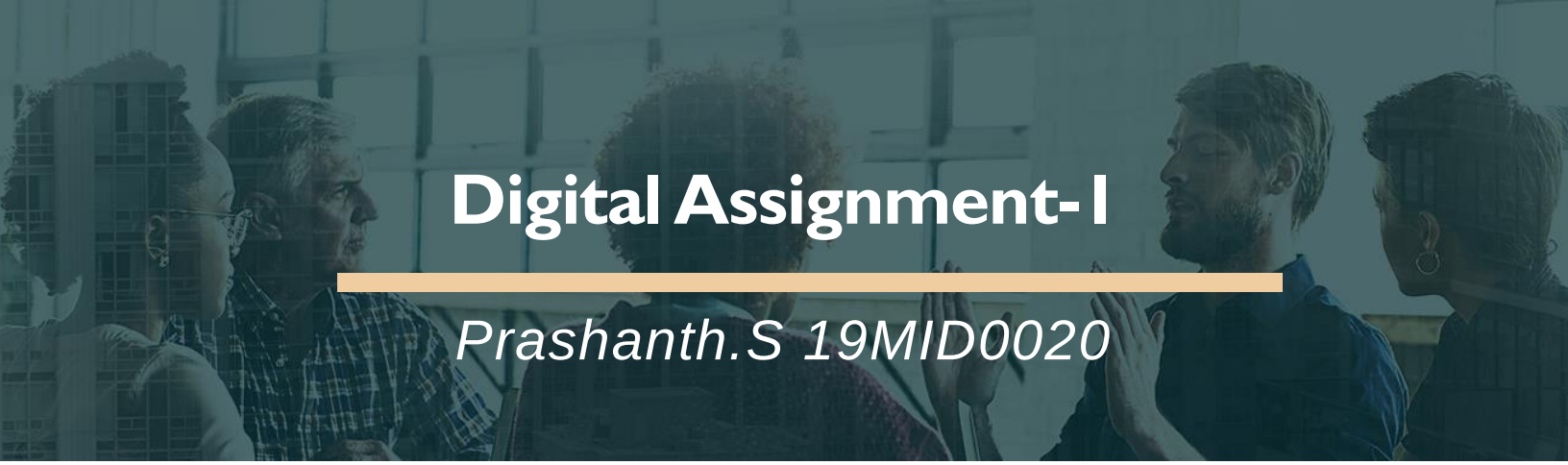


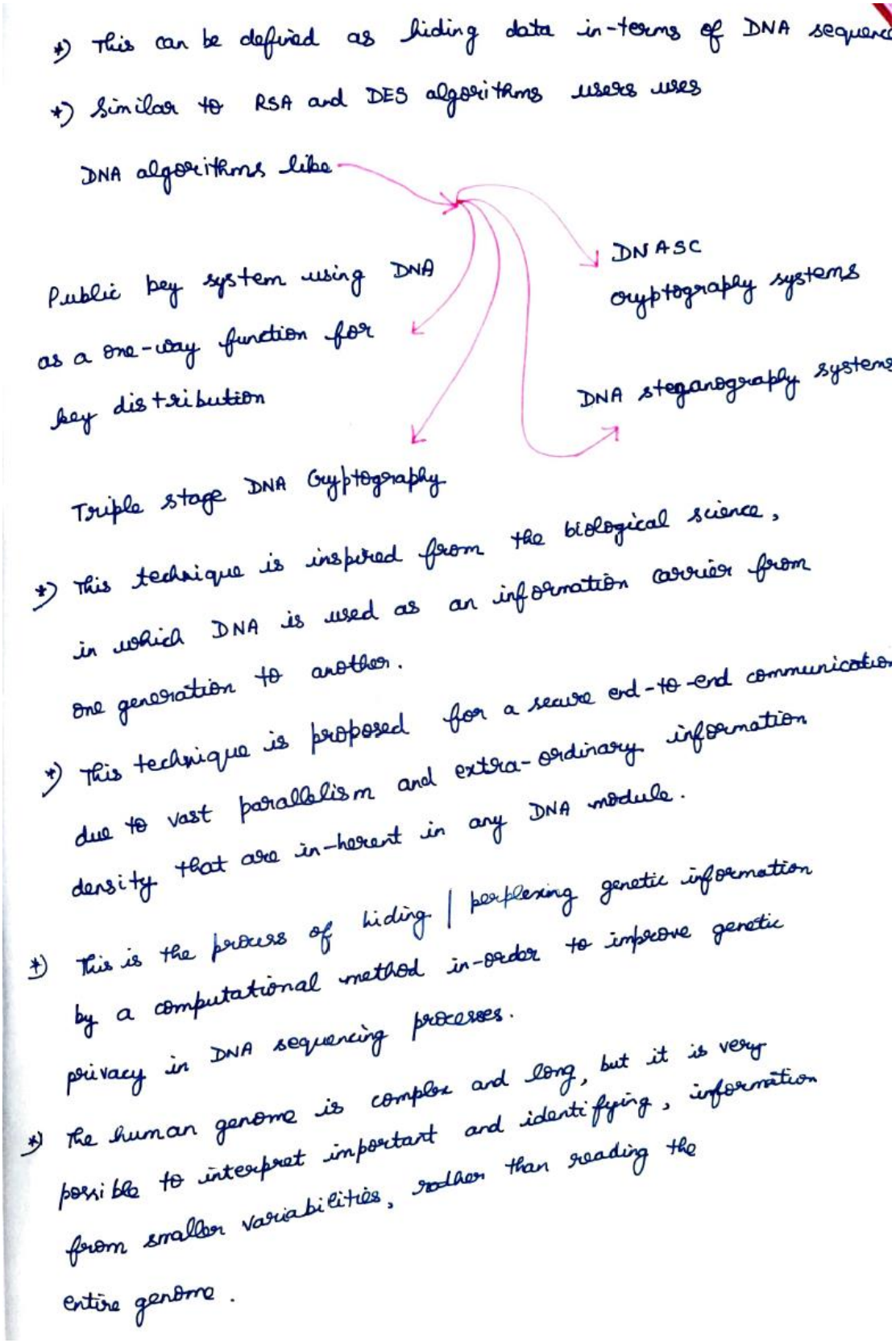
Digital Assignment-I

Prashanth.S 19MID0020

Question-I

1. Make a study on DNA cryptography
    a. Definition of DNA Cryptography
    b. Objective of DNA Cryptography
    c. Explain the following DNA based Encryption Techniques
        i. DNA random One Time Pad Based
        ii. DNA chip-based cryptography
        iii. DNA Fragmentation
        iv. DNA Steganography
    d. Compare any two of the above mentioned encryption technique.

Definition of DNA Cryptography



*) DNA is a double helix structure in which two strands are coiled to-eachother and it is made of nucleotides.

*) 4 bases in Nucleotide

- Cytosine (C) — 10
- Adenine (A) — 00
- Thymine (T) — 01
- Guanine (G) — 11

*) Guanine Hybridization in which double stranded DNA molecules uses single stranded DNA molecules.

