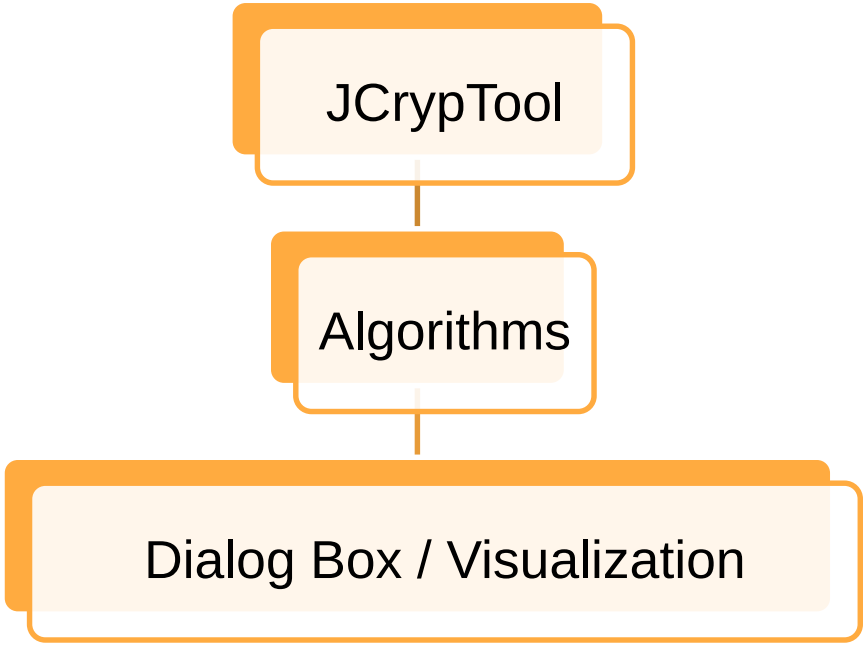
Cryptology

Dec 12 2016

GitHub

Trello

System Diagram



Product Highlights

1. Provide users with SHA3 candidates to choose when using JCrypTool.
2. Design a better dialog box for users to choose different algorithms and read the output more easily.
3. Visualize the Blake algorithm.

Demonstration

Test Results

Problem with Algorithms

The algorithms didn’t output the correct answer.

Test case(for Groestl):

1. Abcd: D8CD6BE396A8F029BC46E48367D3D84150776C10B7A6AFFEDB19E8D0D175A708
2. Aefg: D8CD6BE396A8F029BC46E48367D3D84150776C10B7A6AFFEDB19E8D0D175A708

Problem 1: Unless we change the first character of the input, the output will be the same.

Problem 2: Unless we change the length of the input, the output will be the same for most cases.

Problem solved:

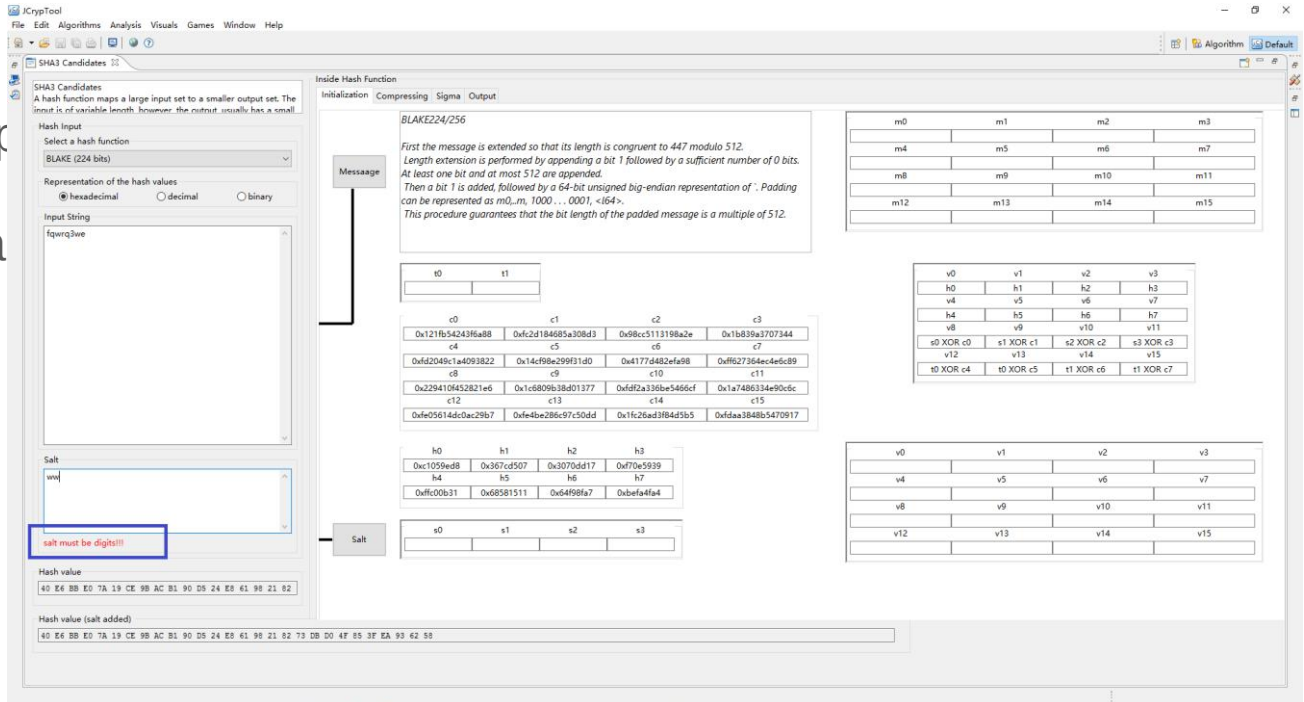
1. Abcd: 4A639E2F274A8B6A4D3AC957456F8FAE8DF80E2AEA89C19276BDACA5586B5F99
2. Aefg: EDFF182DB0D66874D155CA79CD37FF3F625C822B37AE66E3C1903D50AB5C6C3A

