

«به نام خدا»

تکلیف ششم – مرضیه علیدادی – 9631983
(سوال 5)

5.

5.1.

i.

Keyed-Hash Message Authentication Code (HMAC)

Description

By means of a HMAC the recipient of a message is able to verify its integrity and the authenticity of its sender. Therefore both parties use a shared secret (symmetric key).
To create a HMAC, a cryptographic hash function is applied to a combination of the message m and the secret key k. According to the variation chosen below, two different keys k and k' can be used.

Message

Starting example for the CrypTool version family 1.x (CT1)

CrypTool 1 (CT1) is a comprehensive and free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations.

This text file was created in order to help you to make your first steps with CT1.

1) The starting page of the online help offers the best oversight of CT1's capacity. From the starting page you can reach all essential functions via links. The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the main window or by using the search keyw. Press F1 to start the online help everywhere in CT1.

2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (classic)".

HMAC parameter and key

Hash function SHA-256 (256 bits) HMAC variant H(k, m, k'): different keys

Enter your key (k) marzieh

Enter second key (k') alidadi

Inner hash value:

Input for outer hash function (depends on the HMAC variant chosen above)

marziehStarting example for the CrypTool version family 1.x (CT1)

CrypTool 1 (CT1) is a comprehensive and free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations.

HMAC generated from message and key

EF DB 41 E8 C8 2D 35 32 C4 88 40 88 6C 1C AF E2 B2 30 A7 8F 1C CB 3A E4 7D 9D BE 6A 9F F0 D7 F7

Close

Message:

The starting-example text of cryptool

Input:

marziehStarting example for the CrypTool version family 1.x (CT1)

CrypTool 1 (CT1) is a comprehensive and free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations.

Hash:

EF DB 41 E8 C8 2D 35 32 C4 88 40 88 6C 1C AF E2 B2 30 A7 8F 1C CB 3A
E4 7D 9D BE 6A 9F F0 D7 F7

- ii. The same file and text

Hash:

B0 43 DE F4 E0 EA 01 8C 93 B3 CD E6 A4 82 EC 92 35 6F 0D 54 11 80
59 3A 50 10 74 49 86 B0 63 98

