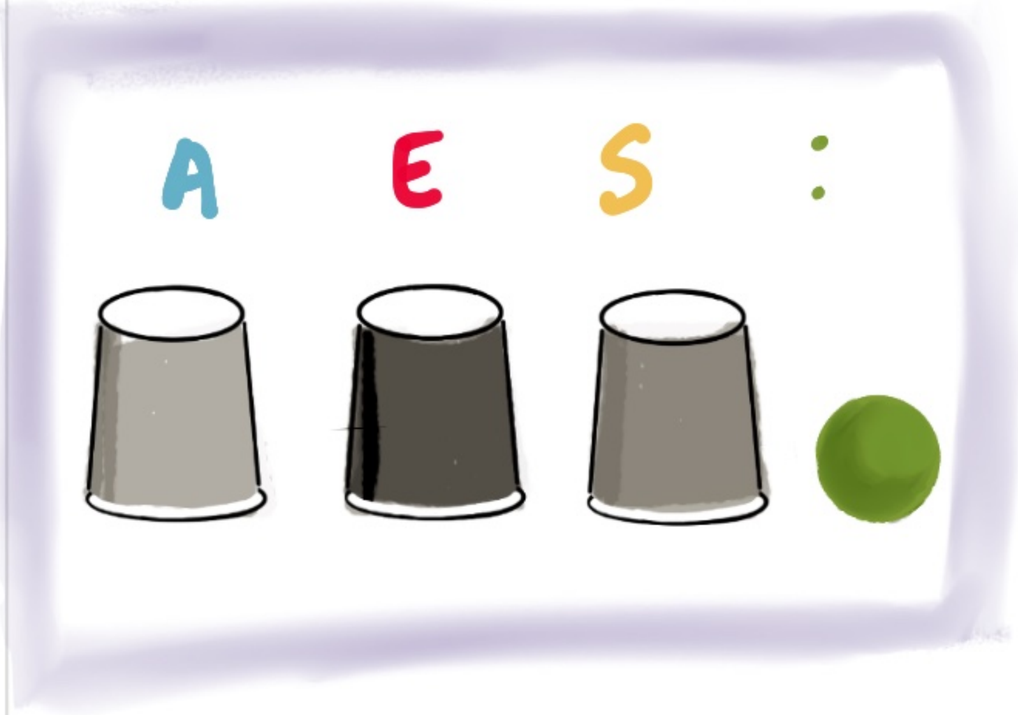


ADVANCED ENCRYPTION STANDARD

By

Gitanjali Venkatraman

INTRODUCTION

THIS BOOK TAKES YOU THROUGH THE ALGORITHM FOR AES - A SYMMETRIC KEY BASED ENCRYPTION — PUBLISHED IN NOVEMBER 2001.

WE BRIEFLY TOUCH ON THE HISTORY, A LOOK AT APPLICATION, FOLLOWED BY THE ENCRYPTION & DECRYPTION ALGORITHM. THIS IS SUPPORTED BY AN EXPLANATION OF THE MATHEMATICS THAT GOES WITH IT.

THIS BOOK ALSO GIVES YOU A VIEW ON SOME OF THE WEAKNESSES IN AES IMPLEMENTATION AND WHY QUANTUM COMPUTERS MIGHT NOT THREATEN AES SECURITY

PRE READS

HOW TO TELL SECRETS
THE STORY OF QUANTUM COMPUTING

} ILLUSTRATED GUIDES FROM THOUGHTWORKS

1997: MOVE OVER, DES!

DATA ENCRYPTION STANDARD - OR DES - IS A SYMMETRIC KEY ALGORITHM TO ENCRYPT DIGITAL DATA

NIST.GOV ADOPTED DES AS A STANDARD IN THE SEVENTIES

IS A 56 BIT ENCRYPTION TOO SMALL TO BE SECURE? (WITH DES)

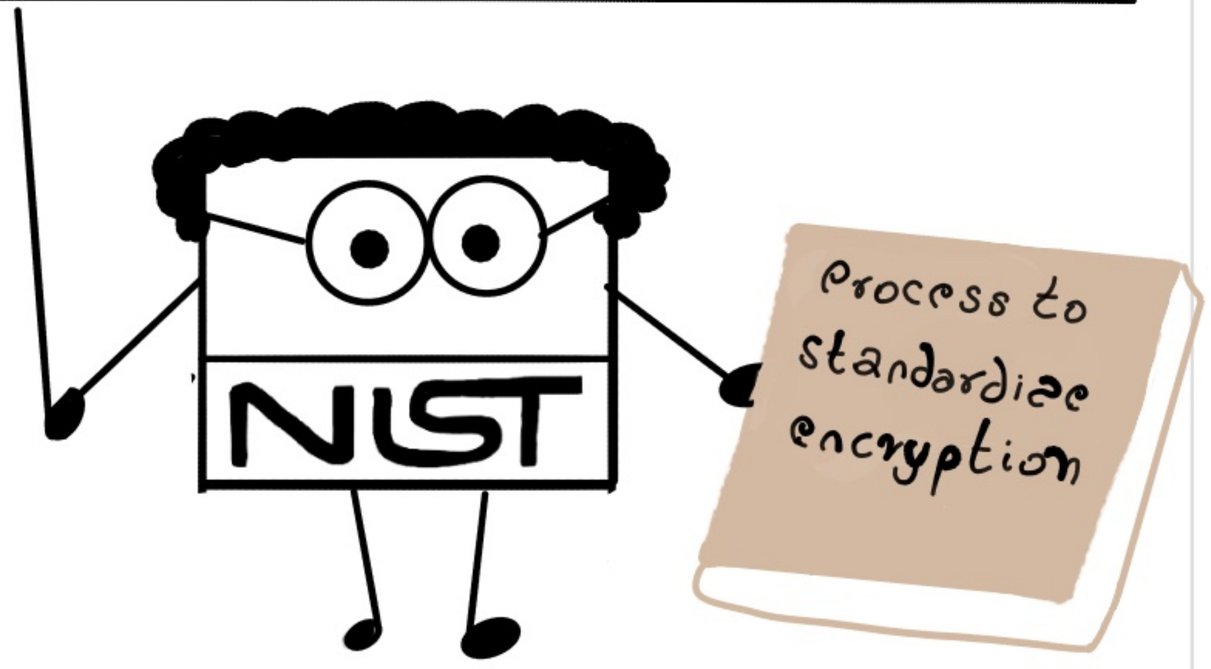
HMM, WHAT IF DES ALSO HAS A BACKDOOR?

available royalty-free world wide

WANTED:

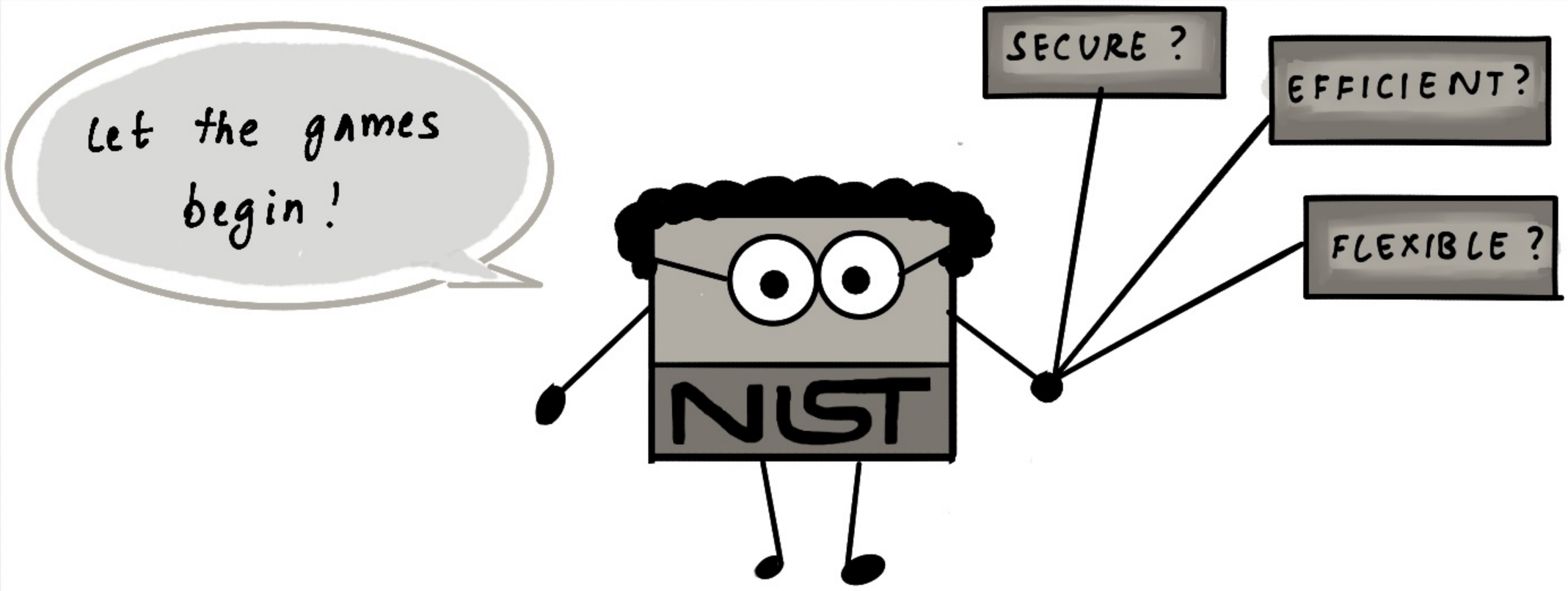
AN UNCLASSIFIED PUBLICLY DISCLOSED ENCRYPTION ALGORITHM CAPABLE OF PROTECTING SENSITIVE GOVERNMENT INFORMATION WELL INTO THE NEXT CENTURY

signed, NIST



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY - US GOVT

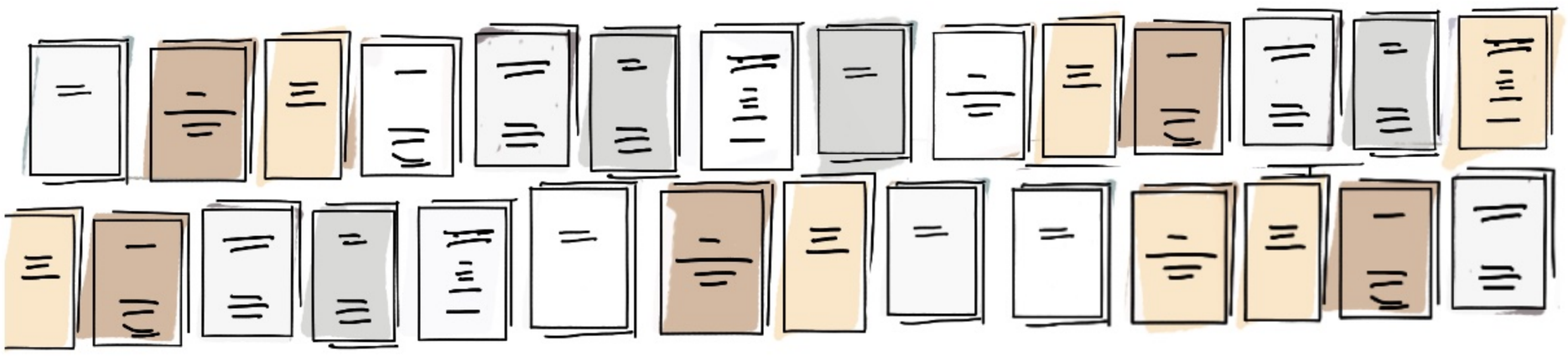
THE COMPETITION



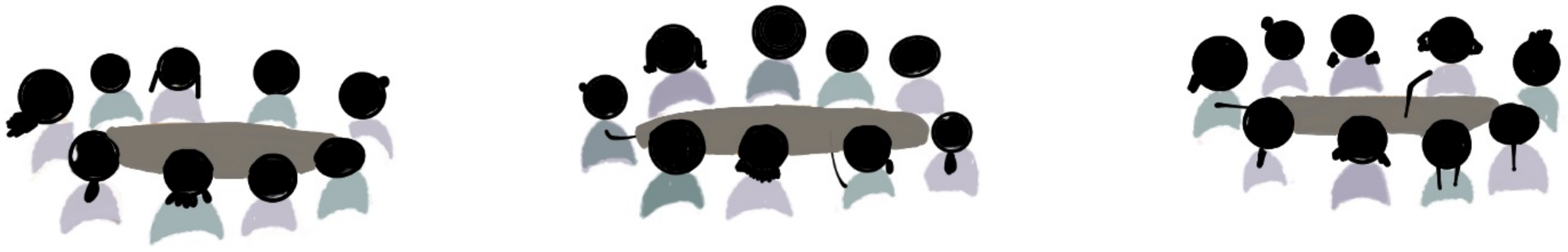
15 CANDIDATES

LOKI97 DFC TWOFISH DEAL CAST-256 MARS E2
SAFER+ FROG RIJNDAEL CRYPTON RC6 HPC SERPENT
MAGENTA

28 PAPERS WITH COMMENTS



3 CONFERENCES



MANY TECHNICAL CHALLENGES AND TWO ROUNDS OF VOTING LATER, THE RIJNDAEL ALGORITHM CAME TO BE CHOSEN AS THE ADVANCED ENCRYPTION STANDARD

WHERE AES IS USED

THE NSA USES AES TO PROTECT TOP SECRET INFORMATION AND NATIONAL SECURITY SYSTEMS

HERE ARE A FEW EVERYDAY INSTANCES OF AES IN USE

DATA IN STORAGE - USED BY APPLE DEVICES AND ON THE CLOUD BY GOOGLE

DATA IN TRANSIT - AWS USE AES-256 IN TLS
NETFLIX FOR VIDEO STREAMING

IN NETWORKS - THE SSL CERTIFICATION

WIFI NETWORKS - THE WPA2 - WIFI PROTECTED ACCESS

VIRTUAL PRIVATE NETWORKS - FOR BROWSING, GAMING
USED BY NORDVPN, EXPRESSVPN

MESSAGING APPS - WHATSAPP, SIGNAL, iMESSAGE

ONTO THE WORKINGS

HOW DOES AES WORK?

USING CONFUSION AND DIFFUSION- LIKE ANY GOOD SECURE CIPHER!

