Rocca S

A Symmetric Key Block Cipher

~Rohan Sudhir Basugade

Introduction

- Rocca S is a cryptographic algorithm focused on efficiency with many opportunities for parallelization.
- It uses a state-based approach and ciphers in 256-bit blocks of data.
- Focus on secure, high-speed data encryption.

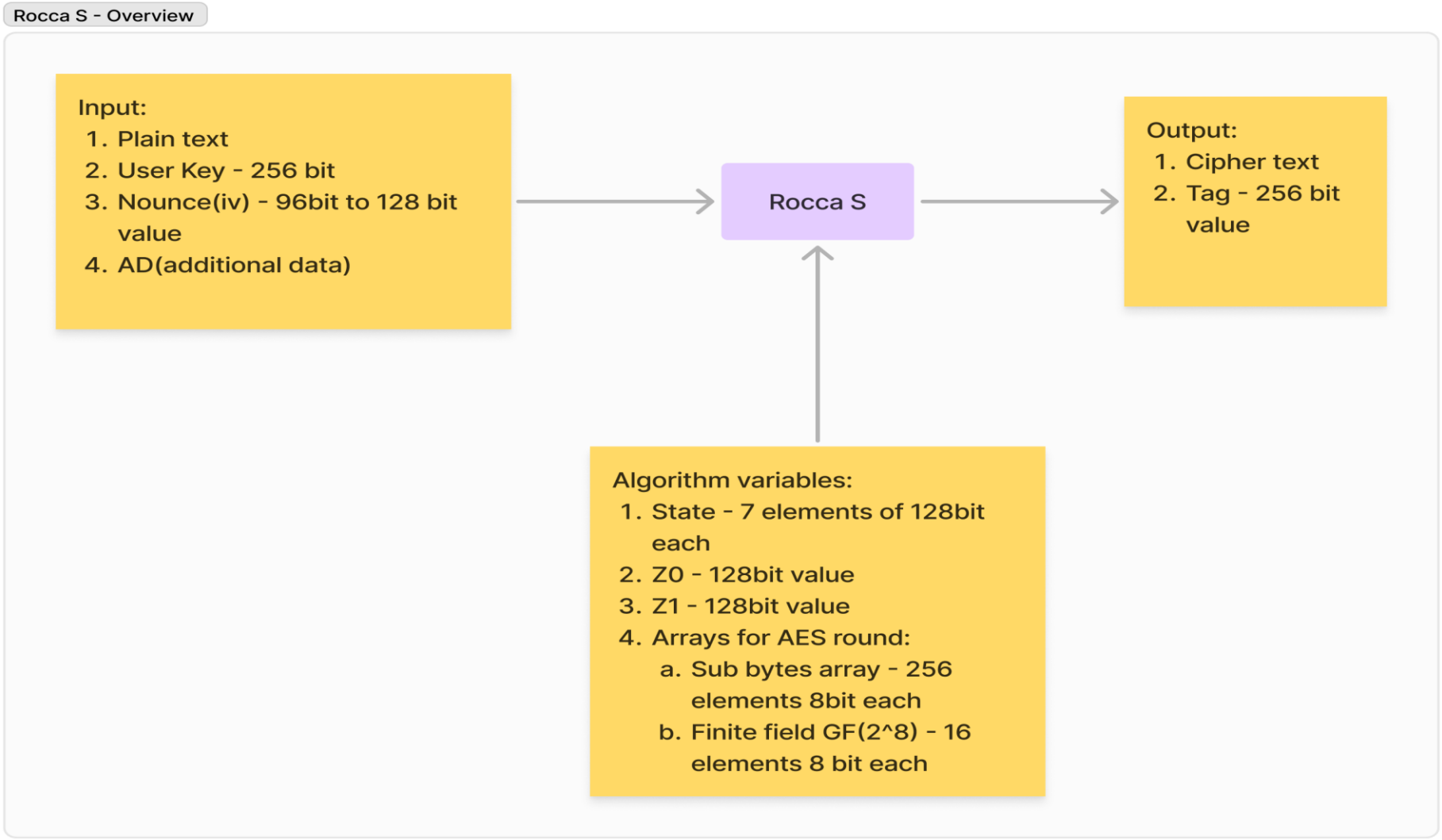
Algorithm Structure

- ROCCA_STATE is composed of 7 elements of 128-bits each.
- The state gets initialized based on the input key and some predefined variables.
- Z0 and Z1 are 128bit values used in the initialization of State.
- SubBytes Array is the same array that’s used in substitution phase of AES.

Algorithm Structure

- Key is 256bit for maximum security. Its divided into K0(left) and K1(right) each 128bits for use in algorithm.
- Nonce is an initializing vector. Varies from 96bits to 128bits.
- Associated Data (2^61 bytes max_size) is used also used to update State and is sent without encryption.
- Plaintext (2^125 bytes max_size) is the text to be ciphered.