*) In the entire process,

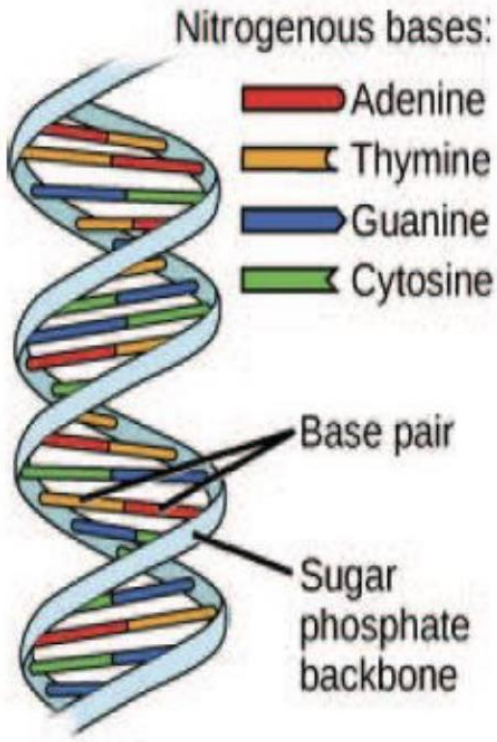
Adenine pairs with Thymine

Guanine pairs with Cytosine

*) Polymerase Chain Reaction (PCR) is the process of amplifying a single / multiple copies to produce millions of copies of DNA sequence.

*) Primer is a strand of nucleic acid that functions as a beginning point for DNA synthesis.

*) ~~Trans coding~~ Transcription and Splicing is the process of removing the non-coding areas and rejoining the remaining coding areas and information of DNA is moved into mRNA.



Main objective of DNA Cryptography

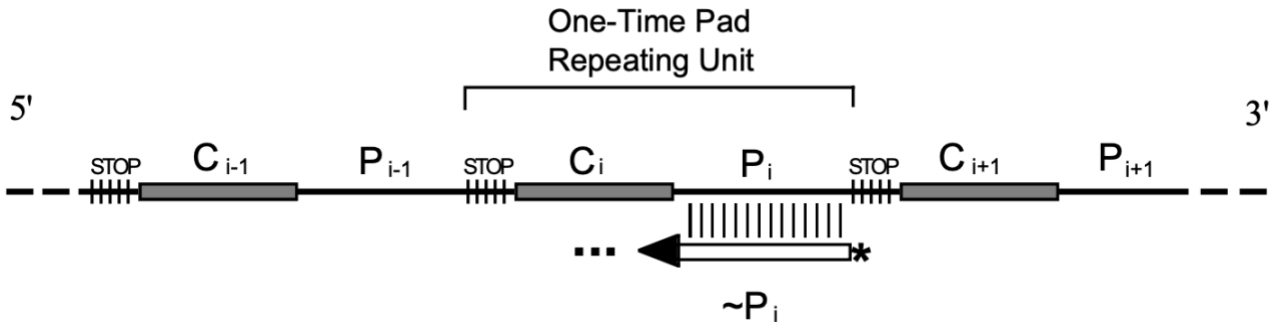
Main objective of DNA Cryptography

*) Encrypt the plain text and hide it in the DNA digital form.

*) It enables the confidentiality of data more high than the modern method with the use of One Time Pad (OTP) keys and its sing.

*) It also generates the key for the huge length of data compared to the modern methods ~~when~~ in which keys are generated only for smaller length of data.

i)DNA random One Time Pad Based



*) One Time Pad encryption uses a code book of random data to convert plain text to cipher text.

