



# Lilliput-AE, a new Encryption Algorithm

**Pierre GENARD**

Université de Lorraine  
January 20, 2024



# Lightweight Crypto Competition Candidate

**Pierre GENARD**

Université de Lorraine  
January 20, 2024

Part 1

# Block Ciphers

NIST

# Part 1

## Block Ciphers

### 1 Block Ciphers

- Key Schedule
- Feistel Network
- DES
- 3-DES
- AES

### 2 Modes



## Block Cipher

5/49

### Block Cipher

$$E_K : \{0,1\}^n \Rightarrow \{0,1\}^n$$

Family of permutations indexed by a secret key  $K$  where  $n$  is the block size.

### Tweakable Block Cipher : TBC

TBC is a family of permutations parametrized by a secret key  $K$  and a tweak value  $T$ .

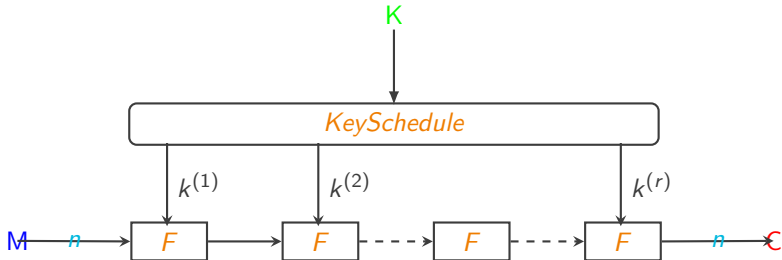
### Authenticated Encryption : AE

Encryption scheme that assures both data confidentiality and authenticity.

## Block Cipher

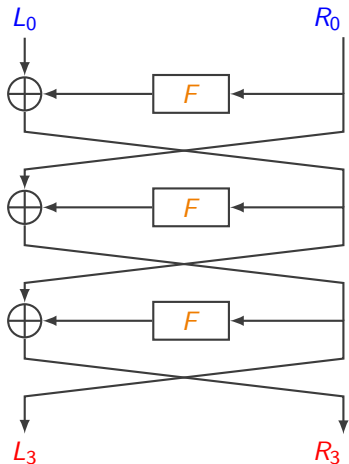
6/49

- Sequence of  $r$  iterations (rounds) on  $n$  bits blocks.
- There is a need for **modes** (ECB, CBC, CTR, GCM, etc.).



## Feistel Network

7/49

Substitution Permutation  
Network : SPN

Substitution: S-Boxes

Permutation: P-Boxes

Typical one: DES

$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \oplus F(R_i)$$

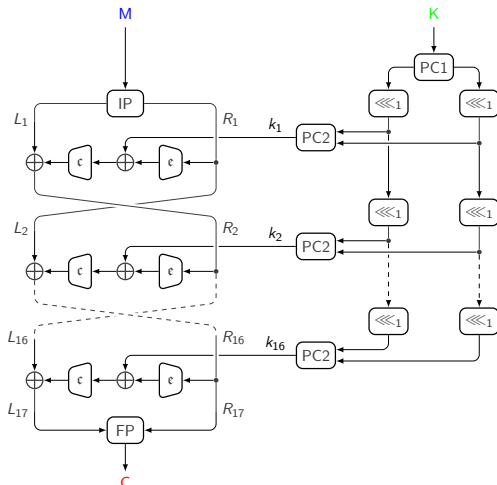
## Attacks

Linear cryptanalysis

Differential cryptanalysis

## Data Encryption Standard : DES

8/49



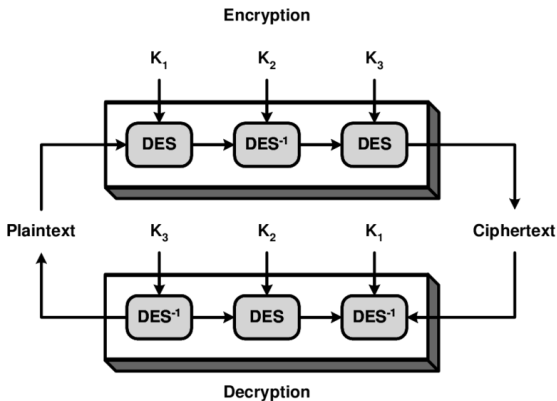
- Key size : 56 bits
- Blocks size : 64 bits
- Feistel network
- 16 rounds
- Triple-DES

