CRYPTOGRAPHY & NETWORK SECURITY

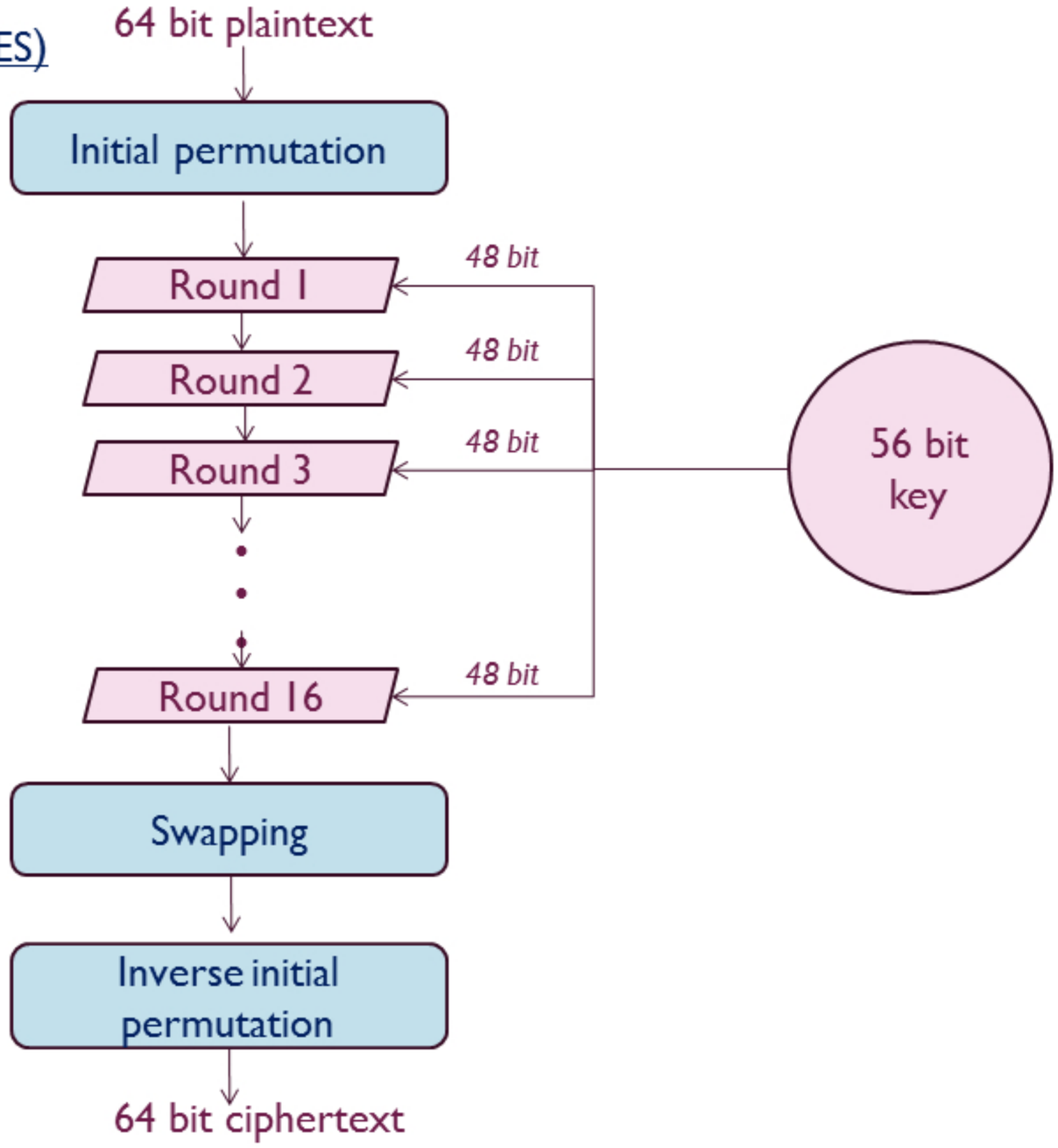
DATA ENCRYPTION STANDARD (DES)

Vijesh Nair

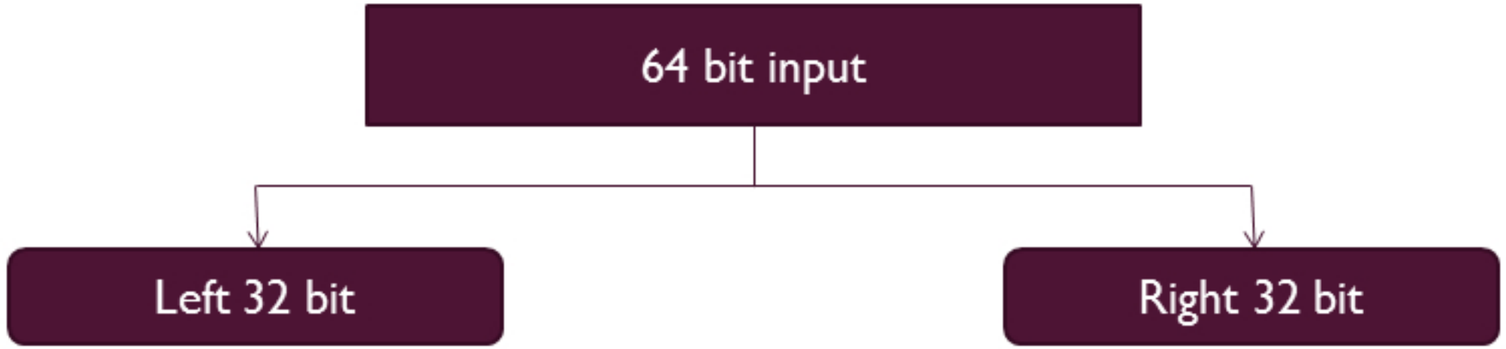
DATA ENCRYPTION STANDARD (DES)

- Block cipher.
- Single key for encryption & decryption.
- 64 bit block data is used.
- 56 bit key is used.
- 16 rounds.

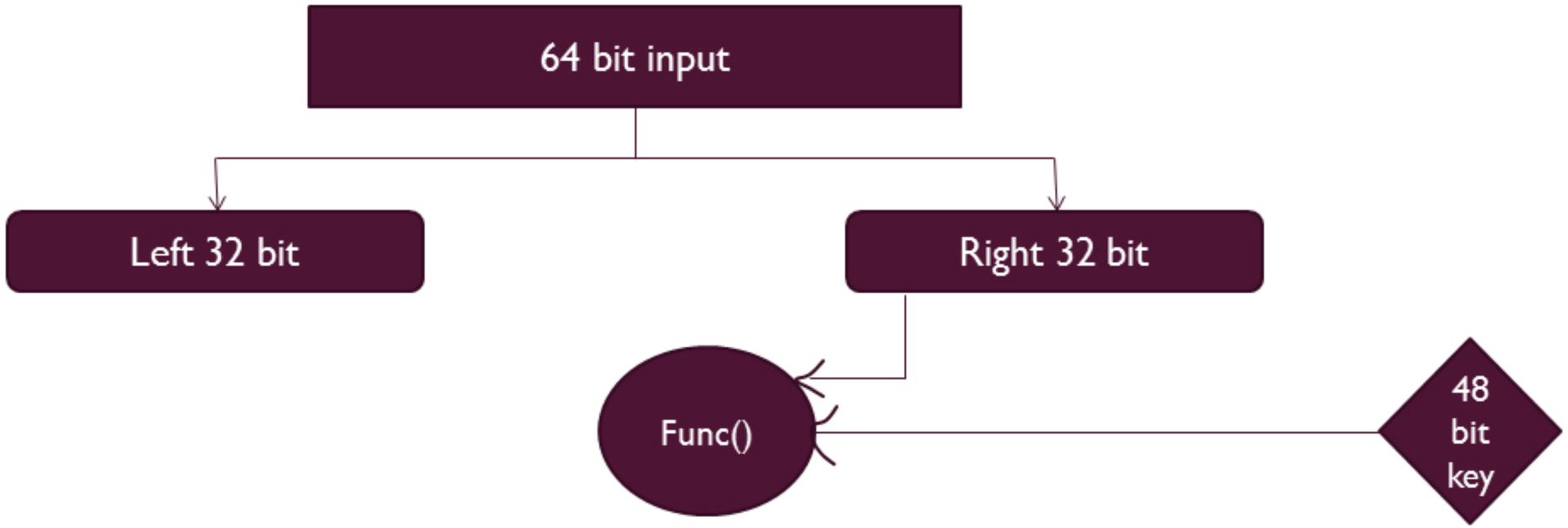
DATA ENCRYPTION STANDARD (DES)