Rocca S - Overview



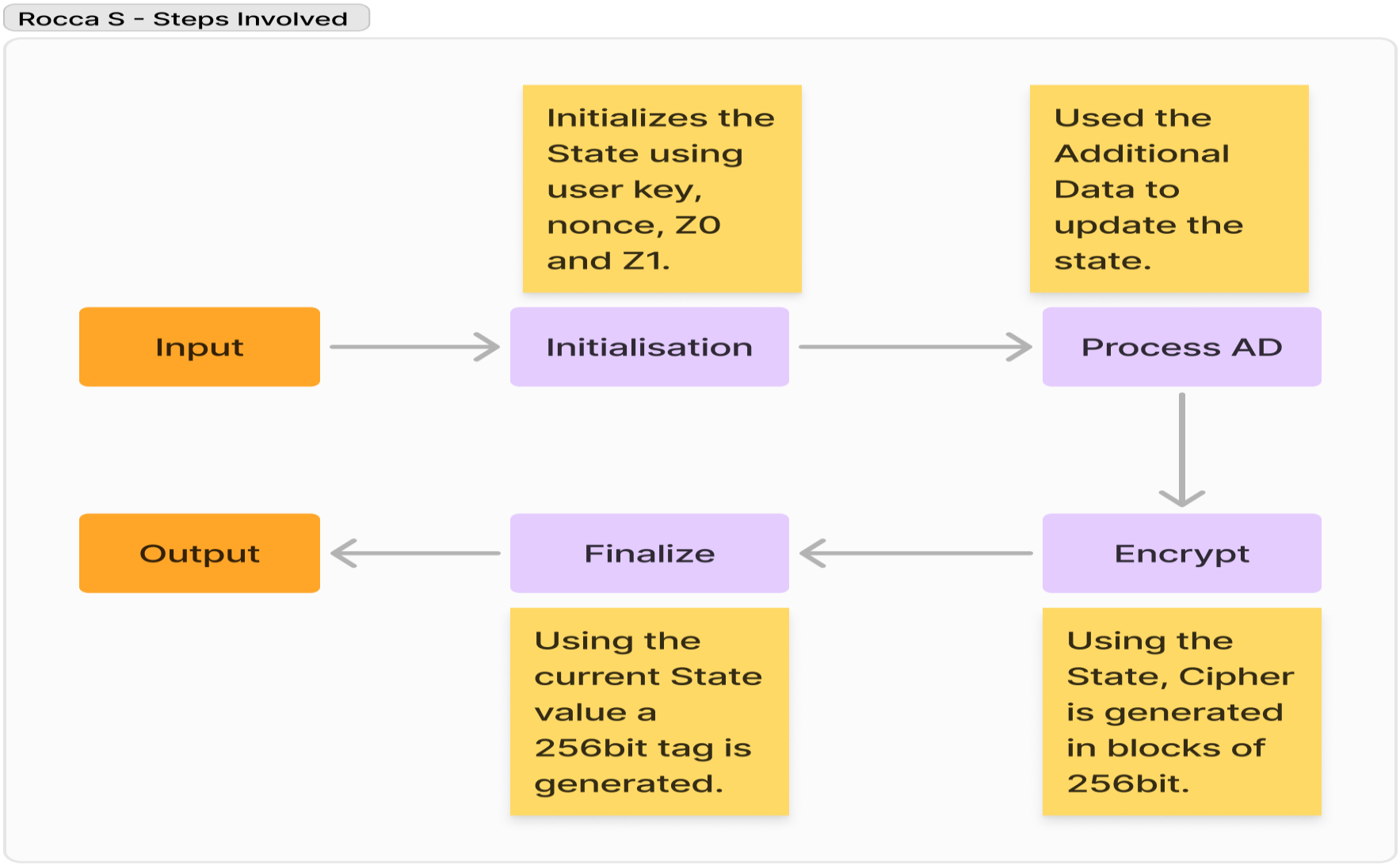
Padding Explanation

- PAD(M) pads M to have a length divisible by 256 by adding 0s to the right.
- PADN(N) pads N to have length divisible by 128 by adding 0s to the right.

