Development Diary

Tuesday 15th October, 2024

Author: Sandra Matthies

Starting the prototype for the HillCipher Known Plaintext Attack. Implement classes, methods and logic for the calculation. Implement HillCipher Encryption and Decryption for testing the attack.

Wednesday 23rd October, 2024

Author: Sandra Matthies

Finish the prototype for the HillCipher Known Plaintext Attack. The prototype can calculate the key matrix of a Hill Cipher based on a known plaintext and the corresponding ciphertext. The prototype is tested with different plaintexts and ciphertexts.

Wednesday 30th October, 2024

Author: Sandra Matthies

Creation of an empty Plugin-File for the HillCipherAttack in the Cryptool 2 application.

Sunday 3rd November, 2024

Author: Sandra Matthies

Transfer of the calculation methods for the HillCipherAttack from the HillCipher Prototype to the HillCipherAttack Plugin and Refactoring.

Sunday 17th November, 2024

Author: Sandra Matthies

Add Validations and Error Handling to the HillCipherAttack Plugin. The Plugin now checks if the input data is valid and if the key matrix is invertible. If the key matrix is not invertible, the plugin throws an exception. I also added a method to calculate the modular inverse of a number. This method is used to calculate the inverse of the determinant of the key matrix.

Tuesday 19th November, 2024

Author: Sandra Matthies

Update search for key, so that as long as the key is not found, the search continues if enough data is available. This is necessary because sometimes the key is not found in the first iteration, but in the second or third iteration.

Sunday 8th December, 2024

Author: Sandra Matthies

Update eigenvalue calculation to use the new method for calculating the modular inverse of a number. The eigenvalue calculation is used to calculate the determinant of the key matrix. The determinant is needed to calculate the inverse of the key matrix.

Sunday 15th December, 2024

Author: Sandra Matthies

Implement the Ciphertext Only Attack based on the Known Plaintext Attack. Add Settings, Inputs, Outputs and Visualization to the Plugin.

Wednesday 25th December, 2024

Author: Sandra Matthies

Add Templates and Descriptions to the Plugin. Add a wiki page for the HillCipherAttack Plugin.

Sunday 29th December, 2024

Author: Sandra Matthies

Extend documentation, update the wiki page for the HillCipherAttack Plugin and update Outputs.

Monday 30th December, 2024

Author: Sandra Matthies

Set default settings for the HillCipherAttack Plugin. Final Testing and remove Logs, Comments and unused Code.

Monday 13th January, 2025

Author: Sandra Matthies

Finalize documentation and testing of the HillCipherAttack Plugin.