$$C = E_{K_3}(D_{K_2}(E_{K_1}(M)))$$



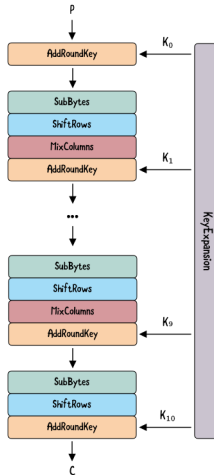
## Triple DES : Overview

9/49



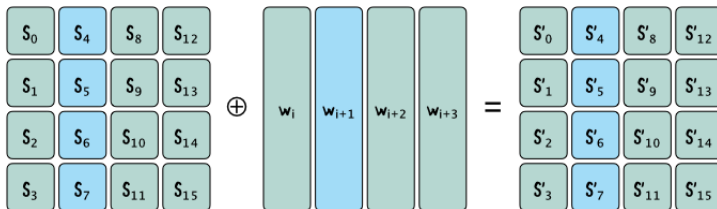
## Advanced Encryption Standard : AES Encryption

10/49



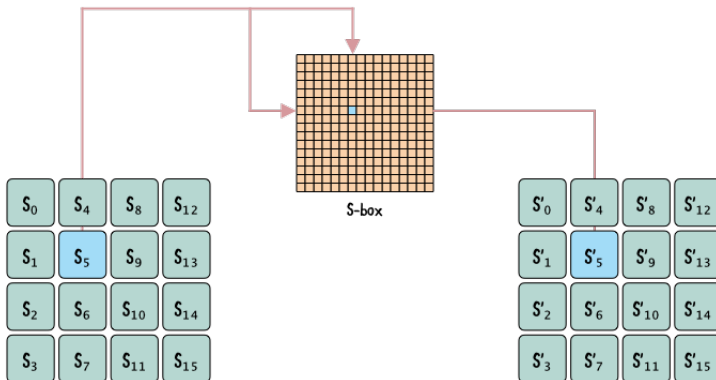
## Advanced Encryption Standard : AddRoundKey

11/49



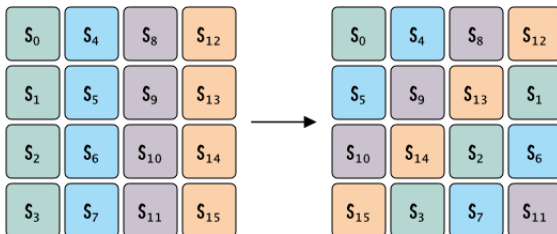
## Advanced Encryption Standard : SubBytes

12/49



## Advanced Encryption Standard : ShiftRows

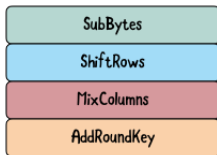
13/49



## Advanced Encryption Standard : AES Round

14/49

Encryption Round

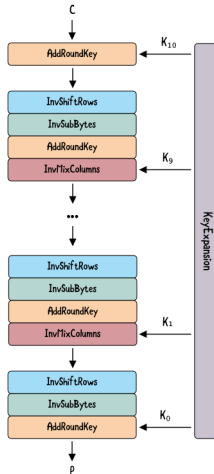


Decryption Round



## Advanced Encryption Standard : AES Decryption

15/49



# Part 1

## Block Ciphers

### 1 Block Ciphers

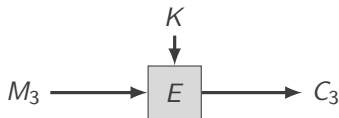
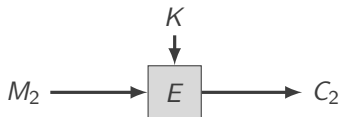
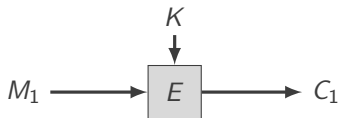
### 2 Modes