PAD - Explanation

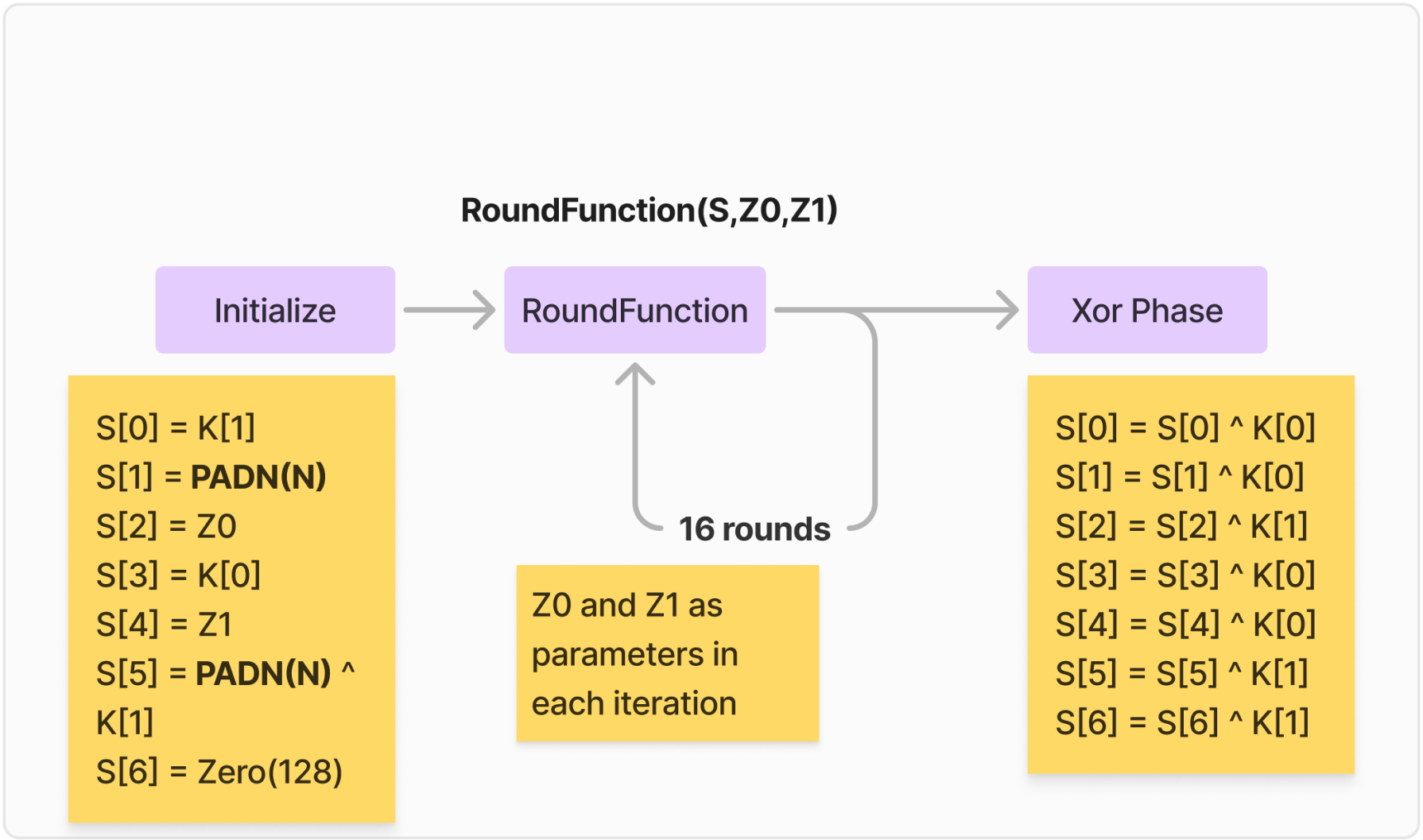
Plaintext - M Suppose it has 256+256+2 = 514 bits	0	1	2	....	254	255	0	1	2	....	254	255	0	1				
	0	1	1	0	1	0	1	1	1	0	0	1	0	1				
PAD(M) wil add 0s to the right so that its length is multiple of 256.	0	1	2	....	254	255	0	1	2	....	254	255	0	1	2	....	254	255
	0	1	1	0	1	0	1	1	1	0	0	1	0	1	0	0	0	0