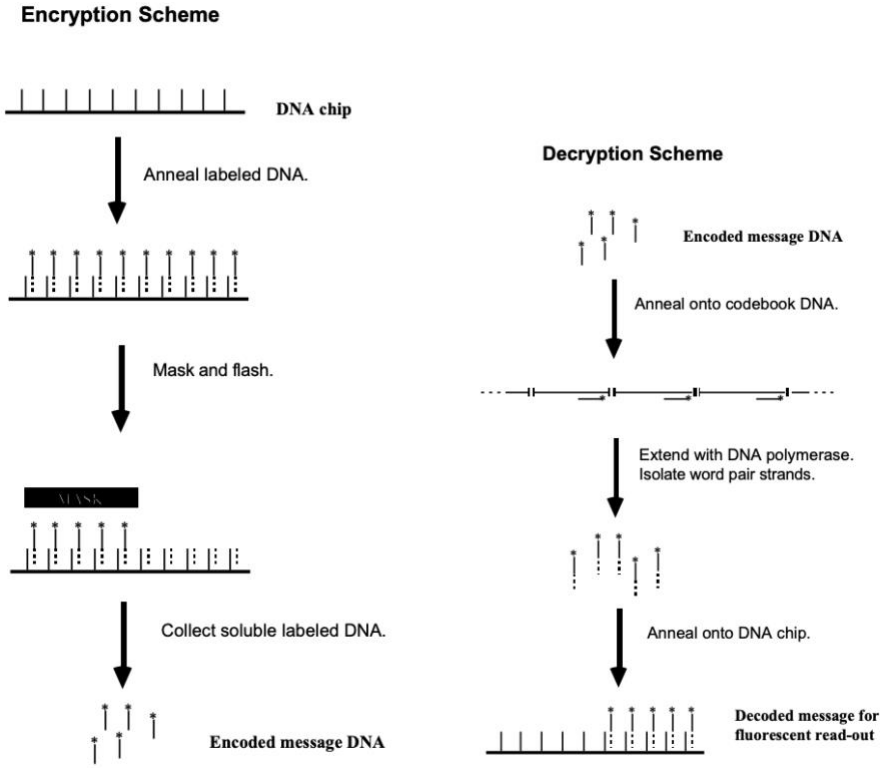
*) Since the codebook serves as the key, if it were predictable (i.e not random) then an adversary could guess the algorithm that generates the codebook, allowing decryption of the message.

→ There are two proposed methods where by a large number of short message sequences can be encrypted.

i) the use of substitution, where we encrypt each message sequence using an associatively matched piece from DNA pad.

ii) the use of bit-wise XOR computation using a bimolecular computing technique.

ii)DNA chip based cryptography



*) The DNA chip is also called micro-array.

*) This DNA chip is made up of nucleic acid and electronic circuits are designed by the semi-conductors.

*) This technology provides excellent progress in the field of DNA based cryptography.

*) A DNA chip is used for storing and handling and maintaining a large amount of genome and biological information.

*) Biochemical prcess are used to encrypt the text and images

*) The limitation of this technique is the sudden change in physical factors provides negative results.

iii) DNA Fragmentation

3) DNA Fragmentation

*) This method is used for the library construction in the DNA sequence.

*) It is used to divide the DNA sequence into small parts.

*) Many encryption algorithms use this as a second layer of security.

*) It is also implemented in the encryption of the key.

iv) DNA Steganography

iv) DNA Steganography

*) Steganography using DNA is appealing due to its simplicity.

*) One method proposed involves taking 'plaintext' input DNA strands, tagging each with 'secret key' strands, and then hiding them among random 'distracter' strands. tagging each with ~~'secret key'~~ stra

*) The plain-text is retrieved by hybridization with the complement of the secret key strands.

*) It has been postulated that in the absence of knowledge of the secret key, it would be necessary to examine all the strands including the distracters to retrieve the plaintext.

*) Based on the likely difference in entropy of the distracters and the plain text, we argue that the message can be retrieved without the key.

*) This is used for hiding one message inside another message. Image, audio, video are reused to protect large amount of data, but data can be damaged due to the sudden change in environment.

Compare any two of the above mentioned encryption technique

Basis for Comparison	Steganography	Fragmentation
*) Basic	It is known as cover writing	It means secret d
*) Goal	Secret communication	Data protection
*) Structure of the message	Not Altered	Altered only for the transmission.
*) Popularity	Less popular	Hora commonly used
*) Relies on	Key	No parameters
*) Supported security principles	Confidentiality & Authentication	Confidentiality, data integrity and authentication.
*) Techniques	Spacial domain Trans for domain Mode-based and ad-hoc	Transposition, substitution, stream ciphers and block ciphers.
*) Implemented on	Audio, video, image and text	Only on text file