- ECB
- CBC
- CFB
- OFB
- CTR



## Electronic Code Book : ECB Encryption

17/49



⋮

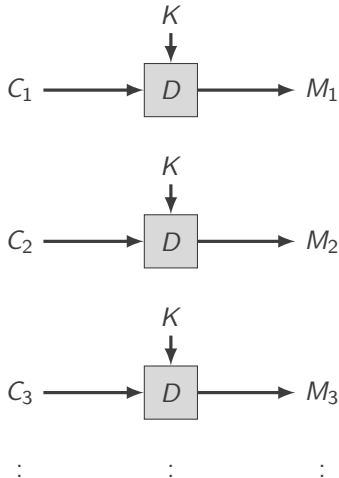
⋮

⋮

- Never use this !
- Parallel
- Random access

## Electronic Code Book : ECB Decryption

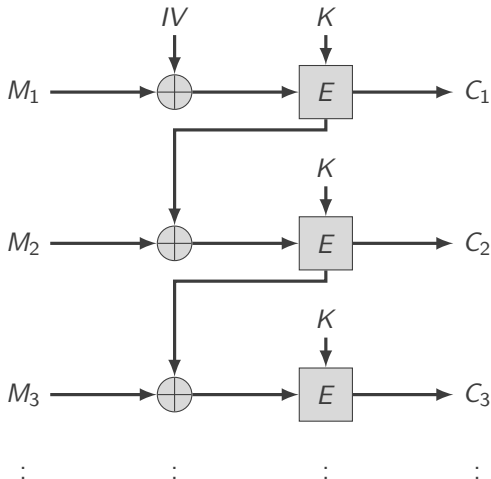
18/49



- Parallel
- Random access

## Cipher Block Chaining : CBC Encryption

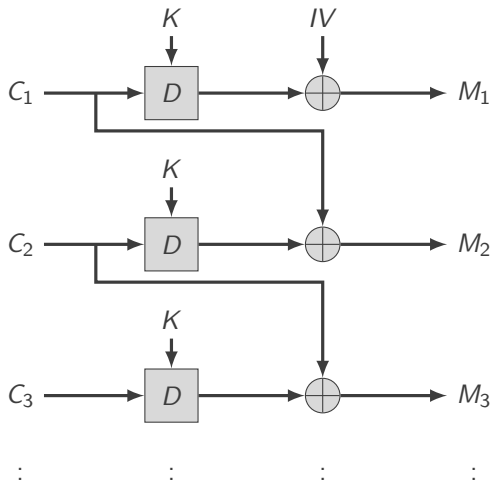
19/49



- Sequential
- Padding flaws

## Cipher Block Chaining : CBC Decryption

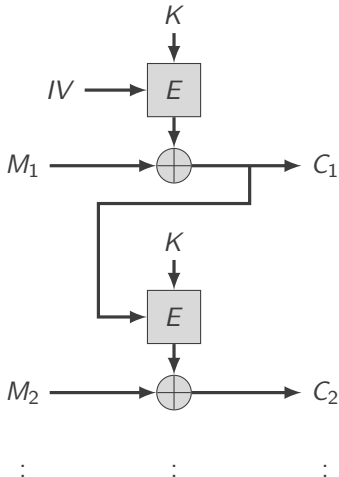
20/49



■ Parallel

## Cipher Feed Back : CFB Encryption

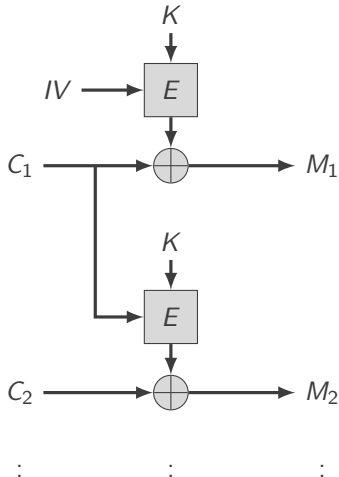
21/49



- Sequential
- Random access

## Cipher Feed Back : CFB Decryption

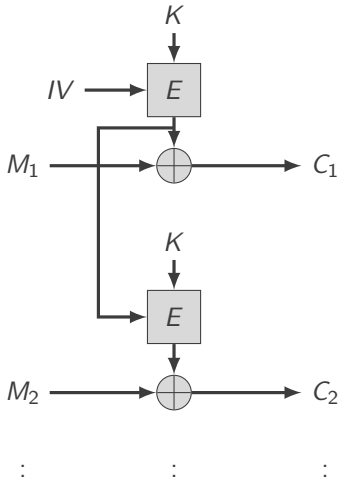
22/49



- Parallel
- Random access

## Output Feed Back : OFB Encryption

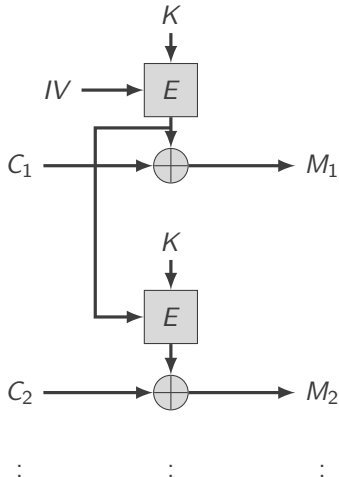