Rocca S – Steps Involved

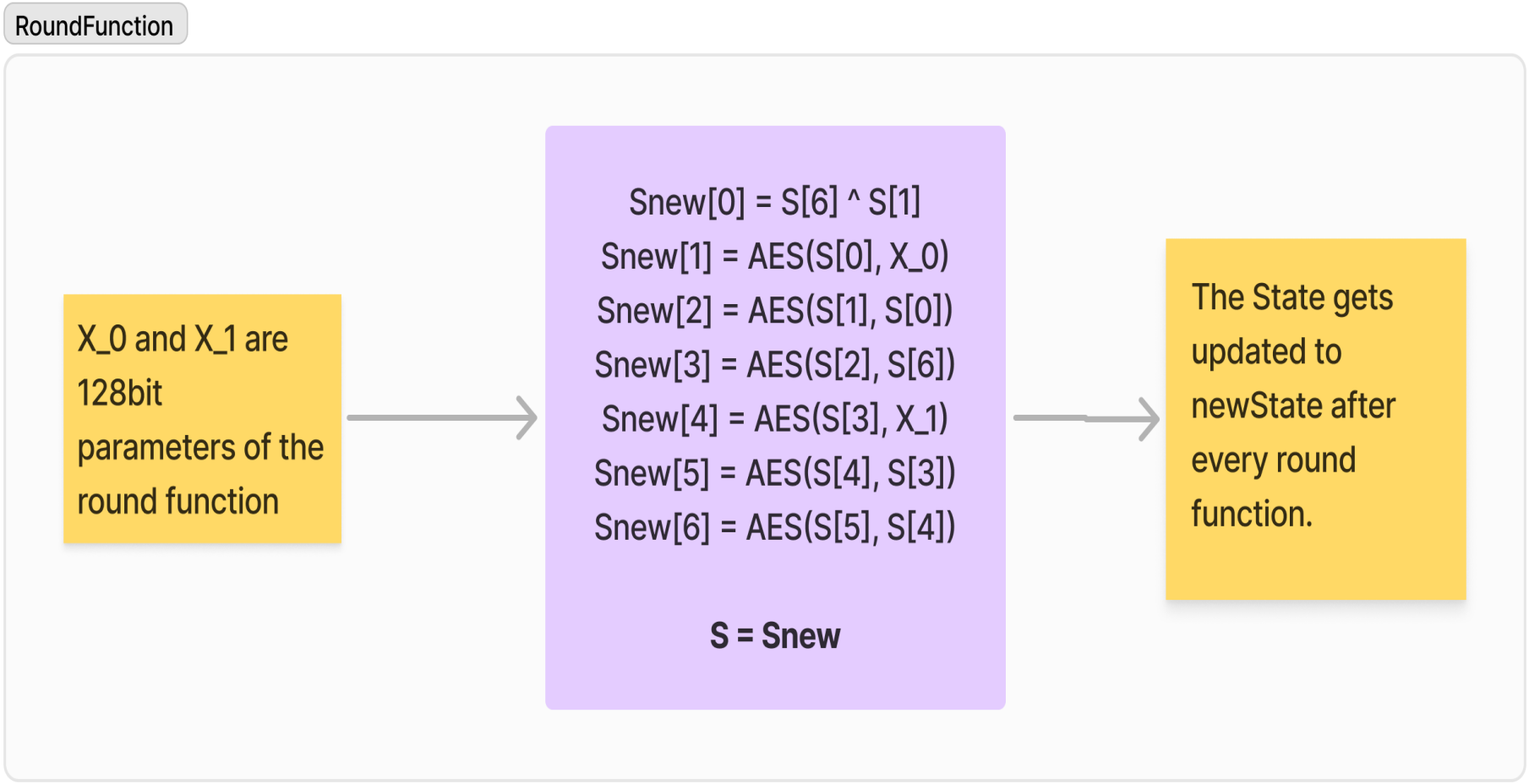


Initialization

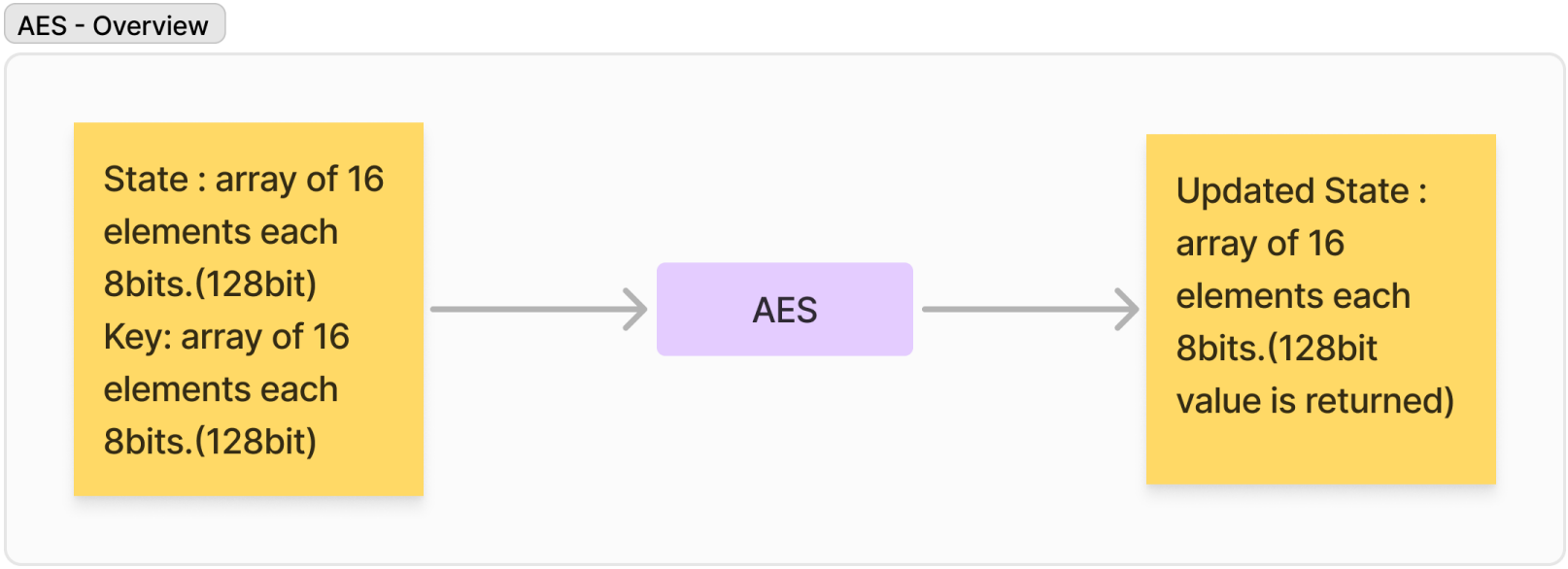
Initialization