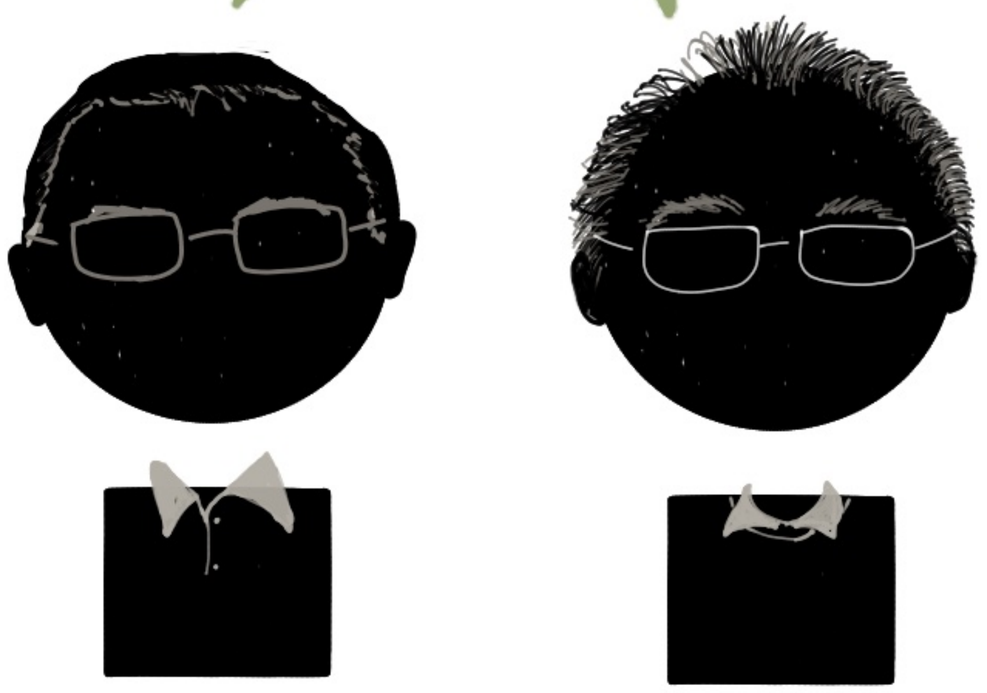
CLAUDE SHANNON

WE USED SP NETWORK A CLASS OF BLOCK CIPHERS-

S - SUBSTITUTION

P - PERMUTATION

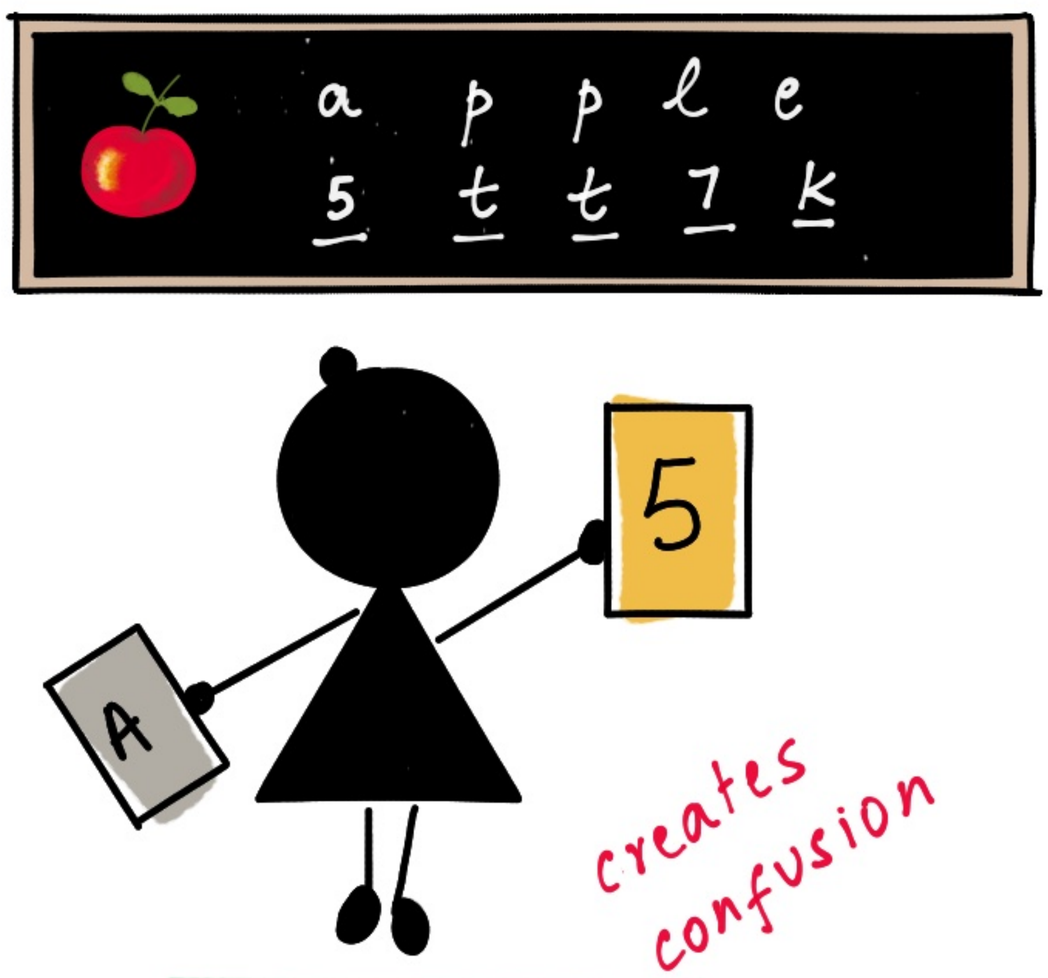
TO CREATE RIJNDAEL



VINCENT RIJMEN

JOAN DAEMEN

AN SP NETWORK CONTAINS ROUNDS OF A REPEATED SERIES OF MATHEMATICAL OPERATIONS



SUBSTITUTION

creates confusion

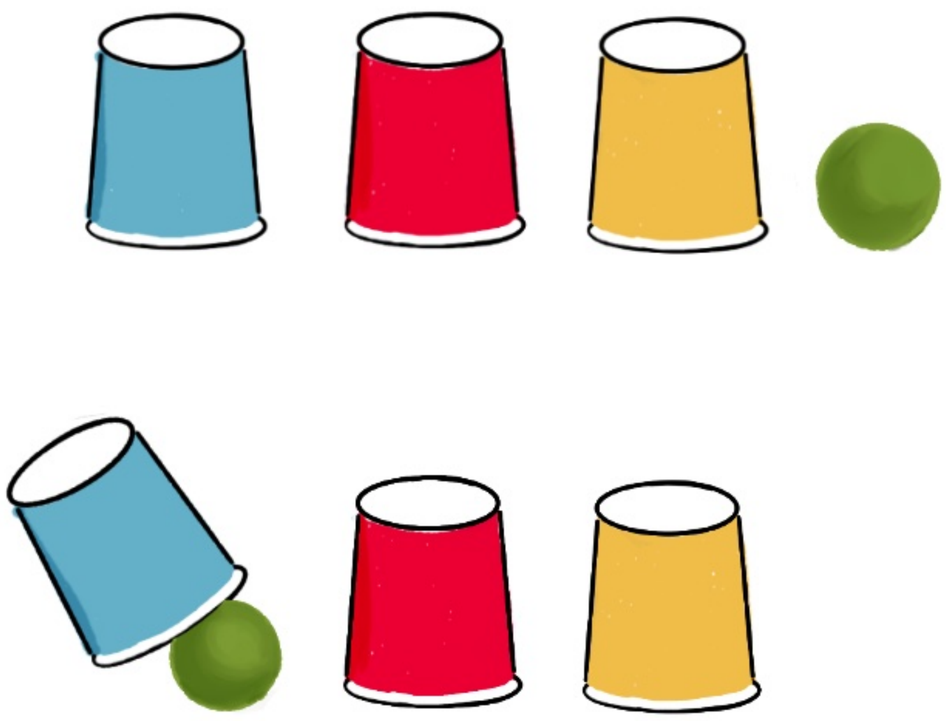
SWAP PLAIN TEXT

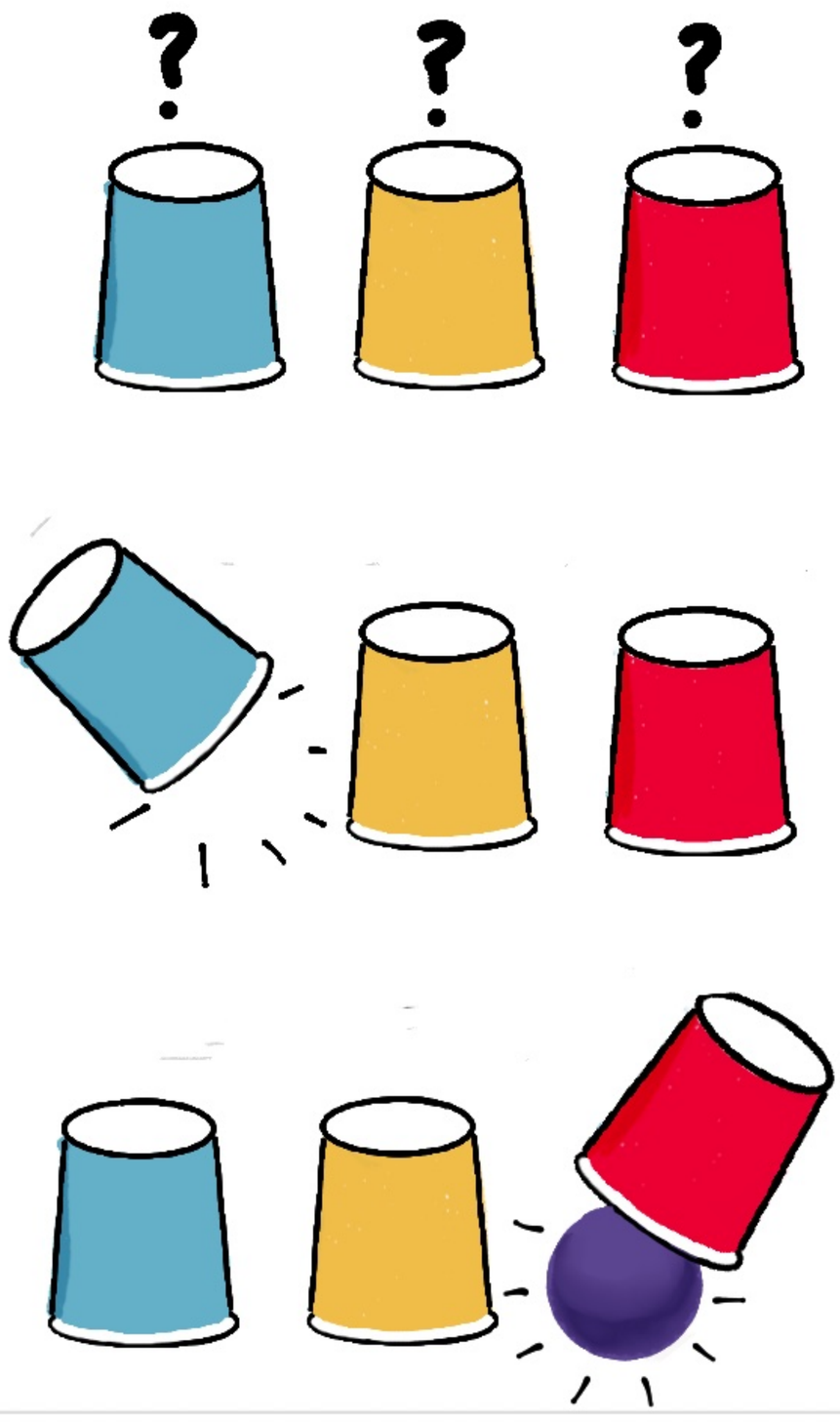
PERMUTATION

creates diffusion

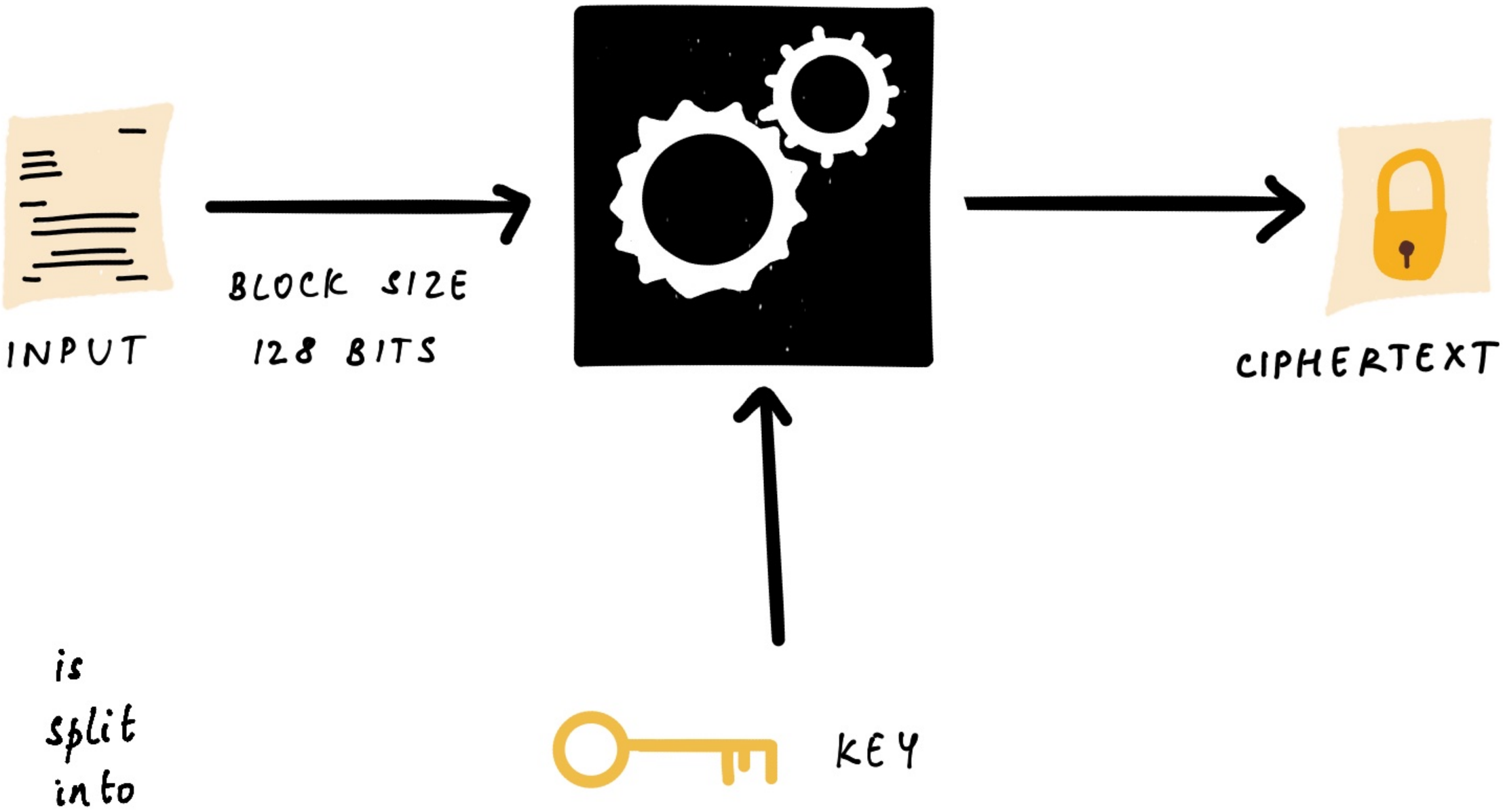
REARRANGE / MIX ELEMENTS

SOMETHING LIKE THIS





HOW AES WORKS

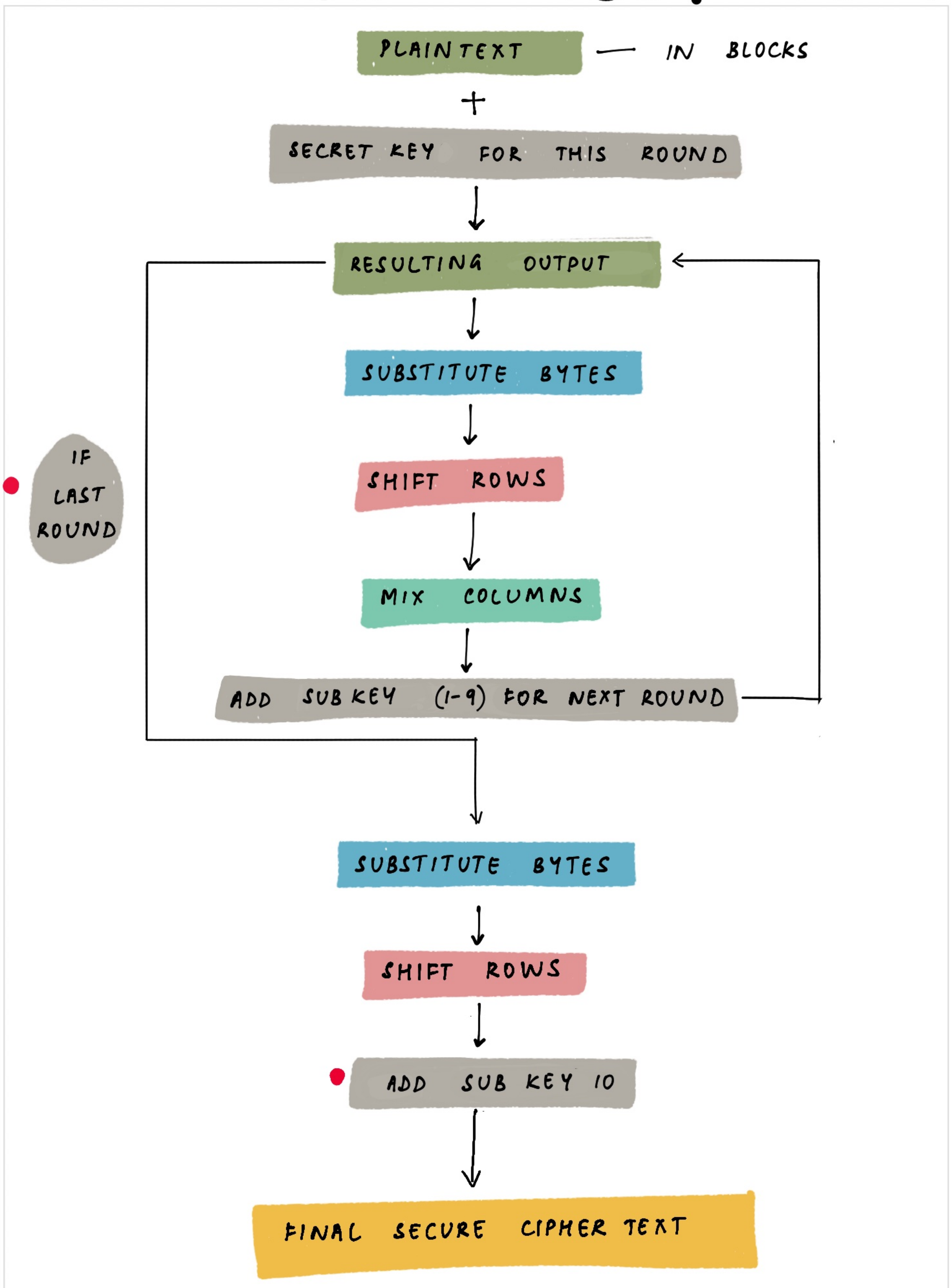


is
split
into
blocks

KEY

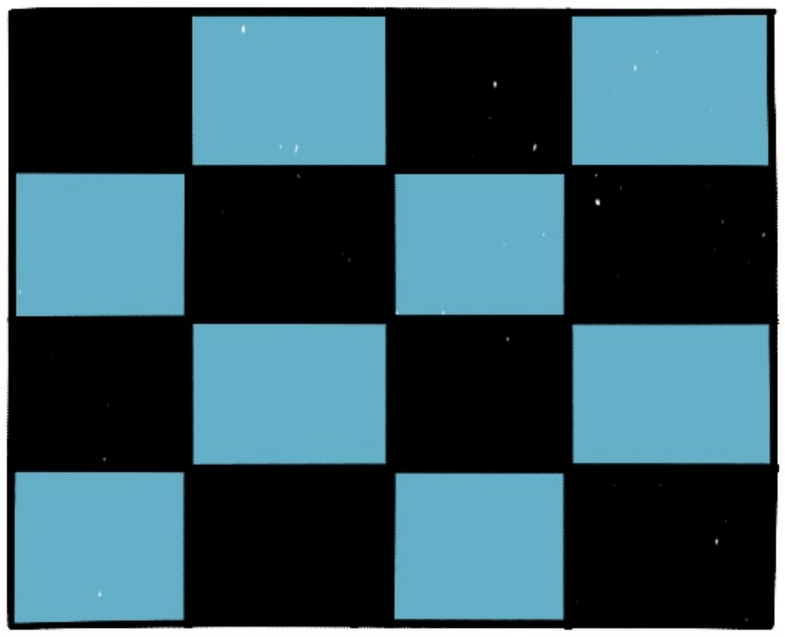
KEY SIZES
- 128 BITS
- 192 BITS
- 256 BITS