Problem with Visualization

Visualization cannot jump automatically when clicking at the button.

Solved: Inp

Also add a



Test Case 1

1. Different input with same length with 256 hash bit length.

Input1: ABCDefgh

Input2: ABCDijkl

Groestl:

Output1:
AA7FF5E8167C47B451C75852A2CF77362708F9D9C15CE349E26D81FB8266B085

Output2:

CE4D4AE59B17F7441F638E519D8A24BE737CDAF9E6A944BF7BF4A609E184A7BF

Blake:

Output1:
E6A2B048BAB77FC6798346A34FE91635507DFABF21CF904D63DD12933675C6DB

Output2:
0FFFB62363102F94C5FA4791F565CA93FAD8BE51EC2067E16F2BED91310E8C7B

Keccak:

Output1:
4A441AB0A95C5CF500363FA8753AE8E4FC5FB5E3EC54BA492F52271835BBC718

Output2:
0235DC28399BF9B391831E2ABDDC156D1F3A920C9FFE3C4ED1B5ABCBC9DFE1EA

Test Case 2

2. Different input with only ONE character different

Input1: uihkjllihjkl1oiuhjnkml7liu

Input2: uihkjllihjkd1oiuhjnkml7liu

Groestl:

Output1:
EE2BE9B9D85A5F72C11AA258742E1B7E8742C1395966B4CF9D5F66F7780AFA79

Output2:
99FDA91895657FFE1D19F4821945D5750CB9C8F19065F2E413D2EF7A1B904AD4

Blake:

Output1:
C054E0ECCC6AD3DE0E539B9F04904C07B6B75ABF528E7A2644F790C4D67B5447

Output2:

42632FE4B23C9C8DCB2C40503D16674EC315DA0BD5EFB1180A985D86D282DF79

Keccak:

Output1:
F802E85C8EB4E33BD81F2F08CA8A8D93D8F33CC69A93F7AEE9E2395FE15D6217

Output2:

61FF7DD62E23B9B99273ACBEFE04E6456A4D8D2EF2E7783DF093635AA0CB43EE

Top three things that worked well

1. Algorithm implementation for SHA3 candidates.
2. Design the dialog box.
3. Visualize the Blake algorithm.

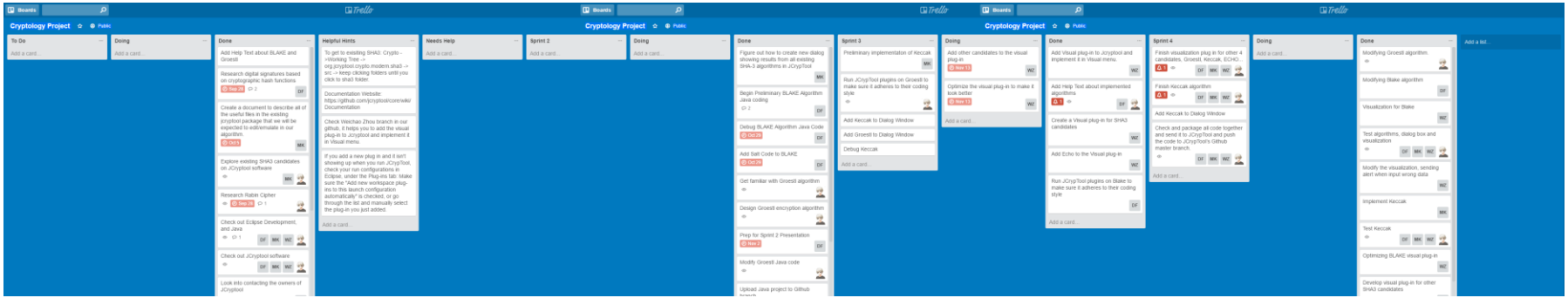
Top three things that we have learned

1. Learn how to develop a plugin based on a project.
2. Java knowledge, especially the basic Java data structure.
3. Learn how to use Github, Trello and Slack.

Future plan

1. Build more visualization for SHA3 candidates.
2. Implement the visualization by import the package other than have a copy for the visualization
3. Check and package all code together and send it to JCrypTool and push the code to JCrypTool’s Github master branch.

Trello


Cryptology Project
To Do
Doing
Done
Helpful Hints
Needs Help
Sprint 2
Sprint 3
Sprint 4

Thank You