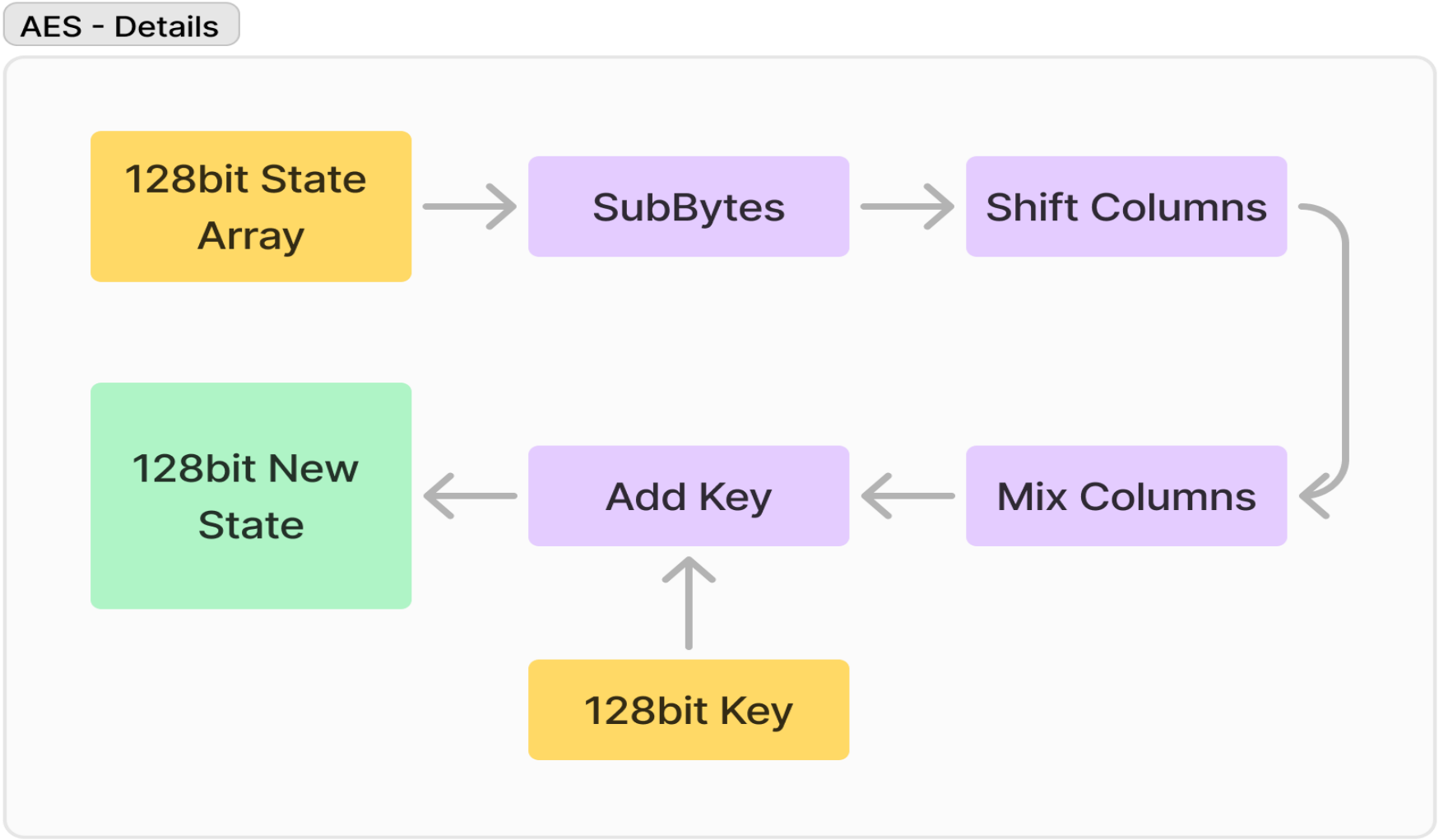
RoundFunction



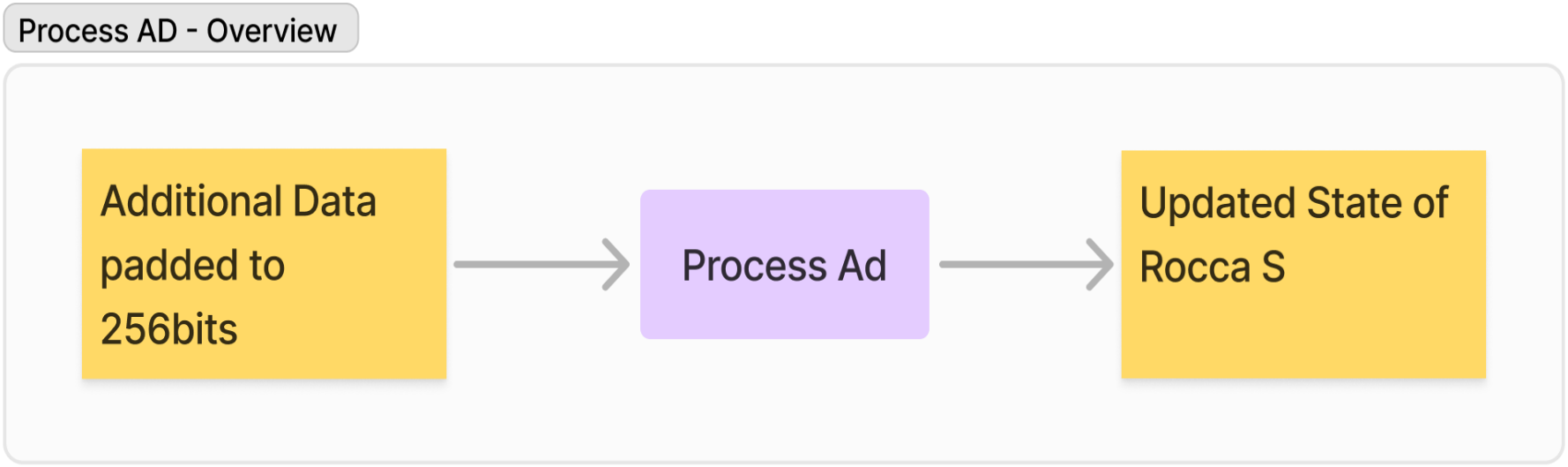
AES - Overview



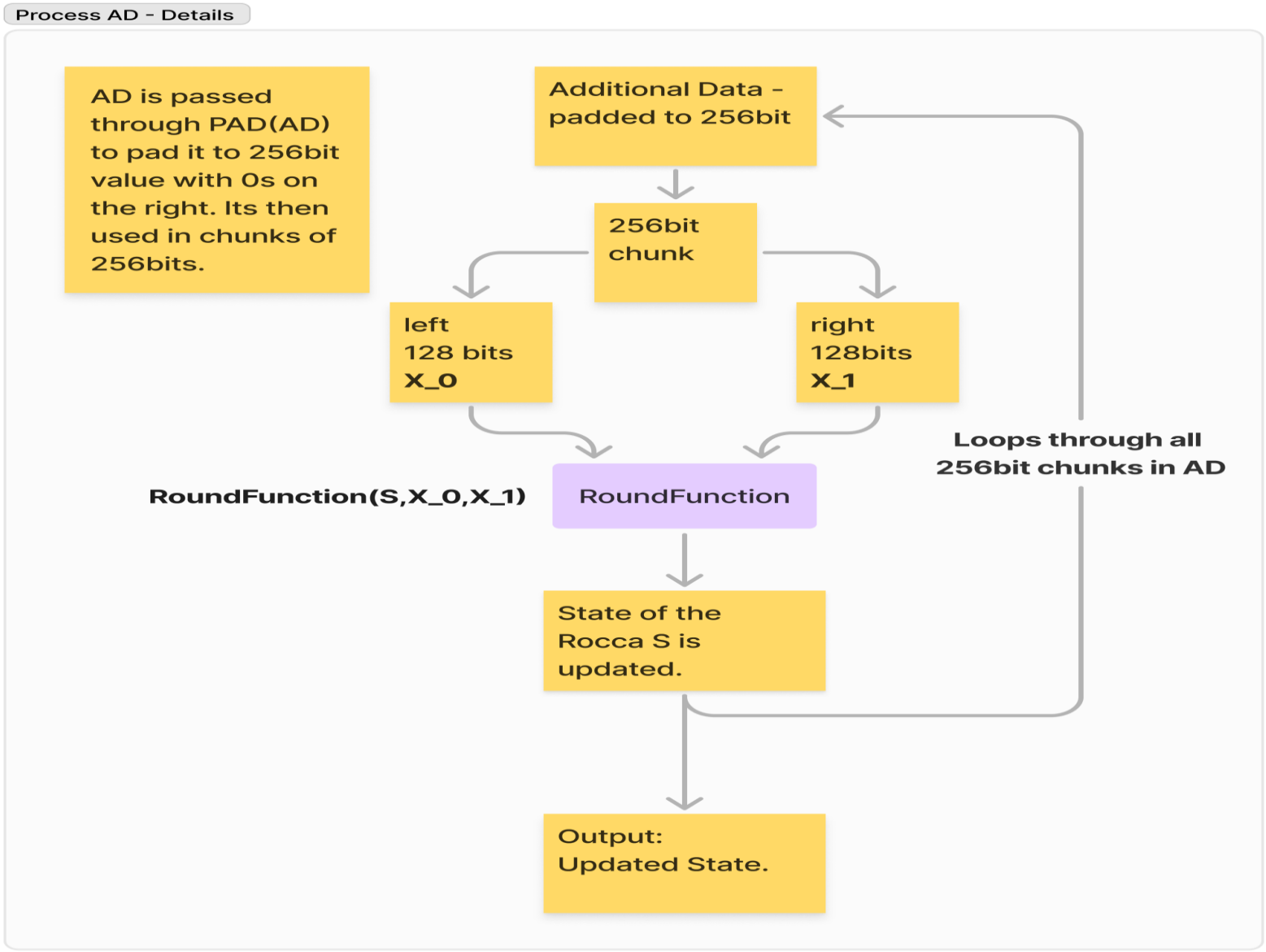
AES - Details


AES - Details
128bit State Array
SubBytes
Shift Columns
Mix Columns
Add Key
128bit New State
128bit Key