23/49



■ Sequential

## Output Feed Back : OFB Decryption

24/49

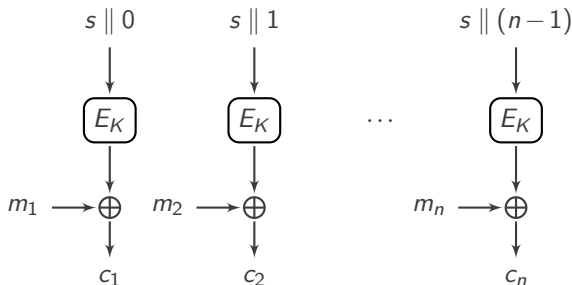


■ Sequential



## Counter : CTR Encryption

25/49



Part 2  
**Lilliput-AE**

**NIST**

## Part 2

# Lilliput-AE

### 3 Scheme

- Modes
- Key Schedule

### 4 $\Theta$ CB3

### 5 SCT-2

## Two Authenticated Encryption Modes

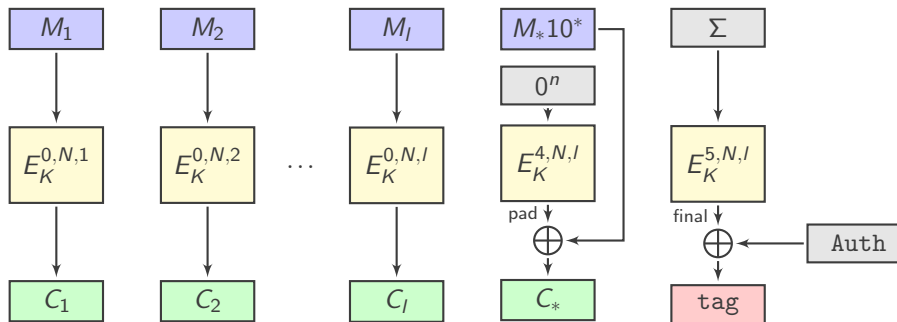
28/49

- **Lilliput-I**: nonce-respecting mode corresponding with ΘCB3.
- **Lilliput-II**: nonce-misuse resistant mode corresponding with SCT-2.

Name	k	t	n	N	$\tau$
<b>Lilliput-I-128</b>	128	192	128	120	128
<b>Lilliput-I-192</b>	192	192	128	120	128
<b>Lilliput-I-256</b>	256	192	128	120	128
<b>Lilliput-II-128</b>	128	128	128	120	128
<b>Lilliput-II-192</b>	192	128	128	120	128
<b>Lilliput-II-256</b>	256	128	128	120	128