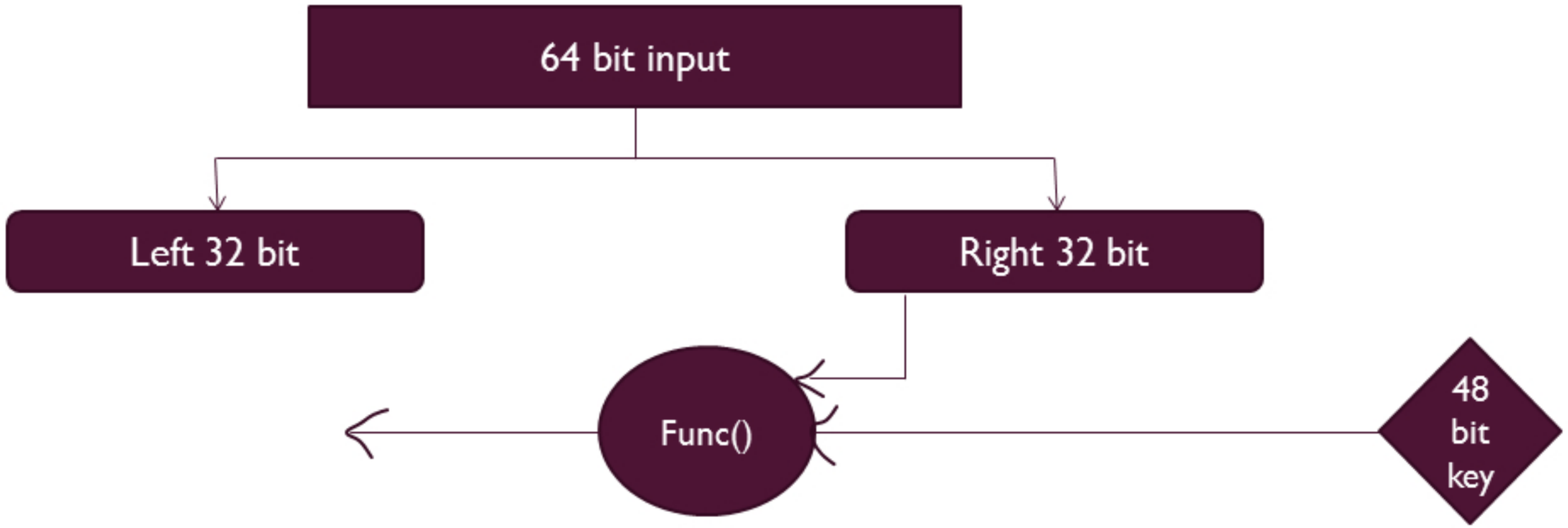
DATA ENCRYPTION STANDARD (DES) - ONE ROUND



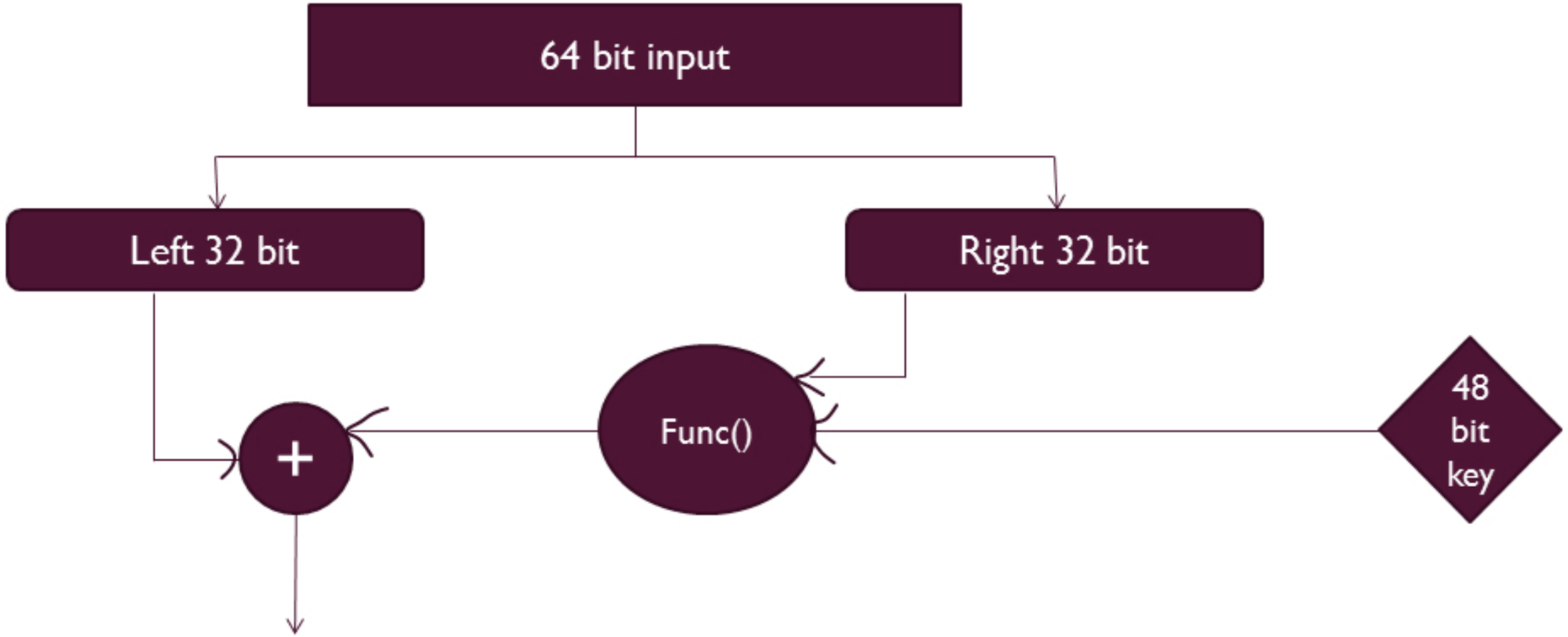
DATA ENCRYPTION STANDARD (DES) - ONE ROUND



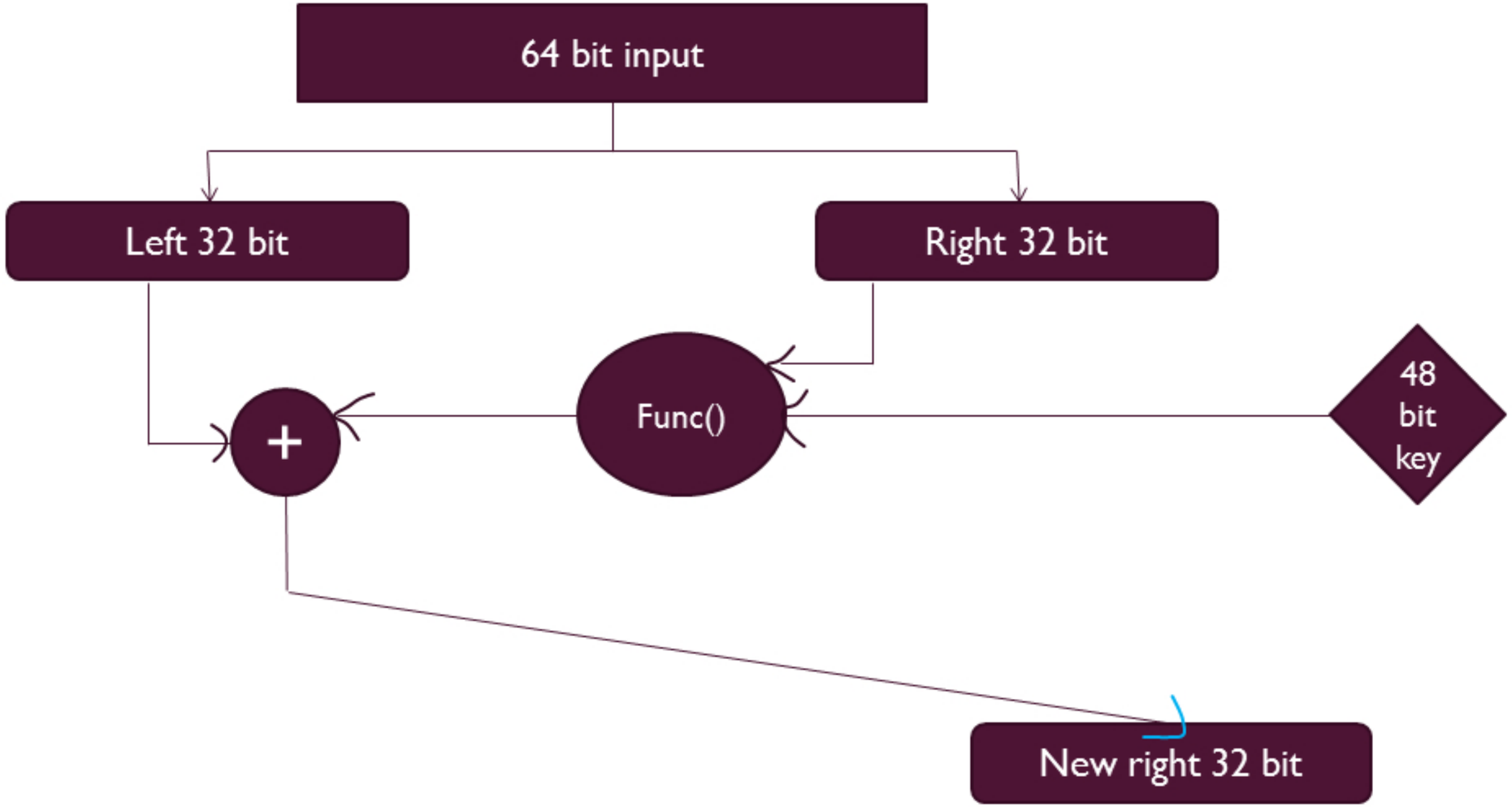
DATA ENCRYPTION STANDARD (DES) - ONE ROUND