HOW AES REALLY WORKS



QUICK OBSERVATIONS

THE ENCRYPTION WORKS ON BLOCKS OF INPUT

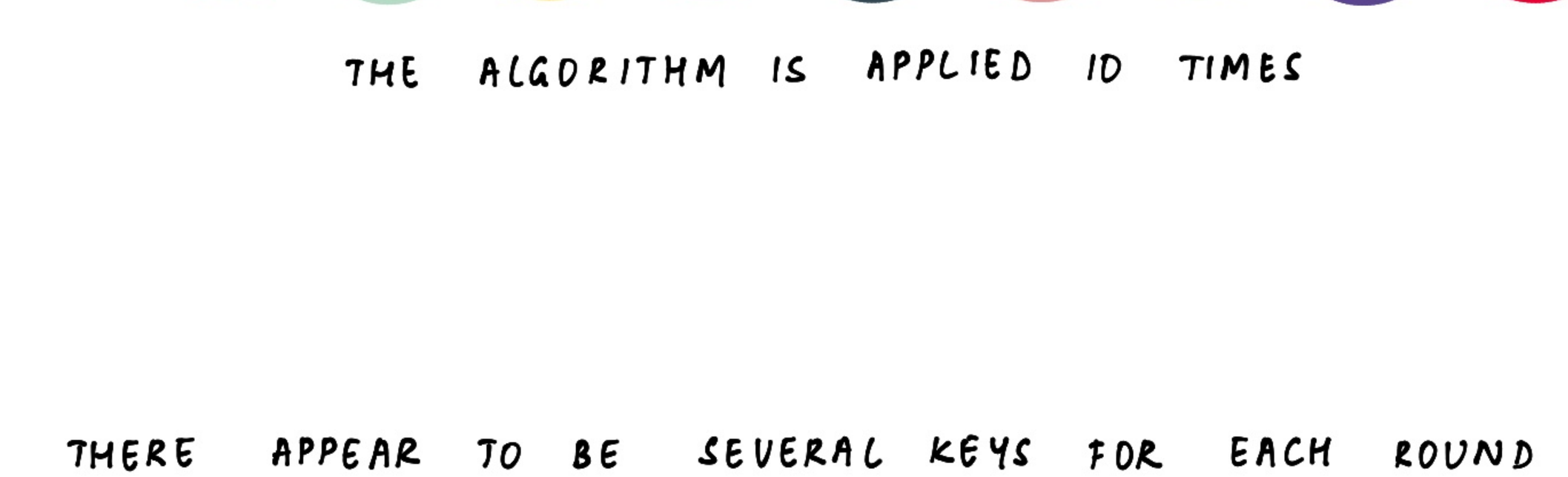


EACH OF SIZE 128 BITS

IT HAS SEVERAL ROUNDS OF ENCRYPTION

THE ALGORITHM IS APPLIED 10 TIMES

THERE APPEAR TO BE SEVERAL KEYS FOR EACH ROUND



ALL KEYS ARE GENERATED BASED ON THE PREVIOUS KEY

ENCRYPTION

STEP BY STEP

THE PLAINTEXT

gitanjaliwriting

g	n	i	t
i	j	w	i
t	a	r	n
a	l	i	g

67	6e	69	74
69	6a	77	69
74	61	72	6e
61	6c	69	67

THE PLAIN TEXT TO ENCRYPT

IS STORED IN A 4X4 MATRIX

EACH CELL IN THE MATRIX IS A BYTE

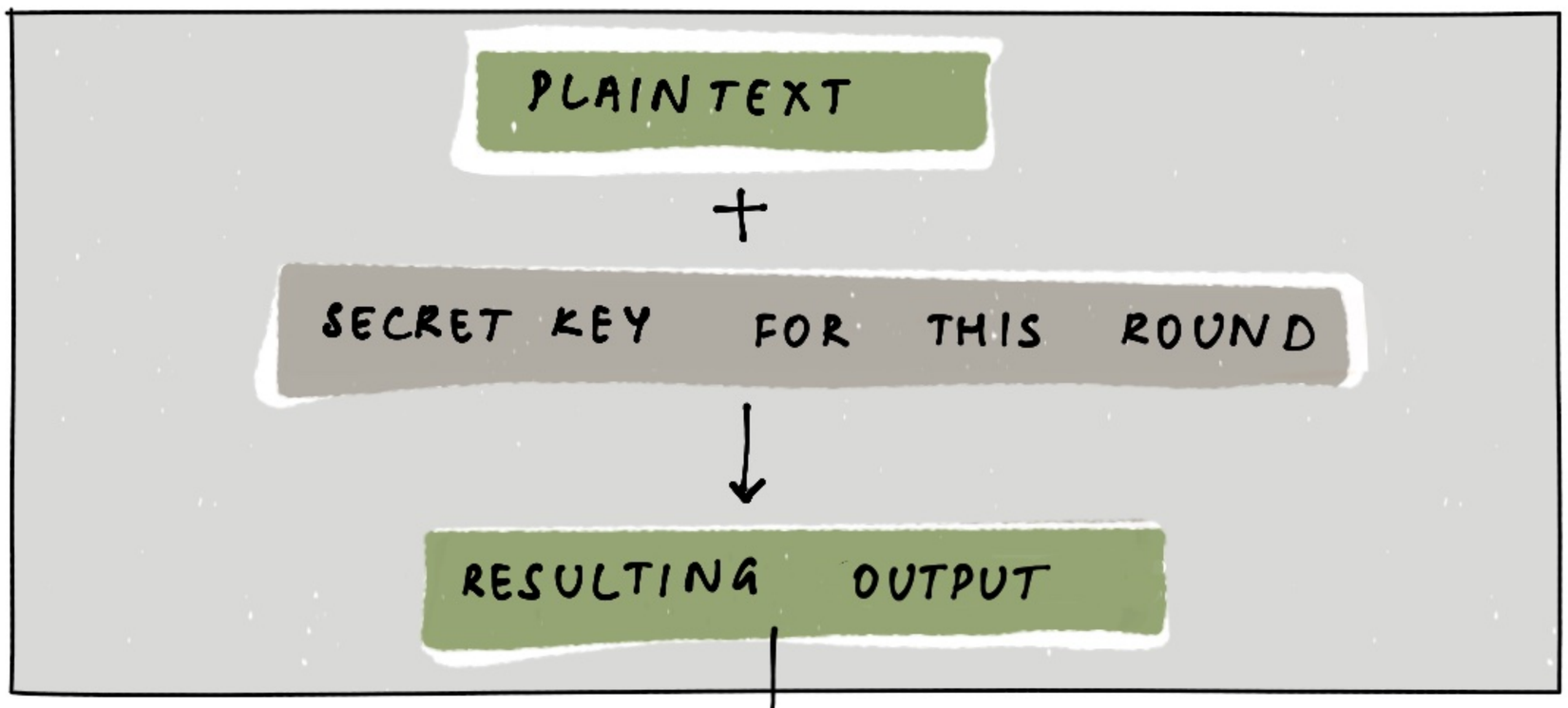
THE MATRIX HOLDS 16 BYTES

THIS IS ALSO REPRESENTED IN HEXADECIMAL

THIS MATRIX IS THE BLOCK

THE SIZE OF THE BLOCK IS 128 BITS

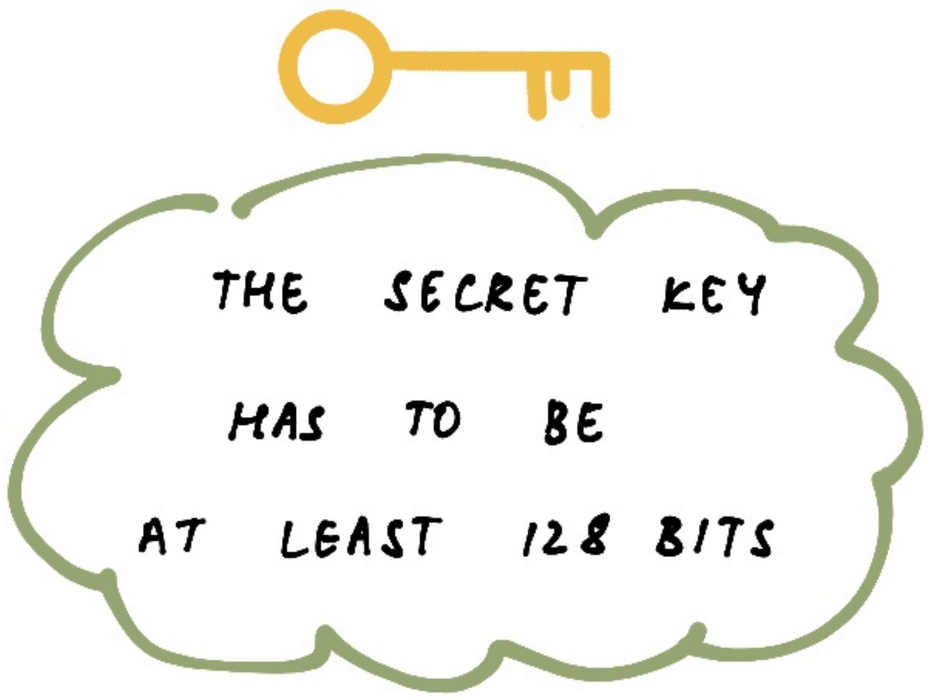
THE SECRET KEY



IS CALLED THE STATE ARRAY

ADD SECRET KEY TO PLAIN TEXT

THIS IS AN XOR OPERATION



TO SIMPCIFY, WE CHOOSE 8 BITS IN OUR EXAMPLE

PLAINTEXT	G	0	1	0	0	0	1	1	1
SECRET KEY	19	0	0	0	1	0	0	1	1
RESULT →		0	1	0	1	0	1	0	0

⊕

PLAINTEXT ⊕ SECRET KEY

67	6e	69	74
69	6a	77	69
74	61	72	6e
61	6c	69	67

gitanjaliwriting

⊕

6d	63	70	77
79	72	61	6f
73	65	73	72
65	74	73	64

my secret password

↓

0a	0d	19	03
10	18	16	06
07	04	01	1c
04	18	1a	03

state array

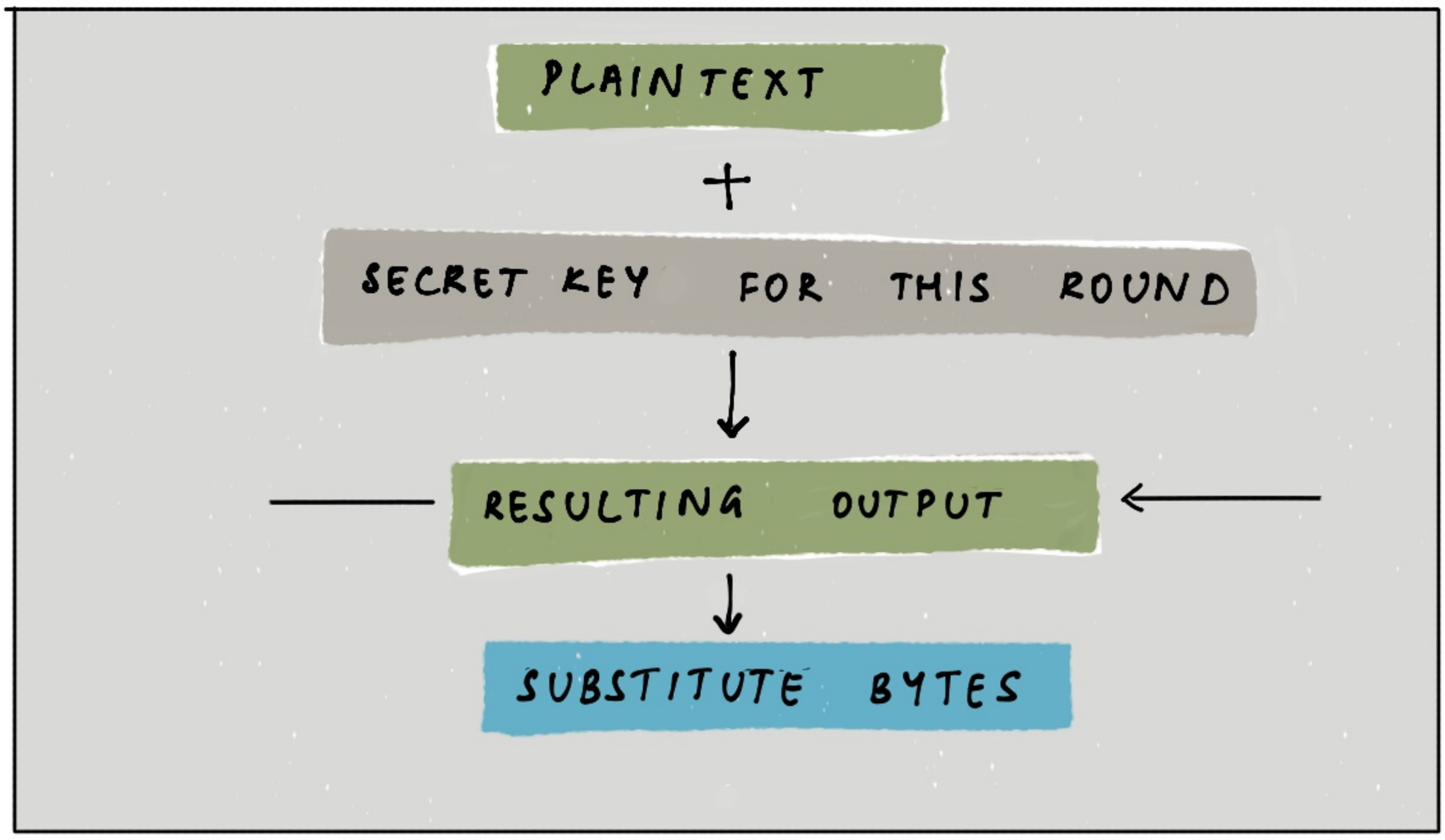
TO MAKE THE STATE ARRAY

XOR EACH CORRESPONDING CELL

6a	0	1	1	0	1	0	1	0
72	0	1	1	1	0	0	1	0
RESULT	0	0	0	1	1	0	0	0

THIS IS 18 IN HEXADECIMAL

SUBSTITUTE BYTES



BYTE SUBSTITUTION IS THE REPLACING OF EACH BYTE WITH ANOTHER USING A LOOK UP TABLE AS GIVEN IN THE NEXT PAGE

0a	0d	19	03
10	18	16	06
07	04	01	1c
04	18	1a	03

BEFORE SUBSTITUTION

67	d7	d4	7b
ca	ad	47	6f
c5	f2	7c	9c
f2	ad	a2	7b

AFTER SUBSTITUTION

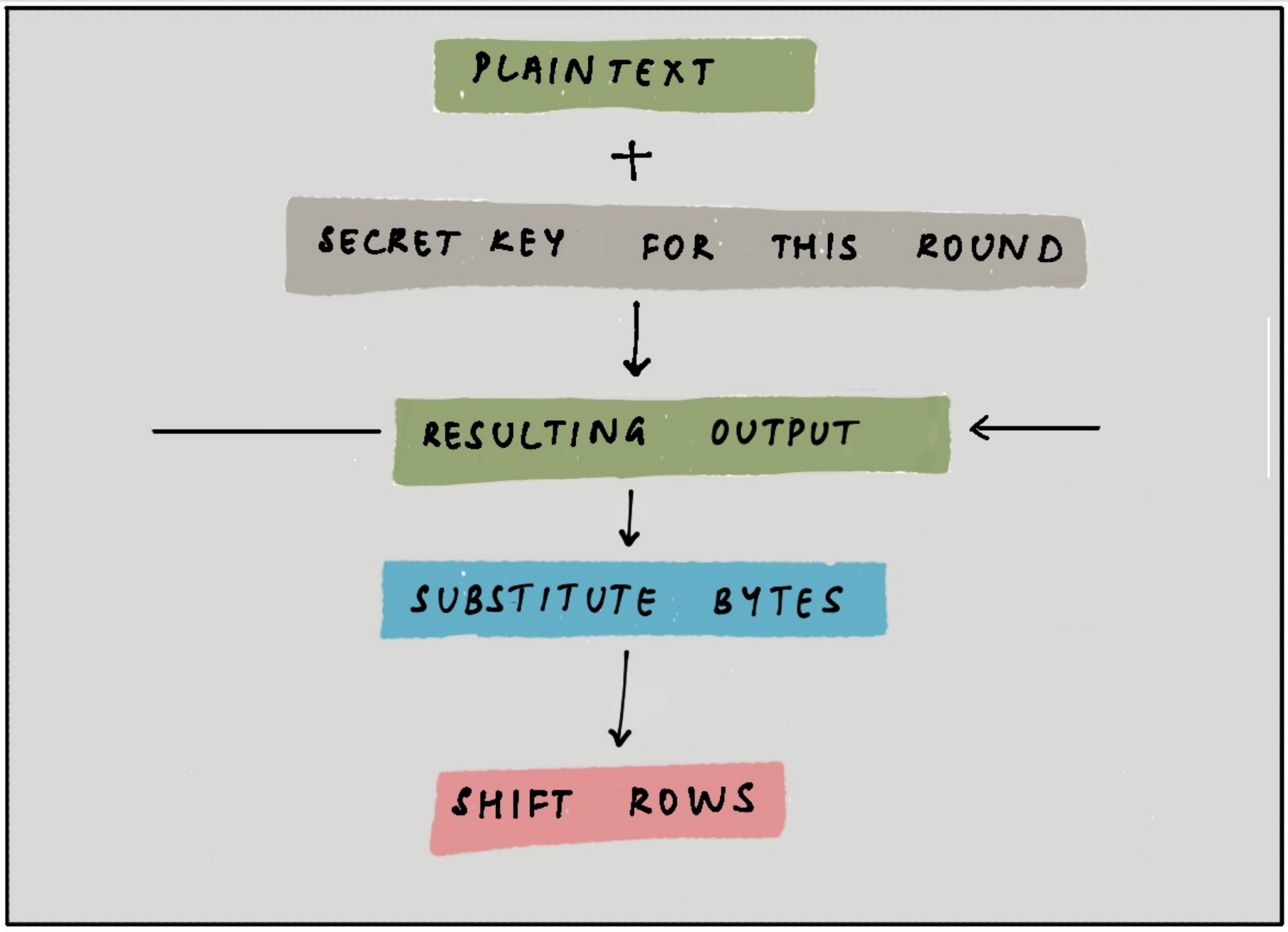
SUBSTITUTION BOX

AES SUBSTITUTION TABLE AKA RIJNDAEL S-BOX

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	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	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	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	06	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	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	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

2d IN HEXADECIMAL IS CONVERTED TO d8

SHIFT ROWS



SHIFTS THE ROWS AS FOLLOWS

ROW 1 : UNCHANGED

ROW 2 : CYCLICAL LEFT SHIFT BY 1 BYTE

ROW 3 : CYCLICAL LEFT SHIFT BY 2 BYTES

ROW 4 : CYCLICAL LEFT SHIFT BY 3 BYTES

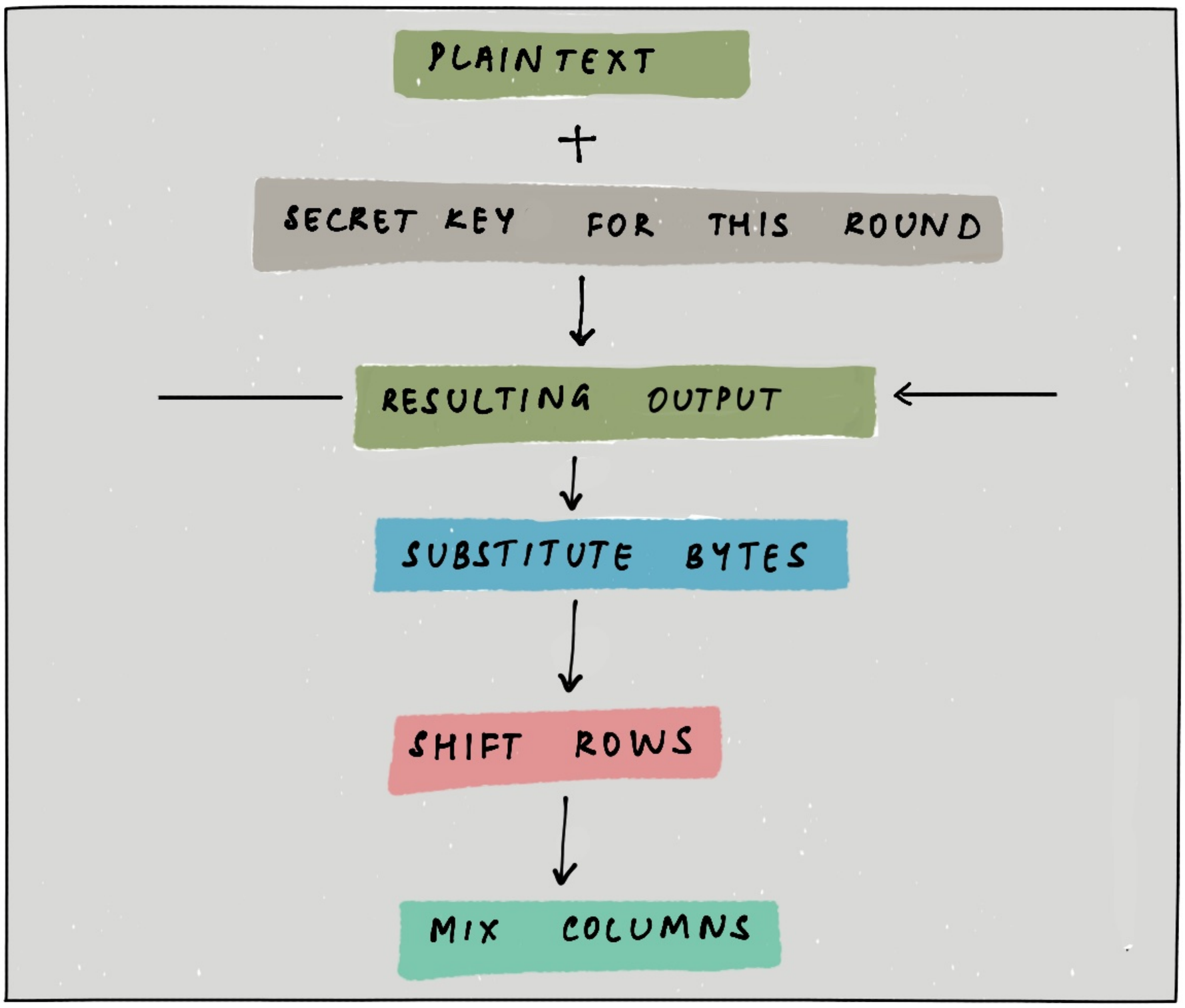
67	d7	d4	7b
ca	ad	47	6f
c5	f2	7c	9c
f2	ad	a2	7b

AFTER SUBSTITUTION & BEFORE SHIFT ROWS

67	d7	d4	7b
ad	47	6f	ca
7c	9c	c5	f2
7b	f2	ad	a2

AFTER SHIFT ROWS

MIX COLUMNS



MULTIPLY THE INPUT STATE ARRAY BY A STANDARD MATRIX — WHICH IS CONSTRUCTED BY A PATTERN OF CYCLICAL SHIFTS

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

A STANDARD MATRIX

*

67	d7	d4	7b
ad	47	6f	ca
7c	9c	c5	f2
7b	f2	ad	a2

INPUT STATE ARRAY
(OUTPUT OF SHIFT ROWS)

MATRIX MULTIPLICATION

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

*

67	d7	d4	7b
ad	47	6f	ca
7c	9c	c5	f2
7b	f2	ad	a2

↓

γ_1	γ_5	γ_9	γ_{13}
γ_2	γ_6	γ_{10}	γ_{14}
γ_3	γ_7	γ_{11}	γ_{15}
γ_4	γ_8	γ_{12}	γ_{16}

IF YOU ARE HAPPY TO ACCEPT THAT THERE IS A WAY TO ARRIVE AT THE ANSWER WITHOUT KNOWING THE METHOD, SKIP THE NEXT FEW PAGES AND ON TO THE KEY EXPANSION STEP.