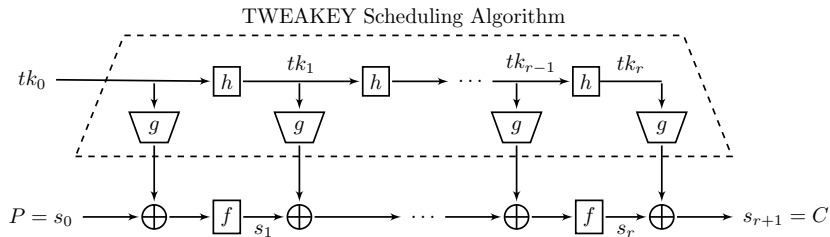
## AE with a Tweakable Block Cipher

29/49



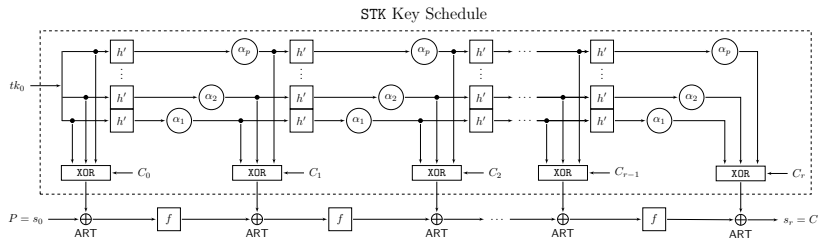
# TWEAKEY Schedule

30/49



# STK Key Schedule

31/49



## Part 2

# Lilliput-AE

### 3 Scheme

### 4 $\Theta$ CB3

- Associated Data
- Encryption
- Decryption

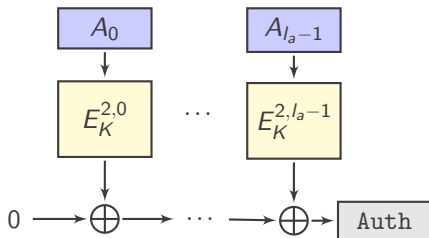
### 5 SCT-2





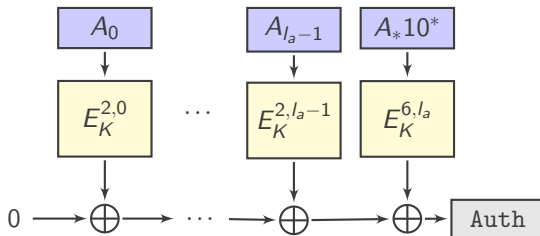
## Associated Data : Without Padding

33/49



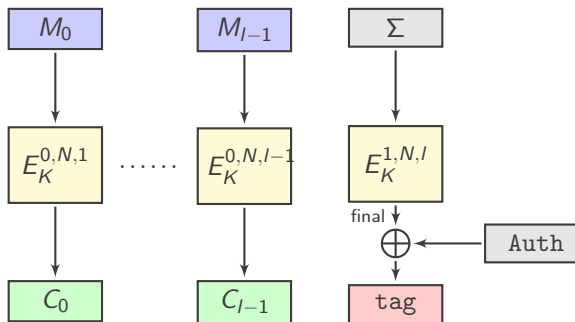
## Associated Data : With Padding

34/49



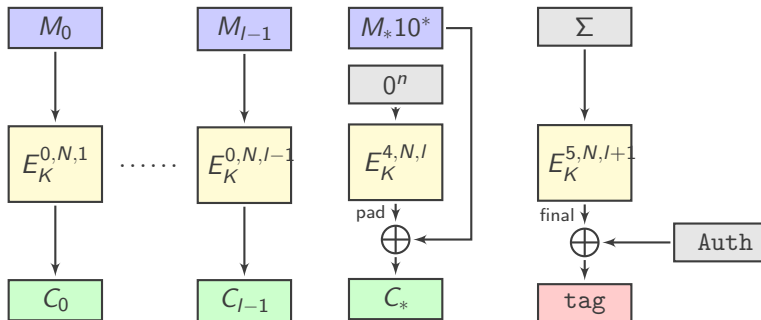
## Message Encryption : Without Padding

35/49



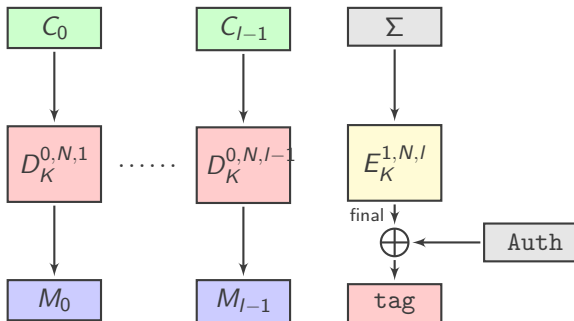
## Message Encryption : With Padding

36/49



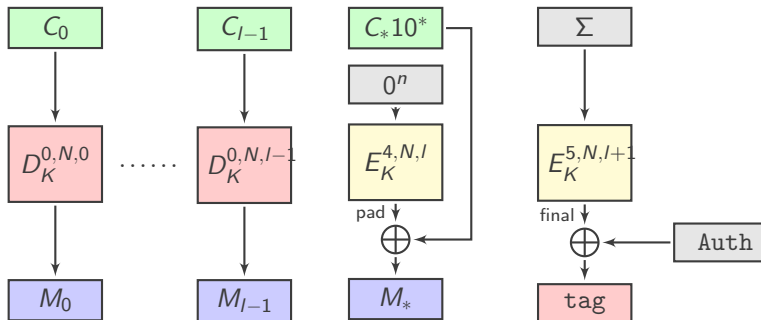
## Message Decryption : Without Padding

37/49



## Message Decryption : With Padding

38/49



## Part 2

### Lilliput-AE

3 Scheme

4  $\Theta$ CB3