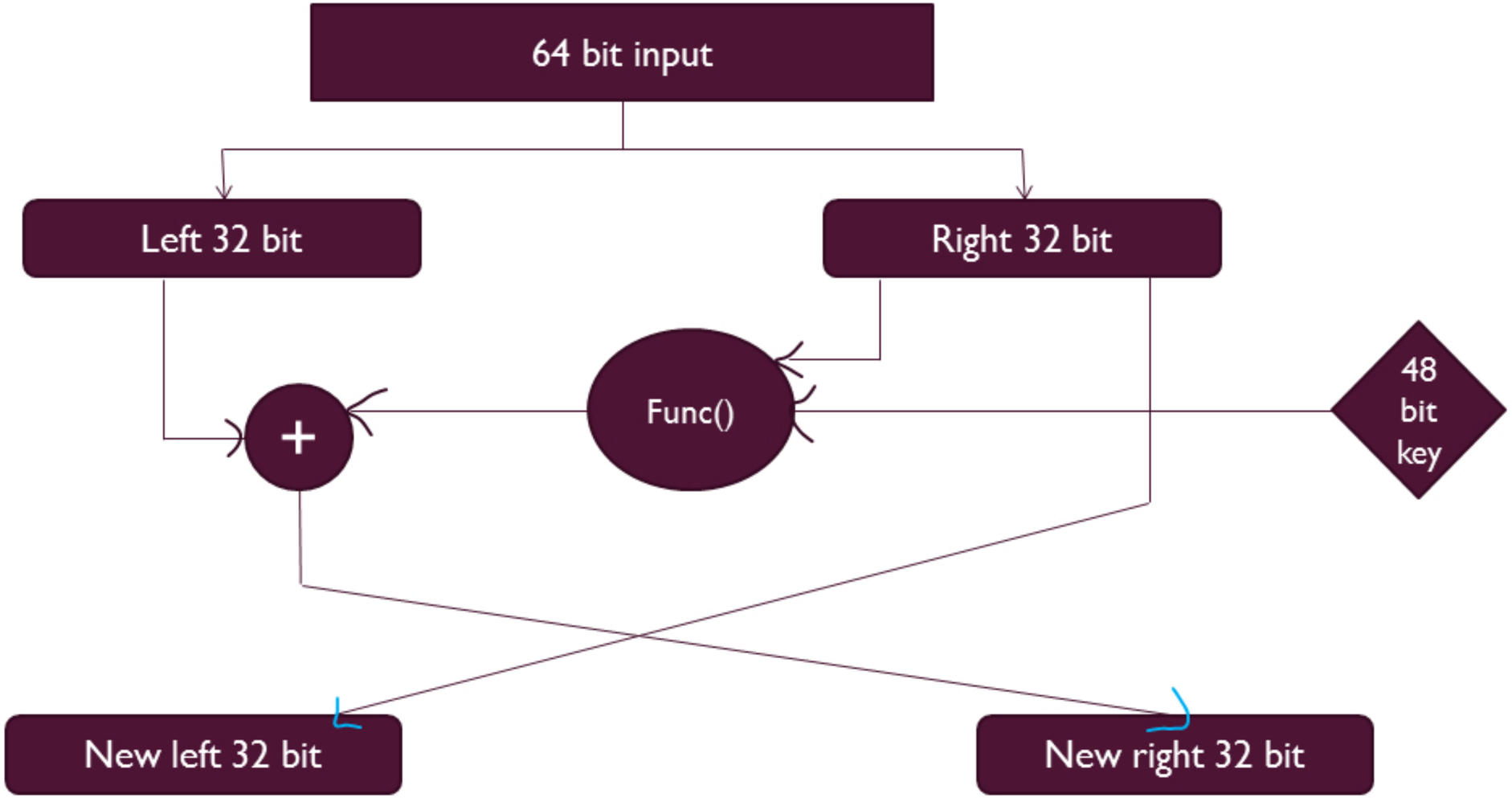
DATA ENCRYPTION STANDARD (DES) - ONE ROUND



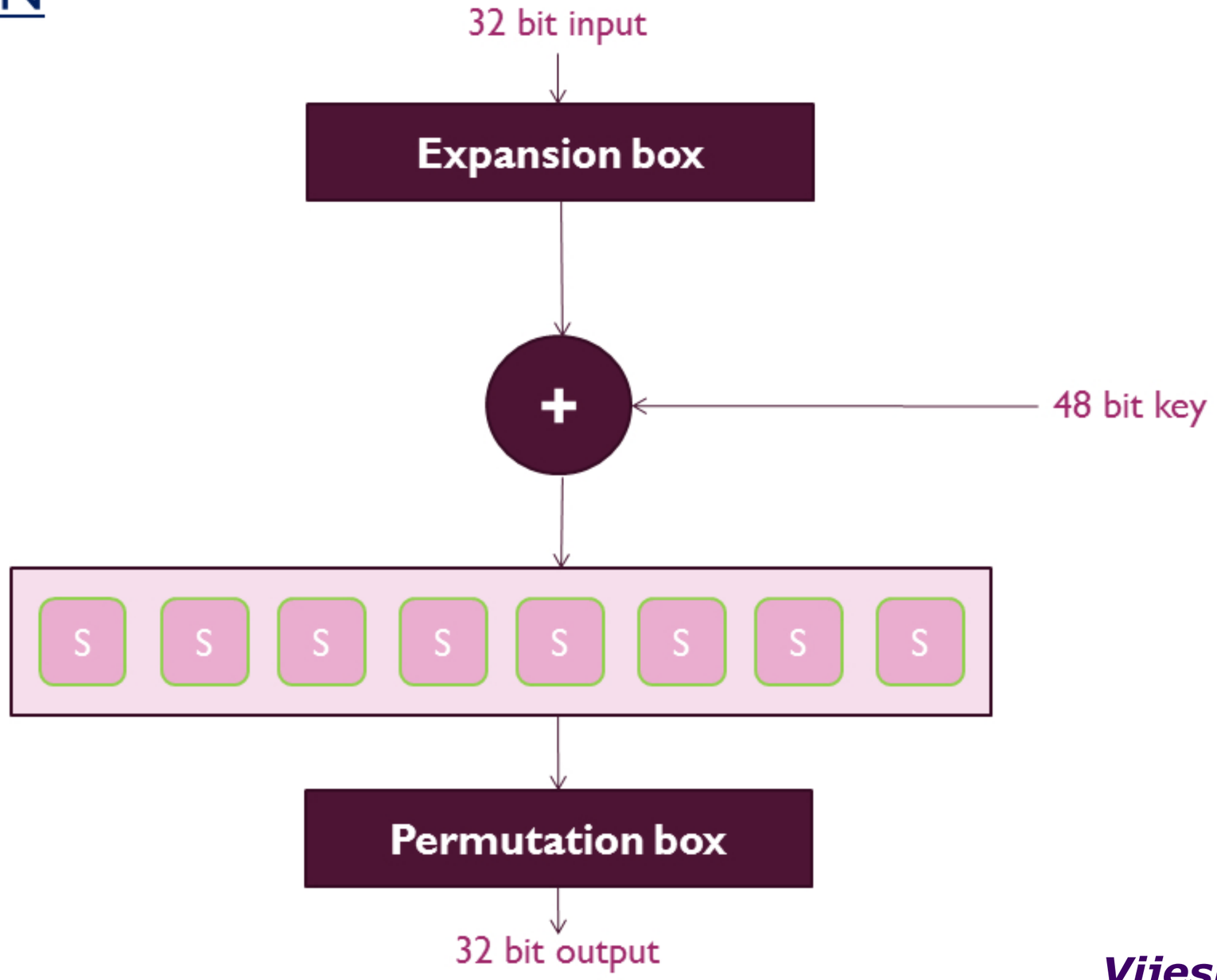
DATA ENCRYPTION STANDARD (DES) - ONE ROUND



