LAB 3

Message authentication and integrity

IZAZOV 1

Napravili smo funkciju koja provjerava je li originalna poruka mijenjana, odnosno je li narušen njen integritet. Ukoliko nije, funkcija verify_MAC vraća TRUE u protivnom False.

Zatim smo mijenjali signature poruke, a poruka je bila nepromijenjena. Funkcija verify_MAC je također vratila False.

IZAZOV 2

Prateći upute, trebalo je samostalno **utvrditi vremenski ispravnu skevencu transakcija (ispravan redosljed transakcija) sa odgovarajućim dionicama**.

message_integrity.py

```python
from cryptography.hazmat.primitives import hashes, hmac
from cryptography.exceptions import InvalidSignature
import os

def verify_MAC(key, signature, message):
    if not isinstance(message, bytes):
        message = message.encode()

    h = hmac.HMAC(key, hashes.SHA256())
    h.update(message)
    try:
        h.verify(signature)
    except InvalidSignature:
        return False
    else:
        return True

def generate_MAC(key, message):
    if not isinstance(message, bytes):
        message = message.encode()

    h = hmac.HMAC(key, hashes.SHA256())
    h.update(message)
    signature = h.finalize()
    return signature
```

```python
if __name__ == "__main__":
    key = "curak_sara".encode()

    # Reading from a file
    with open("message.txt", "rb") as file:
        content = file.read()

    # # mac = generate_MAC(key, content)

    with open("message.sig", "rb") as file:
        mac = file.read()

    is_authentic = verify_MAC(key, mac, content)
    # print(is_authentic)

path = "mac_challenge"
for ctr in range(1, 11):
    msg_filename = f"order_{ctr}.txt"
    sig_filename = f"order_{ctr}.sig"
    # print(msg_filename)
    # print(sig_filename)
    with open(os.path.join(path, msg_filename), "rb") as file:
        content = file.read()
    with open(os.path.join(path, sig_filename), "rb") as file:
        mac = file.read()
    is_authentic = verify_MAC(key, mac, content)
    print(f'Message {content.decode():>45} {"OK" if is_authentic else "NOK":<6}')
```

REZULTAT:

```
(sara) C:\Users\A507\sara\sara>python message_integrity.py
Message    Sell 94 shares of Tesla (2021-11-13T02:59) OK
Message    Sell 52 shares of Tesla (2021-11-09T00:08) NOK
Message     Buy 10 shares of Tesla (2021-11-15T10:53) OK
Message    Sell 51 shares of Tesla (2021-11-14T08:01) OK
Message     Sell 5 shares of Tesla (2021-11-11T00:31) NOK
Message      Buy 4 shares of Tesla (2021-11-10T18:18) OK
Message     Buy 89 shares of Tesla (2021-11-14T11:03) OK
Message    Sell 58 shares of Tesla (2021-11-11T02:57) NOK
Message    Sell 23 shares of Tesla (2021-11-14T21:33) NOK
Message     Buy 38 shares of Tesla (2021-11-15T11:19) OK

(sara) C:\Users\A507\sara\sara>
```

Sara Ćurak

Računarstvo 120