocks

Also exploits biases in S-boxes, which were not designed against the attack

A DES key was recovered in 50 days using 12 HP9735 workstations in a lab setting

Differential Cryptanalysis: Biham and Shamir (1990)

Was known to IBM team whose design rules provided some resistance

Breaks Khafre with 1500 corresponding plain/cipher texts in an hour

Breaks 8 round Lucifer in 2^{21} steps with 24 texts

Breaks FEAL.

Breaks 8 round DES.

DES Results: 2^{47} Chosen plaintext attack.

- Thanks