HOWEVER IF YOU INSIST, STAY ON, AND WE WILL WORK THROUGH THE SOLUTION WITH SOME CONCEPTS IN ABSTRACT ALGEBRA.

JUST KEEP ON TOP OF ADD, MULTIPLY, BINARY/HEXADECIMAL CONVERSION AND XOR.

THINGS TO KNOW & REMEMBER

MATRICES

$$[M] = \begin{bmatrix} 2 & 1 & 3 \\ 4 & -2 & 5 \end{bmatrix}$$

A MATRIX IS A 2-D ARRAY OF NUMBERS

THE ORDER OF THIS MATRIX IS 2 x 3 .

2 ROWS x 3 COLUMNS

ORDER OF MULTIPLICATION MATTERS

$[A] \cdot [B]$ NOT EQUAL TO $[B] \cdot [A]$

ORDER OF THE MATRICES ALSO MATTERS

COLUMNS IN FIRST MATRIX MUST EQUAL # ROWS IN SECOND MATRIX

EXAMPLE

$$\begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix} \cdot \begin{bmatrix} 4 & 6 \\ 7 & 10 \end{bmatrix} = \begin{bmatrix} 2 \cdot 4 + 3 \cdot 7 & 2 \cdot 6 + 3 \cdot 10 \\ 1 \cdot 4 + 5 \cdot 7 & 1 \cdot 6 + 5 \cdot 10 \end{bmatrix}$$

$$= \begin{bmatrix} 29 & 42 \\ 39 & 56 \end{bmatrix}$$

GROUP

- THINK OF A SET OF NUMBERS

..., -3, -2, -1, 0, 1, 2, 3, 4, ...

- THINK OF THE OPERATION ADDITION

+

- ADD ANY 2 ELEMENTS IN THE SET.
  IS THE RESULT ALREADY AN ELEMENT IN THE SET?

-2 + 5 6 + 7 ✓ YES

- DO THEY ALL HAVE ADDITIVE INVERSES?

-3 3 -99 99 ✓ YES

- IS THE RESULT SAME WHEN YOU ADD ELEMENTS

LIKE THIS → (a + b) + c
OR THIS → a + (b + c) ✓ YES

- IS THERE A ZERO ?

45 + 0 = 0 + 45 = 45 ✓ YES

CONGRATULATIONS! YOU HAVE JUST DEFINED A GROUP!!

RING

REMEMBER THE SET

$$\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$$

THINK OF THE OPERATION MULTIPLICATION

$$\bullet$$

IS THE RESULT THE SAME FOR OPERATIONS

	$a + b$	$a \bullet b$
LIKE THIS		
OR THIS	$b + a$	$b \bullet a$

YES

IS THE PRODUCT OF ANY 2 ALSO AN ELEMENT IN THE GROUP

$-2 \bullet 3$	$16 \bullet 9$

YES

IS THE RESULT THE SAME WHEN YOU DISTRIBUTE MULTIPLICATION OVER ADDITION - LIKE THIS ?

$$a \bullet (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

YES

DON'T WORRY IF MULTIPLICATION DOES NOT HAVE AN INVERSE IN THIS SET !

CONGRATULATIONS ! YOU HAVE JUST DEFINED A RING !!

FIELD

FIND A FRESH EXAMPLE SET

RATIONAL NUMBERS -

ANY NUMBER EXPRESSED AS

A RATIO $\rightarrow \frac{a}{b}$

$-\frac{2}{3}$ $\frac{6}{1}$ $\frac{8}{4}$ $\frac{3}{6}$ $\frac{4}{7}$

$\frac{20}{21}$ $\frac{35}{6}$ $\frac{0}{1}$ $\frac{5}{8}$

RATIONAL NUMBERS HAVE INFINITE NUMBER OF ELEMENTS.

THE ELEMENTS FULFILL THE RULES FOR a, b, c

IN THE FORM $\frac{p}{q}$ AND $q \neq 0$

✓ ADDITION

$$a + b = b + a$$
$$(a+b)+c = a+(b+c)$$
$$a+0 = 0+a$$

✓ ADDITIVE INVERSE

$$a + (-a) = 0$$

✓ MULTIPLICATION

$$a \cdot b = b \cdot a$$
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
$$a \cdot 1 = 1 \cdot a$$

✓ • DISTRIBUTIVE OVER +

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$

AS WELL AS ....

✓ MULTIPLICATIVE INVERSE

$$a \cdot (a^{-1}) = 1 \quad \text{where } a \neq 0$$

CONGRATUCLATIONS! YOU HAVE JUST DEFINED A FIELD !!

FINITE FIELD

A FINITE FIELD IS ONE WITH FINITE NUMBER OF ELEMENTS

AN EXAMPLE : THE SET OF ALL INTEGERS MODULO 2

$0 \bmod 2 = 0$

$1 \bmod 2 = 1$

$2 \bmod 2 = 0$

$3 \bmod 2 = 1$

$4 \bmod 2 = 0$

$5 \bmod 2 = 1$

:

:

TWO ELEMENTS

THE ELEMENTS ARE $\{0, 1\}$

ADDITION

+	0	1
0	0	1
1	1	0

MULTIPLICATION

×	0	1
0	0	0
1	0	1

A FINITE FIELD IS ALSO CALLED A GALOIS FIELD

NOTATION : GF(2)