DATA ENCRYPTION STANDARD (DES) - ONE ROUND



FUNCTION DEFINITION



EXPANSION

Let the 32 bit block is this ;
DONTGIVETHEMONEYTOTHATPERSONEVER

D	O	N	T	G	I	V	E	T	H	E	M	O	N	E	Y	T	O	T	H	A	T	P	E	R	S	O	N	E	V	E	R

EXPANSION

Let the 32 bit block is this ;
DONTGIVETHEMONEYTOTHATPERSONEVER

EXPANSION

Let the 32 bit block is this ;
DONTGIVETHEMONEYTOTHATPERSONEVER

EXPANSION

Let the 32 bit block is this ;
DONTGIVETHEMONEYTOTHATPERSONEVER

EXPANSION

Let the 32 bit block is this ;
DONTGIVETHEMONEYTOTHATPERSONEVER

EXPANSION

Let the 32 bit block is this ;
DONTGIVETHEMONEYTOTHATPERSONEVER

DONT	GIVE	THEM	ONEY	TOTH	ATPE	RSON	EVER

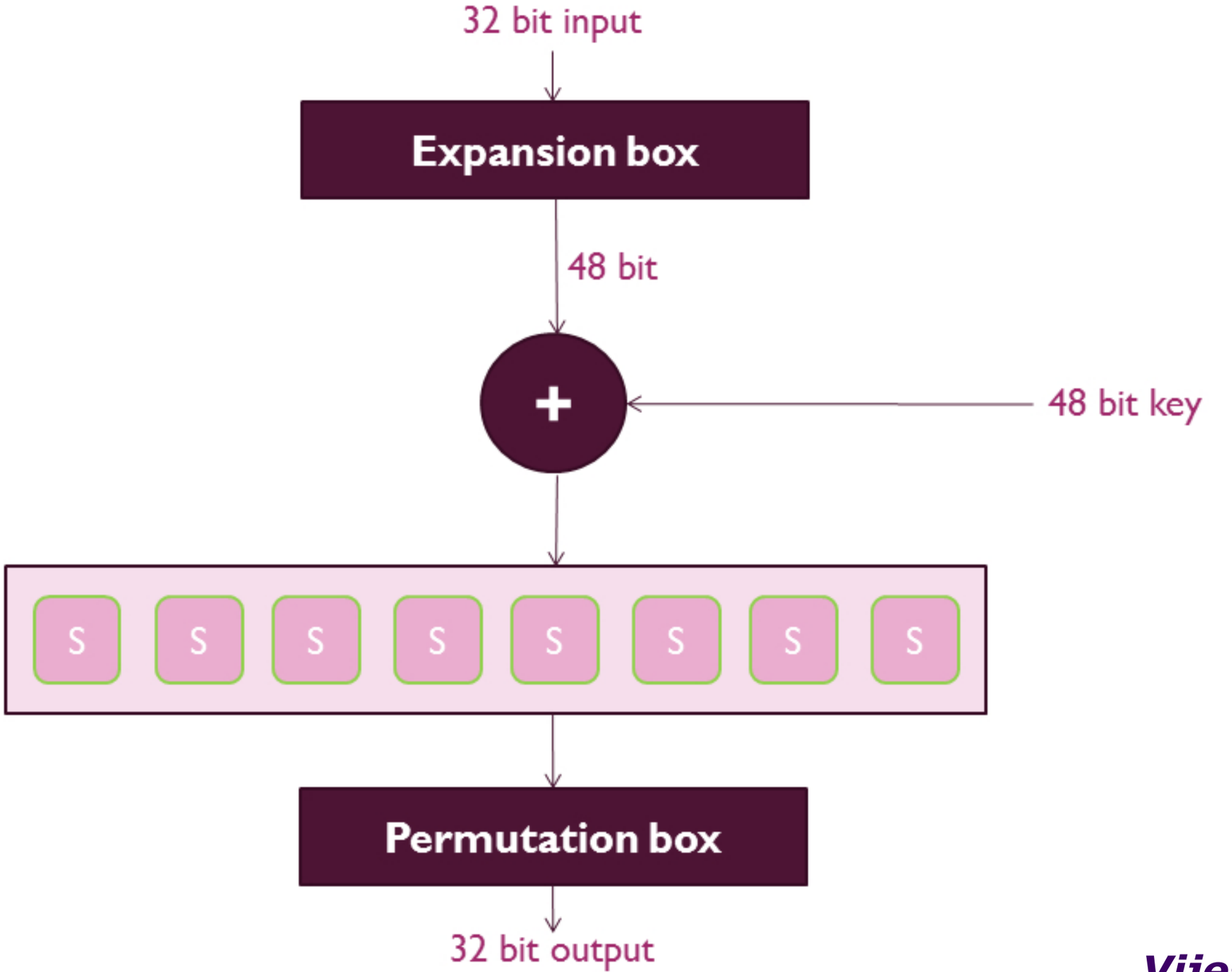
DONT	EVER

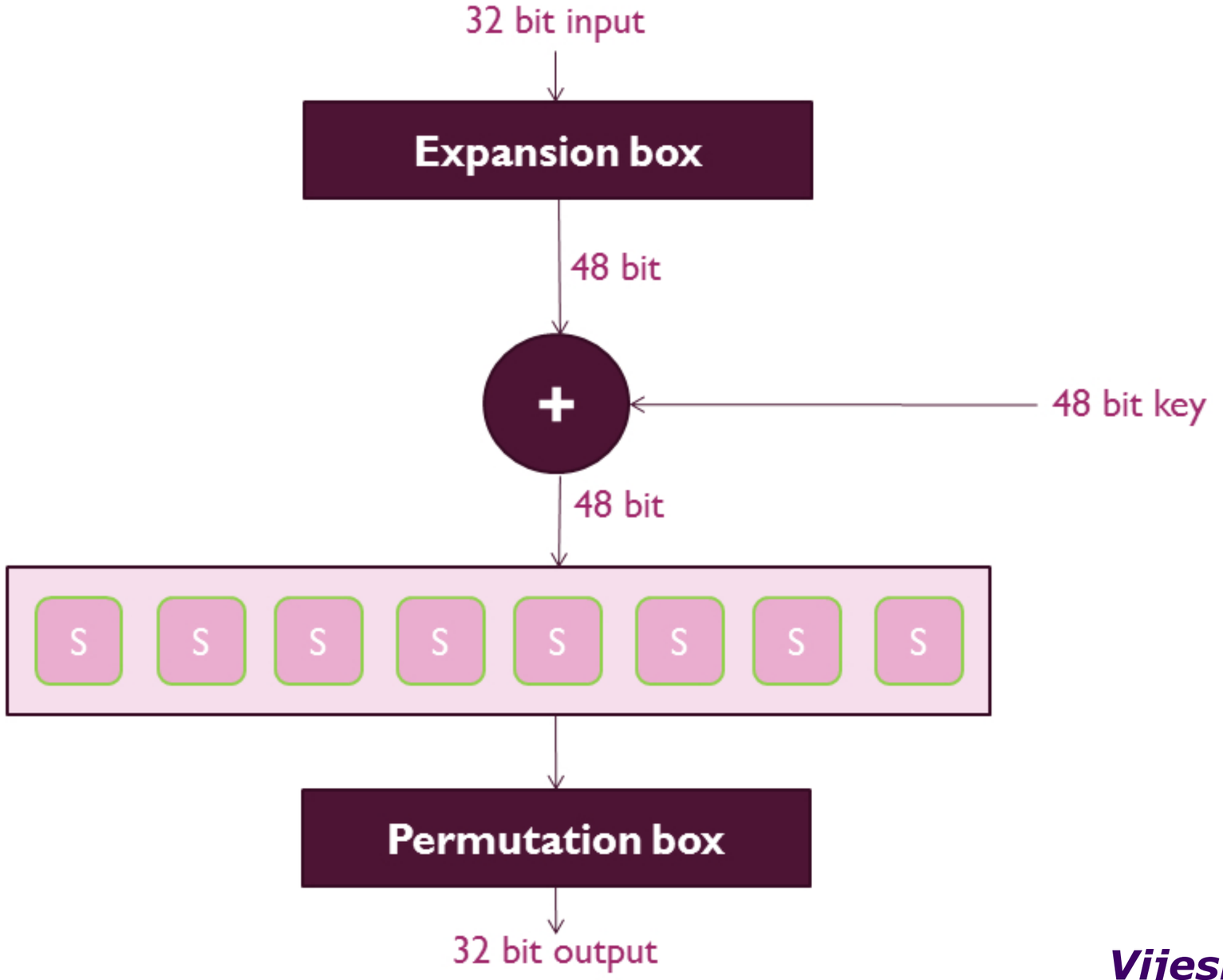
EXPANSION

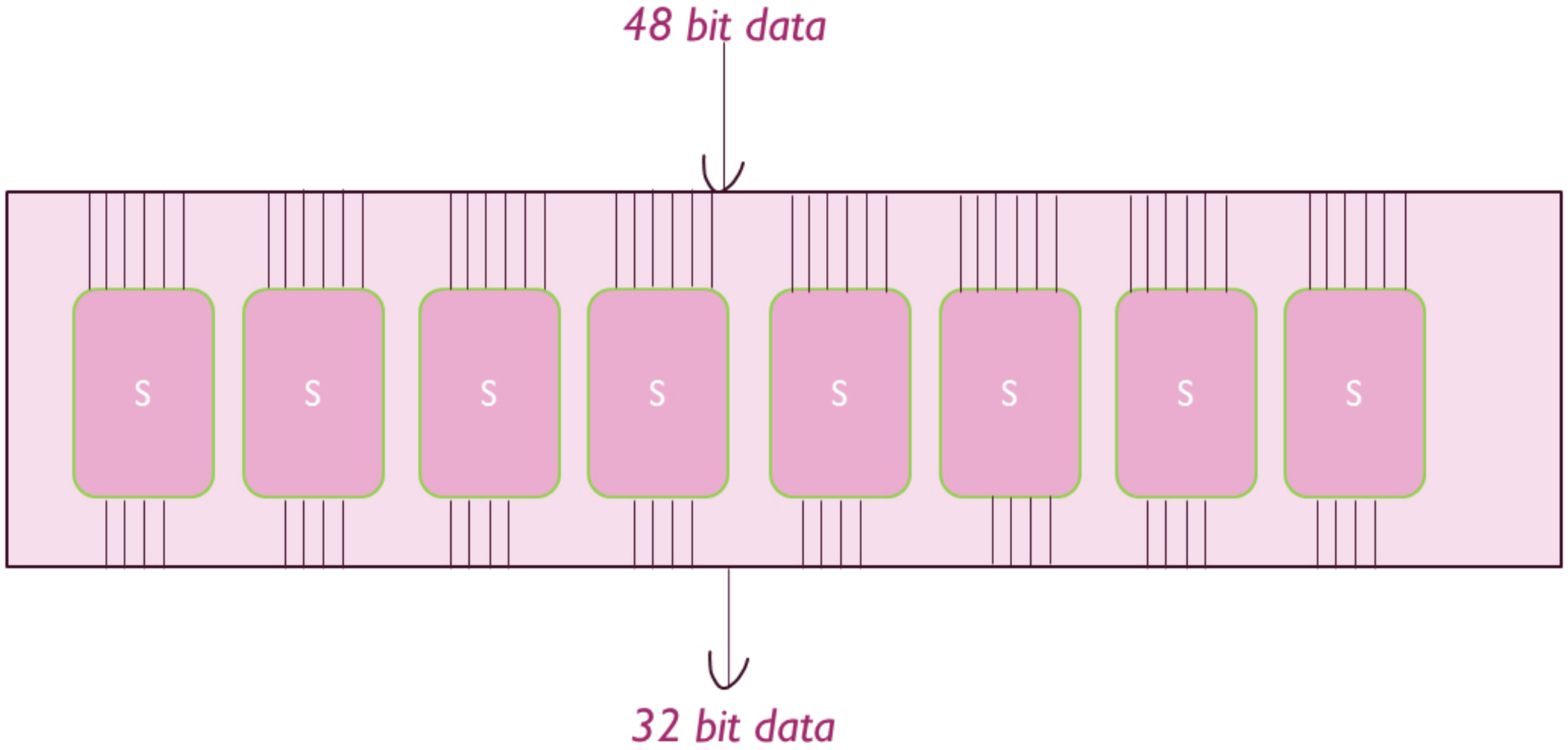
Let the 32 bit block is this ;
DONTGIVETHEMONEYTOTHATPERSONEVER

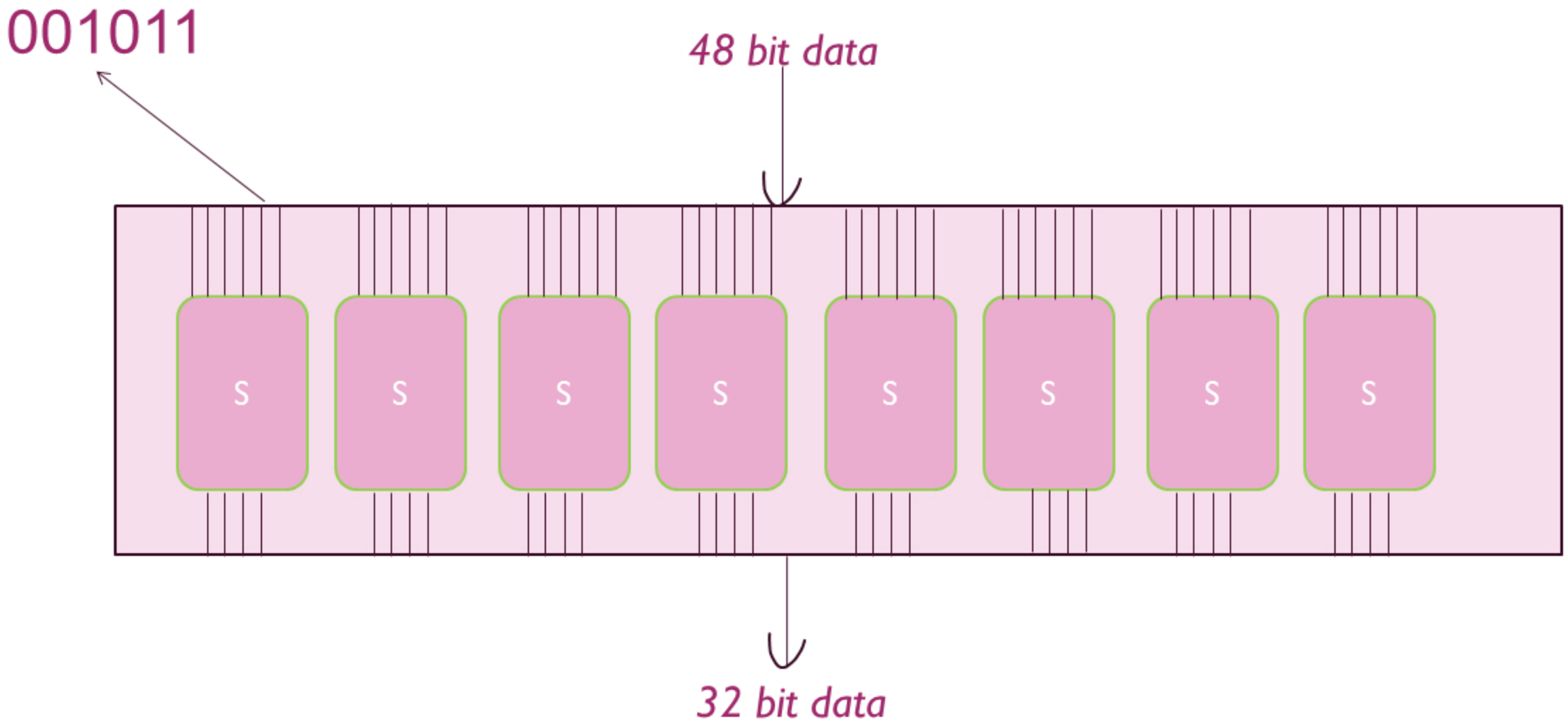
EXPANSION

Let the 32 bit block is this ;
DONTGIVETHEMONEYTOTHATPERSONEVER


32 bit input
Expansion box
48 bit
+
48 bit key
S
S
S
S
S
S
S
S
Permutation box
32 bit output