Question-2

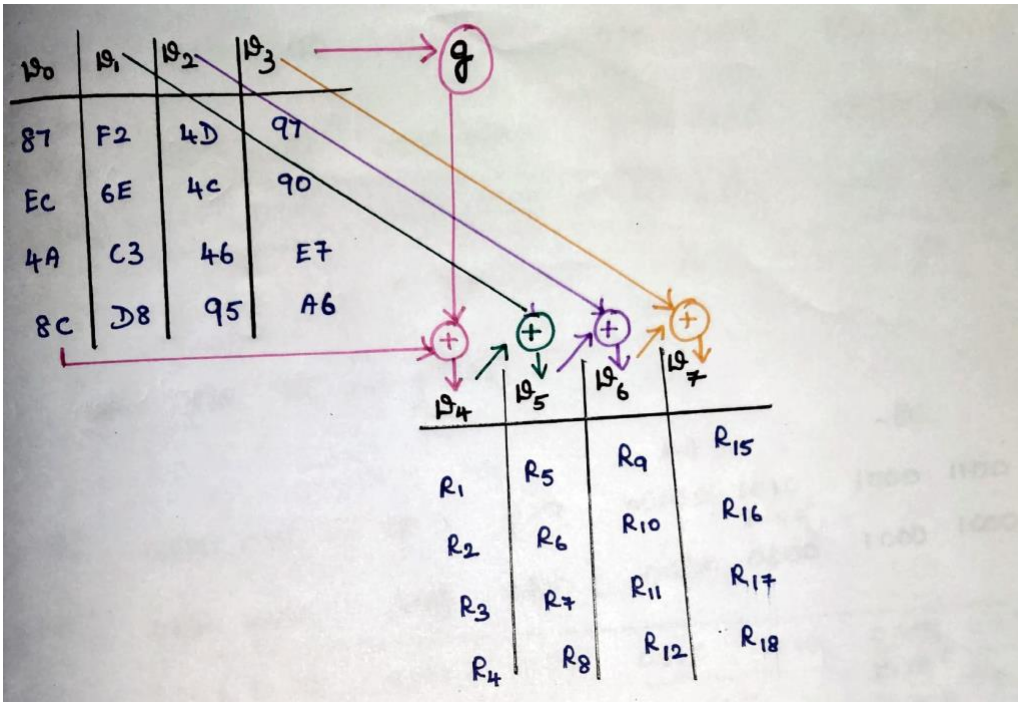
2. In AES algorithm , let the key be

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

Here each column is represented as a word (W_0, W_1, W_2, W_3). Show the step by step process to compute the word W_4.

AES Table

	0	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
40	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16