PRIME NUMBER

OTHER EXAMPLES OF FINITE FIELDS

- INTEGERS MODULO PRIME NUMBER GF(p)
- INTEGERS MODULO POWER OF PRIME NUMBER $GF(p^m)$

WITH THE NUMBER OF ELEMENTS = p^m

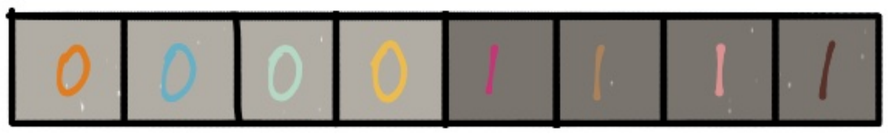
GALOIS FIELDS & AES

FOR AES, A VERY SPECIFIC GALOIS FIELD IS INTERESTING

IT IS $GF(256) = GF(2^8)$

GF(2) INDICATES THAT THE VALUES ARE 0 AND 1

THE POWER 8 CONVENIENTLY FITS IN A BYTE



GIVING 256 COMBINATIONS

OPERATIONS + • ALONG WITH THEIR INVERSES

GIVE RESULTS IN THE SAME SET OF 256 ELEMENTS

THESE ELEMENTS CAN BE WRITTEN AS POLYNOMIALS

LET US LOOK AT POLYNOMIALS AND THEIR OPERATIONS

POLYNOMIALS

A POLYNOMIAL IS A MATHEMATICAL SENTENCE

IT HAS MANY TERMS

CONNECTED BY OPERATORS

UNKNOWNS OR VARIABLES — x y

'POWERS' OR EXPONENTS — x^2 y^3

COEFFICIENTS OR MULTIPIERS — $4x^2$ $\frac{1}{9}y^3$

CONSTANTS — 5 -32

\+ ADD

− SUBTRACT

* MULTIPLY

÷ DIVIDE

EXAMPLES

$x + 2$

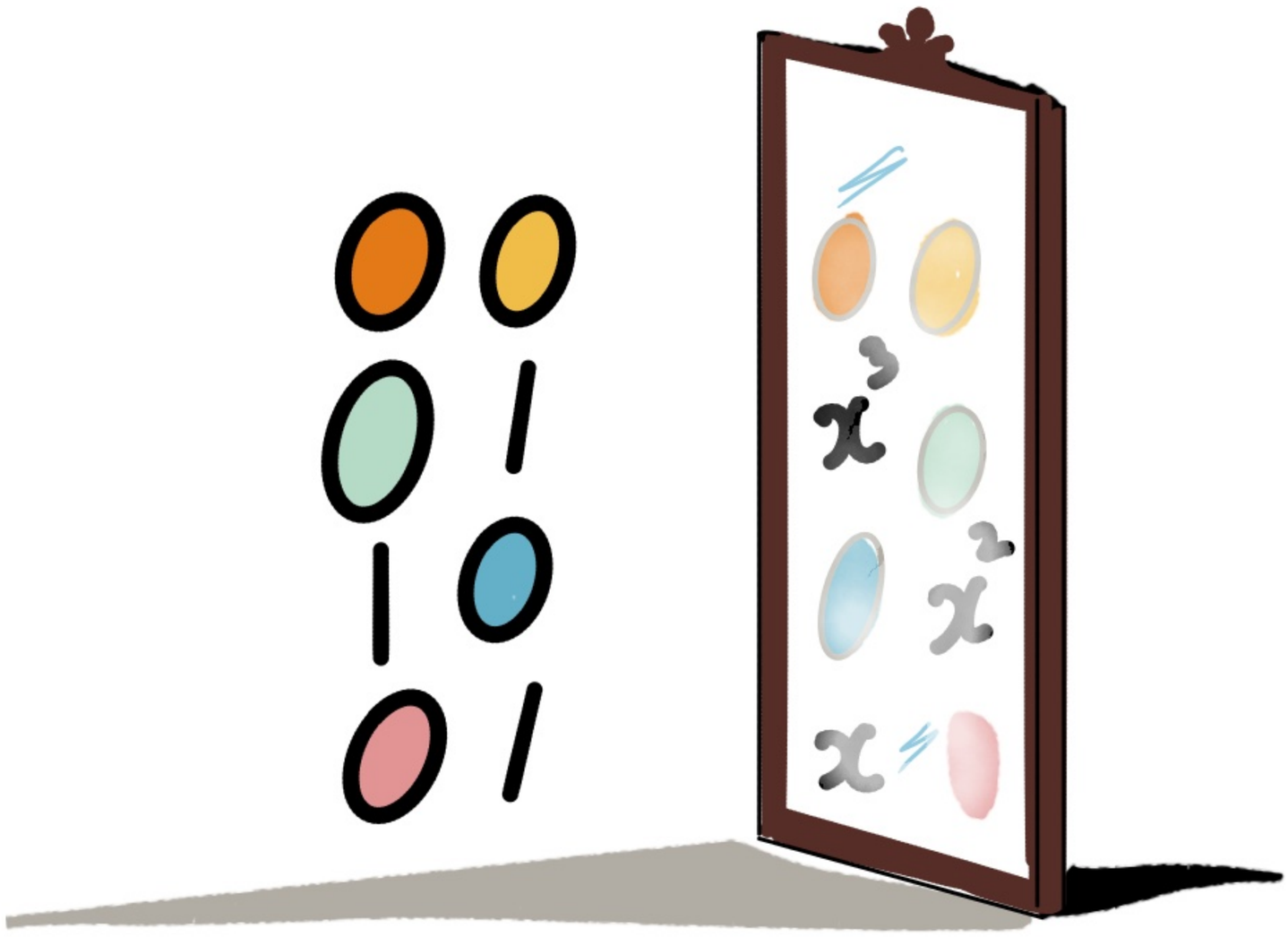
$y^2 - 2y + 3$

$2y - 4x$

$x^2 + 2x + 4$

$3x^6 - \frac{4}{5}x^2y + 2x - 53$

POLYNOMIALS & BINARY NUMBERS



BINARY NUMBERS CAN BE WRITTEN IN POLYNOMIAL FORM!

$$ax^7 + ax^6 + ax^5 + ax^4 + ax^3 + ax^2 + ax + 1$$

FOR UNKNOWN x, COEFFICIENT a IS EITHER 0 OR 1

DECIMAL	BINARY	POLYNOMIAL
1	001	$0 + 0 + 1 \longrightarrow 1$
2	010	$0 + x + 0 \longrightarrow x$
3	011	$0 + x + 1 \longrightarrow x + 1$
4	100	$x^2 + 0 + 0 \longrightarrow x^2$
5	101	$x^2 + 0 + 1 \longrightarrow x^2 + 1$
7	111	$x^2 + x + 1$
10	1010	$x^3 + 0 + x + 1$

POLYNOMIAL OPERATIONS

+	0	1
0	0	1
1	1	0

ADDITION & SUBTRACTION IN $GF(2^m)$ IS XOR

$7 \rightarrow 111$

$3 \rightarrow 011$

$$x^2 + \cancel{x} + \cancel{1} \oplus \cancel{x} + \cancel{1} = x^2$$

$$0000\ 0111 \oplus 0000\ 0011 = 0000\ 0100$$

×	0	1
0	0	0
1	0	1

MULTIPLICATION TAKES PLACE WITH THE FAMILIAR RULES

$7 \rightarrow 111$

$3 \rightarrow 011$

$$(x^2 + x + 1) \bullet (x + 1) = \cancel{x^2} + \cancel{x} + 1 + x^3 + \cancel{x^2} + \cancel{x} = x^3 + 1$$

IRREDUCIBLE POLYNOMIAL

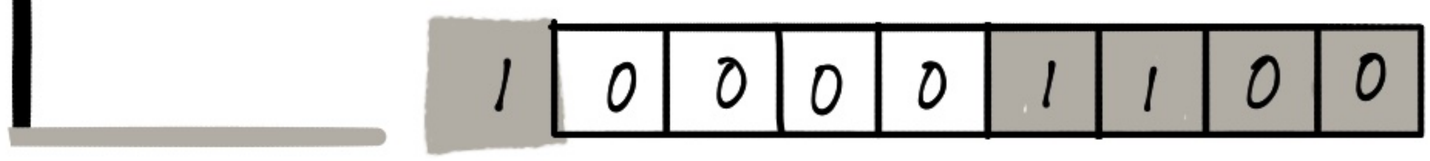
LET'S SAY WE ARE MULTIPLYING

$$x^4 + x + 1$$

$$\times \quad x^2$$

$$x^8 + x^3 + x^2$$

THE RESUCT IN BINARY IS OVER A BYTE AND IS NOT AN ELEMENT IN GF(256)



TO REDUCE IT TO BYTE SIZE, THE CONVENTION IS TO USE THE IRREDUCIBLE POLYNOMIAL AND XOR THE TWO.

IRREDUCIBLE POLYNOMIAL

$$x^8 + x^4 + x^3 + x + 1$$

BINARY FORM

1 0001 1011

Predefined algorithm + performs a modulus

$$\begin{array}{r} 1\ 0000\ 1100 \\ 1\ 0001\ 1011 \\ \hline 0\ 0001\ 0111 \end{array} \oplus$$

RECALL THAT...

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

*

67	d7	d4	7b
ad	47	6f	ca
7c	9c	c5	f2
7b	f2	ad	a2

↓

γ_1	γ_5	γ_9	γ_{13}
γ_2	γ_6	γ_{10}	γ_{14}
γ_3	γ_7	γ_{11}	γ_{15}
γ_4	γ_8	γ_{12}	γ_{16}

WE ARE TRYING TO PERFORM MATRIX MULTIPLICATION IN ORDER TO DO MIX COLUMNS AS AN ENCRYPTION STEP

$$\gamma 1 = 02 \cdot 67 + 03 \cdot ad + 01 \cdot 7c + 01 \cdot 7b$$

ALL OPERATIONS ARE GALOIS / FINITE FIELD ARITHMETIC

WE START BY CONVERTING ALL HEX TO BINARY

THEN, BINARY TO POLYNOMIAL TO DO THE OPERATIONS

FINDING γ_1

$$\gamma_1 = 02 \cdot 67 + 03 \cdot ad + 01 \cdot 7c + 01 \cdot 7b$$

$$02 \cdot 67 = 0000\ 0010 \cdot 0110\ 0111$$

$$= x \cdot (x^6 + x^5 + x^2 + x + 1)$$

$$= x^7 + x^6 + x^3 + x^2 + x$$

$$03 \cdot ad = 0000\ 0011 \cdot 1010\ 1101$$

$$= (x+1)(x^7 + x^5 + x^3 + x^2 + 1)$$

$$= x^8 + x^6 + x^4 + x^3 + x + x^7 + x^5 + x^3 + x^2 + 1$$

$$= x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$$

$$01 \cdot 7c = 0000\ 0001 \cdot 0111\ 1100$$

$$= 1 \cdot (x^6 + x^5 + x^4 + x^3 + x^2)$$

$$01 \cdot 7b = 0000\ 0001 \cdot 0111\ 1011$$

$$= 1 \cdot (x^6 + x^5 + x^4 + x^3 + x + 1)$$

IDENTICAL TERMS CANCEL OUT AS IT IS AN XOR.

$$\gamma_1 = x^8 + x^5 + x^4 + x^3 + x^2 + x$$

FINDING γ_1 - γ_{16}

$\gamma_1 = x^8 + x^5 + x^4 + x^3 + x^2 + x$

$\gamma_1 = 1\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 0$

IRREDUCIBLE POLYNOMIAL $= 1\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 1$

XOR THE TWO

$$
\begin{array}{rl}
1 & 0\ 0\ 1\ 1\ 1\ 1\ 1\ 0 \\
1 & 0\ 0\ 0\ 1\ 1\ 0\ 1\ 1 \\
\hline
0 & 0\ 0\ 1\ 0\ 0\ 1\ 0\ 1
\end{array}
\quad \rightarrow \quad 37_{10} \rightarrow 25_{16}
$$

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

$*$

67	d7	d4	7b
ad	47	6f	ca
7c	9c	c5	f2
7b	f2	ad	a2

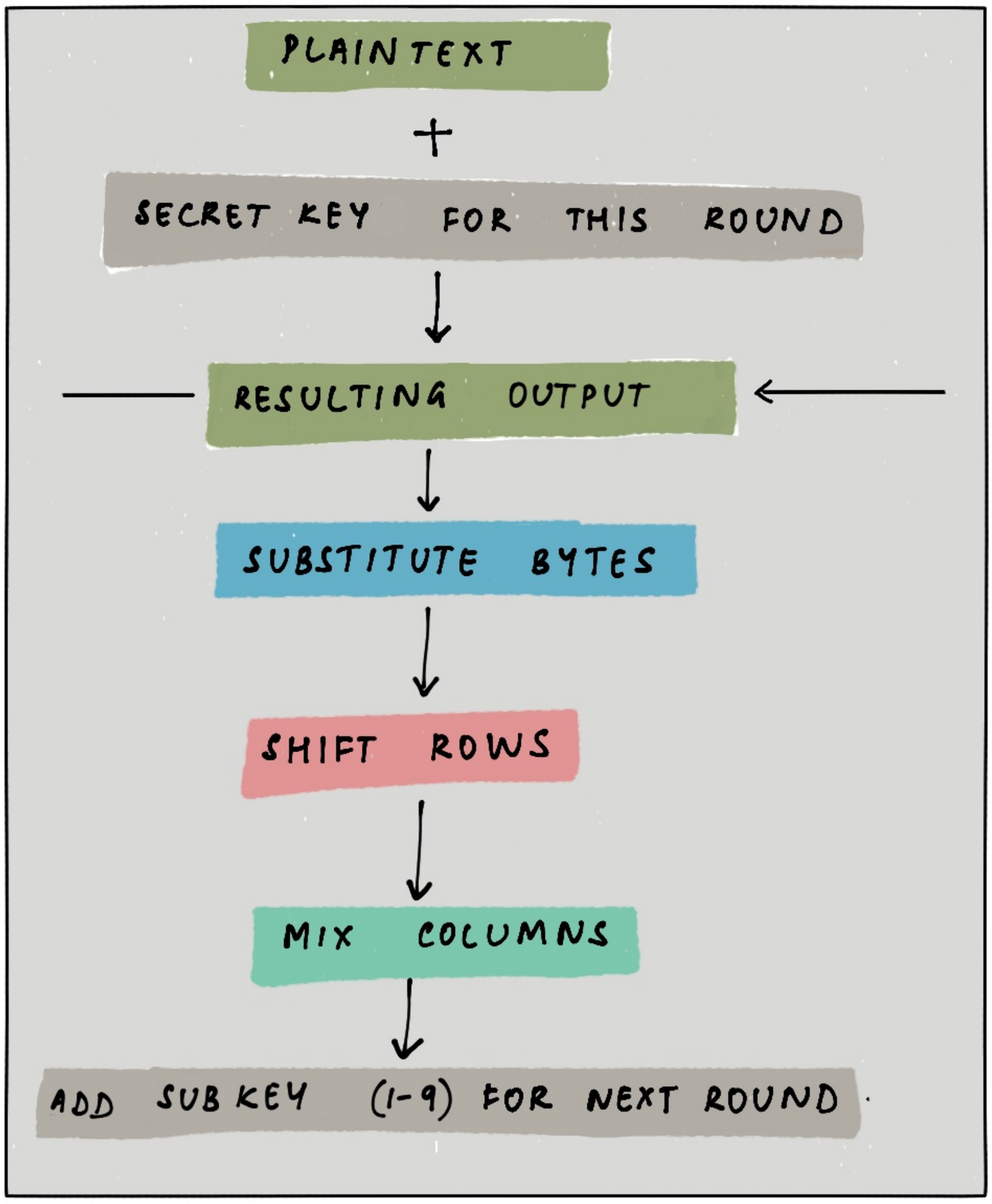
$\downarrow$

25	γ_5	γ_9	γ_{13}
γ_2	γ_6	γ_{10}	γ_{14}
γ_3	γ_7	γ_{11}	γ_{15}
γ_4	γ_8	γ_{12}	γ_{16}

THAT'S HOW EACH VALUE γ_1 THROUGH γ_{16} IS CALCULATED

ADD SUBKEY

ADDING A ROUNDKEY IS TO XOR WITH OUTPUTS OF PREVIOUS STEP



EACH ROUND NEEDS A 128 BIT KEY.

WE ONLY CHOOSE ONE 128 BIT SECRET KEY

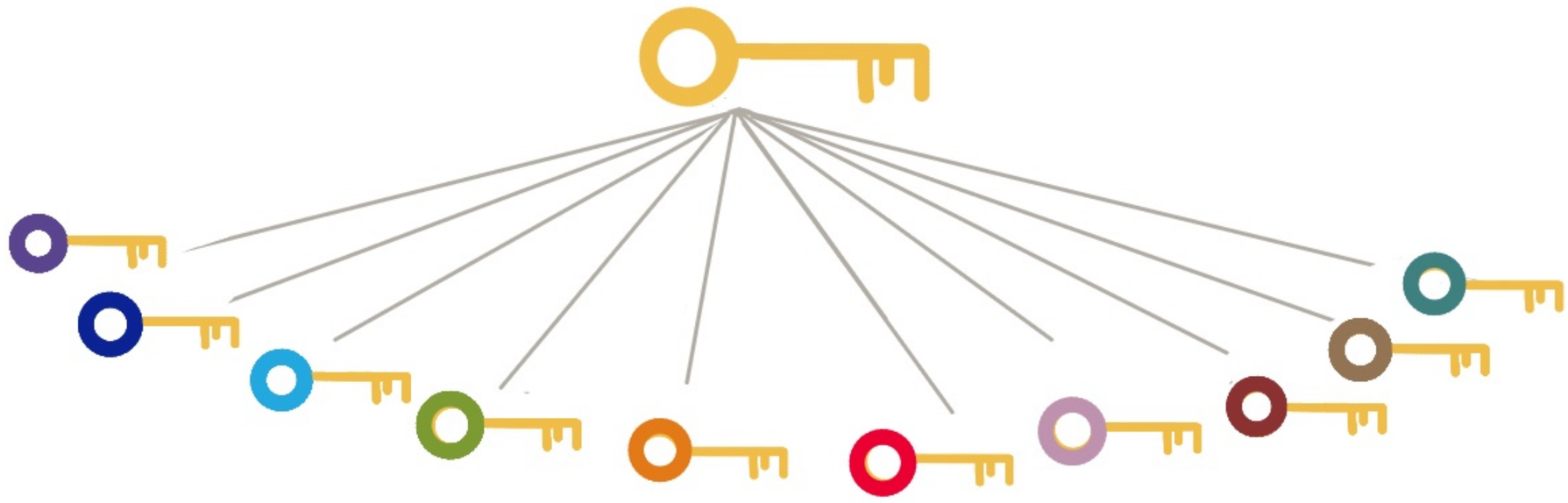
my secretpassword

6d	63	70	77
79	72	61	6f
73	65	73	72
65	74	73	64

WHERE DO THE OTHER 10 SUBKEYS OR ROUND KEYS COME FROM ?