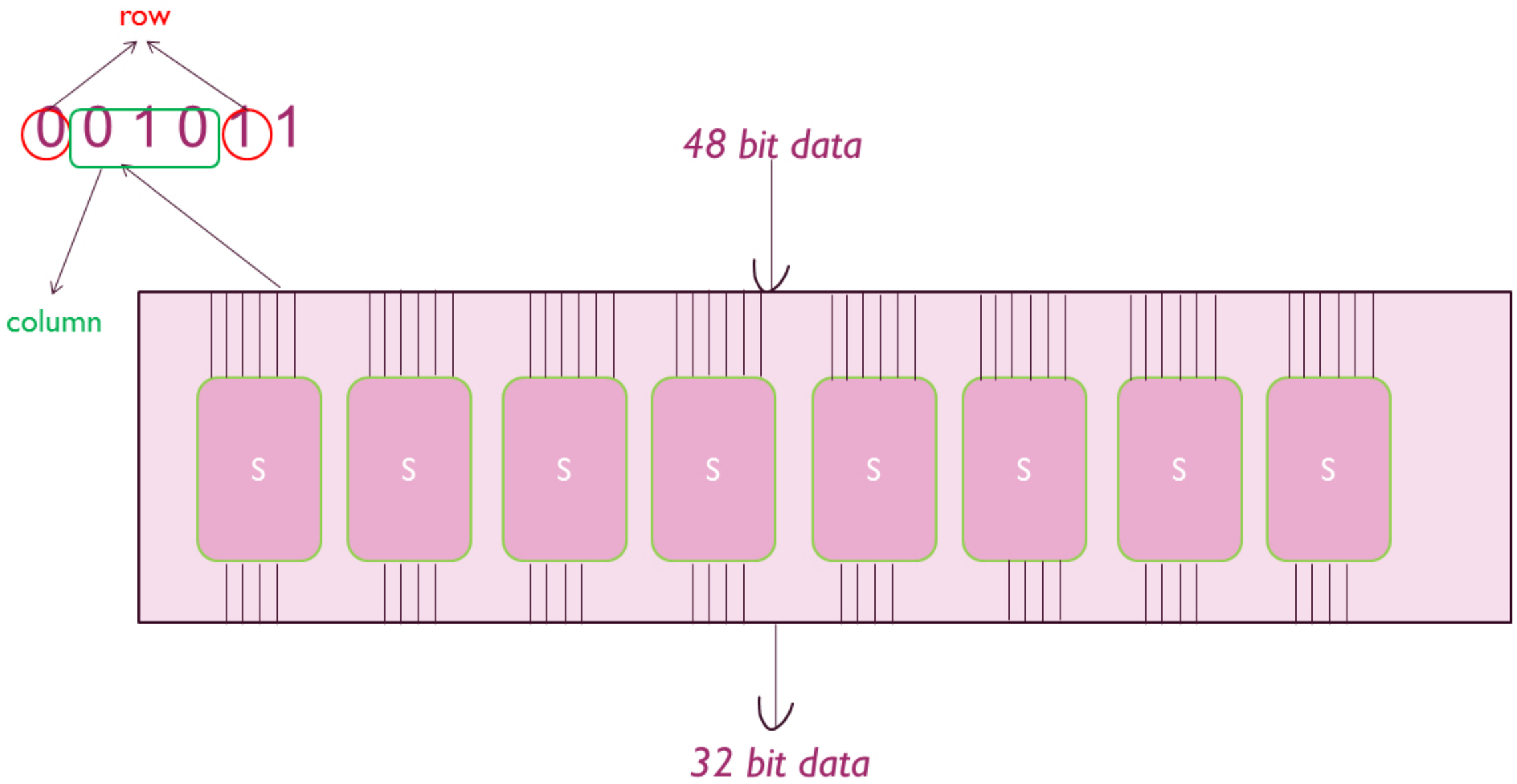

32 bit input
Expansion box
48 bit
+
48 bit key
48 bit
S
S
S
S
S
S
S
S
Permutation box
32 bit output


48 bit data
S
S
S
S
S
S
S
S
32 bit data


001011
48 bit data
S
S
S
S
S
S
S
S
32 bit data

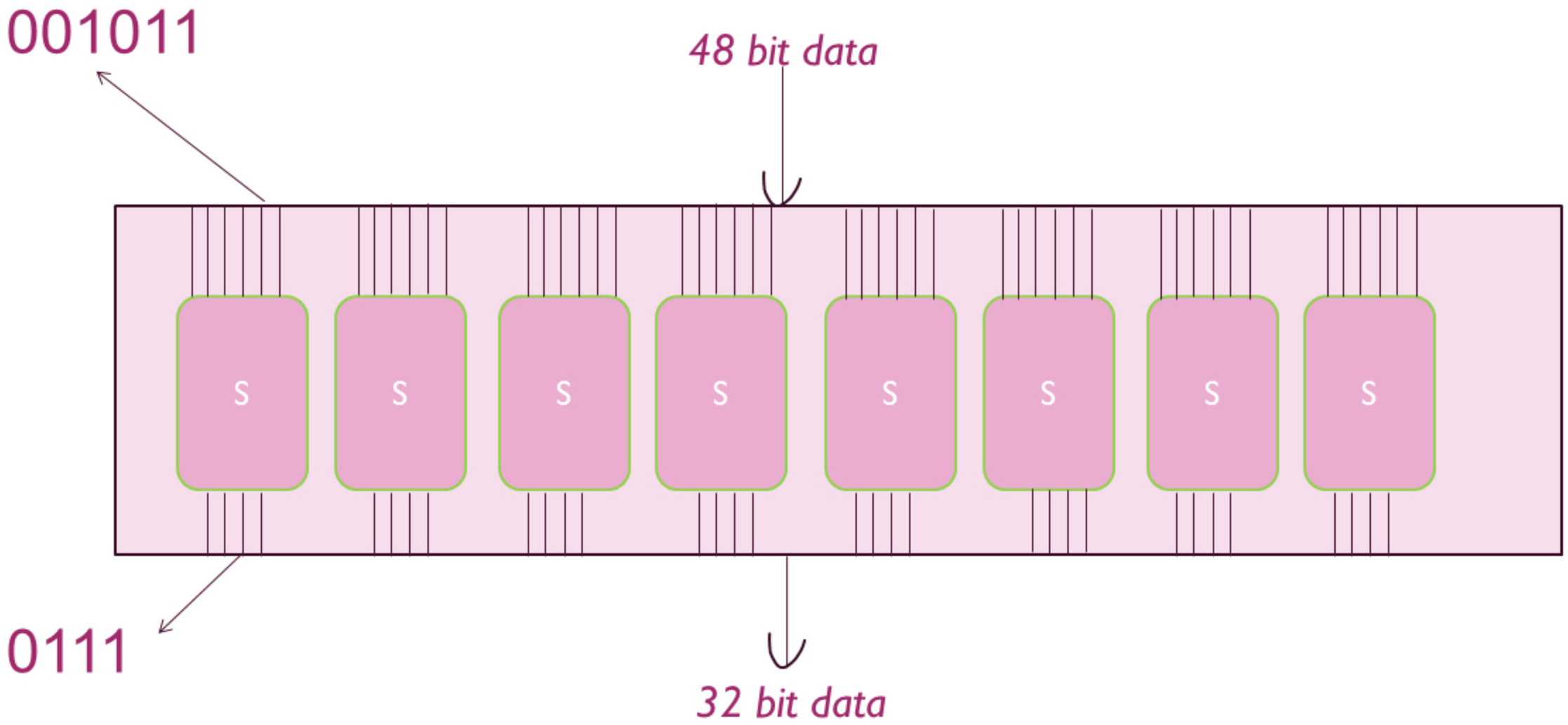
S BOX (Substitution Box)