$w_4 \Rightarrow w_0 \oplus g(w_3)$

$w_5 \Rightarrow w_1 \oplus w_4$

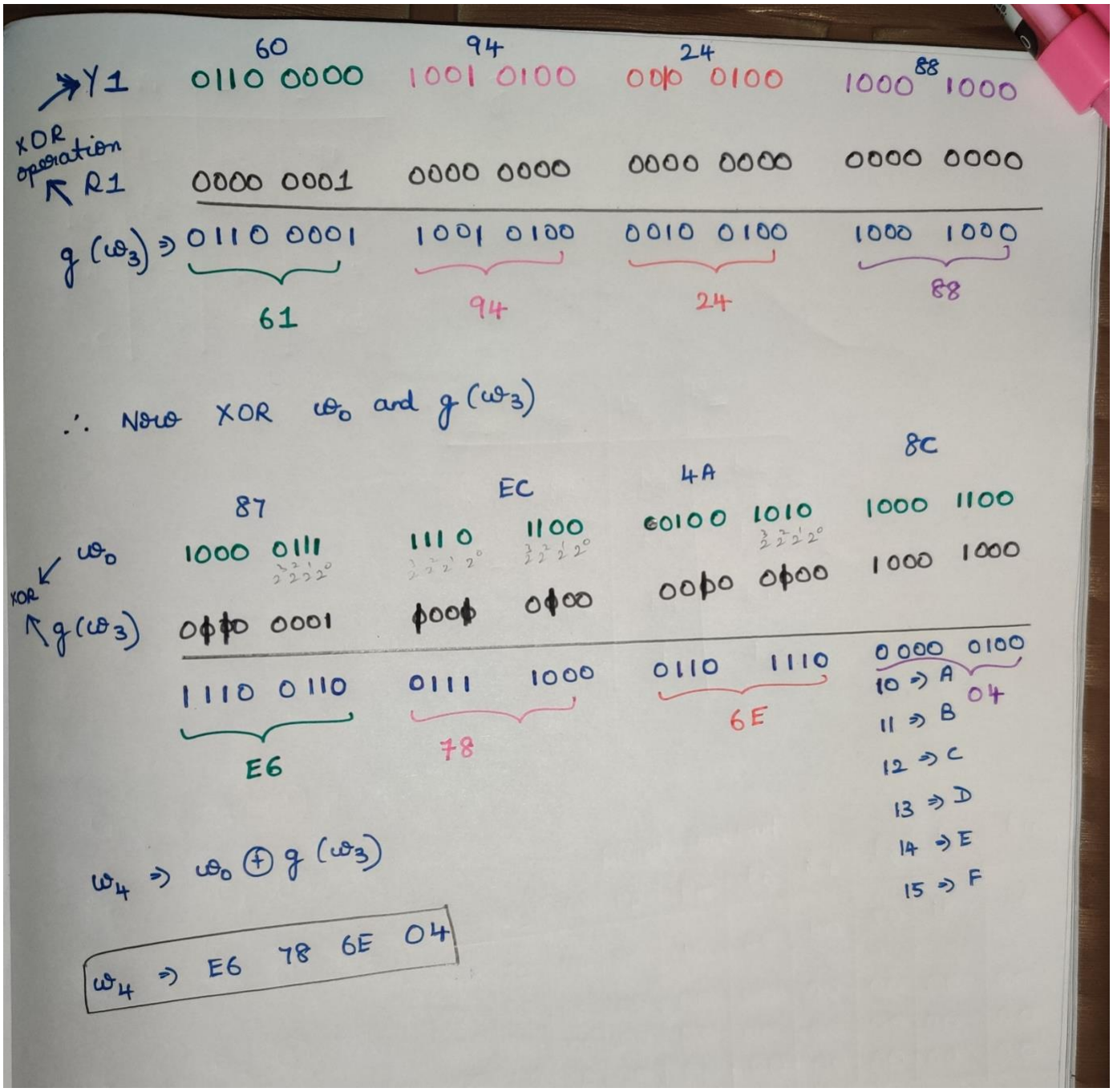
$w_6 \Rightarrow w_2 \oplus w_5$

$w_7 \Rightarrow w_3 \oplus w_6$

Round constant

R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}
01	02	04	08	10	20	40	80	1B	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

B_3	Rotword (X_1)	Sub-word (Y_1)
97	90	60
90	E7	94
E7	A6	24
A6	97	88


60
94
24
88
Y1
0110 0000
1001 0100
0010 0100
1000 1000
XOR operation
R1
0000 0001
0000 0000
0000 0000
0000 0000
g(w3) ⇒ 0110 0001
1001 0100
0010 0100
1000 1000
61
94
24
88
∴ New XOR w0 and g(w3)
87
EC
4A
8C
w0
1000 0111
1110 1100
0100 1010
1000 1100
XOR
g(w3)
0000 0001
0000 0000
0000 0000
1000 1000
1110 0110
0111 1000
0110 1110
0000 0100
E6
78
6E
04
10 ⇒ A
11 ⇒ B
12 ⇒ C
13 ⇒ D
14 ⇒ E
15 ⇒ F
w4 ⇒ w0 ⊕ g(w3)
w4 ⇒ E6 78 6E 04