UNIVERSITETI I PRISHTINES FAKULTETI I SHKENCAVE MATEMATIKO-NATYRORE

Detyra e trete

Lënda: Siguria e te dhenave

Punoi: Florian Shabani, Jon Sadikaj, Syard Dauti

Permbajtja:

1.Definimi i detyres

Duke u bazuar ne skemen e algoritmit Simplified SHA-1,duhet te punohen 3 nendetyrat e meposhteme:

A. Shkruani aplikacionin që do të implementojë skemën e dhënë?

B. Le të jetë dhënë vlera e tekstit H(M) = 4BAFE69C,gjeni M' ashtu qe H(M')=H(M)?

C. Zgjedhni një mesazh M të gjatësisë së çfarëdoshme pastaj llogaritni hash vlerën më anë të Simplified SHA-1, pra e llogaritni H(M) . Pastaj të gjindet M' ashtu që M != M'(jo e barabarte) dhe H(M')=H(M)?

2.Realizimi i detyres

A.Skema e algoritmit Simplified SHA-1 eshte paraqitur ne figurat e meposhtme dhe kete skeme e kemi implementuar ne Java.

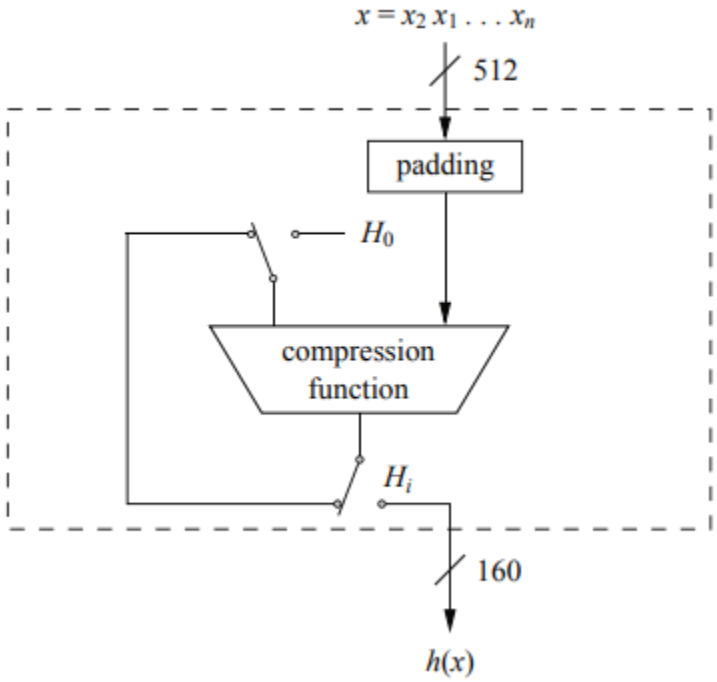

Fig 1. Mbushja e tekstit me bite

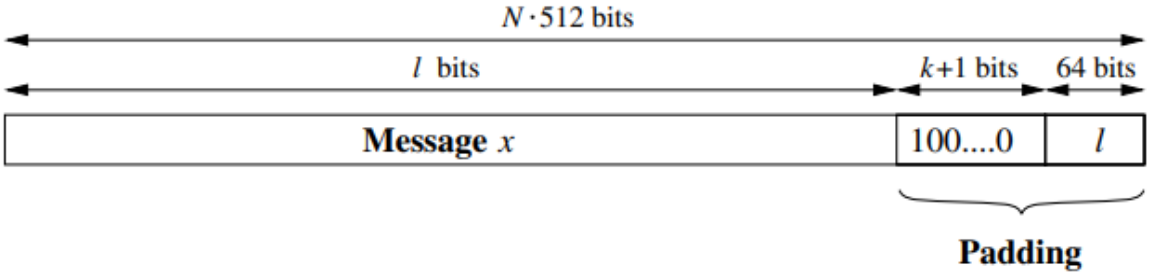

FIg 2. Menyra e mbushjes se bitave

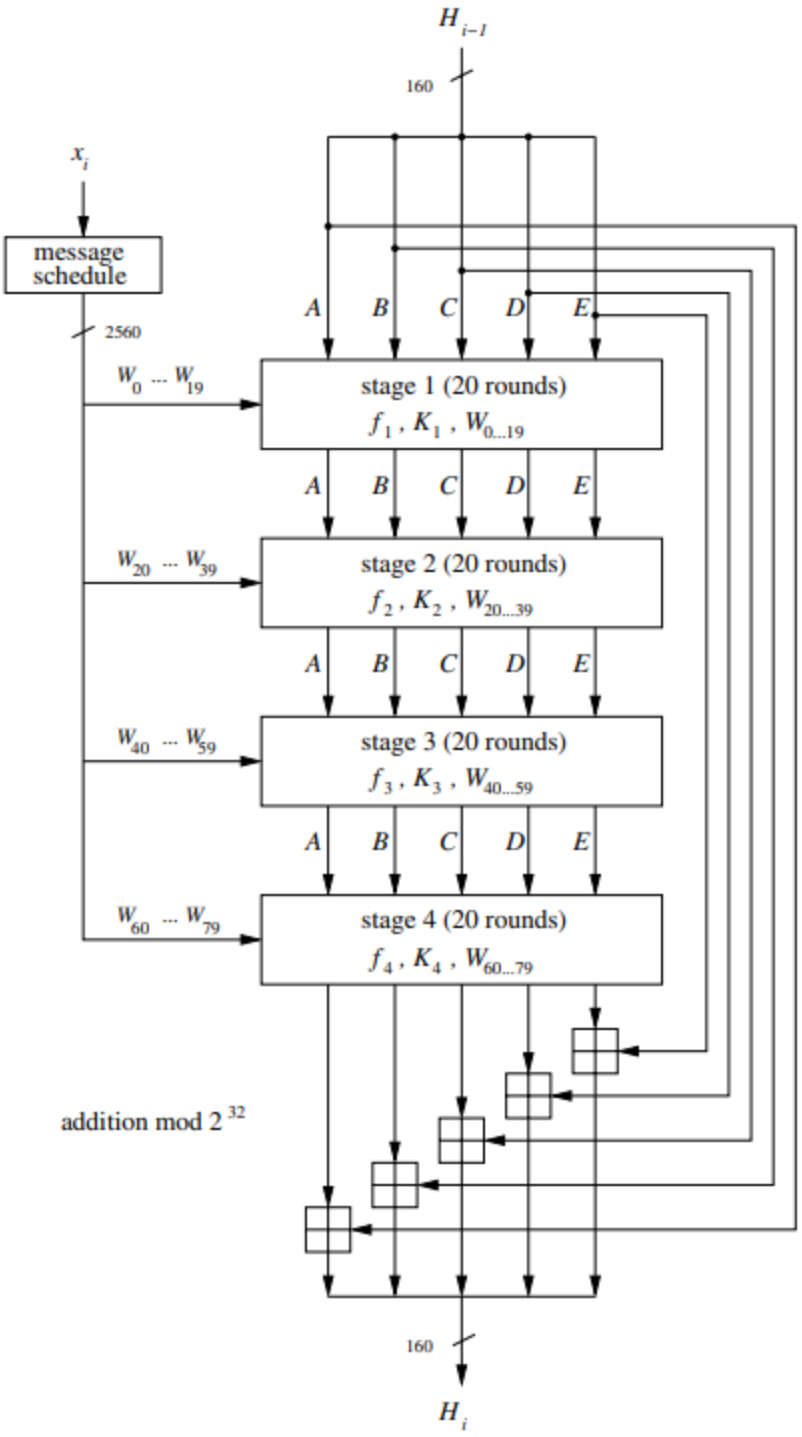

Fig 3. Roundet tek SHA1

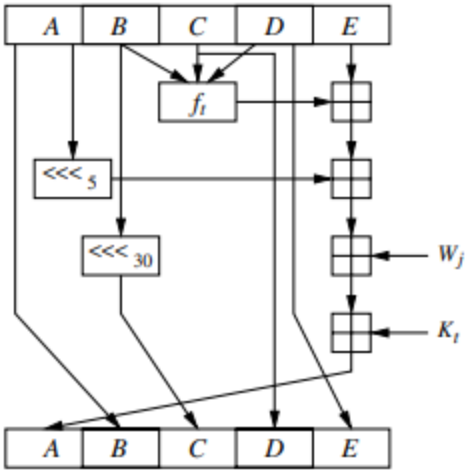

Fig 4. Roundi j ne stagjin t te SHA1

B.

Një kod hash është zakonisht një vlerë e plotë me madhësi fikse që llogaritet duke përdorur një funksion hash. Funksioni hash merr një hyrje, si një varg, objekt ose strukturë të dhënash, dhe kryen llogaritjet për të prodhuar