Team Members :
Vishwanadh Rapolu – 140050046
Rohith Reddy Gangam – 140050060

Topic : To find collisions in MD5 Hash

Description :
Find 2 block collision for MD5 hash function(fixed initial vector) which follows Merkle-Demagard Construction. [1] specifies sufficient conditions on message blocks and the intermediate hash values to form a collision.
We found the collision for 1st block with conditions as mentioned in [1] using single message modification, Multi message modification by [1], [2] and [3]. [3] is faster as compared to others so presenting the results using the algorithm from [3].
All the results depend on the initial seed taken for rand.

Work Done: As mentioned in the description, the aim is to find 2- block collision but our code only finds the first block in both the messages so that the required hash value difference occurs. All the codes(md5_single.cpp, md5_multi.cpp, md_klima.cpp) only find the first block of message 1 and check.cpp, given the first block of message 1 finds the first block of message 2 and finds the hash difference of the both the hashes.

Link to Project: https://github.com/rapoluvishu/CS-406

Libraries used : For rand and srand
#include <time.h>
#include <stdio.h>
#include <stdlib.h>

Steps to run : Outputs the message block of 1st message. Use [3] code for evaluation which gives output in around 8-15 minutes.
For results using [1] – make single
For results using [2] – make multi
For results using [3] – make klima

References :
1. https://link.springer.com/content/pdf/10.1007%2F11426639_2.pdf
2. https://pdfs.semanticscholar.org/0603/6d71d60fd4a8a002f50bf2524ef9c3540717.pdf
3. https://eprint.iacr.org/2005/102.pdf
4. http://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1020&context=etd_projects
5. https://www.nada.kth.se/utbildning/grukth/exjobb/rapportlistor/2009/rapporter09/ekera_martin_09008.pdf
6. http://cryptography.hyperlink.cz/MD5_collisions.html