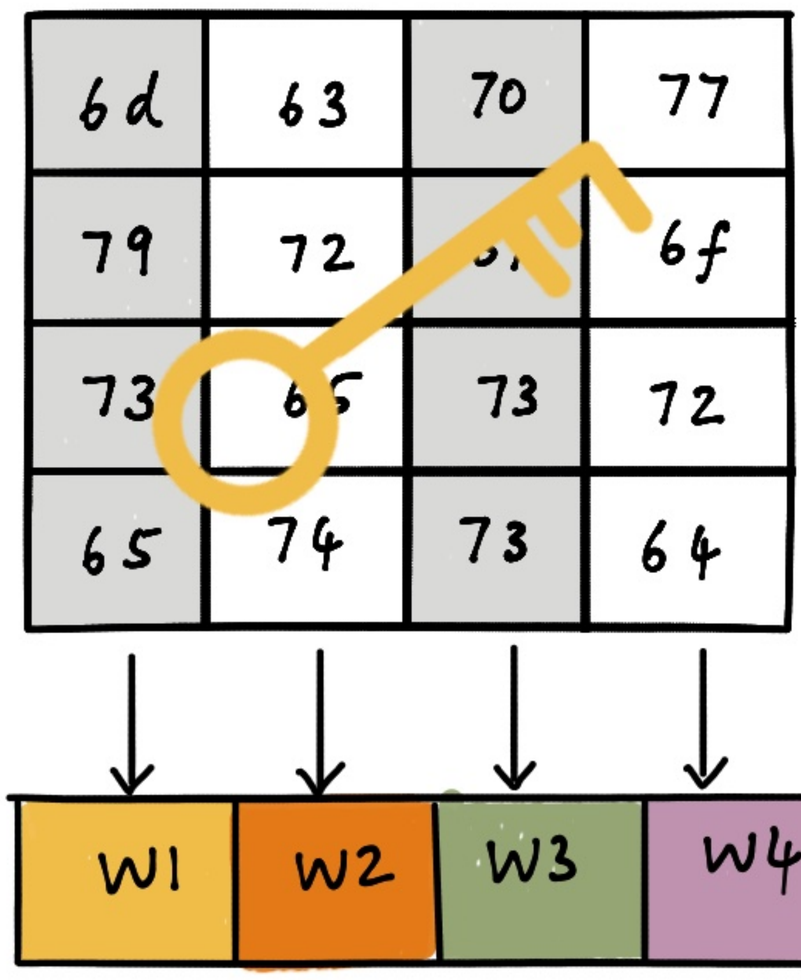
KEY EXPANSION

THE SECRET KEY IS USED TO GENERATE THE 10 OTHER SUBKEYS NEEDED FOR EACH ROUND.



THIS PROCESS IS CALLED KEY EXPANSION

HERE IS THE SECRET KEY IN HEXADECIMAL



TREAT EACH COLUMN AS A WORD

EACH OF SIZE 4 BYTES

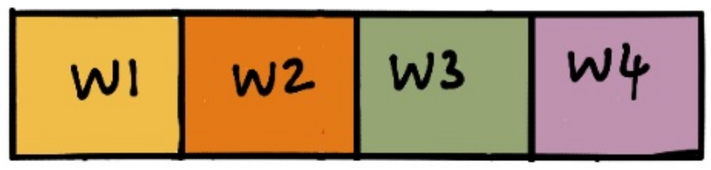
FOR THE 10 ROUNDS WE NEED 4 WORDS EACH

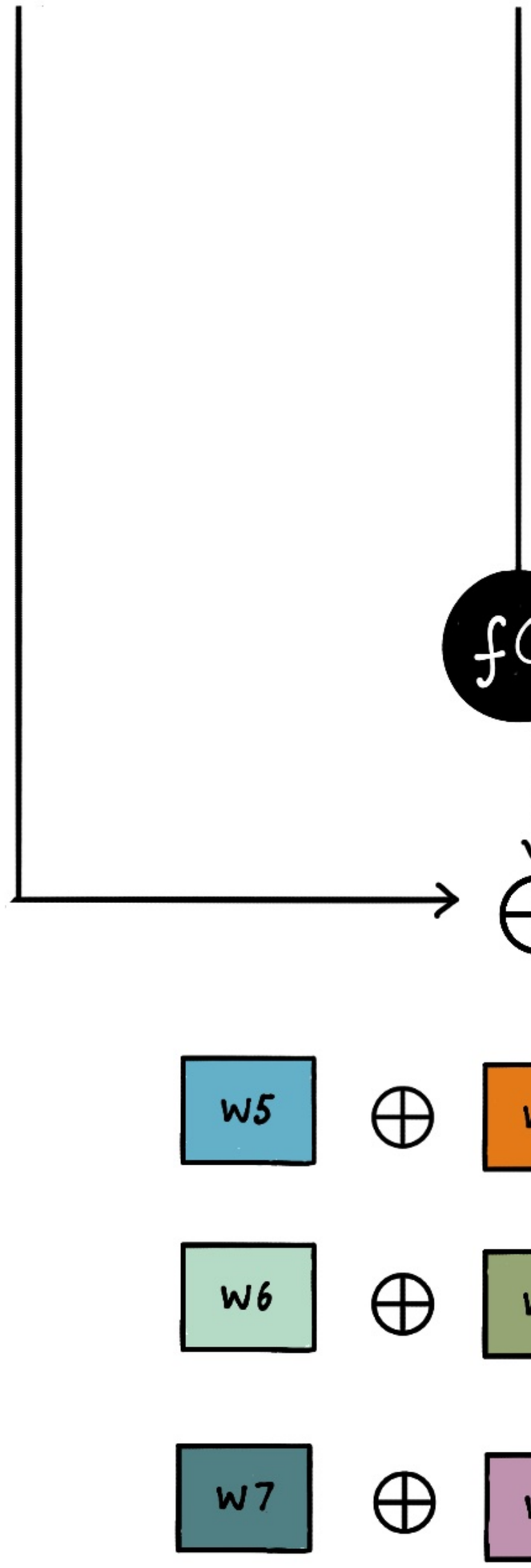
BASED ON W1, W2, W3, W4 WE GENERATE 40 WORDS

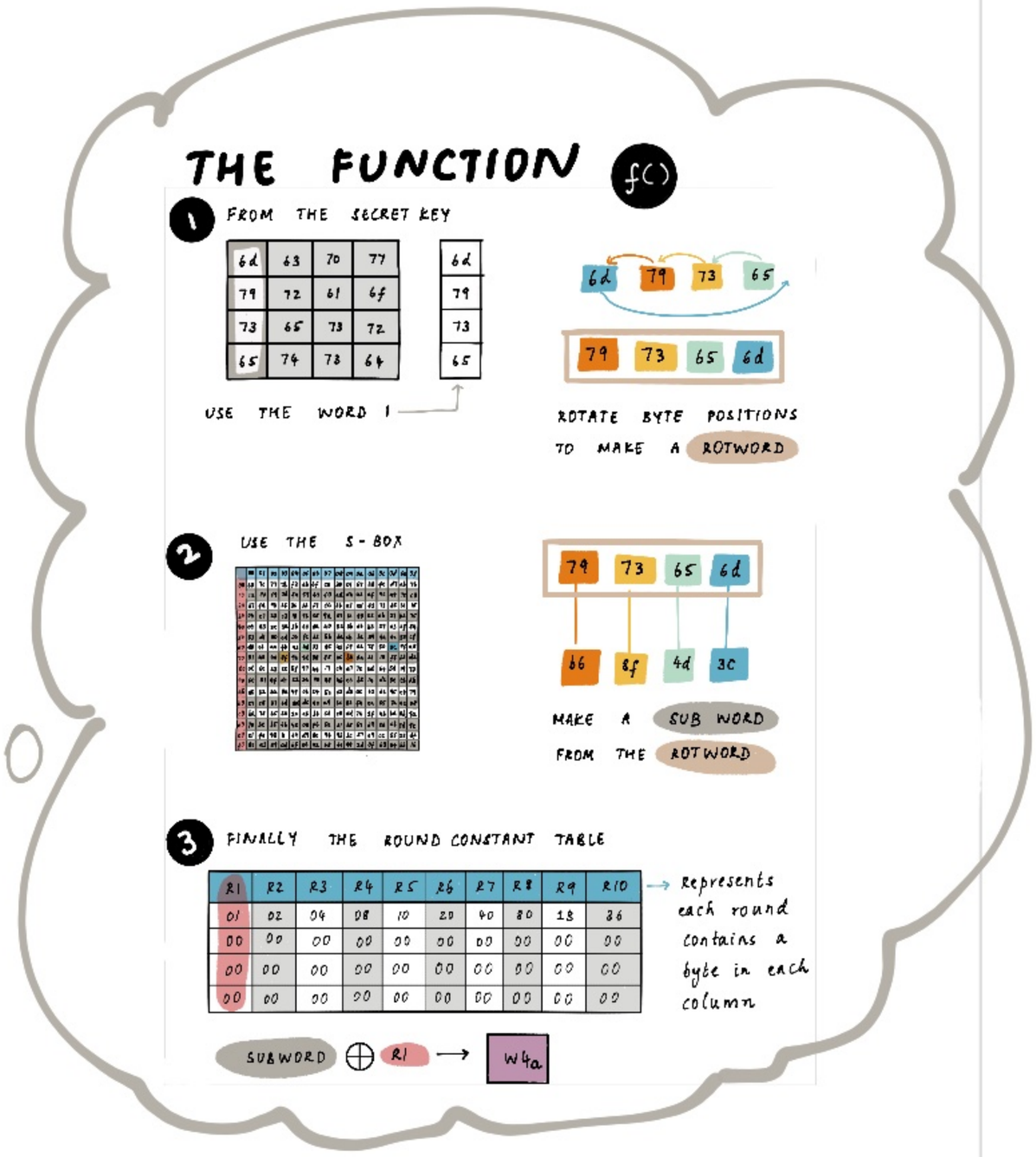
W5, W6 .... W44

FINDING SUBKEY 1

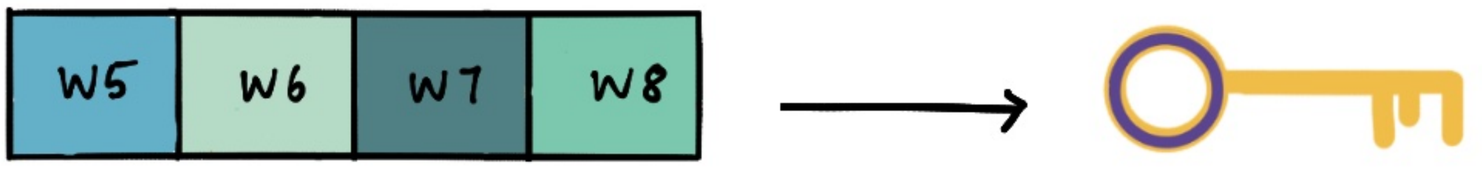
USE THE 4 WORDS







THE KEY IS EXPANDED AND READY TO USE* IN ROUND 1



* USE MEANS TO XOR WITH PREVIOUS STEP

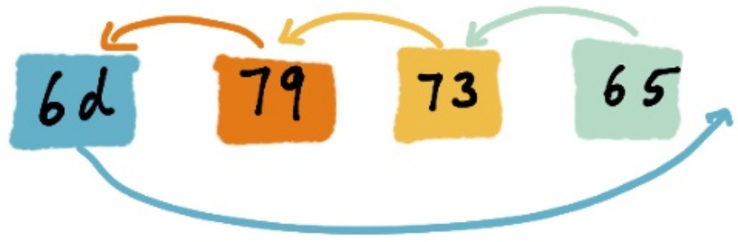
THE FUNCTION f()

1 FROM THE SECRET KEY

6d	63	70	77
79	72	61	6f
73	65	73	72
65	74	73	64

6d
79
73
65

USE THE WORD 1

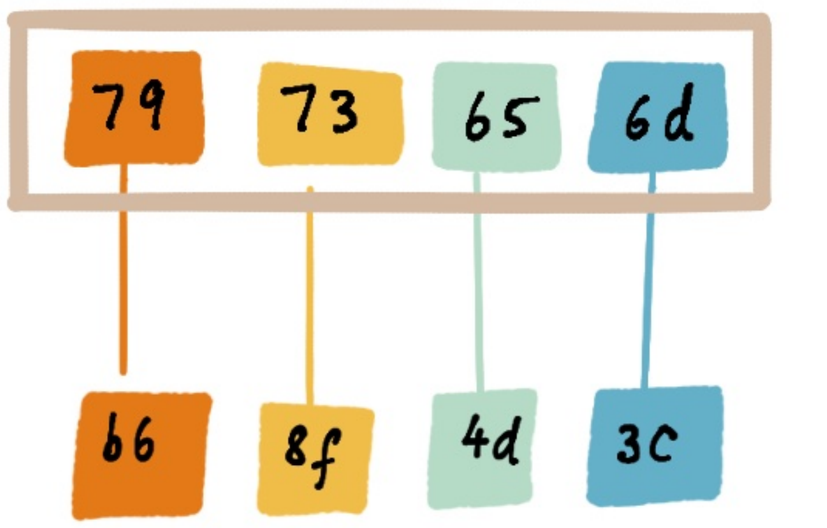


ROTATE BYTE POSITIONS

TO MAKE A ROTWORD

2 USE THE S-BOX

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	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	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	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	06	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	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	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



MAKE A SUB WORD

FROM THE ROTWORD

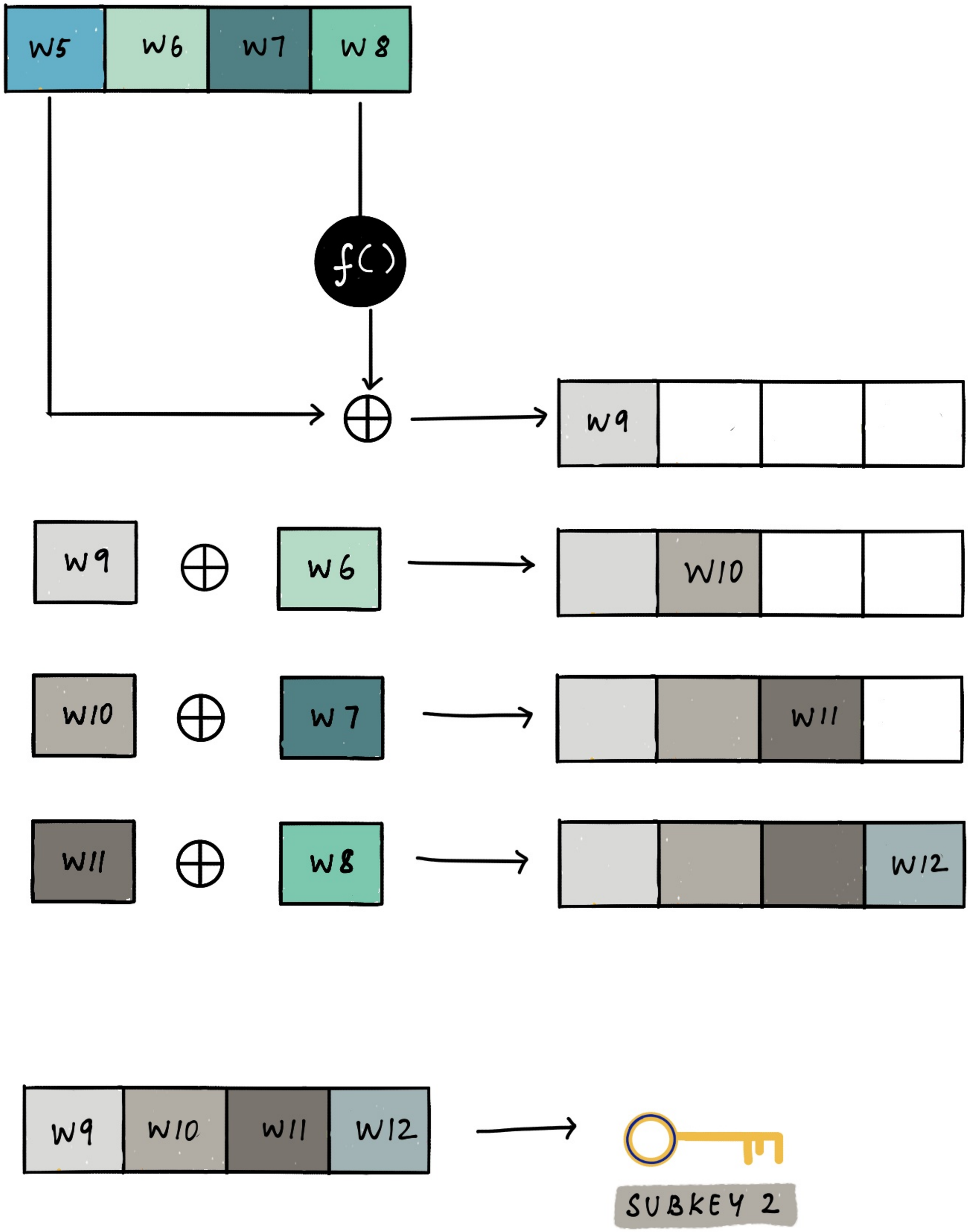
3 FINALLY THE ROUND CONSTANT TABLE

R1	R2	R3	R4	R5	R6	R7	R8	R9	R10
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