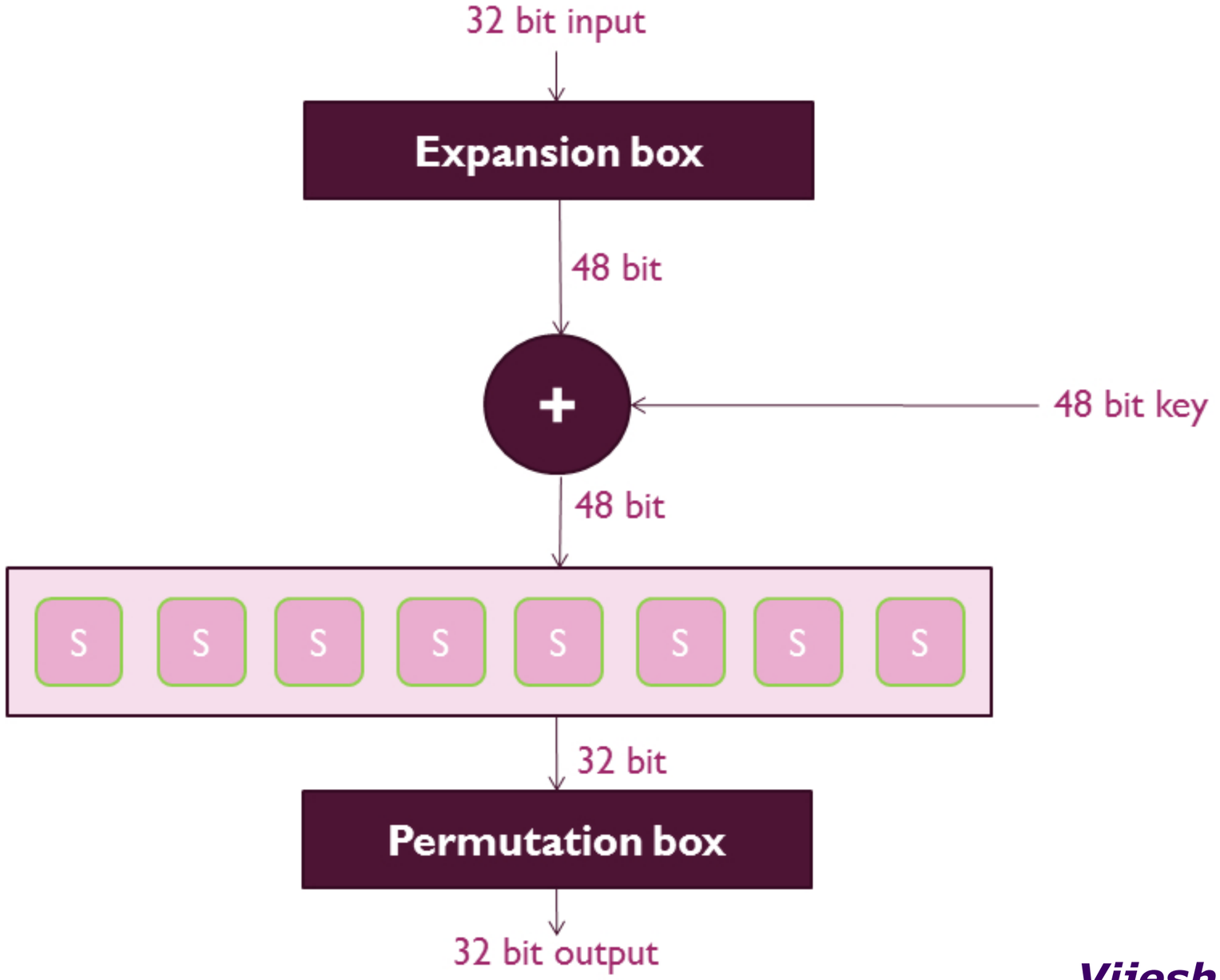
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011


row
0 0 1 0 1 1
column
48 bit data
S
S
S
S
S
S
S
S
32 bit data

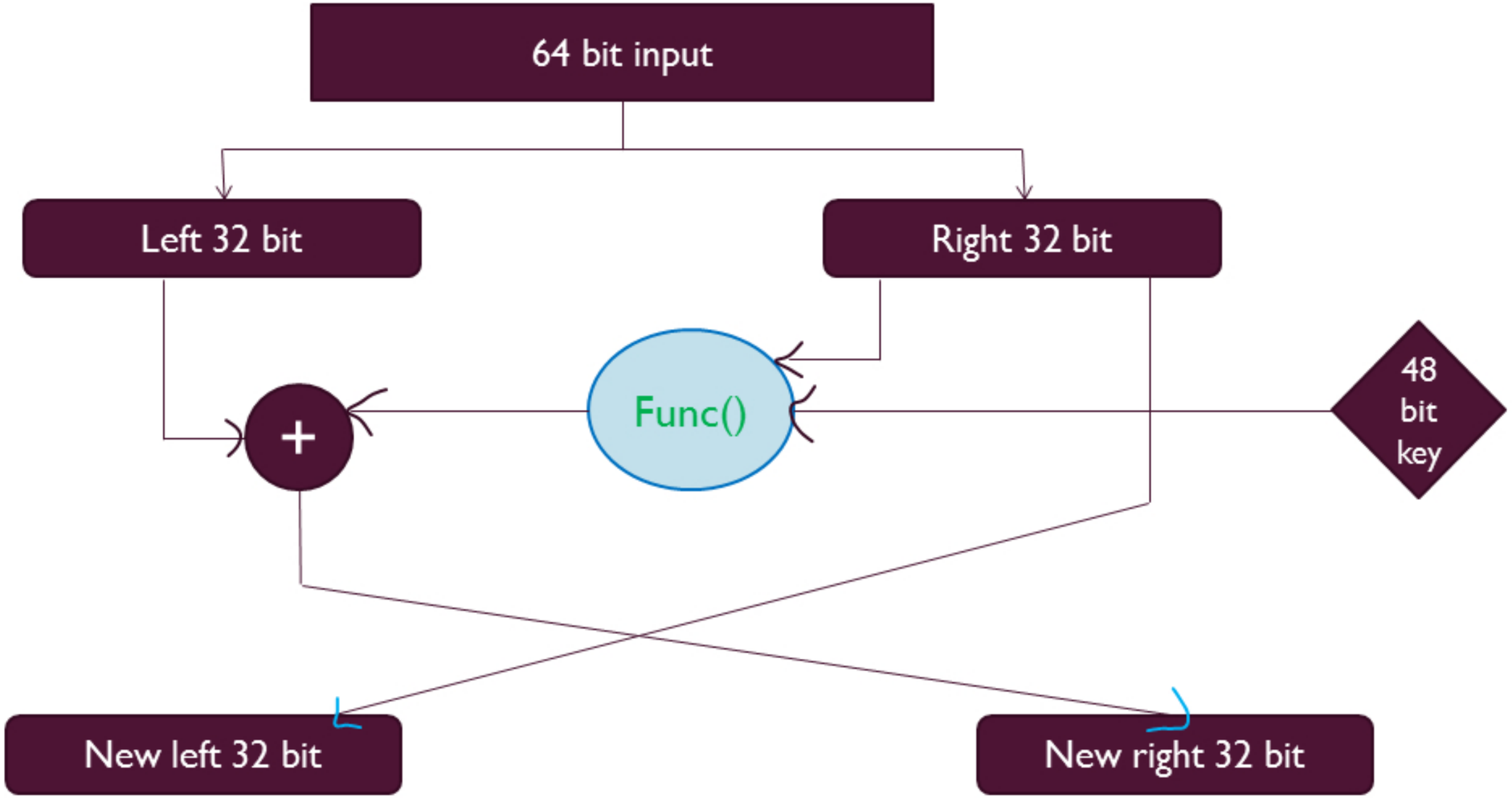
S BOX (Substitution Box)

