UNIVERSITETI I PRISHTINËS “HASAN PRISHTINA”

FAKULTETI I SHKENCAVE MATEMATIKO – NATYRORE

Departamenti: Matematikë | Programi: Shkenca Kompjuterike



Siguria e të dhënave

**Simplified SHA – 1**

**Punuar nga:**

Benita Mehmeti

Erona Gashi

**Maj 2023**

# Përshkrimi I detyrës

Detyra 3. Bazuar në skemën e algoritmit Simplified SHA-1:

1. Shkruani aplikacionin që do të implementojë skemën e dhënë? (2 pikë)
2. Le të jetë dhënë vlera , gjeni H(M) = 4BAFE69C, gjeni M’ ashtu që H(M’) = H(M)?
3. Zgjedhni një mesazh 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 dhe H(M’) = H(M)?

# Hyrje

Me rritjen e mbështetjes së organizatave dhe individëve në internet, është rritur edhe nevoja për zhvillimin e algoritmeve për enkriptim. Një prej këtyre algortimeve është edhe algoritmi SHA – 1, I cili luan rol tejet të rëndësishëm në sigurimin e të dhënave digjitale.

Në kriptografi, SHA – 1 është një funksion njëkahësh I dizajnuar nga National Security Agency (NSA) dhe I publikuar nga NIST. SHA qëndron për Secure Hash Algorithm. Algoritmet SHA janë gjithsej tre dhe dallohen nga njëra tjetra përmes emrave sin ë vijim: SHA – 0, SHA – 1, SHA – 2. SHA – 1 është shumë I ngjashëm me SHA – 0, por e përmirëson një gabim në specifikimin e SHA origjinal, gabim ky që conte drejt dobësisë së dukshme. Nga këto tre funksione, SHA – 1 është më I përdoruri në përgjithësi, aplikohet në një pjesë të madhe të aplikacioneve dhe protokolleve të sigurisë.

SHA – 1 është një funksion kriptografik I cili merr një input dhe prodhon një vlerë hash 160 – bitëshe. Kjo vlerë njëkahëshe njihet si përmbledhje e mesazhit. Kjo përmbledhje e mesazhit pastaj zakonisht jipet si një numër heksadecimal I cili ka 40 shifra. Sidoqoftë, ky agloritëm konsiderohet I pasigurtë që nga viti 2005, dhe kompanitë si Microsoft, Google, Apple, dhe Mozilla kanë ndaluar së pranuari certifikatat SHA – 1 SSL që nga viti 2017.

Për të kalkuluar një vlerë njëkahëshe kriptografike në Java, përdoret klasa MessageDigest Class e gjendur në pakon java.security. Ky dhe shumë algoritme të tjera që gjenden në këtë pako, inicializohen në metodën statike të quajtur getInstance(). Pas selektimit të algoritmit që dëshirojmë ta përdorim vlera njëkahëshe kalkulohet dhe rezultati kthehet në formën e një vargu bajtësh. Për të konvertuar vargun e bajtëve rezultues në formën e tij normale, përdoret klasa BigInteger. Kjo formë pastaj kthehet në formatin heksadecimal për të marrë MessageDigest të pritur.

## Aplikimet e SHA – 1

* Kriptografi: Aplikimi kryesor I këtij algoritmi në kriptografi është për mbrojtjen e komunikimeve nga ndërhyrja e palëve të treta. Nga një input të dhënash, SHA – 1 gjeneron një vlerë njëkahëshe të vetme, të pakthyeshme dhe të një madhësie të pandryshueshme. Integriteti I të dhënave pastaj mund të konfirmohet duke e krahasuar këtë vlerë njëkahëshe me vlerën paraprake. Kjo e bën të mundur konfirmimin se të dhënat nuk janë ndryshuar gjatë transmetimit.
* Ruajtja e fjalëkalimeve: SHA – 1 mund të përdoret për të ruajtur fjalëkalimet. Një vlerë njëkahëshe e fjalëkalimit gjenerohet përmes përdorimit të SHA – 1, në momentin kur përdoruesi krijon fjalëkalimin. Vet fjalëkalimi pastaj zëvendësohet në një databazë me vlerën njëkahëshe. Pas kësaj, sa herë që përdoruesi bën log – in përmes atij fjalëkalimi, dhe vlera njëkahëshe rezultuese krahasohet me vlerën njëkahëshe fillestare.
* Integriteti I të dhënave: Në shumë industry, si në financa, healthcare dhe në qeveri, integriteti I të dhënave është një shqetësim I madh. Integriteti I të dhënave një një sistem kontrollohet përmes algoritmit SHA – 1. Duke përdorur një vlerë njëkahëshe të përfituar nga SHA – 1, krijohet një fingerprint I të dhënave origjinale. Nëse të dhënat ndryshojnë në cfarëdo lloj mënyre, edhe vlera njëkahëshe do të ndryshoj, duke u bërë ky një indikacion se të dhënat janë modifikuar.