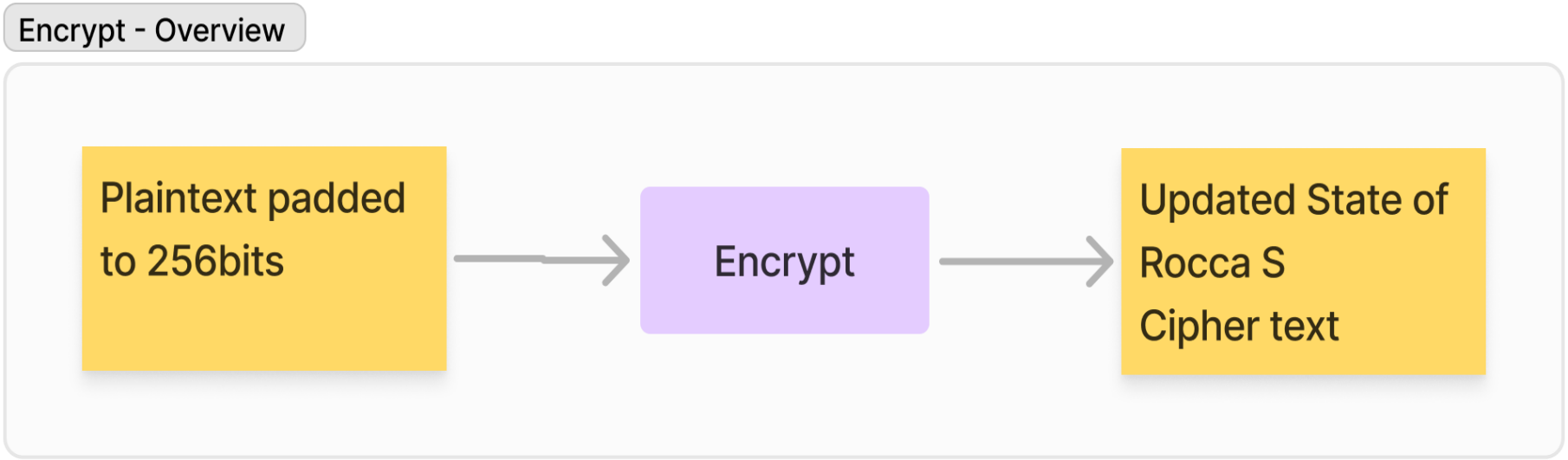
Process AD - Overview



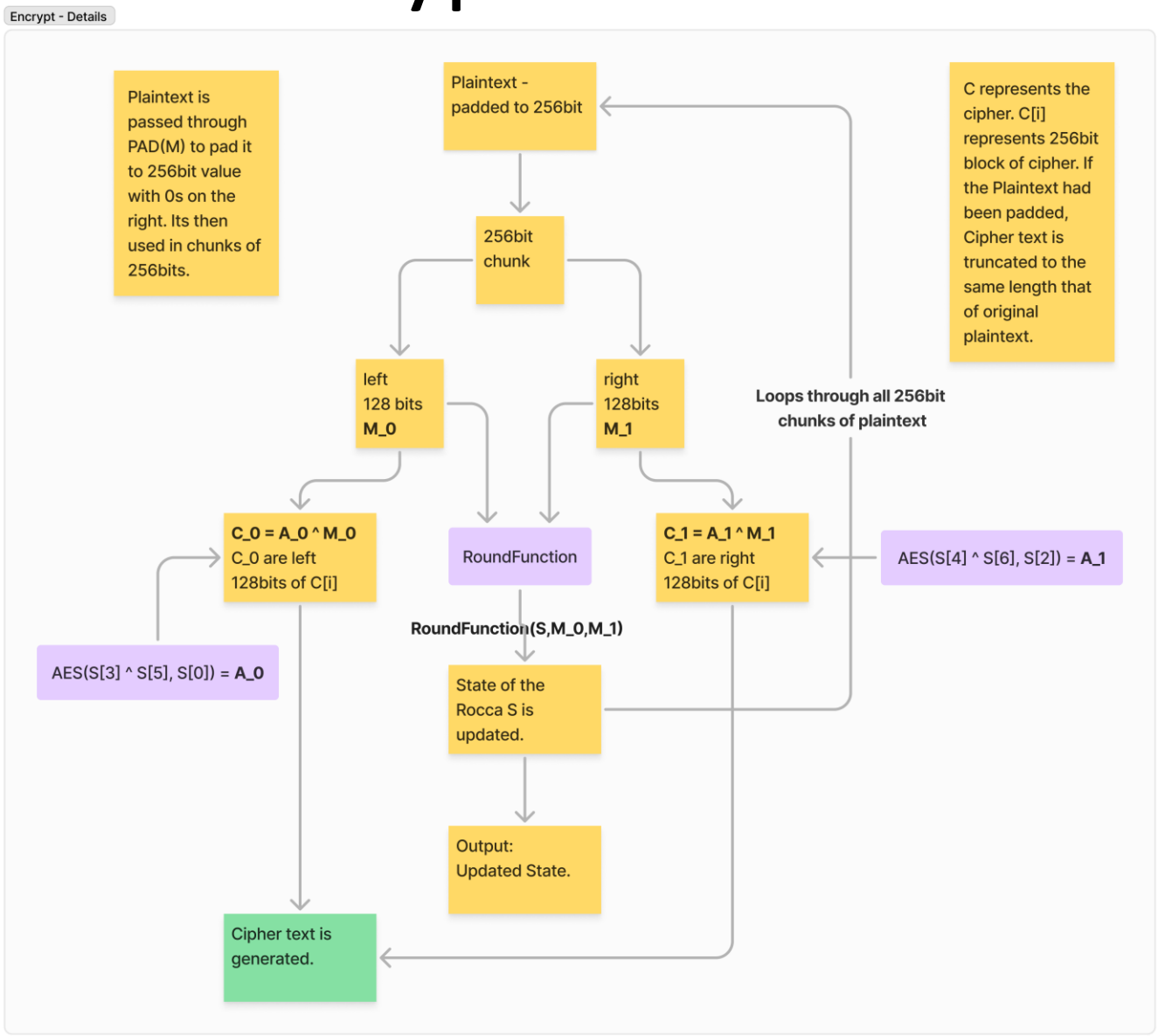
Process AD - Details



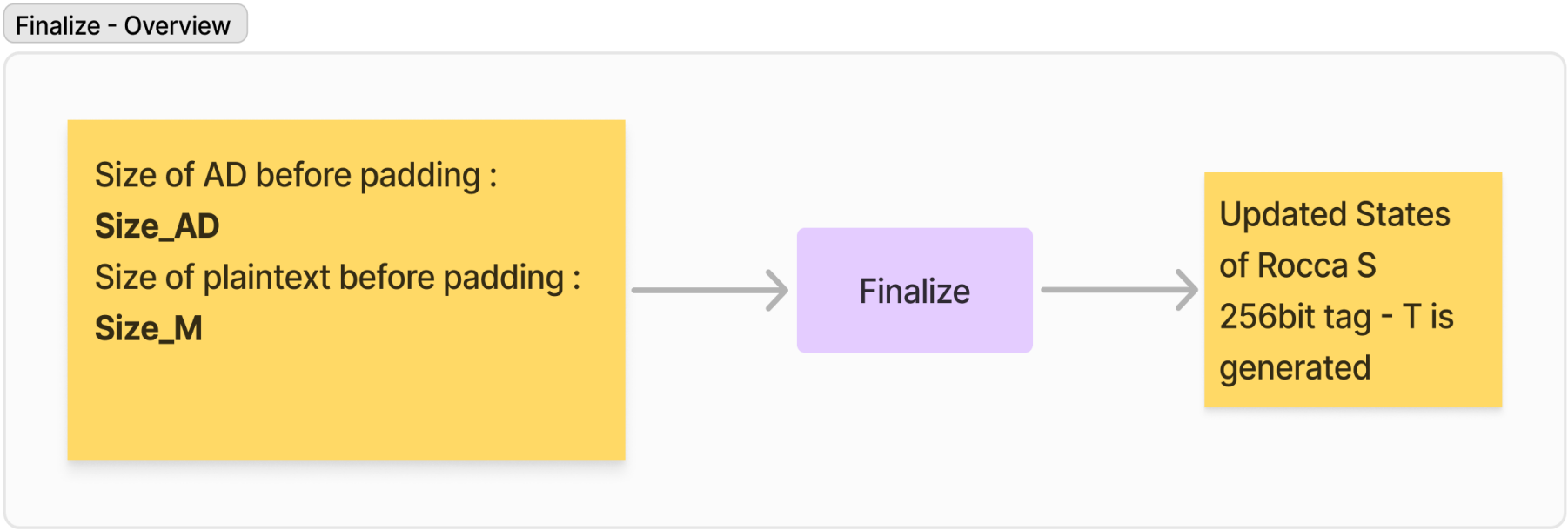
Encrypt - Overview



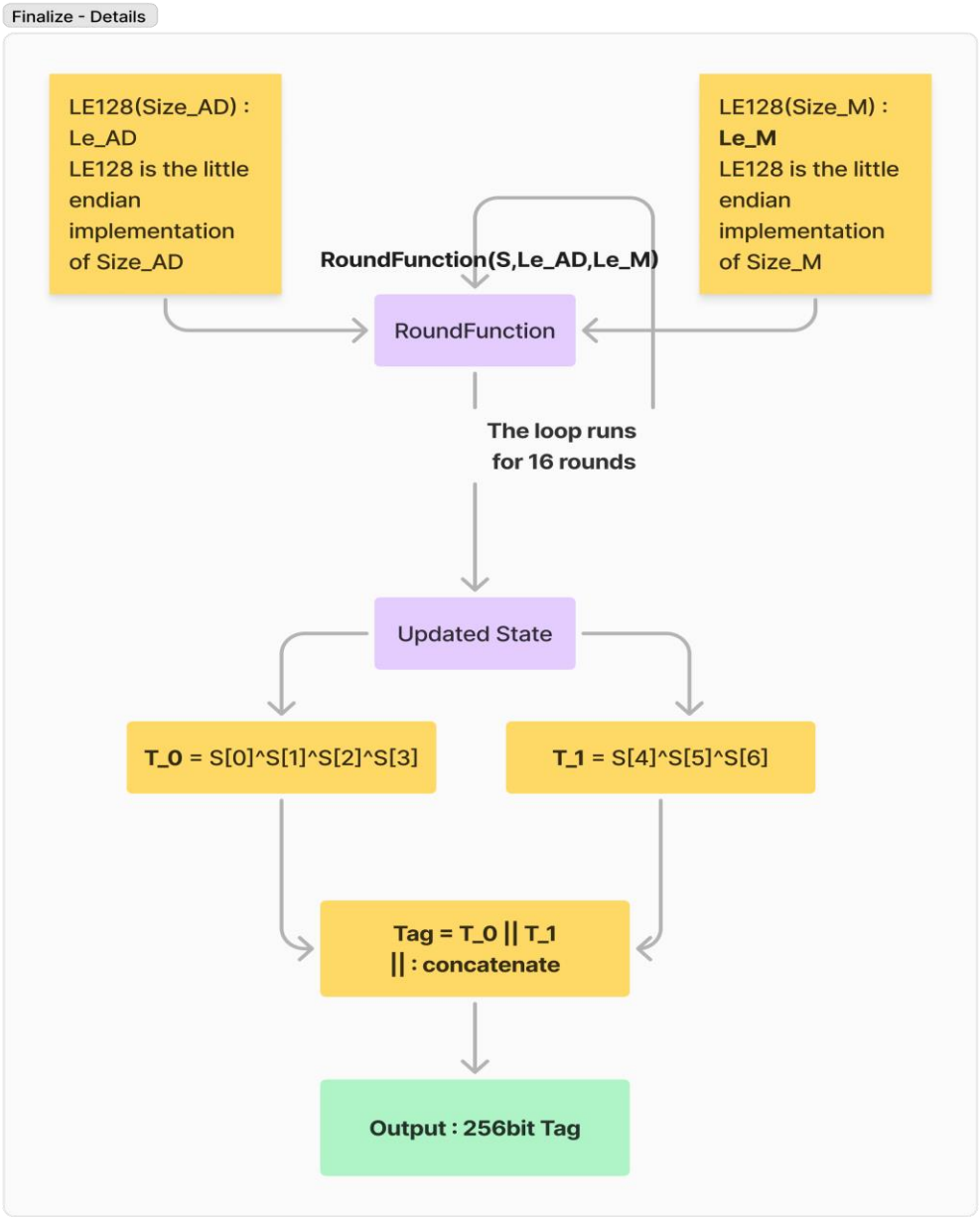
Encrypt - Details



Finalize - Overview



Finalize - Details



Outputs

- The Cipher text that’s generated is truncated to the same length as the original message.
- The Tag generated is a 256-bit value used for Authentication or Integrity?