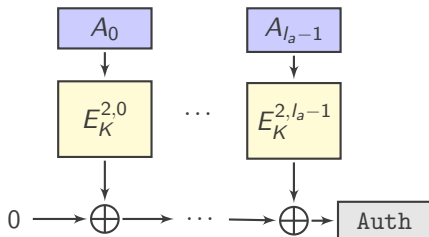
5 SCT-2

- Associated Data
- Tag Generation
- Encryption
- Decryption



## Associated Data : Without Padding

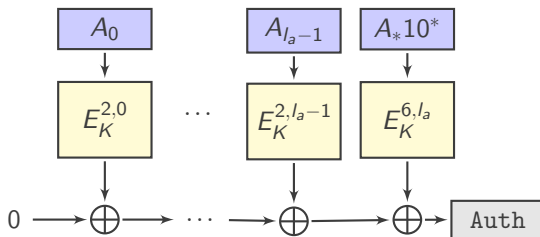
40/49





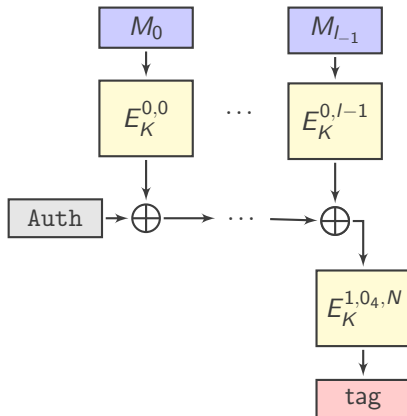
## Associated Data : With Padding

41/49



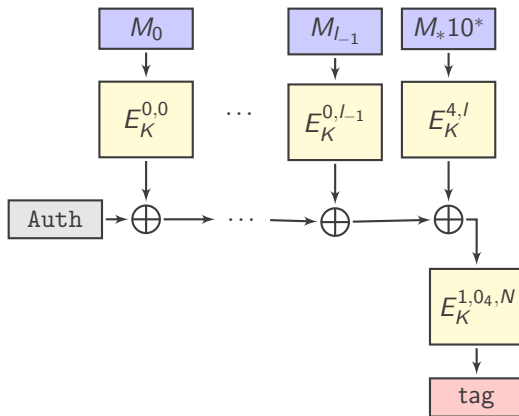
## Tag Generation : Without Padding

42/49



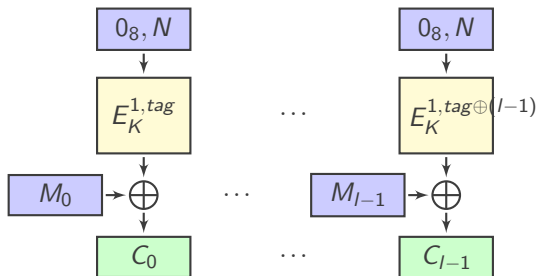
## Tag Generation : With Padding

43/49



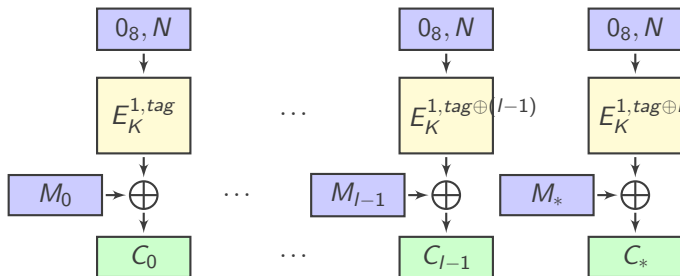
## Message Encryption : Without Padding

44/49



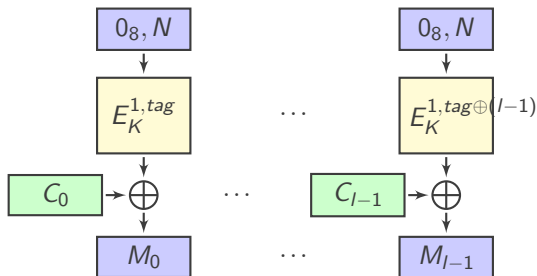
## Message Encryption : With Padding

45/49



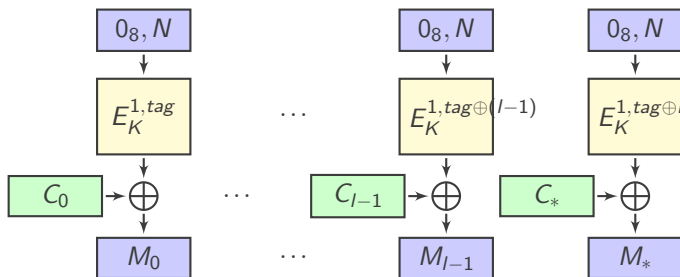
## Message Decryption : Without Padding

46/49



## Message Decryption : With Padding

47/49



**Thanks for your attention!**

**Questions ?**



## References

49/49



Intro to Cryptography



Joy of Cryptography



Salad of Block Ciphers