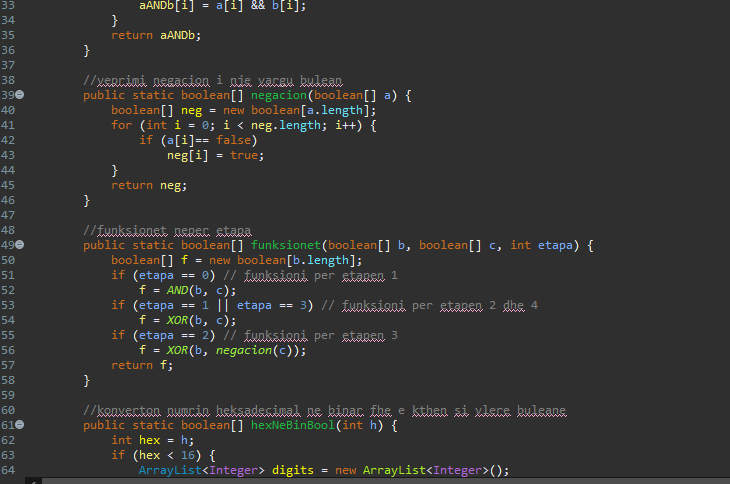
# Implementim I SHA – 1

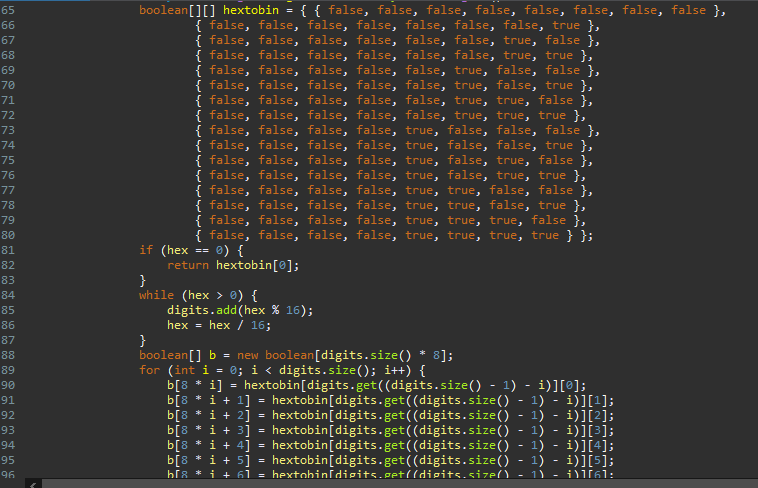
## Aplikacioni që implementon algoritmin

Algoritmin SHA – 1 e kemi implementuar në tre klasa SimplifiedSHA1, SSHA1b dhe SSHA1c në të cilën kemi përfshirë këto metoda:

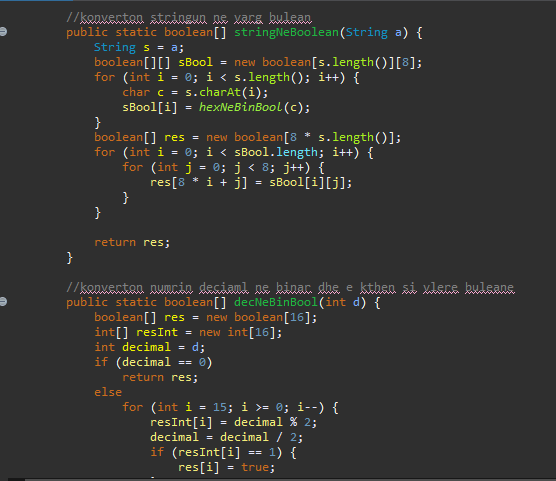
* XOR(), që kryen veprimin XOR mes dy vargjeve buleane. Kjo metodë I ofron këtij algoritmi nonlinearitet, e cila është thelbësore për fuqinë kriptografike të tij. Tjetër ndikim ka në difuzion, që nënkupton se ndryshimet në input do të shpërndaheshin nëpër krejt outputin;
* AND(), që kryen veprimin AND mes dy vargjeve buleane, ngjashëm si te XOR edhe operacioni AND lejon manipulimin efektiv të bitëve individual, poashtu kjo metodë në disa raste specifike mund të përdoret për detektimin dhe përmirësimin e erroreve;
* Negacion(), që kryen veprimin e negacionit në një varg bulean, përdoret për invertimin e bitëve individual, ky operacion poashtu përdoret për lidhje me operacione të tjera për të konstruktuar funksione komplekse logjike;
* Funksionet(), që kryen veprimet e mësipërme nëpër etapa;
* hexNeBinBool(), që konverton numrin heksadecimal në binar dhe e kthen si një vlerë buleane;
* stringNeBoolean(), që konverton stringun në varg bulean;
* decNeBinBool(), që konverton numrin decimal në binar dhe e kthen si vlerë buleane;
* booleanNeHex(), merr një varg vlerash buleane dhe I konverton në varg vlerash heksadecimal;
* inToBoolean(), kthen numrin e plotë si varg të vlerave buleane;
* paddedString(), mesazhi I bërë padded si String;
* mod256(), mbledhja modulo 2^8=256;
* rotateBool(), bën rotacionin për n bit majtas;
* hash(), bën llogaritjen e vlerës hash.

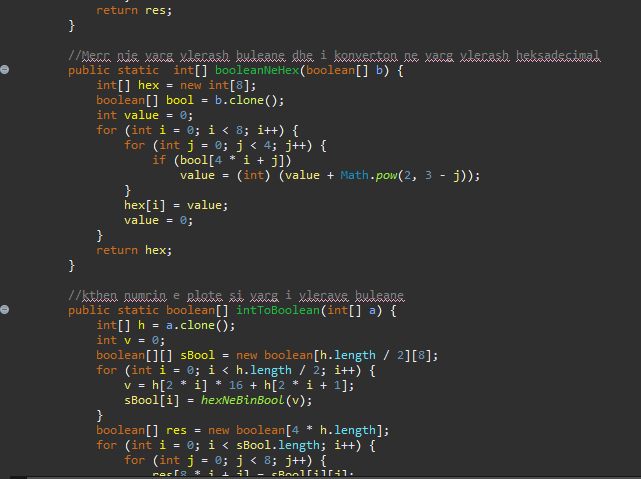




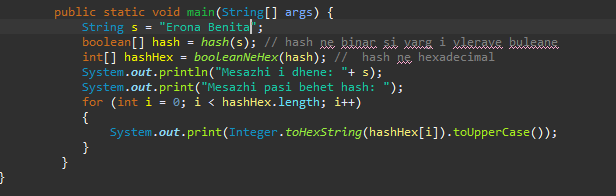


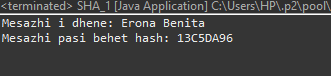








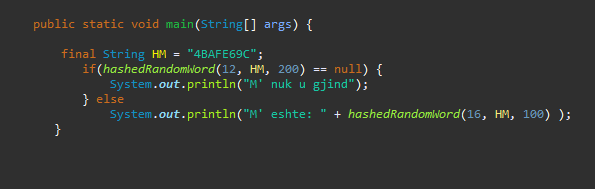


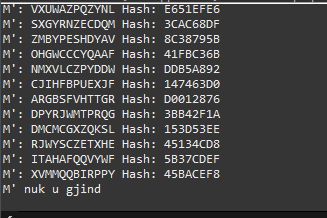


## Second PreImage Resistance

Second pre-image resistance është një veti e funksioneve njëkahëshe kriptografike, përfshirë këtu SHA-1, e cila siguron vështirësinë e gjetjes së një inputi dytësor I cili prodhon të njëjtën vlerë njëkahëshe sikur inputi origjinal.

Koncepti I second pre-image resistance është thelbësor për sigurinë dhe integritetin e sistemeve kriptografike. Nëse një sulmues mund të gjej një input tjetër I cili prodhon të njëjtën vlerë njëkahëshe, potencialisht mund të zëvendësonte atë input me origjinalin pa u kuptuar.





## Collision Resistance

Collision Resistance është një veti fundamentale e funksioneve njëkahëshe, përfshirë këtu edhe SHA-1, e cila siguron që është e pamundur të gjejmë dy inpute të ndryshme të cilat prodhojnë të njëjtën vlerë njëkahëshe. Në fjalë të tjera collision është një situatë kur dy inpute rezultojnë në të njëjtën vlerë njëkahëshe.