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

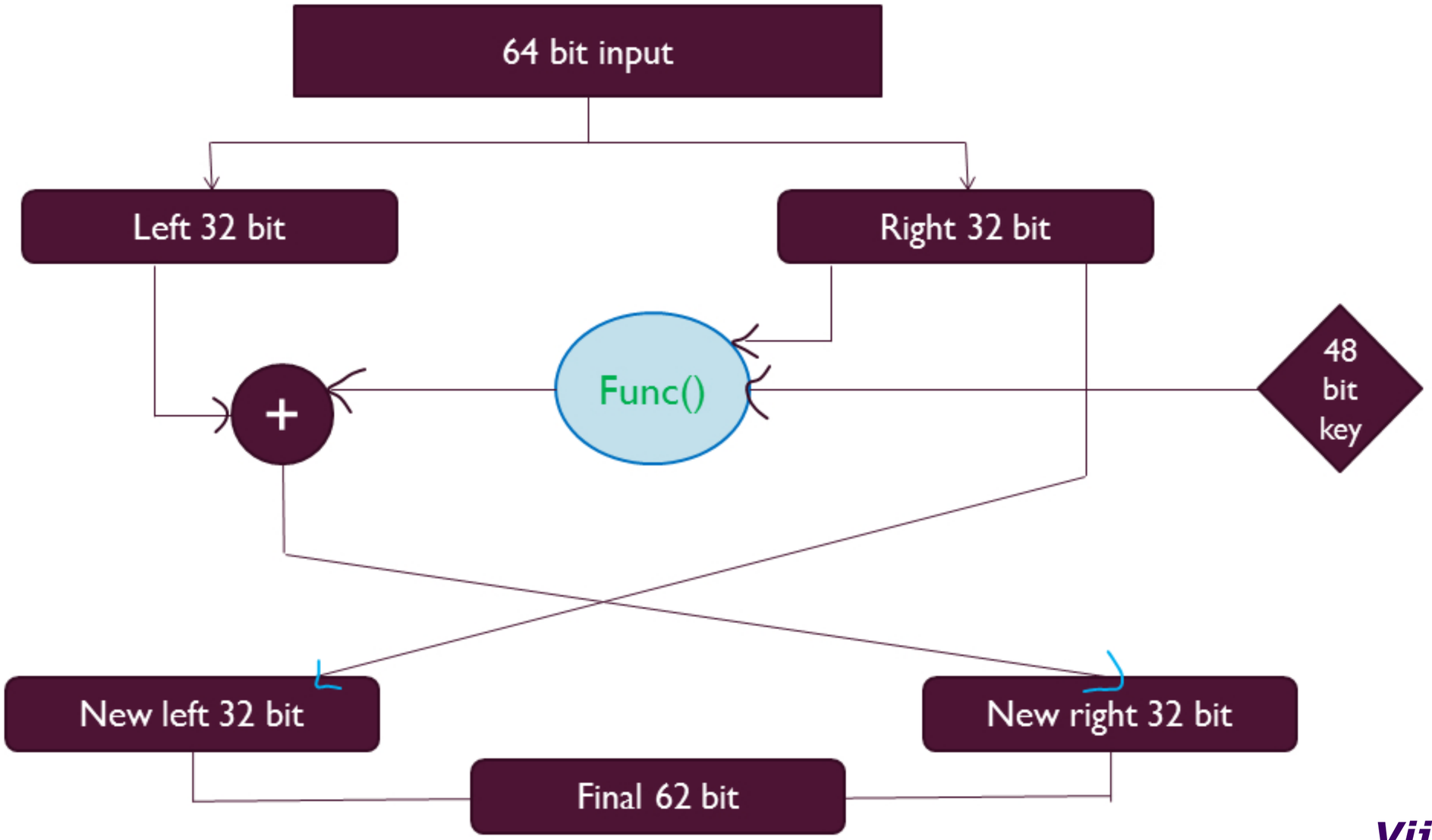

001011
48 bit data
S
S
S
S
S
S
S
S
0111
32 bit data


32 bit input
Expansion box
48 bit
+
48 bit key
48 bit
S
S
S
S
S
S
S
S
32 bit
Permutation box
32 bit output

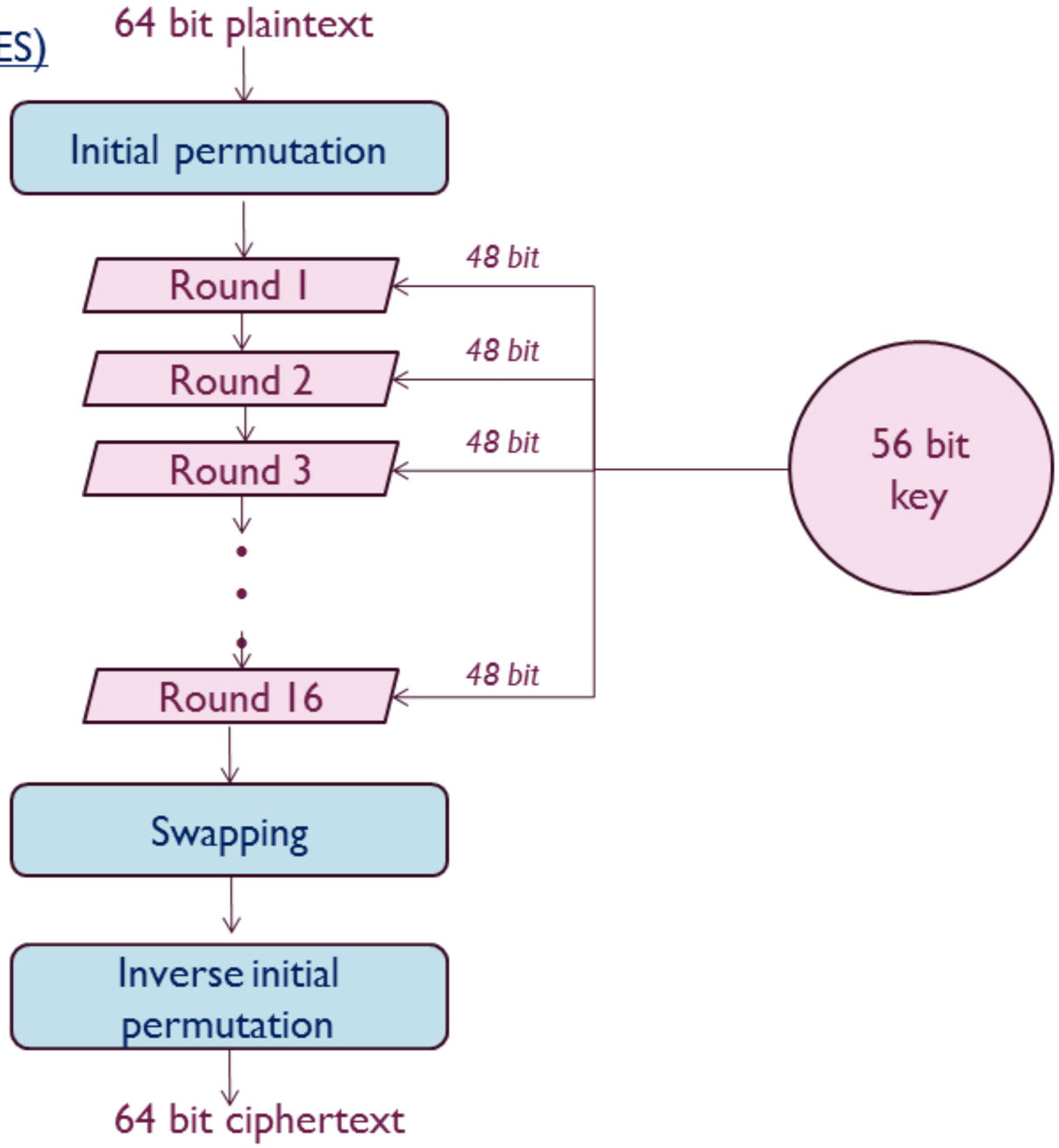
DATA ENCRYPTION STANDARD (DES) - ONE ROUND



DATA ENCRYPTION STANDARD (DES) - ONE ROUND



DATA ENCRYPTION STANDARD (DES)



THANK YOU

Vijesh Nair