Author: RAGHU SAI PHANI SRIRAJ VEMPARALA

PBKDF2 Memo

This memo provides analysis of the code before optimization and it also provides the information regarding call stack , text size and run time information.

Call Stack

The call stack tree provides information regarding the function stack information.

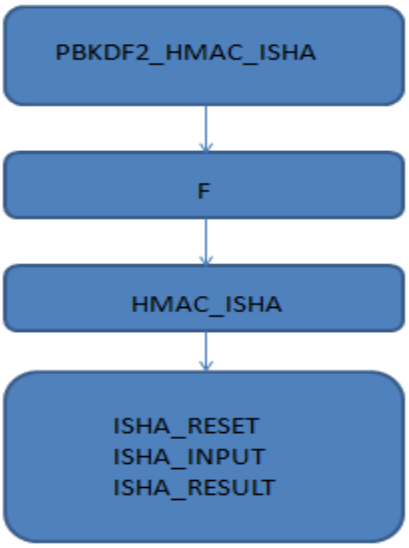
The sequential order of functions called are as follows:

1. PBKDF2_HMAC_ISHA
2. F
3. HMAC_ISHA
4. ISHA_Reset
5. ISHA_Input
6. ISHA_Result

The explanation of flow is as follows:

1. Inside the main function PBKDF2_HMAC_ISHA is called and this function calls the F function thrice.
2. The function F calls HMAC_ISHA 4097 times to generate the key.
3. Each call to HMAC_ISHA calls the functions ISHA_Reset, ISHA_Input and ISHA_Result one after the other.

FLOW DIAGRAM:



TIMING TABLE:

This table consists of the timing and count of function calls:

FUNCTION NAME	TIME(milli seconds)	C(count)
PBKDF2_HMAC_ISHA	8.744	1
F	2.91	3
HMAC_ISHA	0.7	12228
ISHA_Reset	0.002	24567
ISHA_Input	0.1	49152
ISHA_Result	0.1	24576
IshaProcessMessageBlock	0.06	49152

Text Size before optimization:

Optimization Level	Bytes
O0	21056
O3	17812