Tallinn University of Technology

Foundations of Cyber Security

CRYPTO-APPLICATION

Nikita Ojamäe
185827

IAIB23

Tallinn 2019

Documentation

Crypto-application called “Cryptonator” allows user to encrypt text to one-time pad encryption (OTP), decode OTP decrypted text and encrypt text to SHA-512 Base64.

Application can be found here https://niojam.github.io/Crypto-application/

Source code can be found on https://github.com/niojam/Crypto-application

1) One-time-pad encrypt

OTP-encrypt requires input text and key (one-time-pad) which must be the same size as plaintext. Then the plaintext is encrypted by combining it with the corresponding character from the key with using modular addition to corresponding indexes of key or plaintext characters in the alphabet.

If one of the requirements is not completed, then system will alert fixed message and will kindly ask to try again. By pressing the „OTP-encrypt“ button plain text will be encrypted.

2) One-time-pad decrypt

OTP-encrypt requires input encoded text and key (one-time-pad) which must be the same size as plaintext. Decryption is using similar algorithm as encryption, but operations are reversed. By pressing the „OTP-decrypt“ button encrypted text will be decrypted.

3) SHA2

Requires input plaintext. With using special algorithm encrypts plaintext to SHA-512 Base64 format.

By pressing the „SHA512-encrypt “ button plain text will be encrypted.

This function use: [1]
Title: A JavaScript implementation of the Secure Hash Algorithm, SHA-512, as defined in FIPS 180-2 source code
Author: Paul Johnston
Date: 2000 - 2009
Code version: Version 2.2 Copyright Anonymous Contributor.
Other contributors: Greg Holt, Andrew Kepert, Ydnar, Lostinet.
Availability: https://asecuritysite.com/sha512.js
Code adapted from https://asecuritysite.com/sha512.js
Distributed under the BSD License.
More information about this function and license can be found in source code.

4) MD5

Button exists, but functionality is missing

References

[1] SHA-512 encryption, [source code]. Available: https://asecuritysite.com/sha512.js [Used 01.02.2019].