→ represents each round contains a byte in each column

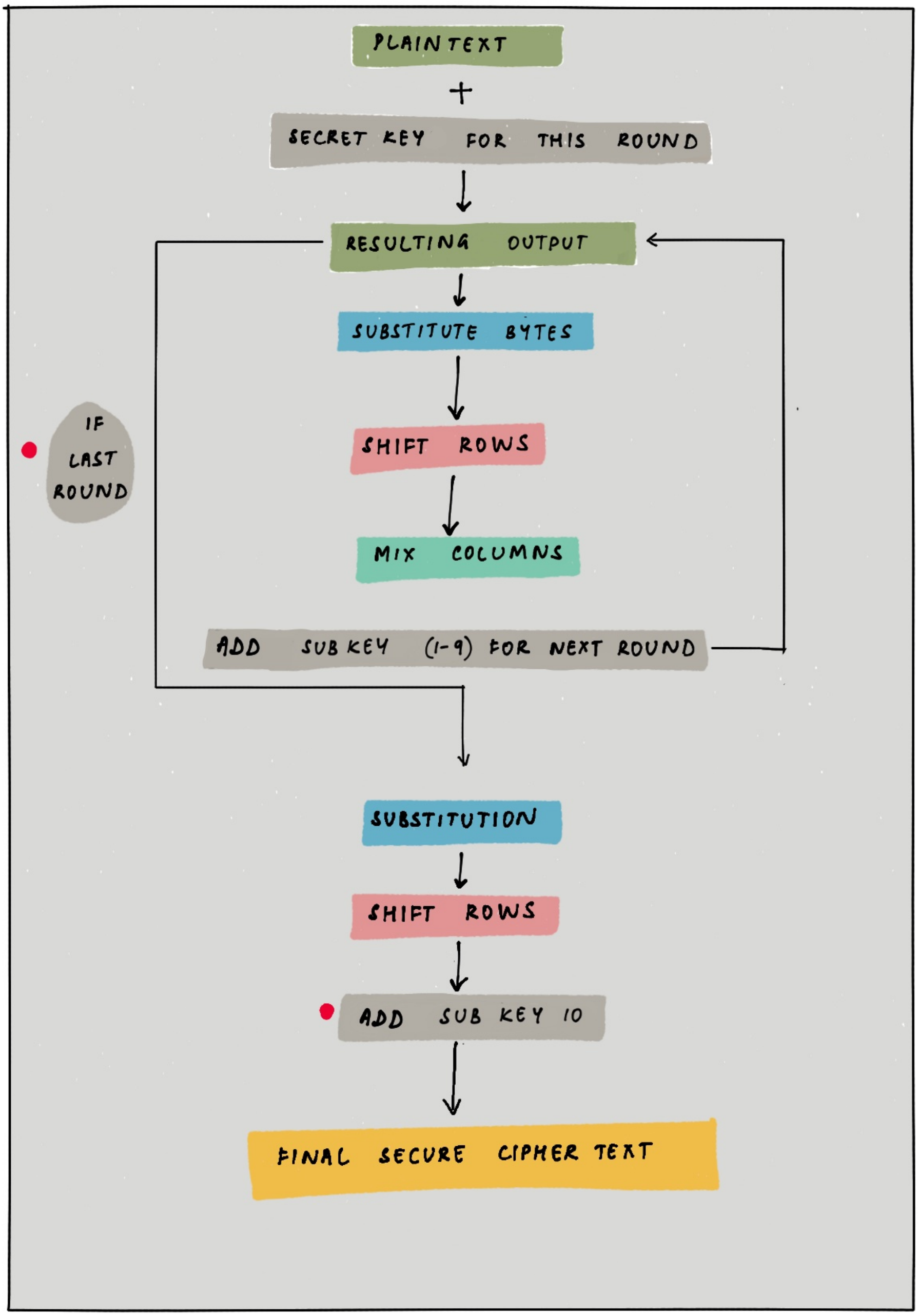
SUBWORD ⊕ R1 → W4a

THE NEXT 4 WORDS



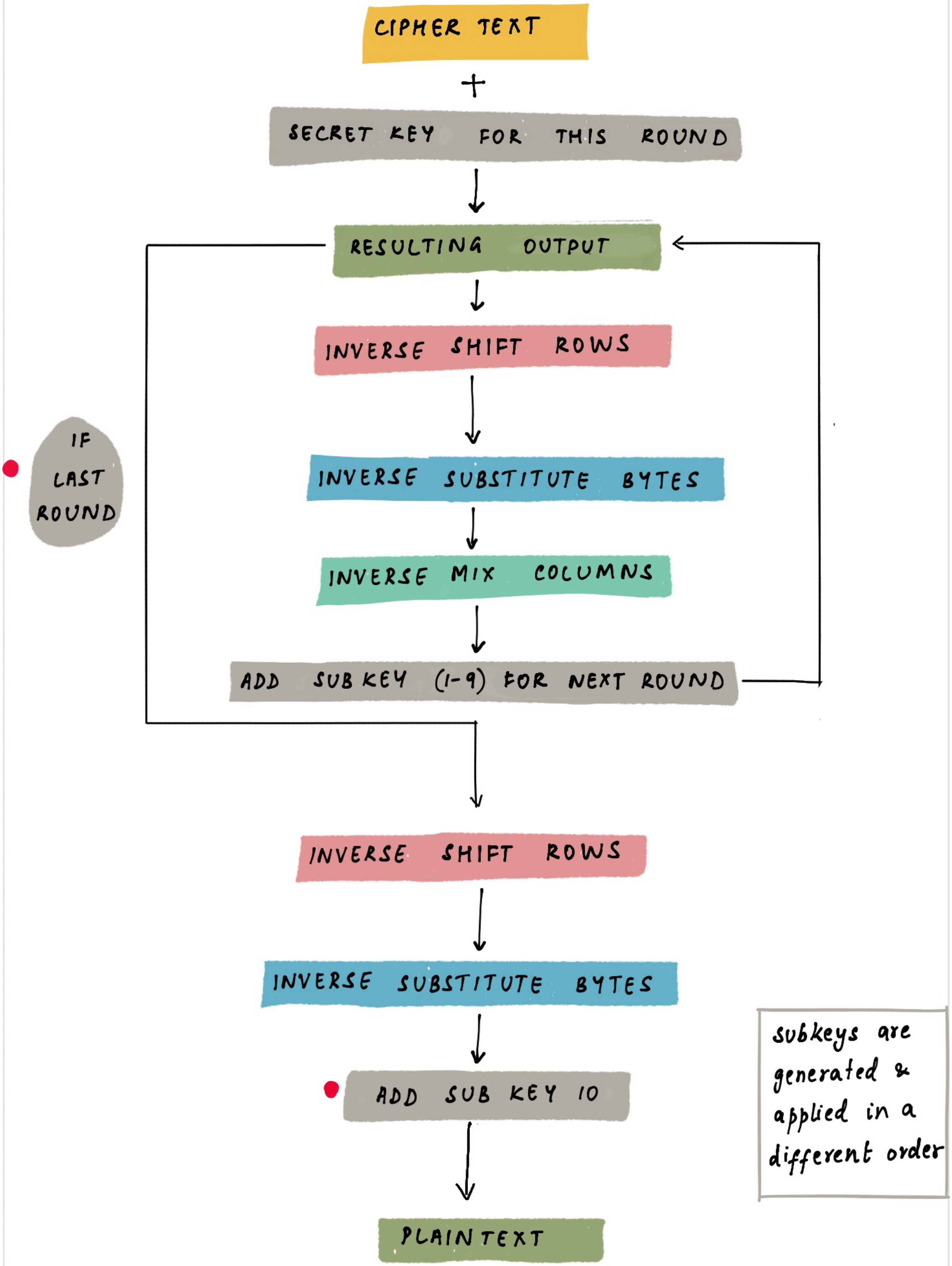
FOLLOW THE SAME PROCESS TO MAKE ALL THE 10 SUBKEYS

THE LAST ROUND

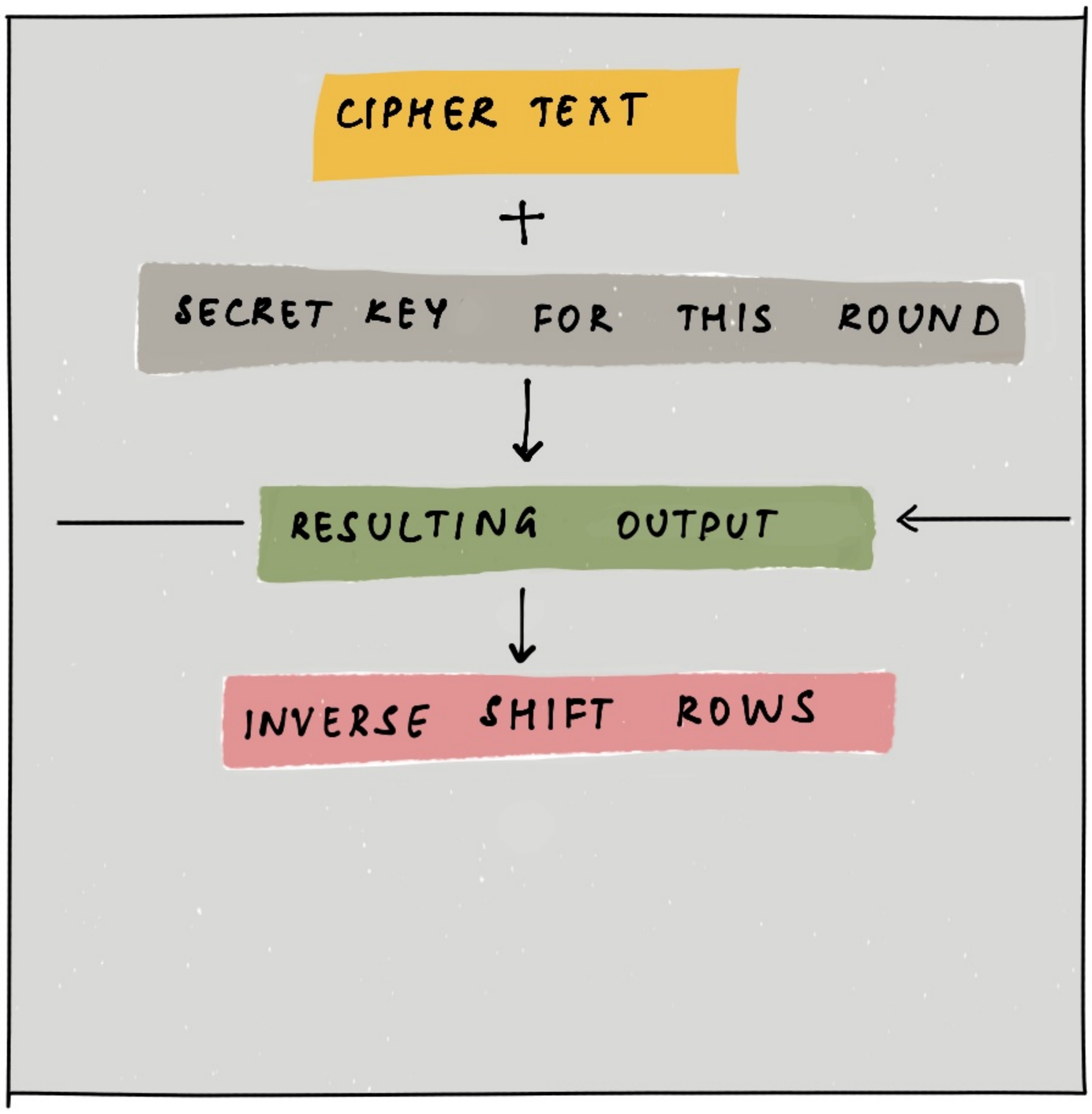


THE LAST ROUND DOES NOT INCLUDE THE MIXCOLUMNS

DECRYPTION


CIPHER TEXT
+
SECRET KEY FOR THIS ROUND
RESULTING OUTPUT
INVERSE SHIFT ROWS
INVERSE SUBSTITUTE BYTES
INVERSE MIX COLUMNS
ADD SUB KEY (1-9) FOR NEXT ROUND
IF LAST ROUND
INVERSE SHIFT ROWS
INVERSE SUBSTITUTE BYTES
ADD SUB KEY 10
PLAINTEXT
subkeys are generated & applied in a different order

INVERSE SHIFT ROWS



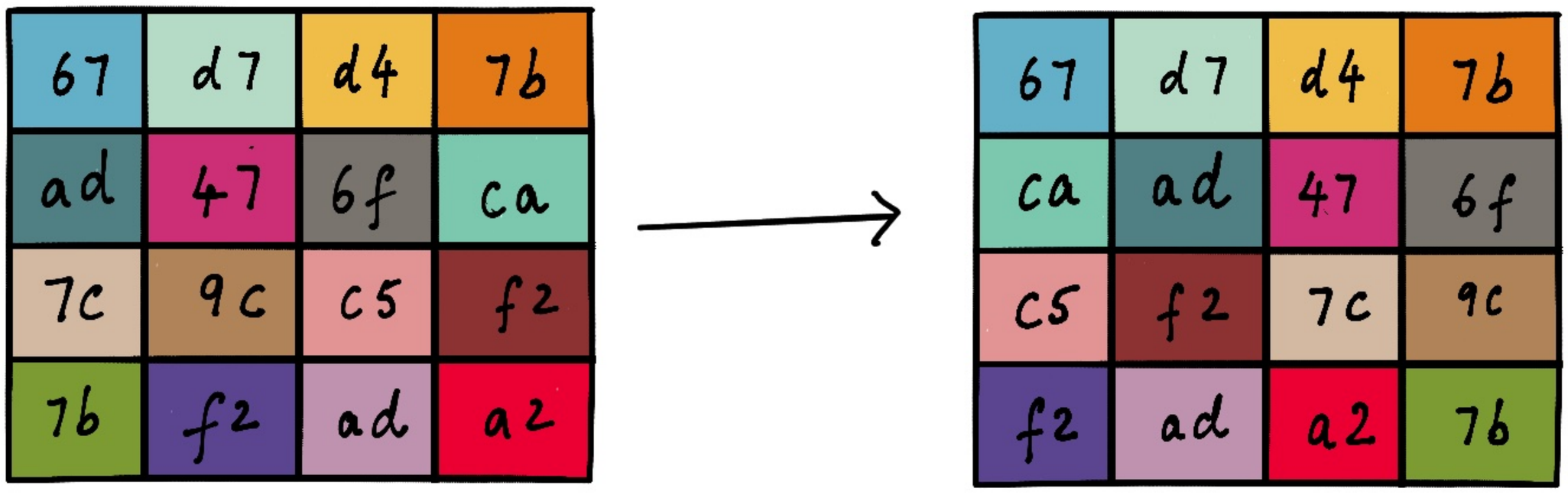
SHIFTS THE ROWS AS FOLLOWS

ROW 1 : UNCHANGED

ROW 2 : CYCLICAL RIGHT SHIFT BY 1 BYTE

ROW 3 : CYCLICAL RIGHT SHIFT BY 2 BYTES

ROW 4 : CYCLICAL RIGHT SHIFT BY 3 BYTES

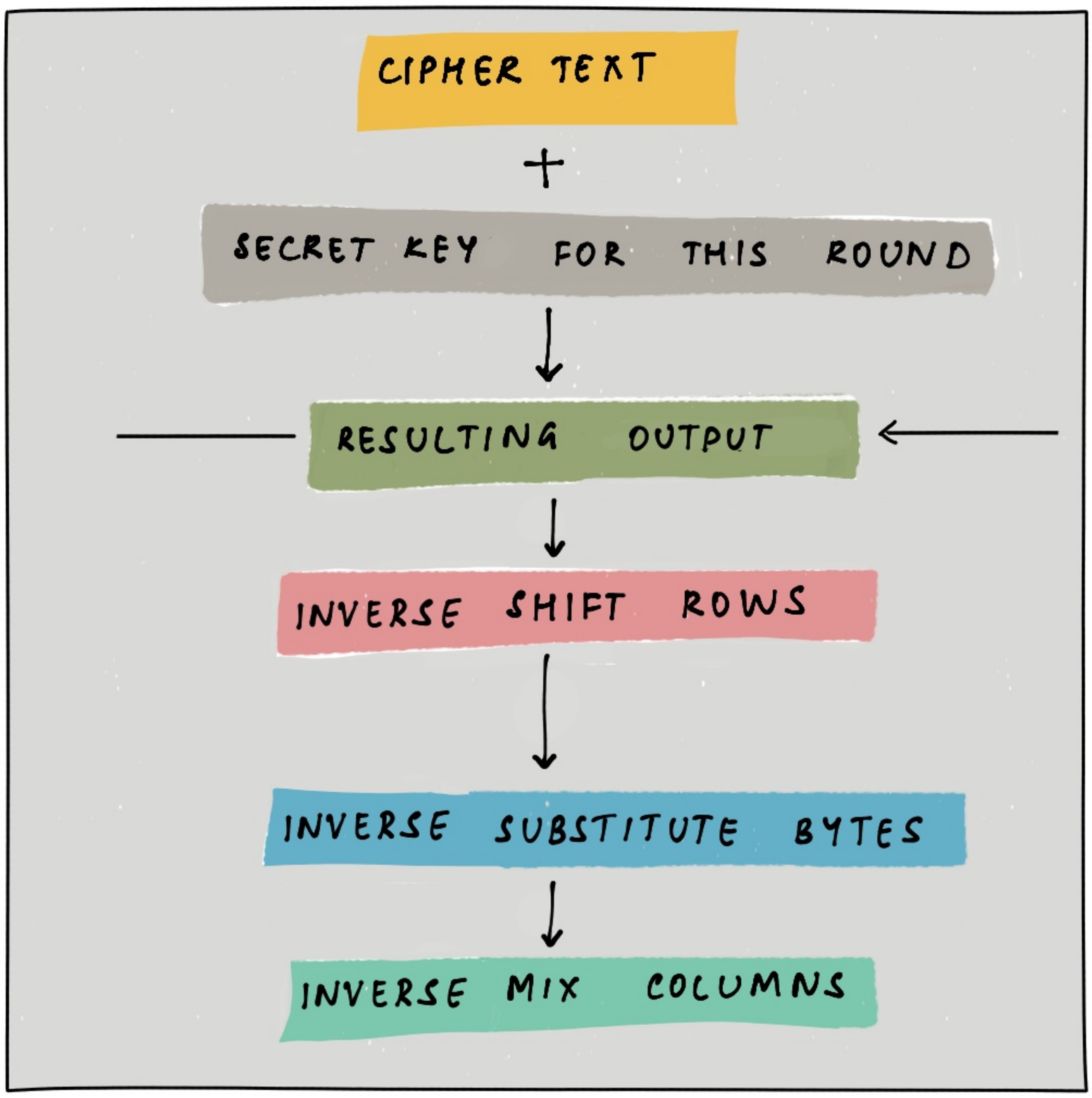


INVERSE SUBSTITUTE BYTES

HERE IS THE INVERSE S-BOX LOOKUP

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
10	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
20	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
30	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
40	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
50	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
60	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
70	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
80	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
90	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a0	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b0	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c0	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d0	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e0	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f0	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