kodin hash.Funksioni hash eshte funksion nje kahesh qe nenkupton se duke pasur vleren e funksinoit hash nuk mund ta percaktojme ne menyre analitike teksin qe i perket kesaj vlere.Menyra e vetme per te nxjerruar tekstin nga vet funksioni hash eshte permes provimit te te gjitha vlerave te mundeshme.Kete qasje kemi perdorur ne kete detyre.

Meqenese ne detyre teksti qe lidhet me hash kodin e dhene eshte i tipit string kemi vleren dhe vlera hash e saj eshte me 8 karaktere atehere permes Java kemi ndertuar kodin i cili gjeneron te gjitha variacionet me perseritje meqense vlera hash e 7 karaktereve prodhon hash cod me 8 karaktere variacionet i kemi marrur te klases se 7-te.

Dhe ekzekutimit te programit kemi par qe vleres hash **“4BAFE69C”** i pergjigjet teksti **“CAOZQPD”**

C.

Duke perdorur SHA1(Secure Hash Algorithm 1) ka shumë pak gjasa që të gjenerohen dy tekste të ndryshme me të njëjtin kod. SHA-1 është projektuar për të prodhuar vlera unike hash për të dhëna të ndryshme hyrëse. Megjithatë, për shkak të madhësisë së kufizuar të hash-it të SHA-1 (160 bit ose 20 bajt), teorikisht është e mundur që të ketë dy vlera te njejta hash per dy tekste te ndryshme.Por meqe kjo mund te behet vetem

duke marraur te gjitha kombinacionet e mundeshme,per nje numer kaq te madh te biteve eshte praktikisht e pamundur.