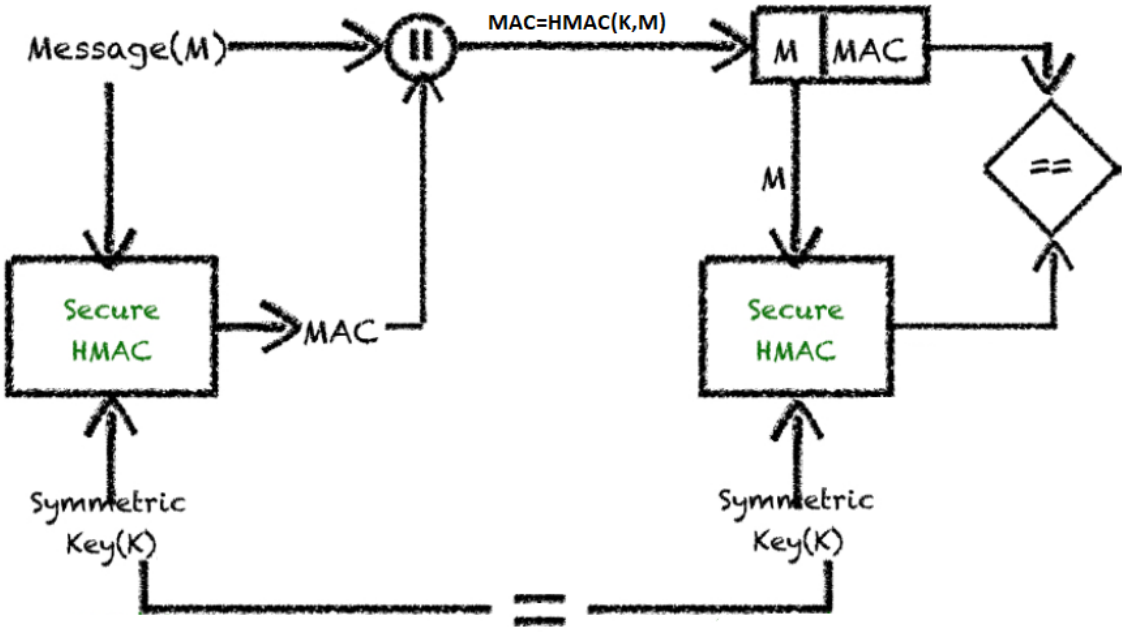
Lab 3

Message Authentication Code (MAC) i digitalni potpis

- osnovni kriptografski mehanizmi za autentikaciju i zaštitu integriteta poruka
- MAC pruža i autentičnost poruke uz njen integritet
- simetričan ključ k+ plain text message m → **MAC=HMAC (k,m)**



IZAZOV 1

- Implementiranje zaštite integriteta sadržaja dane poruke primjenom odgovarajućeg *message authentication code (MAC)* algoritma

1. U lokalnom direktoriju kreira se tekstualna datoteka odgovarajućeg sadržaja čiji se integritet želi zaštititi
2. Učitavanje sadržaja datoteke u memoriju
3. Pomoću HMAC algoritma dobije se MAC vrijednost za danu poruku

4. Provjera validnosti MAC-a za danu poruku
5. Sami mijenjamo sadržaj datoteke i uvjeravamo se da HMAC algoritam detektira promjene

IZAZOV 2

- Treba odrediti autentičnu sliku (između dvije ponuđene) koju je profesor potpisao svojim privatnim ključem

1. Preuzimanje javnog ključa
2. Preuzimanje slika i njihovih potpisa
3. Učitavanje javnog ključa u datoteke (serijalizacija)
4. Generira se hash vrijednost slike i uspoređuje se sa hash vrijednosti odgovarajućeg potpisa dekriptiranog javnim ključem → provjera ispravnosti digitalnog potpisa

ZAKLJUČAK

- MAC osigurava integritet i autentičnost poruke ; generira se za određenu poruku korištenjem tajnog ključa kojeg dijele pošiljatelj i primatelj te upotrebom MAC algoritma