INVERSE MIX COLUMNS



MULTIPLY THE INPUT STATE ARRAY BY A DIFFERENT STANDARD MATRIX —

ALSO A PATTERN OF CYCLICAL SHIFTS

0e	0b	0d	09
09	0e	0b	0d
0d	09	0e	0b
0b	0d	09	0e

*

67	d7	d4	7b
ad	47	6f	ca
7c	9c	c5	f2
7b	f2	ad	a2

HOW SECURE IS AES?

UNBREAKABLE ?

WITH A KEY SIZE OF 2

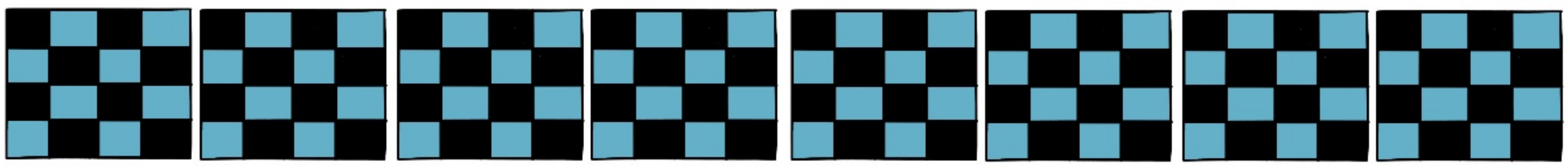
THE NUMBER OF POSSIBLE COMBINATIONS IS 2^2

WITH A KEY SIZE OF 3

THE NUMBER OF POSSIBLE COMBINATIONS IS 2^3

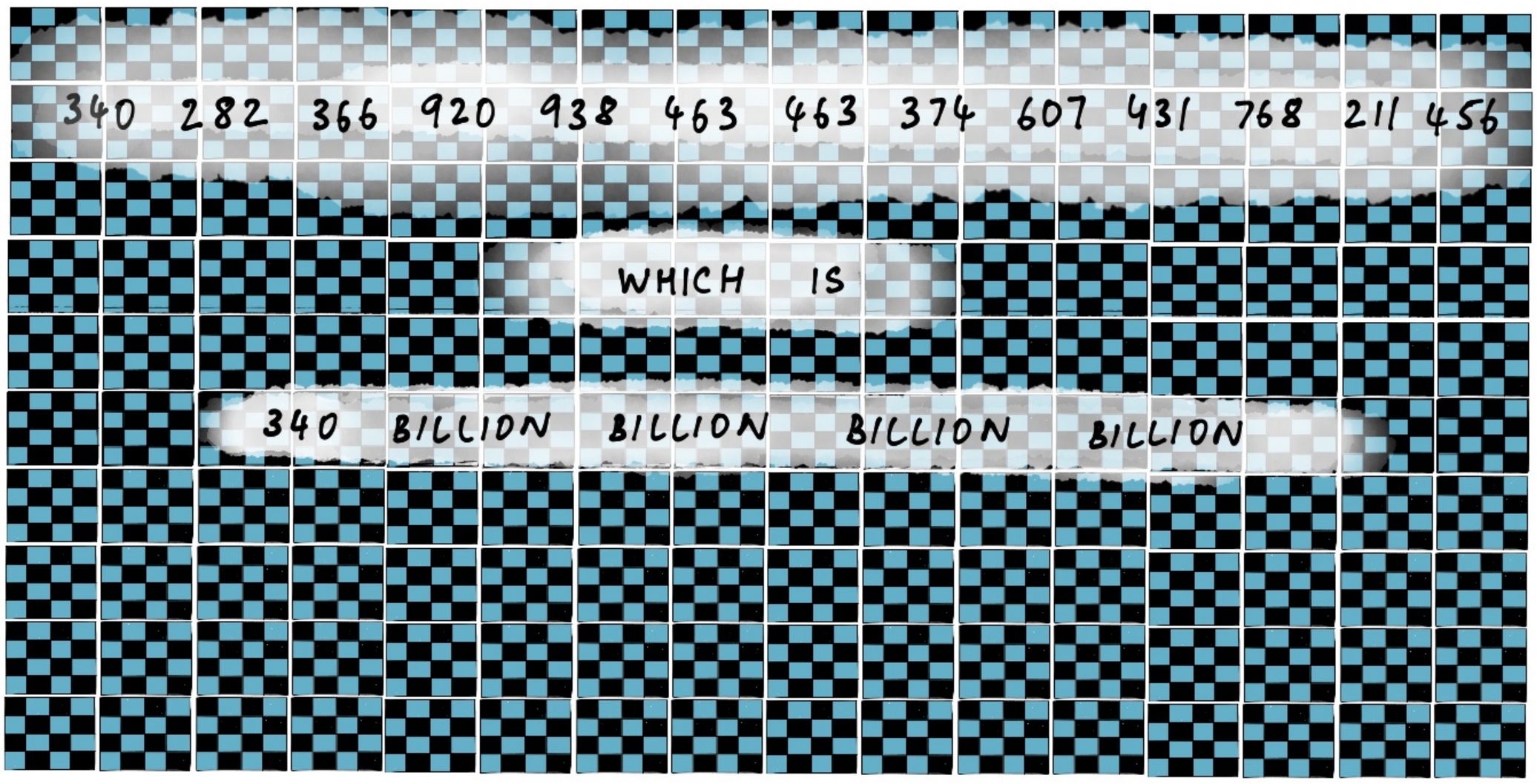
UNBREAKABLE ?

WITH A KEY SIZE OF 128



128

THE NUMBER OF POSSIBLE COMBINATIONS IS 2



Cornell University

arXiv > cs > arXiv: 2112.00399

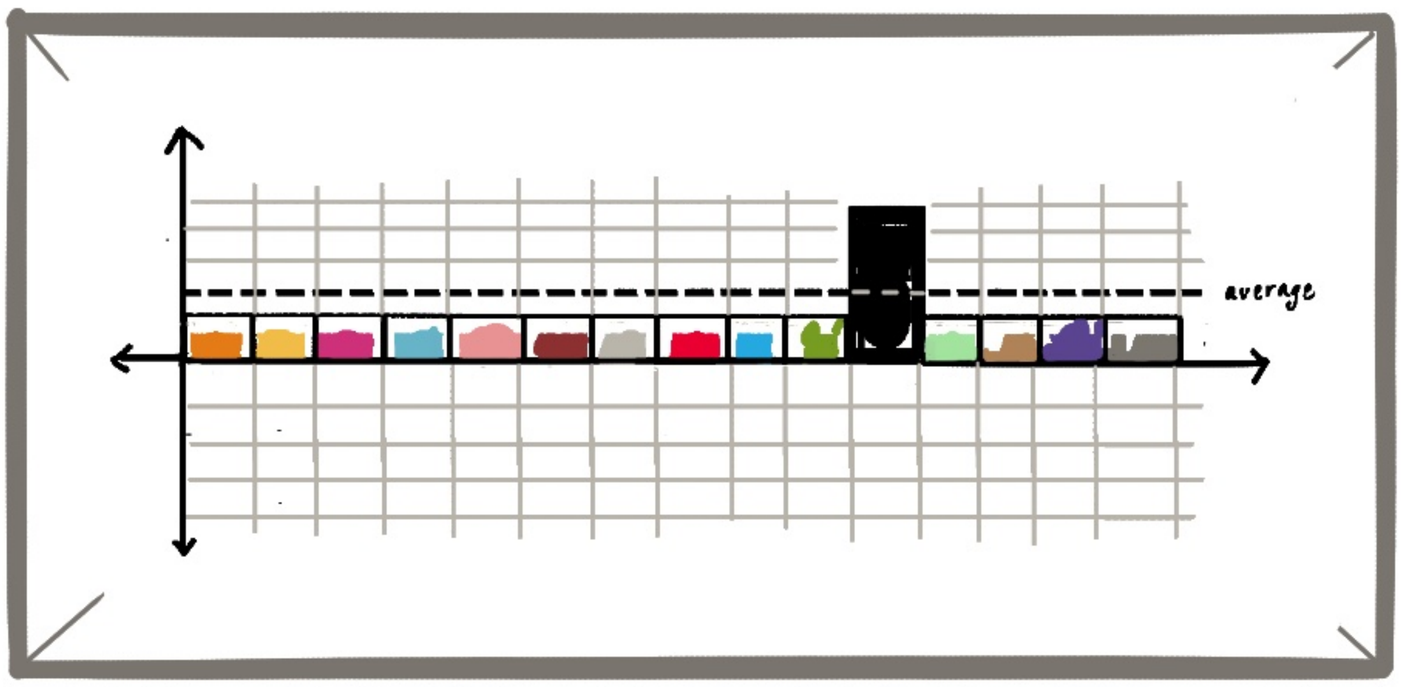
Quantum-Resistant Cryptography

John Preuß Mattsson, Ben Smeets, Erik Thormarker

IT WOULD TAKE 1 BILLION CRYPTOGRAPHICALLY RELEVANT QUANTUM COMPUTERS A MILLION YEARS OF UNINTERRUPTED COMPUTATION TO FIND A REQUIRED AES-128 KEY

NIST VIEW ON AES

csrc.nist.gov/Projects/post-quantum-cryptography/faqs



REMEMBER GROVER'S ALGORITHM?

IT ALLOWS A QUANTUM COMPUTER TO PERFORM A BRUTE FORCE KEY SEARCH WITH FAR FEWER STEPS THAN A CLASSICAL ONE.

THE STEPS IN THIS ALGORITHM WILL NEED TO BE DONE IN A SEQUENCE RATHER THAN IN PARALLEL. THIS IS DIFFICULT TO ACHIEVE IN GROVER'S.

WE ARE STILL A WHILE AWAY FROM A REAL THREAT FROM A QUANTUM COMPUTER OVER 287 LOGICAL QUANTUM GATES.

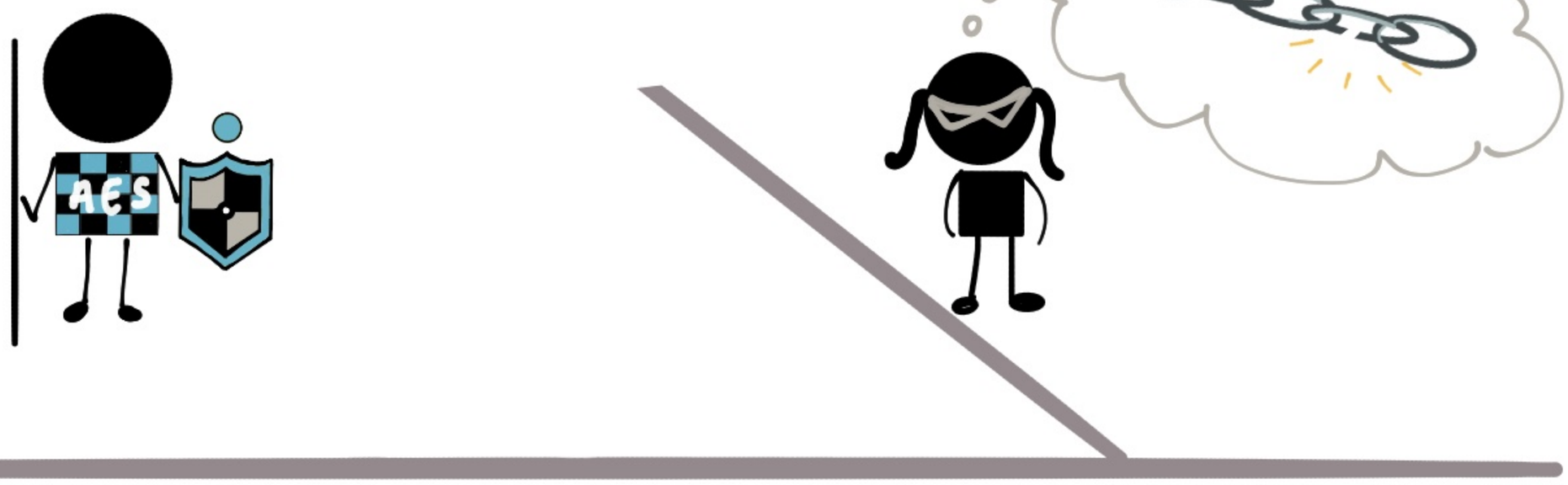
TAKING THESE FACTORS INTO ACCOUNT, IT IS QUITE LIKELY THAT GROVER'S ALGORITHM WILL HAVE LITTLE OR NO ADVANTAGE IN ATTACKING AES.

AES 128 WILL REMAIN SECURE FOR DECADES TO COME.

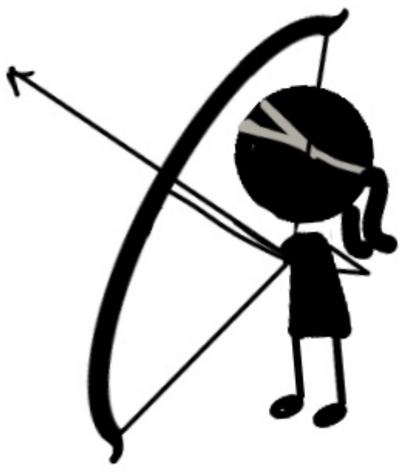
AES 192 & AES 256 WILL BE SAFE FOR A VERY LONG TIME.

CAUTION

THE PAPERS AND INFO ARE BASED ON THE FACT THAT THERE ARE NOT YET ANY IDENTIFIED VULNERABILITIES TO EXPLOIT IN AES.

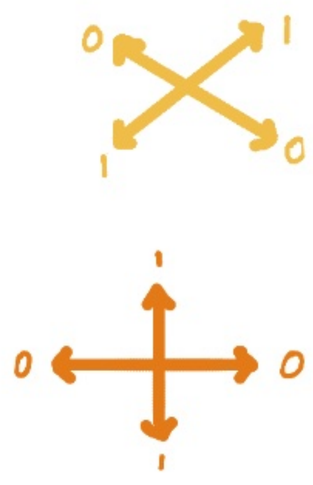


IT IS IN THE KEY-DISTRIBUTION AND EXTERNAL DEPENDENCIES THAT MAY CAUSE WEAKNESS WITH THE ENCRYPTION



QUANTUM KEY DISTRIBUTION AS A CONCEPT IS DISCUSSED THE STORY OF QUANTUM COMPUTING : AN ILLUSTRATED GUIDE

ALICE SENDS POLARISED LIGHT WHICH ENCODES BITS RANDOMLY IN ONE OF 2 METHODS



MY REFERENCES

NIST.GOV - POST QUANTUM CRYPTOGRAPHY

AES SPEC - CSRC.NIST.GOV fips-197.pdf

QUANTUM RESISTANT CRYPTOGRAPHY - arxiv.org - 2112.00399.pdf